Breaking Digital Firewalls

I dedicate this book

to my father
for teaching me the value of hard work,

to my mother
for teaching me the value of compassion,

to my wife Afaf
for teaching me the value of dedication,

to Rania, Sarah, Laila, and Elias
for renewing my motivation,

& to all who are struggling for freedom
and equality around the world…

Örebro Studies in Media and Communications 17

WALID AL-SAQAF

Breaking Digital Firewalls
Analyzing Internet Censorship and Circumvention in the Arab World

Cover photo: Maria Al-Masani

Title: Breaking Digital Firewalls. Analyzing Internet Censorship and Circumvention in the Arab World
Publisher: Örebro University 2014
www.publications.oru.se

Print: Örebro University, Repro 4/2014

ISSN 1651-4785
ISBN 978-91-7529-023-2

Abstract

Al-Saqaf, W. (2014) *Breaking Digital Firewalls. Analyzing Internet Censorship and Circumvention in the Arab World*. Örebro Studies in Media and Communication 17.

This dissertation explores the role of Internet censorship and circumvention in the Arab world as well as Arabs' views on the limits to free speech on the Internet.

The project involves the creation of an Internet censorship circumvention tool named *Alkasir* that allows users to report and access certain types of censored websites. The study covers the Arab world at large with special focus on Egypt, Syria, Tunisia, and Yemen.

This work is of interdisciplinary nature and draws on the disciplines of media and communication studies and computer science. It uses a pioneering experimental approach by placing Alkasir in the hands of willing users who automatically feed a server with data about usage patterns without storing any of their personal information.

In addition to the analysis of Alkasir usage data, Web surveys were used to learn about any technical and nontechnical Internet censorship practices that Arab users and content producers may have been exposed to. The study also aims at learning about users' experiences with circumvention tools and how such tools could be improved.

The study found that users have successfully reported and accessed hundreds of censored social networking, news, dissident, multimedia and other websites. The survey results show that while most Arab informants disapprove censoring online anti-government political content, the majority support the censoring of other types of content such as pornography, hate speech, and anti-religion material.

Most informants indicated that circumvention tools should be free of charge, fast and reliable. An increase in awareness among survey respondents of the need for privacy and anonymity features in circumvention solutions was observed.

Keywords: Internet censorship, filtering, circumvention, Alkasir, Arab Spring, free speech, liberation technology, authoritarianism, freedom of expression.

Walid Al-Saqaf, School of Humanities, Education and Social Sciences, Örebro University, SE-701 82 Orebro, Sweden. walid.al-saqaf@oru.se

Table of Contents

Table of Tables

Table of Figures

Table of Acronyms

ACTA	Anti-Counterfeiting Trade Agreement
ARPANET	Advanced Research Projects Agency Network
ATI	Tunisian Internet Agency
BBS	Bulletin board system
BSP	Blog service provider
CDA	Communications Decency Act
CIS	Commonwealth of Independent States
CMS	Content management system
COPA	Child Online Protection Act
DB	Database
DDoS	Distributed denial-of-service (attack)
DMCA	Digital Millennium Copyright Act
DNS	Domain Name Server
EEF	Electronic Frontier Foundation
FCL	Filtering confidence level
FTP	File transfer protocol
GCC	Gulf Cooperation Council
GUI	Graphical user interface
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and communication technology
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
IP	Internet Protocol
ISOC	Internet Society
ISP	Internet service provider

ITU	International Telecommunication Union
MENA	Middle East and North Africa
MMS	Microsoft Media Server
NSA	National Security Agency
ONI	OpenNet Initiative
P2P	Peer-to-Peer
PIPA	Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PROTECT IP Act)
PRISM	Code name for a mass surveillance program by the NSA
PTC	Public Telecommunications Corporation
RSF	Reporters without Borders
SOCKS	Socket Secure
SOPA	Stop Online Piracy Act
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transmission Control Protocol/Internet Protocol
Tor	The Onion Router
UDHR	Universal Declaration of Human Rights
URL	Uniform Resource Locator
VOIP	Voice Over Internet Protocol
WCIT	World Conference on International Telecommunications

Acknowledgments

There are many people whose support was vital for this dissertation to ultimately see the light of day after six long years of hard work.

I wish to start by acknowledging and thanking my supervisor Stig-Arne Nohrstedt for his guidance and support since I started my post-graduate studies in 2006. His steady encouragement, swift responses, and constant follow-ups were instrumental for me to reach this stage. I thank him for all that he has done, not only as an academic, but also as a friend.

Despite not meeting him as often as my main supervisor, my co-supervisor Åke Grönlund has done a lot in highlighting issues in my work. I recall times when I realized how detailed his comments were, indicating the strong dedication he has given to reviewing my work. I thank him tremendously.

I wish to acknowledge Henrik Örnebring of Karlstad University, whose comments at the 60% and final seminars were instrumental in raising the quality of this study. My gratitude also goes to Christian Christiansen of Stockholm University for his important insights on issues related to my work on Internet censorship circumvention.

I must not forget to thank human rights advocate and dear friend Maria Al-Masani, who has taken the time and effort to design the fabulous cover of this book. Her talent and skills are amazing.

One of the most influential persons that had a direct impact on my academic career and way of thinking is the co-founder and former director of the Master of Global Journalism, Roland Stanbridge. I thank him for being my role model as a teacher through his motivation to think critically and be open-minded and forthcoming.

I thank Peter Berglez, who was among my early acquaintances in Sweden and who later became a close colleague and friend. I recall many occasions when he gave motivating and constructive comments about my work. I will remember him for his humility and friendly smile.

There are also colleagues who have helped me a lot perhaps without realizing. Among them are Mahitab Ezz El Din and Ahmed El Gody, whose comments and collaboration were often extremely constructive. Our friendship extended beyond the working environment and it was truly a great honor to have known them.

I thank my immediate boss Joel Rasmussen, who has been quite accommodating and helpful despite my frequent work-related requests to

handle employment contracts, residence permits and visa applications for the various international events I attended.

I must also acknowledge Annika Gardhorn and Åsa Kroon for helping me during the most critical stages of my academic career.

The following former and current colleagues at Örebro University deserve my gratitude for the support they have provided since I joined Örebro University: Leonor Camauër, Mats Ekström, Johan Östman, and Anna Roosval, in addition to all my colleagues at the department of media and communications.

There are also people outside Sweden that have had a positive impact on my work including Rune Ottosen, Elisabeth Eide and Kristin Orgeret from Oslo and Akershus University College of Applied Sciences. I thank them for being such great partners from across the western border.

I express my most sincere appreciation to Esra'a Al Shafei of the Mideast Youth Network. She is among the first few individuals who believed in my work even before I officially launched Alkasir in 2009. Esra'a helped open many doors for me, particularly through my TED Fellowship. I will remain indebted to her for her support.

I wish to express my utmost gratitude to my wife and love of my life, Afaf, for her support and love throughout the years. I thank her also for tolerating my frequent absence due to travels and long days and nights at work. I use this space to apologize to her for the stress I caused and the family trips and activities I cancelled during the last phase of my doctoral research. She, along with my wonderful kids, served as the main source of motivation to press forward and complete this study as planned so we could spend quality time together. I owe them a fantastic family holiday.

Finally, I thank the thousands of Alkasir users around the world. Without their trust and support, this research would have not been possible.

Örebro, April 2014

Walid

Part I

The Problem

Chapter 1: Introduction

When the Tunisian street vendor Mohamed Bouazizi set himself ablaze in Sidi Bouzid on December 17, 2010, consequently creating the spark that triggered the Arab Spring[1], many academics were caught off guard and started discussing the relationship between the use of social media and the ability to mobilize protests and do other forms of activism. A lot of this research was carried out in developed countries, where it is unlikely to be exposed to any of the severe forms of oppression that many generations in the Arab world had to endure and of which Arabs were eventually fed up, leading to the uprisings that the world saw on TV. Among the repressive acts that were not widely mentioned, however, was Internet censorship. It was a practice that, as an Arab myself, I can relate to very much, because I was one of its victims in 2008 when my own website yemenportal.net was blocked by the Yemeni regime. When the Arab revolutions broke out, those forms of oppression boiled to the surface, inviting scholars and publishing houses from around the world to produce books and develop theories about what happened.

To my dismay, this sudden attention was paid to the region's miseries only after the fact. I sometimes perceived it as an impulsive drive to study what led to the Arab Spring: a reactionary and, if I may dare say so, opportunistic drive. Forms of oppression such as detaining dissidents, kidnapping bloggers, and censoring websites were always there to study, and it was not necessary for a historic event like the Arab Spring to come along for academics to be concerned. Many Arab activists and citizens have been working hard for years to attain freedom and did not suddenly appear in a euphoric Arabian night. Yet, they were regretfully abandoned by the international community to fend for themselves. For decades, they were left under the mercy of ruthless tyrannical regimes, of which many were allies of the West.

I have newly found respect for the Deputy Director of Human Right Watch's Middle East and North Africa (MENA) division, Eric Goldstein, who wrote a thought-provoking and self-critical article acknowledging how he and others in the international community failed to predict the

[1] Also known as the 'Arab Awakening', the Arab Spring is a term used to refer to the peaceful revolutions that sprung up starting from Tunisia in December 2010 and reaching several other countries with calls for the end of Arab dictatorships and for dignity, justice, better living standards, and freedom.

Arab Spring and missed the "thaw" (Goldstein, 2012). While website censorship has been practiced in most of the Arab countries, the author gave the example of an Egyptian protestor telling the New York Times that website censorship and the inability to communicate to the world were frustrating enough for him to join the protest movement. In just a few words, Goldstein identified one of the fundamental reasons that prevented many in the international community from seeing it coming:

> we overestimated the robustness of some of the authoritarian regimes, and underestimated demands for a better life, measured partly in human rights terms. (Goldstein, 2012)

Taking Initiative

Looking back to the autumn day of 2008 when I decided to focus my doctoral study on Internet censorship in the Arab world, I must confess that I too did not see the Arab Spring coming. But I did have a strong desire to fill the knowledge gap in relation to the use of technology for liberation in the Arab region. From communicating with activists and human rights advocates in many Arab countries, I have noticed growing signs of anxiety and panic in ministries of communication across the region. Governments were getting concerned about their inability to control the flow of anti-government content published online by activists and dissidents to undermine the legitimacy of tyrannical regimes through strong, critical, and often evidence-driven political content published and shared widely. This was a new and serious development because Arab governments were used to being in the driver's seat. They were able to do so mainly by stifling opposition and controlling mainstream media through licenses, shutdowns and other forms of censorship. But the Internet was a different animal that authoritarian governments appeared to be unable to deal with. To me, those developments indicated that Arab regimes started to feel vulnerable.

The Internet is not centrally located and cannot be directly controlled by any state. This created a weak spot that some Arab activists have noticed and effectively exploited by taking advantage of governments' ill preparations for such a major paradigm shift in the way information is shared and people communicate. One resort that governments had was to try to censor the Internet, mainly by blocking websites.

Yet this was insufficient, because as I discovered through my travels to several Arab countries, activists have started developing an understanding

of how to overcome Internet filtering using a technique called censorship circumvention and effectively overcame a major technical hurdle set by the government. By using proxy websites or other circumvention tools, and with a little experimentation, those activists were able to end governments' information monopoly by getting around censorship and continuing to publish sensitive and dissident content freely.

To me, it was rather natural that this subject deserved some attention from the academic world, mainly because it is an exciting indicator that reflected a potential to break out from decades of free speech suppression. For the first time, Arabs are able to bypass government control and poke a small hole in a wall that has stood firm for decades. It may well be that this small hole could get bigger over time and be large enough to let many liberty-yearning Arabs escape to freedom. Yet I have found no academic research of significance about the use of circumvention tools by Arab activists. So I decided to pursue the subject myself. I believed that such work could help acquire useful knowledge about means of liberation not only for Arabs, but also for people living in oppressed societies.

I remember suggesting the idea to my supervisor Professor Stig-Arne Nohrstedt, who welcomed and supported it strongly. He believed not only in my work's potential contribution to the scientific domain, but also in its contribution to advancing freedom in the real world. He also highlighted the need for media and communication scholars to involve themselves more in Internet and new media studies if they are to stay up-to-date with the transforming landscape of media. This study was found timely on two fronts. First, it focuses on the growing power of the Internet, which has started making significant inroads into classical media and communication studies as well as various other disciplines in the field of social sciences (Wellman, 2004). Second, it focuses on the Arab Spring, a historic landmark that deserves careful examination and study.

Transforming a Vision to a Plan

From my perspective, it was fascinating to see technology-savvy and risk-taking Arab online activists finding tricks and methods to break national digital firewalls and, as content producers, publish their content regardless of Internet censorship. Yet activists constitute only a subsection of society and it is not enough that they alone are able to break the digital firewall. Despite the growing important role that the Internet has played in the Arab world, however, particularly for mobilizing political movements, communicating, and sharing information, Internet censorship remained

effective in stopping the majority of the public from reaching dissident content. Using circumvention tools remained a niche skill that not many users enjoyed. If one is to effectively neutralize Internet filtering, there is need to scale up the production and access of circumvention solutions so they could be used by more members of the general public. Theoretically, Arabs could then achieve the critical mass needed to render information control by governments useless. Toward achieving such an ambitious vision, a question to ask would be: What would happen if one replaces the existing solutions, whose instructions are often only available in English, with free and easy-to-use software that is homegrown, talks to Arab users in their own tongue, and could be utilized by anyone regardless of the levels of English language and technical competency?

But before answering that question, another question would emerge: Is it technically and financially feasible to develop such a solution? Another important question that would pose itself is whether users will in fact be motivated enough to download, install, and use such software while knowing that the websites they will access are censored[2] probably because they contain content that their governments do not want them to see. How easy or difficult would it be to grant novice Internet users the same powers that allowed their geek peers to render sophisticated and costly firewalls useless? Will that be the only step needed to defeat Internet censorship or will there be need for others such as legal reforms, international pressure, and human rights awareness?

So the aim was to try to answer those lingering questions, and to do so, I decided to take the challenge of creating a software solution that meets those conditions. It had to be user-friendly enough and to have multilingual support with the hope of persuading some of my acquaintances in some Arab countries and perhaps their friends to use it. I gave it the Arabic name Alkasir[3] and used it as the central component of a virtual scientific experiment to study Internet censorship and circumvention possibilities in the Arab context. Through Alkasir, I intended to examine the status of Internet filtering by detecting websites that were blocked and what type

[2] 'Censored', 'filtered', and 'blocked' are used interchangeably throughout this dissertation to mean the same thing, i.e., the restriction to access. And 'censorship circumvention' is the technical process of bypassing such censorship.

[3] Alkasir is an Arabic word (الكاسر) meaning *the breaker*, which can also mean the *circumventor*. The name and logo of Alkasir have been registered in 2009 as a trademark by the Swedish Patent and Registration Office.

of content users actively sought to report about and eventually access. It was also meant to be the bridge that would allow me to reach dozens or even hundreds of users to get their views about censorship and circumvention and what steps could be taken to limit Internet censorship as a way to advance free speech in the Arab world.

Theoretically, if users from around the Arab world actively report blocked websites through Alkasir, it would then be possible to draw a map of Internet filtering in the region. My ambition was initially to target a few Arab countries first. But if Alkasir turned out to be useful in other countries, so be it. However, I certainly did not have it as a goal to reach the global stage and that is why the study was limited from the beginning to the Arab world. In theory and because the Internet is a global network, if Alkasir is to work effectively in Arab countries, it might as well work in others.

The Launch, Challenge, and Progress

The software development stage was not easy. It required significant planning and long hours of work to develop the software architecture and do the design and implementation through computer programming. It took over a year until the software was ready for public launch in trial mode. I launched the program and relied on a mechanism known as crowdsourcing,[4] which requires users to individually report about blocked websites in their countries and have the software aggregate the data using a predetermined algorithm to identify the state of censorship at a given time and place.[5] I released the first version of the software in May 2009 in a public launch at the American University in Cairo (InteractiveME, 2009). From that moment onward, users were allowed to securely download the free software from the official website, https://alkasir.com, install it, and run it. In the process of developing this solution, a lot of theoretical thoughts were involved. Months before the Arab Spring, I published a book chapter about the potential use of technology to overcome censorship and promote transparency (see: Al-Saqaf, 2010). At the time, I was quite nervous because I needed the empirical data to prove my theoretical arguments.

[4] Crowdsourcing refers to the act of outsourcing certain tasks that are traditionally performed by an employee or contractor, to a large group of other people. You can find more explanation about this in the Methodology Chapter (Howe, 2006).

[5] Read more about how Alkasir does this in Appendix A.

Without having a high enough number of users, the research project would fail.

But by October 2012, not only did Alkasir have users in Yemen, but its success exceeded expectations by garnering more than 72,000 users in 123 countries around the world. Finally, I could see streams of data flowing from all four corners of the globe to feed into my research database. I could start bearing the fruits of an idea that started in 2008, when I thought about a method of studying Internet censorship not by using data from other sources, but by inventing a novel method that will get data directly from users in two ways. First, I was able to collect feedback from a total of over 3,500 Arab respondents through two surveys,[6] one before the Arab Spring, in 2010, and one in 2012. Second, I was able to use data that were stored on Alkasir's proxy servers, which helped identify usage patterns and statuses of website accessibility in countries where Alkasir was used.

One can argue that the more widely censorship circumvention software are used and the faster new media technologies develop, the more likely it is that governments would lose their ability to control the free flow of information because government-mandated Internet service providers (ISPs) would find it too difficult to prevent users from accessing censored content. This suggests that circumvention solutions, such as Alkasir, may be an empowering and liberating technology in the hand of users while simultaneously becoming a potential threat to authoritarian governments.

For this research project to work, two conditions had to be met. First, Alkasir must be used by a sufficiently large number of active users, who would be willing to spare some of their time to answer survey questions and use the software to report blocked websites and access them often, which will generate a large enough sample for the content analysis to yield statistically significant findings. Second, Alkasir will have to remain working consistently in countries that are to be studied. In other words, it should not suffer from extended malfunctions or be blocked by ISPs. Unfortunately, Alkasir did get blocked by Saudi Arabia and China in 2012. But by that time, it had already collected a good amount of data about Internet filtering in those countries. The vulnerability of being blocked was one of the project's limitations that are discussed in the technical report in Appendix A.

[6] The total number of respondents from all over the world was over 5,850.

The obvious mismatch between a lone circumvention tool developer and authoritarian states is indisputable. It is true that as the developer of Alkasir, I have the know-how, dedication, a supportive environment, and a small fund set aside for the project. But that is no comparison to states that have greater resources, and an unwavering determination to restrict the public's freedom of expression through a variety of methods such as intimidation, surveillance, or other fear-mongering techniques that they have used for generations. Nonetheless, some governments are certainly taking this threat seriously as can be concluded from the fact that they have blocked many circumvention tool websites, including alkasir.com.[7]

Given the rapid growth of the Internet, particularly in the domain of user-generated content, this reaction by governments is understandable. By mid-2012, over 2.4 billion people, that is, about a third of the world's population, had access to the Internet (Internet World Stats, 2012). Those numbers are expected to increase rapidly as Internet connectivity will be more commonly available on mobile phones, raising the number of Internet users in 2015 to over 3.4 billion, which would constitute 45% of the world's population by then (Cisco, 2011). And it even gets better according to Google's CEO Eric Schmidt, who predicted that the whole world will be online by 2020 (Gross, 2013). Apart from the continuous rise in the number of users, the functions and online services[8] offered will also increase due to new innovations in software and infrastructure, which are expected to raise the annual global Internet traffic to one zettabyte[9] by 2015 (Cisco, 2011).

Hence, it was natural to find the subject of Internet censorship garnering growing attention of scholars and research institutions in different disciplines such as media, communications, computer science, law, political science, and economics. Reports dealing with Internet censorship were also produced by advocacy groups such as Paris-based Reporters without Borders (RSF) and Washington DC-based Freedom House. As a research

[7] It has been confirmed from Alkasir's databases that http://alkasir.com was blocked by some or all ISPs in at least the following countries: Iran, China, United Arab Emirates, Syria, Saudi Arabia, Yemen, Nigeria, and Columbia.

[8] The CISCO report predicts that the increase will mostly be in the use of the Internet for business and multimedia communication and entertainment that include but are not limited to video conferencing, video sharing, motion pictures, online gaming, virtual words, Internet TV, 3D video, home theater, imaging, mobile phone applications, trusted computing, peer-to-peer, and remote backup of data.

[9] A zetta is equal to 10^{27} (10 to the power of 27).

subject, Internet censorship has a cross-disciplinary appeal. On the one hand, it deals with technical aspects such as Internet's structure and application, but on the other, it is quite relevant to nontechnical areas such as Internet users' behavior, state control, and authoritarianism, along with several others that vary in importance to scholars based on their field of study. Previous research has shown that censored content varied widely based on country, culture, and context and ranges from child pornography (Nybergh, 2008) to dissident content (Rininsland, 2012).

Although there are several different technical and nontechnical censorship methods, Alkasir was designed mainly to overcome technical filtering, which is the most common censorship method practiced on the Internet (Zittrain & Palfrey, 2008b, p. 2). However, this study does cover nontechnical censorship by reflecting on earlier research and by analyzing feedback from survey respondents in the region. Arab countries have a common language and largely adhere to Islam, yet have varying degrees and mechanisms of Internet censorship, which makes the Arab world a good case study for this type of research.[10] It is also worth noting that unlike censorship in other areas such as speech, art, print, and broadcast media, films, theatrical plays, and photography, Internet censorship is a relatively new phenomenon and remains an under-researched subject.

It Is *Not* Just about Technology

While it is fascinating to see users' ability to resist control of information by authoritarian states, it is important not to overlook one crucial element that is vital for the success of any effort aimed at combating technical restrictions on the Internet. That very element is what drives individuals to take the extra step in building software to defeat Internet censorship. It is the same special quality that motivates users to actively seek and take hours or days to find the best technical solution to break free from online restrictions. It resembles one of the basic instincts that is born with every human being and remains part of each one of us for life. It is the desire to be free.

Indeed, the struggle for freedom is quite ancient. One of the oldest examples demonstrating the willingness of freeborn men to fight tyranny and defend the unalienable right to speak freely in order to address grievances and criticize those in power is the case of playwright Euripides (480–406

[10] More about this in the Methodology Chapter.

BC). Several discovered writings revealed that Euripides detested oppression and promoted democracy and freedom in his works (Haigh, 2006).

Separated by over two millennia, the desire to break free is what connects the writings of Euripides of ancient Greece to the uprisings of the youth of the Arab Spring. The two promoted the same struggle for freedom from oppression but used different methods. While Euripides used speech, writings, and plays, young Arabs used technology, social networking, and peaceful public rallies. My aim from making this connection is to underline the need to not only look at Internet censorship and circumvention from a pure technical angle, but also understand the motivation behind challenging unjust censorship as something that transcends space, time, and medium. The mind-set that made it possible to develop Alkasir and other tools has little to do with technology and more to do with passion. That mind-set stems from a desire to resist repression and overcome injustice so as to live with dignity, liberty, and respect. Without making that point clear, it is difficult to grasp the theoretical framework provided in this study.

Furthermore, I believe that in order for this dissertation to be relevant and of value to future research, it must avoid the trap that Roy Amara's law warned of:

> We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run. (PC Magazine Encyclopedia, 2012)

I personally interpret Amara's law in the context of my study as an advice to stay true to the original purpose and motivation behind Internet censorship circumvention technologies, which is the protection of free speech. We should indeed not overestimate the short-term positive effects that those tools have. Similarly, we should also not ignore their potential long-term effects as it might well be that they could fail or have adverse outcomes if they were crowned as the ultimate solution to Internet censorship. Instead, one must think critically about why such tools were developed in the first place and, thereafter, develop new methods and find long-lasting solutions to tackle censorship, because the struggle for freedom will probably continue in new and unexpected ways.

Study Outline

This dissertation is partitioned into three main parts plus the appendices. The first part serves as an introduction to the study and focuses on the basics that present its aim, relevance, and importance. The second part

deals with the background and context of the region and case studies and is used to set the scene. The third and final part is the one including the main contribution of the study in the form of empirical findings and conclusion.

The three parts collectively include eight chapters, namely, introduction, literature review, theoretical framework, methodology, background, and contextual analysis, general findings, case study findings, and conclusion. The introduction provides an important point of departure that explains how and why the idea behind the study came about and presents its purpose and research questions along with its relevance, motivation, and importance.

The second chapter is the literature review, which provides an overview of previous work in the area of Internet censorship and circumvention. Among the reviewed works are those dealing with the factors that resulted in states' decisions to censor online content, mechanisms of censorship, and their scope. While only a few studies on the censorship of nudity and pornographic content are mentioned, most of the focus in the chapter revolves around research studying censorship of websites containing political, security-related or informational content in addition to social networking websites.[11]

The third chapter is the theoretical framework that deals with the theoretical approaches used in the study. It starts with free speech theories derived from liberal scholars and thinkers followed by a section on the limits of free speech. As a concept and practice, censorship is then comprehensively covered in a separate section from a theoretical angle. The chapter then proceeds with an overview of how technology could be used as a form of liberation from censorship. And as this study deals with censorship in Arab states, which are mostly authoritarian, a section on authoritarianism explains the potential motives behind censorship, which itself is also theoretically analyzed as a concept and practice. Finally, the chapter provides a brief overview of path dependence theory as a useful general approach in analyzing some of the context-related developments in the Arab world concerning Internet censorship.

[11] As will be indicated later in this study, Alkasir only allowed access to blocked websites that do not have nudity as a main theme. It is worth noting that Faris and Villeneuve (2008) took a comparable decision when they avoided studying filtered pedophile content in their study.

The study's methodology (Chapter 4) describes the factors that led to the selection of Egypt, Syria, Tunisia, and Yemen among all Arab countries as examples of the use of Internet filtering at the national level and the reasons behind selecting the period from October 2010 to October 2012. Also, the chapter thoroughly explains the research methods used to gather and extract data from Alkasir servers as well as the design and publishing of the surveys. Chapter 5 provides a background and context to set the stage for understanding the conditions in the Arab world as a whole and in four case studies that witnessed revolutions during the Arab Spring.

Chapters 6 and 7 presented the general and case study findings of the study respectively. In those chapters, the gathered results were analyzed, contextualized and presented in an attempt to answer the research questions using data collected from Alkasir's servers and the responses of survey respondents. The conclusion of the study in Chapter 8 sums up the findings and what they mean by connecting the empirical findings with theory to identify emerging patters. Toward the end of that chapter, I present a vision of the future direction of the research in light of the expectation that this under-researched area will remain relevant for many years to come. The study also has three appendices, of which the most important is Appendix A, which contains the technical part dealing with the software engineering of Alkasir. As this study relies heavily on Alkasir, it was important to have an elaborate explanation describing how the software was constructed and what its functions are both at the user and at the server levels. This was crucial because the building and developing of the software has been part and parcel of this interdisciplinary study.[12] The software development process, the application design, as well as the algorithms used were described in a moderately technical style that should not require much technical knowledge to grasp. This was done intentionally to create a balance so that the dissertation would be informative and easy to to understand by scholars from different disciplines. The other two appendices B and C are –respectively- the survey questions and the list of websites that have been reported to be blocked during 2010–2012 in individual Arab countries.

[12] Due to the interdisciplinary nature of this study, I have been supervised by two professors: Prof. Stig-arne Nohrsted, who specializes in media studies and Prof. Åke Grönlund, who specializes in information technology.

Purpose

Generally speaking, this study aims at exploring the role and forms of censorship and circumvention during a crucial period of the Arab Spring. It seeks to develop an understanding of how technology was used by Arab Internet users to identify, track, and circumvent Internet filtering. In doing so, the study contributes to the research of media and communication studies using a novel experimental approach.

The study intends to bridging the knowledge gap in this area because unlike earlier works, this study acquires data from users directly to learn about their experiences and views on Internet censorship circumvention. It also involves the creation of a research tool (Alkasir) that could be of use in future social science research related to Internet censorship.

Research Questions

The study endeavors to answer the following five questions:

Q1. What forms of Internet censorship do Arab regimes practice and why? And how do those practices affect users' access to online content?

The aim here is to study what forms of Internet censorship were practiced by Arab governments to prevent the public from publishing or receiving information on the Internet and what could be the motives behind such practices. Furthermore, the question aims to know how such practices affect content producers as well as regular users.

The answer requires tackling Internet censorship from a technical aspect such as Internet filtering and a nontechnical aspect such as harassment or prosecution. When coming to the specific cases presented for the four Arab countries, the study dealt exclusively with Internet filtering using the empirical data obtained through Alkasir. Survey questions were used to identify cases of technical and nontechnical censorship from the perspective of website managers and Internet filtering from the experience of other users. Given the Arab Spring context, comparisons between pre and post Arab Spring survey answers were made to better understand the motives behind censorship and effects on the users throughout this period.

Q2. What usage patterns emerge when users are provided with a technology that can be used to report and circumvent Internet filtering?

This question aims at identifying how eager circumvention users are to access certain types of blocked content vis-à-vis the priorities of governments in their censorship decisions. For example, if a country is blocking

access mostly to websites categorized[13] as informational such as news, it would be useful to know if that is what users sought to access the most or if they preferred to access some other type of blocked content such as social networking websites offering means to share user-generated content and help create online communities. As will be explained in the Methodology Chapter, answering this question is possible by giving Internet users in Arab countries the freedom to report whatever websites they wanted to access and, thereafter, monitor how frequently they visit them.

Q3. How do Arab users view the appropriateness of blocking access to websites containing particular types of content and what could explain those views?

The question mainly whether censorship could indeed be seen as appropriate for certain types of content. It is an attempt to get a perspective from users on the limits of online freedom expression. The survey method was used to answer this question, and answers by Arab survey respondents were then compared with those from non-Arabs to see if there was a particularity for Arabs in judging on what was to be censored. A connection to the theory and the Arab context was used to analyze those findings.

Q4. Why do users in the Arab world use circumvention tools, and how can the effectiveness of such tools improve?

This question is an attempt to understand the value that users found in using circumvention tools to combat the effects of censorship during the Arab Spring so as to shed light on the effectiveness of those tools.

Additionally, respondents were asked to indicate which circumvention solutions they used more frequently in the past year and what they thought were the most important characteristics and factors that make any circumvention tool more effective in combating Internet filtering.

Q5. How can international and foreign actors help limit the effects of Internet censorship?

The effects identified through the first question were used to feed into this one, which uses survey respondents' views to understand how international and foreign actors could—if at all—help limit the adverse effects of Internet censorship.

---

[13] The categorization of URLs is a subjective process and has limitations that are addressed in the Methodology Chapter of this study.

Contribution and Relevance

The study has an explorative experimental design as it involves the creation of Alkasir as a research tool used in an experiment in a real-life situation to explore the actions taken by those who use it. This meant that it would be a unique interdisciplinary study that required significant work in software development in addition to the analysis of the data obtained from Alkasir's server as well as from Web surveys answered by the software users. This study adds to the scholarly work in the area of freedom of speech and its limits, with a more technological orientation to supplement the evolving discipline of new media studies. It contributes to the knowledge of how crowdsourcing and technology could be used to identify and analyze websites that are blocked by ISPs in Arab countries in particular and globally as well. The data sets stored by the software are then analyzed to answer some of the research questions. The gathered empirical data could also be of value to future studies within this domain. New research can tap into the databases of Alkasir, which are constantly updated, to carry out longitudinal studies on censorship patterns, not only in the Arab world, but globally.

The fact that the study started before the Arab Spring and continued until the end of 2012 made the data it gathered throughout this period of immense relevance and significance to scholars interested in understanding the patterns of Internet censorship during this critical period of time for the region. Furthermore, this would suggest that this period is perhaps the most appropriate to study Internet censorship circumvention tools as liberating technologies and examine their role in or impact on the region.

Finally, I developed Alkasir to also promote freedom of speech in the Arab world in particular. When I started working on this project in 2008, I had felt the level of oppression against free speech in the Arab world was unprecedented and prompted action. I believe that the dual purpose behind the program (promoting research and freedom) makes it a contribution to science as well as an effort to fight against censorship of free speech. This allowed me to remain motivated and energetic during the long and tedious process that involved the creation and development of the software. I received several messages of gratitude from users expressing how Alkasir allowed them to access censored, yet important content and disseminate it to others.[14]

[14] Anonymous users in Egypt, Syria and Tunisia have directly sent messages indicating how helpful the program was in bypassing censorship during critical times.

Personal Motivation

As a citizen of Yemen, I have my own personal story of simmering under the 33-year-long dictatorship of Ali Abdullah Saleh, who left power in 2012 but after he had suppressed freedom of speech and journalists through prosecution, harassment, and even assassinations such as the one that may have claimed the life of my father Abdulaziz Al-Saqqaf.[15]

In 2008, I started to realize that Saleh's regime started oppressing free speech on the Web as well. Dissident online content was frequently censored in Yemen, including my own website http://yemenportal.net, which was blocked from access within Yemen in January 2008 (see: Al-Saqaf, 2008). The lingering question I had in mind was: "How far can a person utilize technology to break free from oppression?" I had my own assumptions and subjective views on the issue, particularly as I myself was a victim of it. I was quite eager to try to find an answer, and it started to become both a personal as well as an academic objective.

Given that I have a computer engineering bachelor's degree and a master's degree in global journalism, the project became quite appealing as it combined aspects from those two fields of study. By creating Alkasir, I started this study, which that had its own unique niche within the confines of Örebro University, and arguably, on a global level. Furthermore, I believe that the software could last well beyond the duration of the study as I consider it a token of appreciation to activists trying to overcome censorship and advance freedom of speech.

Ethical Considerations

In planning for this study, there were a few ethical considerations that I had to address. The first was whether it was proper in the first place to grant users the ability to circumvent censorship imposed by their governments. Although the normative stand of this study is for overcoming censorship of free speech, handling this question from the ethical and legal perspectives puts the ultimate responsibility to decide whether to circumvent or not on the end user. Usage of the software is bound to acceptance

[15] Professor Abdulaziz Al-Saqqaf (1951-1991) was an outspoken Yemeni journalist known for establishing Yemen's first English language newspaper Yemen Times in 1991 and for his strong anti-corruption and pro-human rights writings. In 1999, he was killed when a car ran over him in the Yemeni capital Sana'a. The incident was never thoroughly investigated by the authorities despite many pleas, indicating the possibility that he may have been targeted in a staged assassination.

of the terms of use.[16] This was a necessary measure to limit the developer's responsibility for how the software is used.

Another ethical question was whether the software should have been made available to users living in countries ruled by authoritarian regimes only or to also include other countries. Given that the liability in using the software falls on users, it was decided to give them the right to take the ultimate decision whether to use the software regardless of where they live.

The ethical question of users' safety and privacy was also considered. While the level of risk is impossible to determine beforehand, this issue was dealt with by removing clues that could lead to identifying a particular user. That is why, for example, Internet Protocol (IP) addresses of users were not recorded in Alkasir's database. Furthermore, full anonymity of survey respondents was ensured and no personal information was requested. A third taken measure was the deployment of secure sockets layer (SSL) using a secure certificate for the website, where the survey was accessible. Furthermore, the transactions from the client to the server were encrypted from end-to-end to prevent spying or eavesdropping on the connections used by users or survey respondents. Those combined efforts have considerably minimized the risk, which was weighed against the knowledge value from the study, leading to the conclusion that the taken measures were deemed sufficient to meet the research ethical standards required as per research regulations in Sweden involving human subjects.[17]

It is worth noting that the decision not to allow users to report websites providing pornography and nudity content was not based on ethical considerations. It was made mainly to save bandwidth and resources as well as prevent the software from discouraging its use by users in Arab countries where culture detests such content.

[16] Terms of use are available online at https://alkasir.com/doc/en/License.html.

[17] More about research ethics in Sweden is available on the Ethics Review Board website: http://www.epn.se/en/start/regulations/.

Chapter 2: Literature Review

Hundreds of studies were found to have dealt with Internet censorship, of which the majority was published within the last ten years.[18] While there were many technical papers developed by scholars in the computer science discipline,[19] most of them were excluded in this study due to their pure technical nature. The reviewed studies were mostly published in peer-reviewed journals based in one or more of the social science disciplines such as media and communications, political science, and law. Some of the researchers arrived at their findings through quantitative methods using sophisticated software that were operated by specialized researchers to identify how and what was filtered in a specific country, while other studies had a more theoretical approach analyzing the sociopolitical aspects of Internet usage in the respective countries and contexts using qualitative methods such as interviews. It is to be noted that because this dissertation is focused on the Arab context, it was tempting to reflect on studies dealing with the Arab Spring in general. But due to limitations in space and scope, only Arab Spring studies that were concerned with Internet censorship were considered.

This chapter is divided into four sections. The first deals about the studies that contributed to understanding the rationale behind Internet censorship in a number of specific countries. The second section includes reviews of studies dealing with the mechanisms and scope of Internet censorship. The third was dedicated specifically to studies about Internet censorship circumvention. The chapter concludes with a section identifying the perceived knowledge gap that this study aims to fill.

Motives behind Internet Censorship

To effectively cover literature dealing with the motives behind Internet censorship, this section is further divided into subsections based on where censorship takes place, because the reason governments censor particular

[18] Literature was sought after using a combination of online scholar search engines and library resources such as CiteSeer, Scopus, Web of Knowledge, ProQuest, etc., and the following synonyms of the term "Internet censorship" were used in the search: "cyber censorship", "online censorship", "virtual censorship", "website filtering", "Internet filtering".

[19] Studies related to Internet censorship were mostly dealing with technical aspects of data filtering, analysis, traffic inspection, pattern recognition, etc., which are rather technical and require some knowledge in computer science to fully grasp.

content depends on the context of the country in question. The motives behind censorship are a relevant aspect for Internet censorship, particularly in the social science discipline, as they help understand the 'why' component of the subject matter. Initially, the states studied were divided into two types: authoritarian and democratic.[20]

As a practice by authoritarian regimes

When it comes to identifying why Internet censorship is practiced by various governments, several studies have provided useful inputs that could help answer this question. The majority of papers presented a perspective that takes into account a particular context and country. This makes trying to come up with one single answer to understanding the motives behind Internet censorship unrealistic.

Given the importance of context, it is useful to shed light on specific cases in literature tackling censorship practices in particular authoritarian regions or states. While China received the lion's share of such studies (e.g., Fallows, 2008; MacKinnon, 2008; Menon, 2000; Wacker, 2003; Zittrain & Edelman, 2003), there was also literature focusing on Internet censorship in Arab countries (e.g., Shirazi & Greenaway, 2009; Zarwan, 2005), Iran (e.g., Granick, 2005; Mina, 2007), Singapore (e.g., Warschauer, 2001; Ang & Nadarajan, 1996), and Cuba (Kalathil & Boas, 2003). Henceforth, I shall present some selected examples of literature that may help shed light on motives behind censorship. China is given as an example of authoritarian states followed by examples of Arab and Muslim countries, which would bring the review closer to the subject of the study.

China

Among all Internet censorship studies reviewed, China was by far the most widely used case study as it helps explain why an authoritarian regime subjects the Internet to censorship. Rebecca MacKinnon's research about the issue found that regime's rationale was based on perceived threats posed by some online content to the nation and its people. Based on this justification, the Chinese government erected what is arguably the most

[20] There may well be dispute as to which country is authoritarian and which is democratic, but for pragmatic reasons, countries electoral democracies were taken to represent democratic states while non-electoral democracies such as Arab countries, Iran, China, and Central Asian countries were taken as cases representing authoritarian states.

sophisticated and comprehensive national Internet censorship system that has ever existed. The censorship system is metaphorically called the "Great Firewall of China" and could be viewed as an intermediate layer that regulates the movement of information between the Internet on the global level and the Chinese level (MacKinnon, 2006, p. 10).

Regulatory frameworks in China were elaborated by Deibert, Palfrey, Rohozinski, and Zittrain (2008), who noted that legal and administrative regulations in general were a means of ensuring that the Chinese Communist Party will be supported in its attempt to control its supervision of the different types of media. The authors indicated that Chinese authorities have extended many of the traditional formal and informal controls of the media to the Chinese cyberspace and inconsistently enforced vaguely defined laws that provide the government with almost endless authority to censor online content. Among the illegal content censored is that which the government considers dangerous to national security or content that challenges political theory presented by the regime.

The Chinese authorities also deemed some websites illegal and, hence, often went ahead in censoring them on the basis that they allowed prohibited online activities such as those that incite prohibited assemblies or gatherings. Censorship of such websites could then be legally justified by the regime on the grounds of containing illegal content that disturbs social order. The government's heavy-handed approach led to severe self-censorship by users and domestic Internet companies alike. That was manifested in a 2006 call made by major Chinese Web portals to censor "unhealthy" and "indecent" information to prevent harm to society (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, pp. 265–266).

A research by Deborah Fallows for the Pew Internet and American Life Project came up with similar observations indicating that the justification behind Internet censorship according to the Chinese government was to prevent content that could damage China's unity and sovereignty, harm ethnic solidarity, promote superstition, portray violence, pornography, gambling, or terrorism, violate privacy, or damage China's culture or traditions (Fallows, 2008, p. 1). What is interesting is that Fallows found in a survey she carried out about Internet use in China that over 80% of respondents agreed with the government's rationale behind Internet censorship (ibid.). However, Ronald Deibert cautioned in a paper on China's cyberspace against such results and expressed the need to be skeptical, warning that polling results in authoritarian regimes are unreliable due to

the lack of transparency and due to the general climate of suspicion and fear within the country (Deibert, 2010, p. 7).

Although they did not aim at comprehensively identifying the motives behind the excessively restrictive top-down control of the Internet in China, Liang and Lu brought another perspective by arguing that combating cybercrime could explain part of why the Chinese authorities are eagerly keeping their filters active. The authors stress that the Chinese state is quite aware of the tremendous positive impact that the Internet had on development and economic growth. Hence, the authorities are using censorship as one method of limiting the negative effects of cybercrimes on businesses and other beneficiaries. The authors highlighted the need to consider fighting cybercrime as a significant motive behind censorship and added that cybercrime effects are an understudied subject despite posing a serious problem to the Chinese government, which is, therefore, trying to combine its criminal laws with other administrative regulations to tackle it (Liang & Lu, 2010, pp. 116–117). However, the authors did not indicate how human rights and anti-government dissident websites blocked in China could pose a cybercrime risk.

In contrast to Liang and Lu's paper, a study on Internet censorship in China, William J. Cannici Jr. went deeper and beyond the frequently indicated public justification in protecting society from the dangers lurking on the Web. The author contended that Internet censorship policy is guided by a political desire to prevent undermining the regime's grip on power. The author argued that by restricting citizens' access to some websites, the state would reduce their capacity to reach a diffused and unidentified audience in or outside China. By doing so, the authoritarian regime in China hopes to limit the dissemination of dissident and anti-government ideas and information to the Chinese public (Cannici Jr., 2007, p. 4).

On another level, Nart Villeneuve noted that Western companies developing filtering software are getting richer and bigger by selling their products to undemocratic states such as China, adding that efforts by activists and scientists to decrypt and analyze the lists of blacklisted IPs and websites stored in filtering software databases were thwarted after the passage of the US Digital Millennium Copyright Act (DMCA), which could be used to prosecute those who attempt to reverse-engineer software products (Villeneuve, 2007). Those filtering software have their own customized taxonomy, and although they were originally meant to prevent exposing minors to adult and other harmful content, authoritarian governments used them to suppress free speech (ibid.). This trend has also continued

after the Arab Spring, with US companies having much to gain from selling filtering products to authoritarian states (Sonne & Stecklow, 2011).

The complicity with the Chinese government did not stop, however, with filtering software producers. Until 2010, even Google was involved in censorship when its Chinese domain, Google.cn, used to filter its keyword search results based on the Chinese government's directives, which mainly aimed at political content involving keywords that refer to "Free Tibet" and "Falun Gong" and others that the Chinese government consider forbidden to use online (Stevens, 2010). While referring to a speech by US Representative Christopher H. Smith, an American politician and outspoken critic of Chinese human rights practice, Cannici Jr. illustrated how Google helped support Chinese censorship procedures directly (Cannici, 2007, p. 5).

While Western filtering software producers are benefiting financially from censorship in a big market such as China, other companies and businesses in the country hosting the censored content were adversely affected. Villeneuve provided the examples of Radio Free Asia and Voice of America, whose websites were found to be blocked in China, and argued that the money spent on producing programs and content targeting Chinese audiences was not well spent (Villeneuve, 2007).

The MENA region

Compared to China, very few studies went deep to understand the motives of regimes in the MENA countries to practice Internet censorship. Among those studies was an article by Jackie Granick, who indicated that the official rationale behind Internet censorship was the protection of the country from the dissemination of information aimed at disturbing the public mind, which is often a reference to content containing security threats or obscenity. However, the Iranian regime had also stifled dissenting online content, which, according to Granick, is the main target behind Internet censorship. He further notes that the state's attempts to deprive Iranians of news through Internet censorship were meant to have the public effectively cut off from news sources with legitimate information, allowing the state apparatus to unify and solidify its authority (Granick, 2005, p. 12).

Kalathil and Boas did a cross-regional comparative study of authoritarian regimes involving some Muslim countries and identified more commonalities than differences when it comes to motives behind censorship. By analyzing Internet use in eight countries—China, Cuba, Singapore,

Vietnam, Burma, the United Arab Emirates, Saudi Arabia, and Egypt—the authors found that while governments found legitimacy from substantial public support for censoring pornography and obscene content, such censorship existed only as part of the real reason for blocking online content (Kalathil & Boas, 2003, p. 140). In other words, authoritarian governments started on the track of defending public morality and later diverged to suppressing dissident and anti-government political views.

Shirazi and Greenaway found remarkably similar conclusions in a study utilizing critical discourse analysis on filtered content in Iran and Saudi Arabia in an attempt to understand the motives behind Internet censorship. The study started by analyzing the two countries' justification for censorship. Iran's rationale to practice Internet filtering was to protect citizens from "anti-Islam" online content that promotes "Internet imperialism" through foreign- and Persian-language news agencies, websites, and major social networking websites such as Facebook and YouTube. The Saudi rationale was similar in protecting the society from "morally inappropriate" content, but no mention was made of "Internet imperialism" that the Iranian state emphasized. Instead, the Saudi regime's emphasis was more on protecting Islamic traditions and preventing social discord (Shirazi & Greenaway, 2009, pp. 5-7).

The two countries were taken as examples of repressive regimes that exploit the mainstream religious beliefs to justify sweeping restrictive practices targeting opposing political views and dissident content. Instead of achieving its original purpose of protecting Islamic values, such censorship ends up undermining citizens' capacity to pursue democratic goals by restricting their rights to access information and free expression (Shirazi & Greenaway, 2009). What makes the study by Shirazi and Greenaway (2009) interesting is that it went deeper than that of Granick (2005) in describing how states could publicly portray a particular justification to gain legitimacy on the crackdown of online content for political gains.

More often than not, those public justifications could be successful, as shown in a study by M. Kramer, who found that some public voices in authoritarian countries express views that approve the blocking of pornography for the sake of protecting public morality. On the other hand, however, the same regime suppresses opposition parties during election campaigns by blocking their websites, which naturally means lesser outreach to the potential voters on the Internet (Kramer, 2010).

Human Rights Watch reported several cases of Internet censorship in a number of Arab countries, which were seen as a violation of citizens'

rights to access information based on the Universal Declaration of Human Rights (UDHR) adopted by the United Nations in 1948 (Zarwan, 2005). However, in the same report, there was reference to the Johannesburg Principles,[21] which state the right to protect a "legitimate national security interest" (p. 12). Defining "national security interest" could vary widely depending on who is asked. For example, government or opposition representatives may define "national security interests" differently based on their own viewing angle and responsibilities. Hence, the Johannesburg Principles contain a vague expression that could be abused by authoritarian regimes to achieve political objectives.

Research conducted by the OpenNet Initiative[22] (ONI) on Internet filtering in the MENA indicated that although most countries in that region do not have laws criminalizing online activity or regulating the Internet, they do practice Internet censorship extensively, making the MENA region one of the most repressive Web environments in the world (Deibert, Palfrey, Rohozinski, & Zittrain, 2008). Studies carried out by the ONI suggest that the motives behind state censorship in that region are often socially and religiously driven, which leads to the filtering of websites ranging from pornography to anti-Islamic content. However, some of those countries applied laws that usually involve traditional mainstream media to the Internet. Among those countries is Jordan, whose telecommunications law forbids the use of the Internet to violate "public morals" or endanger "the national good" (p. 310).

Although they are not all located in the MENA, predominantly Muslim countries around the world do share some common characteristics with Arab states mainly due to common religious beliefs. And, hence, it is useful to mention the study by Barney Warf about Internet usage in some Central Asian countries. The author took a rather different approach than

---

[21] Johannesburg Principles are short for the Johannesburg Principles on National Security, Freedom of Expression and Access to Information. Those principles were issued on October 1, 1995 and since then, have become "widely recognized as an authoritative interpretation of the relationship between these rights and interests, reflecting the growing body of international legal opinion and emerging customary international law on the subject." (Zarwan., 2009:12)

[22] The OpenNet Initiative started as a collaborative partnership of the Citizen Lab at the Munk Centre for International Studies, University of Toronto; the Berkman Center for Internet & Society at Harvard University; and the SecDev Group (Ottawa). It aimed at investigating, exposing and analyzing Internet filtering and surveillance practices around the world.

other earlier researchers when he noted how censorship on the Internet expanded the digital divide in predominantly Muslim countries in Central Asia because while those who had the skills and determination to use technical tools to circumvent censorship were able to bypass filtering, those who did not were left behind. Yet, just like Saudi Arabia and Iran, Central Asian governments justified online free speech restrictions on the basis of protecting public morality from ideas that could potentially result in societal decadence or promote anti-Islamic values. Another justification was to prevent radical fundamentalism, and, hence, Internet censorship was seen as a required measure to combat terrorism and Islamist extremism (Warf, 2013, p. 280).

While the aforementioned studies focused on using religion to restrict censorship content, a 2012 study by Ben Wagner took a deeper look into the pre-Arab Spring Internet censorship doctrine of Tunisia, which was known to be among the most relentless Arab countries in restricting free speech online. The author argued that the Tunisian regime created what he called "push-button autocracy," which refers to the "empowerment of state institutions and structures—in contrast to empowering individual agency" (Wagner, 2012, p. 485). This meant that Internet censorship was used to monopolize information so it could be in the hands of the authorities and away from the public. Although Tunisia did block pornographic content, the government did not define what pornographic content was but delegated that task to software imported from the West (p. 489). Given that Tunisia has not only blocked pornography, but also many political websites as per research by ONI (2010), this meant that when blocked content did not deal with pornography, the government had to rely on itself in adding those political websites to the blacklist. Based on the work by Wagner and ONI, one can conclude that unlike the cases with Saudi Arabia and Iran, Tunisia prioritized political censorship over offensive sexual content.

Bowman and Camp studied the relations between Internet communications, activists, and the states in four countries: Uganda, Libya, Egypt, and Northern Sudan. During the popular protests that started in Tunisia and moved to Egypt, Syria, and, to a limited extent, Sudan, there were various acts of Internet censorship in the Arab countries that were part of this study. The authors argued that one of the main motives to censor the Internet in such situations was governments' fear of the potential impact of using the Internet to undermine their authority, citing the power of social media in speedy communications and mobilizing groups and the viral

impact in disseminating information regardless of geographical location (Bowman & Camp, 2013, p. 11). Special emphasis was put on the Egyptian government's action to cut off access to the Internet on January 27, 2011, which can be seen as the most severe form of Internet censorship. The paper saw such a drastic act as an effort to cling to power and quell dissent at a time of growing public resentment during the peak of the popular uprising (p. 5).

A conclusion that can be derived from reviewing the selected literature around Internet censorship in authoritarian regimes, whether Arab, Muslim, or not, is that there are often multiple motives behind Internet censorship that vary based on context. But one persistent motive was to maintain the upper hand in controlling the flow of information and to minimize the capacity of dissidents and activists to undermine the state's authority. As indicated earlier in this section, such motives become particularly salient during times of crises, for example, the peak of the popular uprising in Egypt in January 2011.

Democratic states

While several of the studies reviewed in the earlier section showed that authoritarian governments' motives were mainly political, it is important to note that censoring the Internet is not only confined to such repressive systems of government. Even democratic states have tendencies to practice Internet censorship, such as in the United States (e.g., Depken & Craig, 2006; Bambauer, 2012), Australia (e.g., Simpson, 2008), the United Kingdom (e.g., Brett, 2009), the Netherlands (e.g., Stol, Kaspersen, Kerstens, Leukfeldt, & Lodder, 2009), and South Korea (e.g., Wang & Hong, 2010). This section briefly goes through the three main arguments calling for Internet censorship in democratic states, namely, the protection of minors, intellectual property protection, and online security. I attempt to review some of the literature in these three domains and conclude with a brief comparison with authoritarian states.

Protection of minors

Upon reviewing literature about Internet censorship, the most notable difference between China along with most Muslim states on the one hand, and democratic states on the other was found to be that the latter group recognized the right of adults to access online pornography while the former didn't. Several researchers took on the subject of Internet censorship more vigorously after the United States came close to adopting a policy

that would censor pornography under the pretext of protecting minors. When the Communications Decency Act (CDA) was passed by the US Congress in 1996, it was originally introduced on the grounds that it would reduce the chances of children accidentally encountering pornography on the Web. The CDA was eventually turned down by the US Supreme Court in 1997 for being unconstitutional as it violated the right to free speech (Himma, 2004).

Since the defeat of the CDA, the perceived effects and implications of Internet pornography were studied by several researchers. Vandiver addressed the challenges of regulating pornography in the United States without jeopardizing freedom of expression, and compared that to policies practiced by the authoritarian Chinese regime (Vandiver, 2000). Meanwhile, Ybarra and Mitchell concluded that Internet pornography had a considerable potential of harming children and adolescents (Ybarra & Mitchell, 2005; Lee & Tamborini, 2006; Lo, So, & Zhang, 2010). Yoder, Thomas, and Kiran (2005), on the other hand, detected a significant association between the consumption of Internet pornography and loneliness. Despite the diversity of the reviewed literature on Internet pornography, however, no consensus was apparent on whether Internet censorship is the right approach in dealing with it.

Unlike Muslim and Asian countries, empirical studies found no evidence of nationwide Internet censorship in democratic countries (ONI, 2013). However, the subject of Internet pornography itself has been written about extensively, with a particular focus on child pornography or pedophilia, which was seen as a serious threat to minors. It was considered a growing problem that required regulatory and technical means to address, not only because of the mere repulsive nature of such content, but also because it promotes an underground illegal market of child sexual abuse (O'Donnell & Milner, 2007). A study by Wortley and Smallbone on child pornography found that while it was possible to try to manually identify pedophile content on the Web, it was more difficult to identify such content in the hidden net[23], (Wortley & Smallbone, 2012). A 2003 report by the General Accounting Office[24] analyzed content on peer-to-peer (P2P) file-sharing platforms and discovered the direct exchange of not

[23] The hidden net refers to any location on the Web that is not possible to search using public search engines, e.g., private networks and computers, CDs and DVDs, P2P networks, password-protected directories, etc.

[24] This office serves as an investigative unit run by the US Congress.

only copyrighted software and movies, but also excessive amounts of pedophile content, which constituted 44% of the images downloaded through such platforms, and with non-pornographic content constituting a mere 14% of the total analyzed images (GAO, 2003).

In the United States, a study by Kramer found through a survey with members of the public that protecting children from pornography, avoiding material that could offend personal and community standards, and preventing material that is illegal to process (e.g., bomb plans, security) were viewed by those surveyed as three legitimate reasons to use Internet filtering (Kramer, 2010).

Similarly, Depken and Craig also aimed at understanding what could prompt the support for Internet censorship in the United States by survey results from 4,247 respondents. The study found that support for censoring pornography came from respondents who had kids, were married, were of old age, used the Internet to get religious content, and/or work in the public sector. The authors concluded that there was a divide among respondents along personal characteristics when it comes to their views on state-imposed Internet censorship. Opposition to government Internet censorship came mostly from males living in urban areas and who used the Internet to access political content, had greater skills in using the Internet, worked in information technology fields, and viewed government regulation or censorship as a major concern (Depken & Craig, 2006). The study found that a solid 47% of all respondents in the United States agreed somewhat or strongly with Internet censorship of certain content (ibid.).

Yet, limiting contentious obscene material was found by Michael D. Mehta to be technically quite difficult. By presenting some case law examples where limiting such online content online was attempted in the United States and Canada, the author concluded that Internet censorship was not an effective approach and is unlikely to reduce targeted online material from reaching the public (Mehta, 2002).

In focusing on legislation in Australia to implement Internet filtering policies[25] against child pornography, Cairo and Wilken argued that filtering online pedophile content would result in censoring more than the in-

[25] The Australian Communications and Media Authority have the legal authority to force ISPs in Australia to block access to certain overseas websites based on a black list mainly consisting of child pornography. The black list is created based on consumer complaints. The Authority also has the right to take down illegal content hosted on servers within Australia.

tended content, but will go beyond that to censor legitimate content, which meant further restrictions on freedom of expression in the name of protecting minors (Cairo & Wilken, 2012, p. 25.10).

Similar conclusions were reached by McLelland and Yoo, who highlighted the specific case of the Japanese literary manga[26] genre called yaoi, which is composed of illustrations that are of sexual nature to portray fantasy tales of mostly underage male homosexual relationships and are mostly produced and consumed by young heterosexual Japanese women. In their study, the authors argued that international legislation that aims at restricting child pornography, even in virtual and fictional forms, would result in criminalizing yaoi, which ends up affecting the freedom of expression of mainly women who wish to enjoy "sexual fantasies in a secure, supportive environment" (McLelland & Yoo, 2007, p. 93).

Protecting intellectual property

Several studies, particularly by law scholars in the United States, were interested in studying the impact of potential laws and regulations that restrict online content for the protection of intellectual property. Many argued against such laws due to the likelihood that they could violate free speech. Similar views have protested aggressive legislations such as the Anti-Counterfeiting Trade Agreement[27] (ACTA), the Stop Online Piracy Act[28] (SOPA), and the PROTECT IP Act[29] (PIPA) (Bridy, 2009). While SOPA and PIPA were both postponed indefinitely following protests in the United States and around the world due to their potential impact on the privacy of citizens and companies (Weisman, 2012), US-initiated ACTA

[26] Manga is a globally popular form of Japanese graphic novels or comics, often containing sexual depictions.

[27] ACTA is a US-initiated multinational treaty to standardize intellectual property rights in a way that would make it possible to use punitive measures against ISPs that do not comply to certain demands of keeping logs of Internet users, removing copyrighted content, and doing other measures to protect intellectual property.

[28] SOPA was introduced by the Republican Party in the US to give law enforcement units expanded authority to counter copyright infringement online.

[29] PIPA, also known as PROTECT IP Act, refers to Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act, which was a proposed law to give the US government and copyright holders extra tools to counter websites involved in copyright-infringing activities, mostly outside the United States. Despite repeated attempts, the US Senate as of 2014, still did not pass it.

was rejected by the European Union (EU) in 2012 following several mass public protests (Whittaker, 2012).

Even though those attempts were stopped, there are still other laws in the United States that do regulate the Internet to protect intellectual property. One of the attempts to identify such laws and how they hinder free speech online in the United States was done by Hannibal Travis, who gave a comprehensive overview of the legal, technical, and political implications around the removal of online content based on copyright infringement. He illustrated the rapid development of tools that detect, flag, and remove content that media production companies or associations would want removed to not affect their profit (Travis, 2013).

Jill Barton, on the other hand, took a critical look at how YouTube and similar US corporations practiced what he called "backdoor censorship," when removing copyrighted content that belonged to media corporations, for example, movies, songs, etc. He argued that taking down such content without the users' approval constitutes a violation of the US First Amendment. For a democratic country that has a constitutional right to free speech, Barton believes that censorship on that level stifles weaker voices by media giants in the name of protecting their copyright, and he called for reforming copyright laws so they could be in more harmony with the First Amendment to safeguard freedom of expression in the United States (Barton, 2008, p. 67).

In describing the changing architecture of the Internet, Deibert underscored concerns of the entertainment, software, and other commercial entities about intellectual property theft and copyright violations, which were said to have reduced their potential profits by limiting the distribution of their goods and services. The author indicated that those corporations took it upon themselves to restrict access of users from publishing or exchanging such content through a combination of methods ranging from new laws that could be implemented globally such as the DMCA to developing codes that are built directly into the media themselves (Deibert, 2003, pp. 506–507). The DMCA is what compels YouTube and social media and file-sharing platforms to take down any content usually without the consent of the users.

However, Brandon Brown argued that it was not easy to implement the DMCA on Web 2.0 websites, especially when dealing with large and fast-paced user-generated content. So he suggested taking a less rigid approach when dealing with copyrighted content and implementing a balancing test that would allow for a more just arrangement that protects free speech

while minimizing the expenses associated with tracking and dealing with copyright infringements (Brown B., 2008, pp. 466–467).

Lawrence Lessig, who is one of the world's leading proponents of reducing legal restrictions on the ability to share and use online copyrighted content, argued that ideas should be shared widely and not be treated as mere property. He opposes censoring of content by corporations as it limits the potential of the Internet as a power that enables people to use ideas and content produced by others to innovatively create new ones that could thereafter be shared openly. To him, this is necessary to create a culture of openness and creativity that harnesses digital technology (Lessig, 2002, p. 623).

Security

In a paper about cybersecurity threats to freedom on the Internet, Ammori and Poellet identified the increasing threat against security on the Internet in the form of espionage, attacks on vital services, and other forms of cybercrimes such as identity theft and fraud. But the authors warned that measures to protect cybersecurity should not cause restrictions to online freedom of expression and so they emphasized the need to have discretion checked with trust-ensuring procedural safeguards (Ammori & Poellet, 2010).

The risk of cybersecurity becoming a pretext for censorship was highlighted by Gregory T. Nojeim, who pointed to the need to strike a balance between cybersecurity and freedom, privacy, and innovation on the Internet. He further warned that the intensifying discourse in the United States and other countries to focus on cyber national security in the form of espionage, terrorism, and cyber attacks is negatively impacting individual liberty and privacy in the United States (Nojeim, 2010).

Donald K. Anton assessed how online surveillance as carried out covertly by the National Security Agency (NSA) contradicted principles of free speech in the United States. This comes in the aftermath of the mass surveillance scandal exposed to the public by the former NSA contractor Edward Snowden, who disclosed up to 200,000 classified documents to the press detailing NSA's clandestine mass surveillance program with the government code name PRISM that extended to reach private communications on Google, Facebook, and other major platforms (Anton, 2013).

Several papers made critical observations of the NSA's PRISM mass surveillance program, which had tremendous international impact as it was revealed that the spying program had targeted thirty-five world lead-

ers and many EU officials (Ball, 2013). Laure Paquette indicated that the PRISM was a breach of the privacy of world citizens and that the whistleblower involved, that is, Snowden, needs to be protected for his role in advancing human rights through exposing the program. The rationale behind the PRISM was stated by the Chair of the US Senate Intelligence Committee, Senator Dianne Feinstein, who said that the surveillance program was used to identify individuals with suspicious communication links to Al-Qaeda or Iran (Paquette, 2013, p. 6).

Gellman and Poitras wrote an article identifying nine US Internet companies that supported US and British intelligence data mining on a global scale with the justification of protecting citizens from potential threats (Gellman & Poitras, 2013). Several studies also focused on the use of FinFisher, which is a surveillance software produced by the German/UK company Gamma Group, in 36 countries, of which many have repressive regimes (Marquis-Boire, 2013). Vernon Silver identified cases where this software was used to track and attack activists and stifle free speech (Silver, 2012). And as the production and marketing of surveillance software in democratic countries continue, authoritarian governments could see this as a boon and strengthen their repressive tendencies so as to solidify their political power (Clemente, 2013, p. 6).

Censoring violent and hate speech in democratic states was also reflected upon by several researchers from the angle of being a potential security threat, particularly when it comes to offenses made against religion. A case in point is the controversial anti-Islamic clip "Innocence of Muslims," which triggered protests and riots in several Muslim countries, leading to dozens of deaths (Ahluwalia & Miller, 2012, p. 627). Taking that particular video as an example, MacKinnon and Zuckerman (2012) argued that increased censorship on the Internet to restrict hate speech will not help in fixing the broader environment in which hate is nurtured. Instead, they recommend that media develop innovative means to neutralize "destructive trolls such as the ones who created, promoted, and exploited" the anti-Islam movie (MacKinnon & Zuckerman, 2012, p. 24).

Tackling the subject of hate speech as well, Foxman and Wolf argued that attempts aiming at restricting the transmission of contentious online

material[30] and censorial laws do more damage than good in a deliberative democracy and should be abandoned in democratic states (Foxman & Wolf, 2013, p. 80). The alternative approach they advocated was to rely mainly on counter-speech and education (p. 129).

Direct censorship versus indirect censorship

Kalathil and Boas as well as Zittrain and Palfrey indicated that political motives behind Internet censorship revolved around stopping dissidents from using the Internet to threaten authoritarian regimes. However, while studies have shown authoritarian regimes to have a direct approach in practicing Internet censorship, some democratic states such as the United States appear to have developed different forms of censorship that end up harming freedom of expression online just as much, if not worse (Kalathil & Boas, 2003; Zittrain & Palfrey, 2008a).

Notwithstanding the rejection of the CDA by the US Supreme Court, that did not mean that Internet censorship in the United States did not exist according to a study by Derek E. Bambauer, who strongly criticized what he described as "indirect" or "soft" Internet censorship practices by the US federal and state governments. He contends that *indirect* censorship strategies are being used in the form of persuasion, pretext, payments, and deputizing intermediaries and are worse than outright direct "hard" censorship in the form of blocking websites (Bambauer, 2012).

This view however was contended by James Grimmelmann, who raised several questions about Bamauer's claims about the legitimacy of "hard" censorship and warned that such an argument may be understood as support for formal censorship (Grimmelmann, 2013).

To sum up the findings concerning censorship in authoritarian and democratic states based on the reviewed literature, it could be said that Internet censorship in authoritarian states appears to be more direct and obvious and is often justified for cultural and social reasons, while moving beyond that to block dissident content suggests a desire to suppress dissent and prevent political opposition from undermining state authority. On the other hand, democratic countries appear to have a less pervasive approach

[30] In 1998, the US Congress enacted the Child Online Protection Act (COPA) - sometimes referred to as CDA II-, which prohibited websites from allowing children to view sexually explicit material. However, it too never took off after several failed litigations resulted in its permanent injunction in 2009.

to censorship and one that takes protection of children, intellectual property, and security as the main justifications.

However, as demonstrated earlier, Internet censorship practices in democratic states were not viewed to be the best approach to achieve the intended goals. In fact, they may result in more harm than good. A case in point is the exposed online mass surveillance practices committed by the US government, which demonstrated that even if it does not block websites like China or Saudi Arabia, the clandestine surveillance that it practiced on such a mass scale remains a form of censorship and a violation of free speech. It could even be argued that while authoritarian states have practiced censorship within the confines of their own borders, the fact that the US surveillance was on a global scale makes the level of its abuse more global.

Empirical Studies of Internet Censorship

There are some studies of Internet censorship that aimed at gathering empirical data and studying practices of Internet censorship in certain countries or regions. Understanding the scope of Internet censorship on a global scale was an endeavor done by a few, albeit significant, studies. In this section, I aim at specifically focusing on works that took an empirical approach to measuring and analyzing Internet censorship.

Empirical studies on technical and nontechnical censorship

When it comes to mechanisms of Internet censorship, filtering online content was the focal point of a significant number of studies (e.g., Al-Hajery, 2000; Deibert, Palfrey, Rohozinski, & Zittrain, 2008; Heins, Cho, & Feldman, 2006; Peltz, 2002; Zittrain & Edelman, 2003). Some studies, on the other hand, focused on nontechnical means of censorship, such as the use of force and intimidation through threats, beatings, prosecutions, offline surveillance, and similar policies that targeted online journalists, bloggers, and cyber activists. An overall conclusion was that such acts contribute greatly to increasing the level of self-censorship (Freedom House, 2009).

Deibert and Rhozinski (2008) indicated that the arrest of bloggers, particularly in China and Iran, constituted a significant threat against content producers. Such nontechnical forms of Internet censorship along with technical filtering and other Internet censorship methods were growing rapidly and spreading globally (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, p. 164).

Samir N. Hamade indicated that authoritarian governments in the MENA depend on a number of methods to suppress free speech on the Internet through a set of multilayered censorship practices. Those regimes rely on a number of complementary strategies in addition to technical filtering, such as arrest, intimidation, and a variety of legal measures used to regulate the posting and viewing of Internet content (Hamade, 2008).

The Global Internet Freedom Consortium (GIFC), which is an exiled Chinese censorship circumvention service with ties to the banned Falun Gong spiritual movement[31] (Park & Crandall, 2010), produced a number of papers related to Internet censorship, one of which focused on Internet filtering by describing different technical mechanisms applied by Chinese authorities to block access to certain online content. It also presented a timeline showing how censorship evolved from basic static IP address blocking to Domain Name Server (DNS) hijacking, which is a method used to fake a particular domain name, drop the connection, or translate the domain to a wrong IP address (GIFC, 2007, p. 4).

On a less technical level, Elijah Zarwan was thorough in describing how Internet censorship is implemented in Egypt, Iran, Syria, and Tunisia through filtering, prosecutions, surveillance, physical attacks, and other acts targeting website owners and bloggers, as well as violations of privacy, which all constitute oppressive Internet censorship practices (Zarwan, 2005).

Although the most frequently mentioned method to practice Internet censorship is filtering of content on the Web, mostly on the ISP level, other technical means were also used to prevent Internet users from viewing or publishing content. Among those measures were acts by search engines to hide search results that met specific criteria. A case in point is a study by MacKinnon, who described how censorship was implemented by Google, Yahoo!, and Microsoft through offering censored versions of their search results to the Chinese market in order to maintain their business operations in China (MacKinnon, 2008). This method of censorship is technical but is done on the host server and not the ISP level. MacKinnon also noted how blog service providers (BSPs) in China applied censorship to prevent users from posting blog entries or comments containing specific keywords. This censorship mechanism could be automated on the fly, preventing the

[31] Falun Gong is a system of beliefs and practices that emerged in China. But it was banned by the Chinese government in 1999.

posted article from appearing at all, or giving the BSP administrators the time to manually check and remove such entries (ibid.).

The main nontechnical method used around the world is legal prosecution with many reported cases of lawsuits and indictments against bloggers and activists who were found guilty for using the Internet in ways that allegedly violate the law. The legal aspect of censorship was covered on a country-by-country basis in research done by RSF and Freedom House, as they both provided empirical data indicating who was prosecuted and based on what laws (Freedom House, 2009; RSF, 2005). Such acts against bloggers caused self-censorship, which prevented users from expressing their opinions online for fear of legal or other repercussions (Paireepairit, 2008).

Rundle and Birdling looked into Internet censorship from an international perspective and concluded that many of the filtering practices represented an obstruction of the basic human right of freedom of expression. The authors noted that efforts have started to introduce international principles on Internet-related practices to uphold the minimum acceptable standard. Thereafter, the United Nations Educational, Scientific and Cultural Organization (UNESCO) proposed a code of ethics for the information society in 2007, which would be voluntarily applied by states and the private sector (Rundle & Birdling, 2008, p. 97).

Rundle and Birdling contend that online content filtering practices had important implications for global politics, civil society, and democracy and are in violation of UDHR's Article 19, which was intended to protect free speech and communication and defends people's rights to access information. They state that Internet censorship restricted the ability of civil society organizations, from businesses and academia to activists, to access information vital to their operations and to communicate with the rest of the world freely. The authors also noted that such censorship raises questions about the global communications infrastructure because it diminishes the network effect generated by the interaction of individuals and organizations worldwide, which is one of the main functions of the Internet (Rundle & Birdling, 2008, p. 78).

Furthermore, Zittrain and Palfrey indicated that technical filtering could be flawed because it occasionally over-blocks content that was not intended to be blocked, which adds to the conclusion that Internet censorship in general is an obstacle to the use of Information and communication technologies (ICTs) for development, limiting innovation, creativity, and stronger democracies (Zittrain & Palfrey, 2008a, p. 44). Another inde-

pendent project was done by Sarah Houghton-Jan, who carried out an empirical study through which she tested the effectiveness of several commercial Internet filtering tools often used in libraries to prevent access to sexual content. She concluded that nonsexual text and image content was also inadvertently blocked in the process, and such content ranged from war and genocide to safer sex and public health. Furthermore, the same tools failed to block sexual content in cases when it was either new, had no text, was not in a standard text format, was part of a page with search engine results, was in an e-mail attachment, was part of Web feeds, or was part of non-English content (Houghton-Jan, 2008, p. 14).

A conclusion that could be derived from Houghton-Jan's work is that an important obstacle that prevents effective control of such online content stems from the decentralized nature of the Internet, which makes anyone able to publish anything regardless of where he/she is in the world. Consequently, if a central authority or government wants to block such content from being accessed through the use of Internet filtering software, there is risk of over-blocking of legitimate content, which, in turn, restricts freedom of expression.

Generally speaking, reviewed literature around mechanisms of Internet censorship has shown that acts of censorship varied from technical to nontechnical methods, with Internet filtering being the most dominant yet flawed, because it was often found to over-block or fail to block various types of content that was originally meant to be blocked.

Studies on the global scope and extent of censorship

Among the different literature reviewed, only one study attempted to collect empirical data from most of the countries where Internet censorship or filtering was found to exist. This study constituted part of the book edited by Deibert, Palfrey, Rohozinski, and Zittrain and entitled *Access Denied: The Practice and Policy of Global Internet Filtering*. The book contained regional and country-specific reports done by the ONI project in which extensive data on Internet censorship patterns in the targeted regions and countries were presented. The book also included comparative studies to assess the level of Internet censorship in various countries around the world (Deibert et al., 2008).

Given that the ONI Internet filtering study was the only comprehensive piece of research that aimed at measuring Internet censorship on a global scale, it became the main target in this section of the literature review. There were, however, other studies that targeted a particular country and

focused on a particular group of online content. An example is the work of MacKinnon, who carried out an extensive study on censorship practiced by blogging platforms in China (MacKinnon, 2008). In this section, I examine these two studies, as I believe they make good case studies.

ONI's Internet filtering study

One of the earliest studies on Internet filtering was carried out by the ONI. The results of that study were posted online at ONI's website at http://opennet.net. ONI's findings concerning the Arab world have shown in their 2009 report that Internet filtering practices in the region had reached unprecedented levels, particularly in Tunisia, Syria, Saudi Arabia and Yemen (Hartley, 2009). A summary of all the empirical data of the study up to 2008 was presented by Faris and Villeneuve (2008).

The results suggested that the type of content filtered varied widely based on the country and region in question.

In indentifying what type of content was blocked and in which country, the study categorized content based on genre and put them in four categories (Faris & Villeneuve, 2008, p. 26):

- Political: dissident websites criticizing the regime, advocacy, etc.
- Social: pornography, gambling, etc.
- Conflict/security: separatist, guerilla, armed opposition, etc.
- Internet tools: circumvention software, anonymizers,[32] proxies, etc.

On the other hand, each category was assigned a particular level of filtering, which had to be from one of the following five levels (ibid.):

- No evidence of filtering
- Suspected filtering
- Selective filtering
- Substantial filtering
- Pervasive filtering

Furthermore, the study also measured the level of transparency and consistency of censorship. Transparency is to indicate whether censors publicly declare that the website was filtered and display information to the Internet user in a clear way. The lack of transparency is often due to attempts to mislead the user by returning another page with a "not found" or "server error" message. To measure consistency, ONI researchers tested

[32] This is usually a reference to software that replaces the real Internet Protocol (IP) address of the user with that of the proxy server when viewed by the target server.

different ISPs in the same country to see if filtered content had been blocked consistently by all ISPs they examined or not (p. 238). As described in their methodology, ONI researchers tested specific lists of websites that were categorized based on their content and flagged as candidates for being potentially filtered based on previous experience. The tested websites were of various genres ranging from pornography to political satire and crude humor. The tests were carried out for various ISPs in different locations in each country (p. 5). The data collected by the ONI study was a result of collaborative efforts by several ONI researchers who studied forty countries to understand what types of content was blocked, what blocking mechanisms were used, and what Internet regulations existed. The study covered eight regions: Asia, the MENA, the Commonwealth of Independent States (CIS),[33] United States/Canada, Europe, Latin America, sub-Saharan Africa, and Australia/New Zealand. While many countries in Asia and MENA exhibited relatively high levels of Internet filtering, the United States, Canada, Europe, Australia, and New Zealand had narrow and focused targeted filtering of online content, which was primarily child pornography and, to a limited extent, hate speech. Filtered content in Latin America was found to be similar in scope to the United States, Canada, Europe, and Australia, but the technology in filtering was not as developed, and, hence, they did not apply Internet blocking as widely (Deibert, Palfrey, Rohozinski, & Zittrain, 2008, p. 153).

When it comes to the MENA region, ONI's research found that filtering of websites deemed socially inappropriate, such as pornography, was quite extensive. Furthermore, critical political speech was also targeted, and censorship of such content was on the rise. The situation was similar in some Asian countries, with China leading the way as the developer of the world's "largest and most sophisticated filtering system," which filtered political content pervasively (p. 263). Meanwhile, all CIS countries except Uzbekistan and Turkmenistan, which were not tested, were found to not practice substantial or pervasive filtering. The study also found that CIS countries applied legal measures "designed to promote self-restraint (or self-censorship) on both the ISP providers as well as content producers" (p. 184).

Among all studied regions, sub-Saharan Africa had implemented the lowest level of Internet regulatory restrictions, and the reasons behind that

[33] CIS countries include Russia, Ukraine, Belarus, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, and Uzbekistan.

were weak infrastructure and poor economies, which led to having a small percentage of the population with regular Internet access (p. 154).

Despite the variations among different countries in the type of censored online content, at a fundamental level, the main target was information that was deemed culturally or politically sensitive in the respective country (p. 32). What the study lacked was the actual lists of blocked websites and comparisons between what had been blocked in countries that share common social or political interests, for example, Arab countries.

Studying censorship in China's blogosphere

The other reviewed empirical study was the one done by MacKinnon on blog censorship in China. MacKinnon attempted to find what types of user-generated content were censored by Chinese Internet companies. She concluded after her eight months of testing that, among the politically sensitive material targeted, a significant amount did survive censorship (MacKinnon, 2008). Unlike ONI's automated testing methods, MacKinnon's study was based on manual entries, which was a "highly labor–intensive and time–consuming" task, as she led a team of individuals to test fifteen prominent BSPs and her tests were conducted by attempting to post passages related to politically sensitive material on various blogs to discover which content got filtered. Testers attempted to post 150 entries through each of the 15 BSPs on fifty politically sensitive topics, which ranged from the Chinese-language equivalent of "Falun Gong" to "Tibet independence" and from "riots" to quotes by the Dalai Lama. The study discovered an unexpected high degree of variation in the type of content blocked by the different BSPs and in the level of filtering as well. MacKinnon concealed the real names of the BSPs when she published her results for fear of repercussions by the government.

> People who work in the Chinese Internet sector have expressed strong concern that published results of an independent academic study showing who censors more than whom could be used as a tool for reward and retribution by regulating authorities. (MacKinnon, 2008)

She assigned alphabetical letters to the BSPs and ordered them by the number of passages censored from highest to lowest. On top of the list was BSP "A," which had blocked sixty of the 108 passages. The most tolerant BSP was "O," which had blocked only one. The results have indicated that not a single tested passage was censored by all 15 BSPs. The passage dealing with Falun Gong topped the list as the most censored

topic with 13 BSPs blocking it. It was closely followed by the post on Tibet independence, which was censored by 12 BSPs. Nine BSPs censored an item about the Tiananmen Mothers website, and nine BSPs also censored an excerpt of the Dalai Lama's open letter to the Chinese people.

Although Internet censorship in China is not confined to political content —as indicated by ONI's study (Deibert et al., 2008, pp. 263–271)— MacKinnon had restricted her research to politically sensitive content and limited it to blogs. She noted that the study left out some social networking, instant messaging, mobile services, and bulletin board systems (BBS), extremely popular and widely visited. She also stated that further research was needed in order to understand the global trends and emerging practices in the field of Internet censorship (MacKinnon, 2008).

What MacKinnon's study lacked is perhaps a complementary survey of a sample of Chinese blog posters to understand how effective those BSPs were in censoring what they want to post and how/if they are able to bypass censorship in such cases. However, such a survey could end up being too hazardous for the researcher or the subject.

The aforementioned two studies have illustrated two different approaches to measure what is being filtered by the censors. The first by ONI was global and automated and had used several researchers and sophisticated software to verify the status of filtering on the ISP level, while MacKinnon's study was limited to Chinese blogs and covered a particular genre of content, namely, politically sensitive content.

Studies of Censorship Circumvention

The subject of Internet censorship circumvention appears to be one of the most under-researched within Internet censorship, particularly from the nontechnical perspective. I have unfortunately found not even a single study on circumventing Internet censorship that uses data from actual users of those tools, and I believe one of the reasons may be the highly demanding interdisciplinary nature of such a topic. Studying censorship circumvention requires some understanding of how Internet censorship works on a technical level as well as a familiarity with how different circumvention solutions function. On the nontechnical level, such a study would also require surveying users to know which software they use more comfortably and how, why, and to what context. Furthermore, the researcher would then have to make ethical judgments and tolerate the risks of studying a subject that may be taboo in certain countries.

Murdoch and Anderson briefly touched upon the circumventability of Internet censorship by mentioning how each of the filtering methods could be bypassed. They noted the possibility of circumventing the Transmission Control Protocol/Internet Protocol (TCP/IP)[34] header filtering using proxies that serve as a bridge between the client and the restricted online content (Murdoch & Anderson, 2008, p. 68). However, they did not go any deeper in exploring the pros and cons of each circumvention method and did not provide information about software used in that respect.

On the other hand, GIFC released a white paper on circumvention methods and programs used for circumvention. The following is a summary of the circumvention solutions that they described in detail (GIFC, 2007):

1. **Freenet:** Designed by Ian Clarke in 1999 as a decentralized, P2P network, Freenet is a program capable of supporting anonymous information transfers. Its number of users and speed remained low but the idea still had potential to serve as a circumvention method for P2P connections because it had no central network. However, the authors did not find the product competitive enough with the other circumvention solutions designed to bypass website censorship, as it required users to feed content into the network, which was a serious limitation.
2. **Triangle Boy:** This product was launched in 2000 mainly to circumvent IP blocking. It received attention when the venture capital company, In-Q-Tel, started investing in it. It was successfully used in countries such as Saudi Arabia and China on a limited scale. However, the Chinese government was able to block it and render it useless in 2001. It was later superseded by more effective solutions.
3. **Garden:** Launched by Garden Networks (www.gardennetworks.com) in 2001, this program was able to circumvent IP blocking, and applied techniques to rewrite URLs[35] to defeat DNS hijacking. It remained one of the most popular

[34] The TCP/IP belongs to the Internet protocol suite, which is a set of standard protocols that are used on the Internet and other similar networks.

[35] A URL is a uniform resource locator that corresponds a particular address or location on the World Wide Web and typically starts with "http://" or "https://" (e.g., http://www.oru.se/English/Library/).

circumvention solutions used in China and had a user base of around 20,000 in 2007.

4. **Ultrasurf:** Among the most popular circumvention solutions in the world, this program was launched in 2002 by UltraReach (www.ultrareach.com), an Internet technology company founded by a group of Silicon Valley technologists. It had as many as 100,000 users as of 2007 and remained active in overcoming all types of censorship mechanisms.
5. **DynaWeb:** Produced by Dynamic Internet Technology Inc., this solution was originally founded in 2001 to provide e-mail services to China for US government agencies and non-governmental organizations. It was able to avoid being blocked in China by applying a sophisticated set of techniques. Its 150,000 users could be served through hundreds of varying IP and domain names at a time. The program could automatically replace an IP or domain name if it found any of them to be blocked.
6. **GPass and FirePhoenix:** These two products were released in the summer of 2006 by World's Gate Inc., which aimed at providing users in countries ruled by repressive regimes with solutions to circumvent Internet censorship. GPass expanded the use of circumvention from merely accessing blocked content on the Web to using it in other application protocols, such as Microsoft Media Server (MMS) protocol, file transfer protocol (FTP), and instant messengers. On the other hand, FirePhoenix was used as an interface through which all traffic between the computer and the Internet went through. The two programs had around 15,000 users by 2007.
7. **The Onion Router (Tor):** Originally supported by the US Naval Research Laboratory and later inherited by the Electronic Frontier Foundation (EFF) in 2004, this program is one of a few that are open-source and developed with a community of volunteers. However, being open-source makes the project vulnerable to blockage by the Chinese authorities. It also depended on what is called "multi-hop trafficking," which is efficient for anonymity purposes but results in latency, causing its traffic flow to be slower than the other solutions. It had a user base of around 10,000 by 2007.

However, the GIFC paper did not explain the methodology used in carrying out the study, particularly in finding the number of users. Furthermore, it only focused on China's Internet censorship and Chinese users as the main group using those products. The assumption was that if they worked in China, they could work in any other country, but they did not substantiate this argument. The study did not discuss one of the most common methods of circumvention, which is the use of Web-based proxy servers.

At this point, it is useful to refer to a study I personally did in 2008 in relation to circumvention tools. In that study, I described three circumvention methods that can be used without the need for installing external software:

- **Virtual Point Networks (VPNs):** These are server nodes that serve as a tunnel through which traffic from all applications at the client go through to communicate with the Internet. Most of these types of circumvention solutions are available for a fee.

- **HTTP[36] or SOCKS[37] proxy servers:** These are servers that are utilized only by some applications, for example, a Web browser or a chat client. Unlike VPNs, they need to be configured on every piece of software that connects to the Internet. They could be local proxy servers on the machine itself, or remote server.

- **Web-based proxies:** These are website that are used directly on the browser window as they encapsulate or frame a remote Web page within the proxy website itself. This entails a lot of encoding and decoding of data to ensure that the links go through the Web-based proxy itself. They are similar in function to Web-based translation tools that translate full Web pages. An example of a Web-proxy is Google Translate, which attempts to fetch a remote website, replaces the original language with the target language, and displays it back to the user in encoded format. There is no direct connection here between the user and the target website, which

[36] Hyper Text Transfer Protocol (HTTP) is the protocol used to access Web pages and could also be used to tunnel plain unencrypted traffic through a proxy.

[37] Socket Secure (SOCKS) is used to communicate traffic via a proxy server and unlike HTTP proxies, SOCKS connections encrypt all traffic.

> only sees Google's server as the visitor. Another example is YemenPortal.net, which has the ability to reach blocked links by using an internal Web-based proxy to encode content in a way that would allow the blocked website to appear as if it were being opened directly (Al-Saqaf, 2008, p. 175).

Another study on censorship circumvention was done by Nart Villeneuve, who presented a mostly nontechnical paper summarizing tactics used to evade or resist Internet censorship in a number of countries around the world. Some of those tactics involved doing research on how filtering software worked. Others were focused on legal challenges and advocacy campaigns targeting the censors (Villeneuve, 2007, p. 79).

There were other studies dealing with Internet censorship circumvention but they were either technical papers confined to a specific solution (e.g., Dingledine, Mathewson, & Syverson, 2004; Feamster, Balazinska, Harfst, Balakrishnan, & Karger, 2002) or merely introductory manuals available on the Web to help people choose the program they think is the most effective (The Citizen Lab, 2007).

A survey done in 2010 by Leberknight, Chiang, Poor, & Wong aimed at presenting a taxonomy of the principles, techniques, and technologies of Internet censorship and anticensorship and came up with conclusions on how to overcome challenges and use opportunities in anticensorship research based on developments since 2000. The authors concluded that Internet censorship can be confronted best by developing censorship-resistant systems that maintain anonymity, improve trust, are easily usable, have a technological edge, and are supported by existing infrastructure. Furthermore, the success of censorship circumvention tools would largely depend on their ability to exert political and economic pressure on censoring authorities to make the very act of censorship too costly to continue (Leberknight, et al., 2010, p. 19).

Perhaps the most comprehensive series of studies to evaluate Internet censorship circumvention tools was done by scholars affiliated to the Berkman Center for Internet and Society over a period of four years from 2007 to 2011 and in the form of three successive studies conducted in 2007, 2010, and 2011. The studies had the same aim of evaluating the effectiveness of the most prominent circumvention tools available at the time, and every new study was meant to identify trends or changes happening over time. I hereby present summaries of the key findings of each of the three studies.

The first study by Palfrey, Roberts, and Zuckerman was conducted in 2007 but was published two years later. The study did an evaluation of ten different tools and assessed them based on six criteria: utility, usability, security, marketing, sustainability, and openness. The key findings were that while all the tools succeeded in the main test of circumventing Internet filtering, each had its own problems regarding performance and/or security, and so the ultimate decision on which particular software to choose will largely depend on the aim of the user. In cases when maximum privacy is needed, for example, for an activist in an authoritarian state, using tools that do not provide any anonymity should be avoided, while favorable solutions would be ones that provide a higher degree of anonymity such as Tor. The degree of anonymity, however, is often negatively correlated to the speed levels because the more encryption there is, the slower the transfer would be. In essence, the conclusion was that there would be need for a trade-off and compromise of one aspect in favor of another, and so there is no perfect circumvention solution (Palfrey, Roberts, & Zuckerman, 2009).

In 2010, the same scholars repeated the tests but expanded the tested solutions to eleven instead of ten. The report arrived at three key findings: first, circumvention tools had very limited users as a percentage of those affected by Internet censorship. Second, the majority of users of such tools preferred using the simplest of circumvention methods instead of the more sophisticated ones. Third, when users sought for circumvention solutions, they opted for using search engines with well-known keywords such as "proxy," which often lead them to simple proxies rather than more reliable ones. Furthermore, the study found that in democratic countries, the majority of users of such tools were students circumventing school firewalls, and as the installed firewalls were not sophisticated enough, it was possible to use simple proxies for circumvention. However, in countries with pervasive nationwide censorship such as China, such tools were of little use while blocking-resistant[38] tools were more effective. The researchers identified that hundreds of thousands of users were served by the various circumvention tools including Ultrasurf, Freegate, Tor, and Hotspot Shield, along with seven simple Web proxies (Faris, Palfrey, Roberts, York, & Zuckerman, 2010).

[38] A blocking-resistant circumvention solution is one with the ability to find ways of remaining active despite vehement attempts to have it blocked or de-activated.

Unlike the earlier two reports, the last study done by Roberts, Zuckerman, and Palfrey and released in 2011 did not mention the seventeen assessed circumvention tools by name but rather put each of them in one of three categories based on the method of circumvention used: simple Web-based proxies, VPNs, or other methods.

The study justified the omission of the names of those tools "for fear of providing a roadmap that filtering countries could use to shut down the evaluated tools" and came up with a much more extensive list of findings from two tests, one conducted in February and the other in March of 2011. The tests were done using human testers in four Asian countries, namely, China, South Korea, United Arab Emirates (UAE), and Vietnam. The research also coincided with the Arab Spring. This made the study more relevant, particularly as the Internet played a significant role in those events (Roberts, Zuckerman, & Palfrey, 2011, p. 1).

The main findings of the 2011 study could be summarized in two main conclusions. The first was that tools have become less able to deliver on their promises and some failed to circumvent censorship consistently while others appeared to have been blocked from operating. This meant that challenges to circumvention tool developers have increased significantly with governments eager to take them head-on and in a more serious manner. The second conclusion was that the performance assessment ended up in results similar to earlier reports as some tools were performing better in some areas such as speed and utility and worse in areas such as security and privacy (p. 4).

The three Berkman Center studies serve as a valuable resource on how circumvention tools operate, how they are used, and what challenges they face. However, I wish to raise a few critical points about those studies. In the 2011 study, the names of the tools were not mentioned, which resulted in a tremendous loss for readers who wish to use the report as a basis for assessing a particular tool whether for research or other practical purposes. This, in my view, is not easily justifiable merely based on fear of providing information that governments could utilize to shut them down. Governments are already well aware of many aspects of the circumvention tools and they can do their own research as well. I argue that such tools are already quite popular, and an additional academic paper would not constitute any significant threat.

Another aspect that could be a limitation in the three studies is the fact that in order to do the study, the researchers had to heavily rely on the cooperation of the circumvention tool developers for basic information

such as number of users, traffic, etc., which, albeit understandable given the limited knowledge one could get from outside, makes any information provided by the competing developers not possible to verify independently. I do not believe it is easy to overcome this limitation, but this should have clearly been stated as a limitation in those studies. Furthermore, the researchers could have proceeded to contact actual users of circumvention tools perhaps through a survey to get their input and help them verify and cross-validate the information they obtained, particularly about speed, popularity, and reliability of the different tools.

Finally, the study confined itself to circumvention solutions that had high usage patterns while ignoring other circumvention tools that albeit may not be as popular, still have promising ideas that could have served as inspiration to discuss potential integration with more established tools to create more robust hybrids that can lead to stronger, faster, and more blocking-resistant solutions.

Filling the Knowledge Gap

As shown in the preceding sections of this Literature Review Chapter, the topic of Internet censorship and circumvention is quite rich and was covered from various angles by many scholars. However, there are some knowledge gaps that become apparent when considering the recent developments in the Arab world, particularly the Arab Spring and what followed. The studies by ONI did not extend to cover the fluctuations in Internet censorship before, during, and after the Arab Spring. That in particular is one knowledge gap this study aims to fill with a focus on the countries that had significant developments such as Tunisia, Egypt, Syria, and Yemen.

Additional gaps are the lack of data about the perception of the appropriateness of Internet censorship, particularly in relation to censoring various types of content. Some of the studies tackled surveys about the appropriateness of censoring pornography and some other categories, but they were not as elaborate and were confined to the United States. This study aims at filling that gap by using surveys presented in English and Arabic to get the perspective of Internet users in the Arab world and compare their feedback to that from non-Arab countries.

There were no studies addressing the use of Internet censorship circumvention tools with the perspective of the actual user in mind. Additionally, it was not possible to find literature that explained the usage patterns of Arab users when attempting to circumvent censorship during the peak of

the Arab Spring, which is arguably one of the major developments of the last few years. And although there were studies to evaluate circumvention tools in general, they were focused on the tools but not the users of the tools. This is a significant knowledge gap that this study aims to address on two levels. The first is on the level of actual use of a circumvention tool offered to Arab users, as that will help identify usage patterns and interests without the need to fill any surveys and will be quite objective as it does not involve communicating with the users, who remained anonymous. The second level is through actual Web surveys, which users of the software would answer anonymously to help shape an understanding of what particular factors help make circumvention most effective.

Finally, although it is not a knowledge gap per se, but as most of the literature produced around Internet censorship was carried out by Western scholars with very little contribution from scholars from non-Western societies, adding a study by an Arab researcher with a good understanding of the language and culture of the region may be of value to help supplement the available literature and introduce more diversity. Furthermore, a similar study would have been difficult to do for a non-Arabic speaker due to the immense work that would otherwise be required to translate the Arabic text to understand the types of different Arabic websites before proceeding to do the necessary content analysis.

Chapter 3: Theoretical Framework

This study is built on a framework that stands on four fundamental theoretical pillars: freedom of speech, authoritarianism, censorship, and liberation technology. Those areas are tackled first from a general standpoint and thereafter treated in relation to Internet censorship and circumvention. Relevant theories and concepts related to those four pillars are elaborated and linked together on different layers to form the theoretical foundation on which the whole research was built.

Furthermore, this dissertation uses path dependence theory to a limited degree in order to develop an understanding of the context in which Internet censorship is practiced in the Arab world and how it was contested using circumvention software. Therefore, this chapter ends with a brief and general description of path dependency and its application.

Freedom of Speech

The concept of free speech can be derived from a definition of the broader "freedom of expression" term, which according to Thomas Scanlon includes the right to "any act that is intended by its agent to communicate to one or more persons some proposition or attitude" (Scanlon, 1972, p. 206). This definition is rather general and may well go beyond traditional speech and publication, as it could also include displaying or refraining from displaying symbols, protests and demonstrations, sit-ins, strikes, art performances, drawings, assemblies, blogging, tweeting, and many other acts that have an intended meaning sought to be conveyed.

Freedom of speech as a human right

One of the historic and important documents that upheld free speech is the 1789 Declaration of the Rights of Man during the French Revolution:

> Article 4: Liberty consists in the freedom to do everything which injures no one else; hence the exercise of the natural rights of each man has no limits except those which assure to the other members of the society the enjoyment of the same rights. These limits can only be determined by law. (Declaration of the Rights of Man, 1789)

A couple of years later, the First Amendment was adopted to the US Bill of Rights, creating a new era of free thinking and innovation and making it perhaps the most widely known and publicly valued provision of the US

Constitution (Donnelly, 2010). The part of the First Amendment referring to free speech was conveniently called the "free speech clause":

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances. (Legal Information Institute, n.d.)

The main aim of the First Amendment and the other nine amendments constituting the Bill of Rights was to ensure that the autonomous US states would be protected from potential abuse by the newly formed confederation and avoid the return of a tyrannical rule similar to the British Empire from which the new republic had gained independence (Amar, 1991, p. 1133).

In the aftermath of the Second World War, the United Nations General Assembly convened on December 10, 1948, and adopted the UDHR at Palais de Chaillot, Paris. In the declaration, there was direct reference to freedom of expression in Article 19, which said:

> Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. (United Nations, 1948)

The unanimously approved UDHR resembled remarkable similarities to the 18th-century declarations in France and the United States, particularly in proclaiming equality and freedom for all humans[39] and could be said to have been the "enlightened conscience of mankind" as Johannes Morsink puts it in his analysis of the philosophy behind the declaration (Morsink, 1984, p. 309). Although free speech came out of a Western tradition and was argued for on platforms where Western powers have leverage, it is safe to say that it remains a valid right for all of humanity (Rønning, 2009, p. 18).

There is, however, disagreement in the free speech academic circles about whether it should be considered as a human right. For example, Larry Alexander argues that although it may be valuable to provide some protection to free speech, it should not be elevated to the level of a human right due to the difficulty to apply it in absolute terms across all cultural

[39] It is worthy to note however that the declaration did not deter the committing of grave atrocities such as the massacres in Bosnia, Rwanda, and other genocides committed by countries that did ratify it.

and historical contexts (Alexander, 2005). Although Alexander's argument suggests that free speech cannot be a right in the literal sense, it does not invalidate existing theories—to be briefly presented in the following section—on why free speech should be protected. Marshal King goes one step further in challenging the free speech principle altogether, arguing against isolating free speech as a standalone independent value apart from other liberties (King, 2012).

Hereafter, an attempt is made to present the main positions in free speech theory.[40] At this point, the subject of freedom of speech is pursued as a holistic concept without getting into fine details about the various different forms of speech. Otherwise, one could risk obscuring the complex nature of free speech, particularly in relation to its limits (Greenawalt, 1989, p. 120). Nonetheless, free speech theory by Emerson (1963) and the theory of freedom of expression online by Balkin (2004), which will be described in detail in the next sections, are taken as points of departure to form the theoretical framework to be used in deciding the research methods and in analyzing the findings of this study.

Free speech theory

Media and communications scholars interested in exploring freedom of speech will have to go through legal, social, political, and philosophical literature about free speech theory to appreciate how heavily influenced this area is by an Anglo-American perspective that is mainly rooted in the First Amendment. This does limit the understanding of the freedom of expression considerably (Smith L. A., 2001). Nonetheless, credit is due to the American liberal theorists who started the active development of free speech theory in the 18th century, which was a period marked with increased attention to free speech within the context of political theory and practice (Israel, 2009).

The early theoretical debates aimed at defending free speech in general and the First Amendment in particular (Barendt, 2007). It is important to note, however, that the theory was affected by several Enlightenment philosophers from Europe such as Immanuel Kant, Johann G. Fichte, Carl F. Bahrdt, and Georg W. F. Hegel (Smith L. A., 2001).

[40] The term 'First Amendment theory' is used interchangeably within American literature to refer to free speech theory. In some literature, the theory is also called progressivist or republican free speech theory.

In taking a historical look at the early arguments supporting freedom of speech, one can observe that they all revolved around the importance of free speech for the collective social good that it would bring. The English author John Milton was among the pioneers in the 17th century to openly call for free speech and for abolishing censorship. He argued in his renowned "Areopagitica" speech of 1644 that protecting free speech from censorship contributes to public good by pointing to the societal problems that need to be reflected upon (Milton, 1873).

However, it was in the United States where most of the work around free speech theory developed, with James Madison putting forth the argument that free speech would enhance political stability by exposing wrongdoings of government and establishing a system of checks and balances (Madison, 1962). On the other hand, John Stuart Mill defended the free exchange of opinions no matter how unpopular they may be on the basis that there can be no view that is infallible (Mill, 1946). As a US constitutional court judge known for his strong support of free speech, Oliver Wendell Holmes argued for competitive and free trade in ideas as a way for society to experiment and adapt to changing conditions (Holmes, 1919). Similarly, Judge Learned Hand believed in free speech but for its value in addressing social problems without reverting to conflict or violence (Hand & Dilliard, 1952). Judge Louis Brandeis was for free speech as a way to seek the truth without fear of government retaliation because such fear would result in repression and instability (Brandeis, 1953). Finally, Alexander Meiklejohn emphasized the function of free speech as a means to empower citizens with information because informed citizens make for better democratic participation, which, in turn, benefits the whole of society (Meiklejohn, 1948).

One of the relevant popular quotes that emerged in the 18th century on the value of an informed electorate for democracy is that by the principal author of the US Declaration of Independence, Thomas Jefferson:

> Whenever the people are well informed, they can be trusted with their own government; that whenever things get so far wrong as to attract their notice, they may be relied on to set them to rights. (Jefferson & Hunt, 1994, p. 4)

More recently, however, attempts were made to focus on the justification of free speech for its role in supporting individual autonomy in addition to the traditional argument around the "collective good" of society (Blasi, 2010). Martin Redish is one of the scholars calling for understanding the First Amendment in light of what it does to foster *individual self-*

realization, which he argues is the true value of free speech[41] (Redish, 1982, p. 645).

As a modern free speech theoretician, Thomas Emerson sums up the functions of free speech in four elements. The first is its function in assuring individual self-fulfillment, which resembles the right of every individual, as a member of society and a social animal, to form and express beliefs and opinions (Emerson, 1963, pp. 879–880). Second, free speech is the best process of advancing knowledge and discovering the truth because only after considering all facts and arguments, no matter how unusual—as no opinion is infallible or immune from challenge—could the most rational judgments be made (pp. 881–882). Third, freedom of expression allows participation in decision-making through a political process in which individuals can express their opinions about how they ought to be governed, for example, in the form of democratic participation such as elections (pp. 883–884). Finally, free speech functions as a balance between stability and change by allowing individuals to have open discussions, addressing social problems, proposing remedies, adapting to changing conditions, creating political unity and cohesion, and preventing problems of social control as no group would prevail over the other (pp. 884–885).

Emerson's theory appears to have captured many of the values for which early free speech proponents advocated, and would therefore serve as a suitable theoretical point of departure for this study in justifying the importance of free speech. Notwithstanding the fact that this dissertation focuses on the Arab world, free speech is taken from a normative point of view that applies to all peoples regardless of geography, ethnicity, or other factors that divide them. Free speech in the Arab context is seen as valuable to Arabs as it would to all other societies.

When reviewing relevant literature in the area of free speech, one can conclude that liberal free speech theory has focused more on individual rights even when it could compromise collective rights. However, Douglas Sanders reflects on this contentious issue, noting that the voice of individual rights proponents has been historically louder, with some scholars arguing that collective rights are inconsistent with individual rights. In an

[41] The debate around collective vs. individual rights to free speech is complex and goes beyond the scope of this study. However, it remains ongoing with the modernistic view on the importance of free speech for individual autonomy being challenged by an opinion that calls for preserving the more traditional free speech theories that emerged in the 17th century with Milton and others.

attempt to show that the cause for collective rights is not lost, Sanders indicates that while some rights such as freedom of expression are seen as an individual right, collective rights such as freedom of religion and other cultural rights need to be respected (Sanders, 1991, p. 383). Despite the attempt by Sanders to introduce some possible solutions to help alleviate the inevitable conflict between individual and collective rights, the debate about where to draw the line and strike the balance is likely to continue.

Limits of free speech

Despite being of value for the individual as well as for society at large, free speech can occasionally be abused. There is a general consensus among advocates of free speech that the production and dissemination of child pornography, hoax messages, or false information, for example, could actually harm others and, hence, should be restricted. In other words, there have to be some restrictions on speech (Warburton, 2009, p. 8). If we look back in history, we could easily identify many prominent cases where a limit on free speech was enforced based on this "harm" rationale without necessarily defining how to assess the harmfulness of speech. The prosecution and trial of Socrates in 399 BC exemplify how ancient the practice of censorship is. The trial was initiated due to the belief that the teaching of Socrates had corrupted the youth (Stone, 1989). As the jury considered this act of expression "harmful" to the youth, it found it acceptable and, in fact, necessary to censor it, which meant the death of Socrates, who expressed his willingness to rather give up his life than to stop teaching (Smith & Torres, 2006).

John Stuart Mill tried to determine the boundaries of free speech in his popular 1859 "On Liberty" essay, wherein he proposed the one condition, referred to as the "harm principle," on which free speech could be restricted:

> the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. (Mill, 1946, p. 8)

Following up on Mill's work, the free speech scholar Thomas Scanlon used the term "Milliam principle" to identify cases where the degree of harm could be tested. He summarizes those points in the following:

> There are certain harms which, although they would not occur but for certain acts of expression, nonetheless cannot be taken as part of a justification for legal restrictions on these acts. These harms are: (a) harms to cer-

> tain individuals which consist in their coming to have false beliefs as a result of those acts of expression; (b) harmful consequences of acts performed as a result of those acts of expression, where the connection between the acts of expression and the subsequent harmful act consists merely in the fact that the act of expression led the agents to believe (or increased their tendency to believe) these acts to be worth performing. (Scanlon, 1972, p. 213)

Scanlon argues that free expression should not be censored just because the act of expression differed from common opinion or from what the government says. Censorship in such a case assumes the government's superior judgment, which is a blatant bias. Scanlon also argues that censoring an act of expression should not be allowed for cases where the information provided could lead to the recipient believing in something and acting on it even though the original claim is incorrect. However, cases where free speech could be censored must involve harm-inducing speech directed to a subordinate individual, for example, a father to his child or when a squadron is ordered to massacre civilians (Gazi, 2010).

The Milliam principle is but one of several proposed principles to identify the limits of freedom of speech devised over the years.[42] There is certainly no one-size-fits-all method that could define a standard limit to freedom of speech. Context is crucial when it comes to free speech restrictions. In the United States, for example, the First Amendment does not cover certain areas of speech as they conflict with other laws or norms in the country. There were instances, for example, when US courts ruled against protecting speech containing obscenity, libel, fighting words,[43] and commercial advertising (Schauer, 2004, p. 1777). Later on, further court cases emerged, adding more to the list of unprotected speech including inciting imminent lawless action, military secrets, inventions, nuclear information, and weapons (Fein, 1984).

While the Milliam principle can be used as a normative approach to find when to restrict or censor particular content, proper application of the principle can only take place with the accumulation of experience over

[42] Another popular principle is called the 'Offense Principle', which goes one step further in restriction by considering any speech that could offend others without potentially hurting them, e.g., burning flags, holding controversial rallies, etc. See Cohen-Almagor's 1993 work "Harm Principle, Offence Principle, and the Skokie Affair" for more insight.

[43] 'Fighting words' refers to speech that could incite hatred or violence as a reaction from the target and definitions and limits vary by jurisdiction.

time and with the identification of real cases where harm did materialize, and so it is more of a trial-and-error procedure. Furthermore, when basing a decision to censor a particular form of speech based on the Milliam principle, there is a dilemma of having to deal with laws that may clash with the right of free speech. Examples are state secrets and privacy laws. In such situations, understanding the context and analyzing the particular situation carefully are key in order to effectively implement the Milliam principle.

In certain cases where there is an overlapping or nonexistence of jurisdiction, for example, the Internet, judgment becomes even more challenging and requires a lot of due diligence.[44] It is worth noting that there is an ongoing argument as to how to regulate speech. The prominent philosopher Ronald Dworkin, for example, argues against the regulation of what people are allowed to say, because such action does not take into consideration the perspective of affected individuals and their circumstances. Laws in the United States, for example, are only issued based on the view of the majority in Congress or other legislative bodies, and individuals can only submit to the new laws without question[45] (Dworkin, 1978). Furthermore, he argues that interpretation of what is right and what is wrong when deciding on a particular subject would differ based on who has the power to decide (Dworkin, 1982), which poses a great challenge to applying standard global regulations on free speech.

When considering free speech as a universal right, one must also recognize that there are also other universal human rights such as the right to life, the right to peace, the right to privacy, and the right to religious freedom. If not in conflict, those rights could be upheld without limits. But when two or more of those rights are in conflict with each other, there will be a need for compromise. Justifying limiting free speech could be argued if it conflicts with another right that was at a particular context assessed as of more value than the right to free speech. As demonstrated by Gazi's earlier example of the inappropriateness of allowing a squadron to massacre innocent civilians (Gazi, 2010), free speech can and should be legiti-

[44] To avoid falling into the 'legal jurisdiction' trap when studying Internet censorship of online content in this study, a more simplified approach was carried out based on universal values that are not bound to any particular law. More about this is explained in the Methodology Chapter.

[45] This is a problem with representative democracy in general because when limits on free speech become instituted rigidly, they carry with them negative consequences on the rights of citizens.

mately censored because the right to free speech can be compromised when it violates the right to life.[46]

And so what the Milliam principle suggests is that one can only judge whether free speech should be limited or not if it conflicts with other rights, and that decision would depend heavily on the particular context in question.

Theory of freedom of expression for the information society

With the advent of the Internet and digital technologies, new opportunities emerged for the expansion of speech opportunities by allowing citizens to reach people on a global scale in ways that were not possible before. Yet if free speech theory is one that was meant to transcend time and medium and could be applicable to all forms of speech over time and space, why would there be need to develop a theory specific to the Internet? Someone who conveys an opinion at a public event, through a newspaper article, or by calling into a TV show might as well use the Internet to publish a blog post, send a tweet, or create a YouTube video, and that would resemble how free speech theory could apply to all media.

Yet, introducing a new theory of free speech for the information society is possible given the way digital technologies are changing the social conditions of speech, which consequently leads to changing the focus of free speech itself (Balkin, 2004, p. 1). Such a theory may not necessarily compete or contradict traditional free speech theory, but rather complement it by filling some gaps or strengthening weak points.

Jack Balkin introduced the theory of freedom of expression for the information society with the rationalization that Internet changes the social conditions that impact how people practice free speech because it makes features of free speech more *salient* including interactivity, nonexclusive appropriation, creative innovation, and mass participation (Balkin, 2004, p. 55). He criticized the traditional free speech theory, citing that it was developed for a time when the role of ordinary citizens was confined to spectators, consumers, and passive recipients. Yet the Internet has allowed citizens to move from being mere recipients to interactive creators of con-

[46] As an example, limiting the right to free speech was deemed necessary when it violated the right to life in the case of the Rwandan 1994 genocide. The International Criminal Tribunal for Rwanda in Arusha indicted three Rwandan media professionals for abusing free speech and using the media to commit genocide (Thompson, 2007, p. 362).

tent, participants, and innovators with an ability to "route around and glom on" to the mass media (p. 43). Nonexclusive appropriation is a form of free speech because it takes content from other sources, such as news websites, and uses it in a blog or other form and, thereafter, makes it accessible and nonexclusive so as to promote the free sharing of ideas (p. 11).

In terms of creative innovation, Balkin argues that the Internet allows citizens to promote a democratic culture where old things are used to create new ones in innovative ways, sometimes breaking traditions, dissenting, or creating new ways of expression (pp. 35, 47). Balkin notes that mass participation, particularly in the cultural domain, was one of the Internet's major contributions to free speech. Yet, it is also a major challenge as it allows for the massive accumulation of wealth and consequent conflicts over capital (p. 3).

While highlighting the Internet's capacity to promote free speech, Balkin conditioned that on the need to confront attempts by powerful players to use intellectual property and other justifications to restrict content. He recognized the need to face attempts by telecommunications networks to abuse their powers and stifle online free speech mainly through limiting forms of participation and cultural innovation that may not agree with their interests. He suggested two main methods that could help protect free speech on the Internet: 1) legislative and administrative regulation of the technology, and 2) the design of specific technologies that could neutralize attempts to stifle online free speech (p. 54). The latter suggestion by Balkin was taken seriously for the purpose of this very study, that is, to design a specific technology to counter Internet censorship.[47] Designing and deploying a censorship circumvention tool to counter Internet filtering was seen as a feasible option. The first recommendation of Balkin, that is, to establish legislative and administrative regulation, was found to be impractical to be part of this study, as it would require a legal approach that would take this study well beyond its original scope. However, it remains of value to briefly mention a few views in relation to regulation for the protection of freedom on the Internet.

Some scholars such as Joseph Sommer argued that most legal issues posed by digital technology are not new and can be dealt with using pre-

[47] Censorship here refers to all means that may restrict free speech, which include but are not limited to regulation, violence, technical limitations, and even self-censorship.

sent laws, adding that not only is the introduction of cyber law unnecessary, but could also be "dangerous" (Sommer, 2000, p. 1145). Sommer uses the very principle of free speech by referring to the First Amendment while indicating that cyber law could violate citizens' right to be free from public regulation by introducing repressive measures, while the application of the First Amendment to online cases could indeed protect free speech (p. 1198). In relation to the area of intellectually property, Frank Easterbrook also rejects the argument that calls for new cyber laws, contending that traditional laws are capable of handling regulatory problems on the Internet just as they are capable of handling offline problems (Easterbrook, 1996).

Lawrence Lessig, who advocates open access and sharing of information online, has a different view and warns that as the Internet expands its influence and power, it could become regulated in one way or the other, not only by law, but also by social norms, markets, and architecture in a way that may not be in the interest of online freedom. This suggests the need to understand how the Internet is evolving and introduce new legal measures that could protect the creativity and innovation that the Internet made possible (Lessig, 1999).

Lessig was clear in indicating that the Internet does need to be regulated, but in a way that would protect freedom:

> I'm not against regulation. I'm against stupid regulation, where stupid means regulation designed to protect an incumbent against competitors. (Lessig, 2013)

Citing the importance of online free expression through creativity and amateur remixes of copyrighted online content, Lessig advocates the introduction of reforms to existing copyright law with digital technology in mind (Lessig, 2008). There is a tangible sense of anxiety demonstrated by Balkin and Lessig as to the future of freedom on the Internet. As the Internet grants citizens new means of free speech, online restrictions could be seen as a natural consequence, particularly in countries ruled by authoritarian regimes and controlled by interest groups that are capable of exercising repressive practices including censorship and copyright regulation. Evgeny Morozov has spoken widely about his skepticism of the notion of Internet freedom[48] and stressed that when it comes to freedom of expres-

[48] For more insight on Morozov's views, see: (Morozov, 2012).

sion and democratization, the Internet could in fact have both an empowering and a disempowering effect (Morozov, 2011).

Authoritarianism

Recalling the limits of free speech and particularly how Thomas Scanlon described how the Milliam principle could be used as a guide to understand when free speech can be limited, two possible outcomes from any free speech restriction come to mind:

1. the free speech restriction was valid and met the Milliam principle's threshold of imminent harm or
2. the restriction was unwarranted and would be considered a violation of free speech as the situation did not rise to the critical degree to prompt censorship. (Scanlon, 1972)

Restrictions to free speech by authoritarian regimes often go under the second point above as censorship is practiced not based on what is required to prevent harm, but on other motives that do not meet the Millian principle. I hereby turn to the theory on authoritarianism in order to start contextualizing the empirical study by indicating when, how, and why states violate the Milliam principle of free speech.

Authoritarianism as a regime form

Classic political science literature classifies national regimes in general into three main types: democratic, authoritarian, and totalitarian (Roskin, Cord, Medeiros, & Jones, 2011). Authoritarianism and totalitarianism do, however, share some commonalities in their suppression of the free flow of information through media and other channels.

Political sociologist Juan Linz made a clear distinction between authoritarian and the more repressive totalitarian regimes (Linz, 1964). While the latter aims at gaining consistent and steady popular support, an authoritarian regime is content with passive mass acceptance (as cited in Landman, 2005, p. 71).

There is also what is referred to as a "hybrid regime," which combines features from more than one regime type. An example of such a hybrid regime is "competitive authoritarianism," which refers to an authoritarian regime that has democratic mechanisms but which are violated to the degree that renders them ineffective (Levitsky & Way, 2002).

Within authoritarianism, there are a set of sub-classifications such as the populist authoritarian regimes, which emerged as a rebellion against

old oligarchies and sought to mobilize and incorporate the masses for reform (Hinnebusch, 2006, p. 380). Another example is the bureaucratic authoritarian regime, in which military officers use authoritarian power to exclude working classes in favor of bourgeoisie and foreign capital, sacrificing mass welfare in the process (O'Donnell G., 1973).

One key characteristic of authoritarian regimes, according to Linz, is to depoliticize the population by depressing the political participation of the public (Linz, 1964, p. 304).

Unlike democratic ones, Linz notes that authoritarian regimes do not base their legitimacy on fair and free elections, but on emotional justifications to combat societal problems, for example, underdevelopment and insurgency, which people will want the government to address. In doing so, those regimes hope to establish themselves as worthy to rule because they are best fit to address those problems. They end up lowering their bar of perceived legitimacy to the minimum of mass acquiescence, which portrays them as a "necessary evil" to tackle the society's pressing problems (Casper, 1995, p. 43).

When they do call for public participation in politics, for example, through election campaigns, rallies, and referenda, authoritarian regimes tactically control the message reaching the public in a way that suppresses anti-regime participation and dissuades opponents from acting politically and forming strong coalitions (Casper, 1995, p. 45).

It follows from those characteristics that different forms of oppressive practices from political persecution to media control would become effective tactics to limit political plurality and depoliticize the public, consequently preventing the opposition from reaching the critical mass needed to change the regime.

Authoritarianism in the Arab context

While the broad outline of authoritarianism presented earlier serves as a good point of departure, in this section, I present some aspects that appear to be common in the Arab context, which is crucially important given the focus of this study. The three aspects that will be address are the political, economic and cultural aspects.

The political aspect

When it comes to the Arab world, authoritarianism is indeed the most prevalent type of regime (Pratt, 2007). Several aspects could be considered in explaining how Arab authoritarian regimes succeeded in resisting transi-

tioning to democracy. A study by Frantz has shown that authoritarian regimes in the MENA outlasted other authoritarian regimes in sub-Saharan Africa, East and Southeast Asia, and Latin America. She attributed their success to the regimes' ability to arrange smooth, albeit undemocratic, transfers of leadership of the state within the same regime with little public resistance (Frantz, 2012).

While Frantz did not provide a comprehensive road map describing how regimes were able to prevent the masses from resisting such undemocratic successive transfers of power, Goldstone provided a more detailed recipe of how masses were kept unorganized and depoliticized by the Arab leaders, whom he referred to as "sultans."

> To keep the masses depoliticized and unorganized, sultans control elections and political parties and pay their populations off with subsidies for key goods, such as electricity, gasoline, and foodstuffs. When combined with surveillance, media control, and intimidation, these efforts generally ensure that citizens stay disconnected and passive. (Goldstone, 2011, p. 9)

Generally speaking, all authoritarian regimes tend to give themselves a head start to predetermine the election results because of information monopoly through "campaigning advantages" assisted with monopolizing the media and depriving the opposition from the same (Ezrow & Frantz, 2011, p. 72). In Hallin and Mancini's categorization of national media systems, this falls under the Mediterranean or polarized pluralist model, characterized by—among other things—frequent state intervention (Hallin & Mancini, 2004).

When it comes to manipulating the media for political gains, William Rugh's research of media in Arab states has shown varying levels of control to maintain the upper hand in the media. In his work published in 2004, Rugh presented a media typology through which he categorized media systems in the region into four groups, mobilization, loyalist, diverse, and transitional press, with each having its own patterns of repression that distinguish them from one another. The mobilization group includes Syria, Libya, and Sudan and is distinguished by exclusively government-owned media that allow no room for political debate. On the other hand, Palestine and all Gulf countries except Kuwait were put in the loyalist group, which has private media that are supportive of the regime and allow no political debate. Meanwhile, Lebanon, Morocco, Kuwait, Yemen, and post-Saddam Iraq were placed in the diverse group, characterized by the availability of private media ownership and liberty to have active

political debates with pro and con positions to the government. Finally, the transitional group, which includes Algeria, Egypt, Jordan, and Tunisia, is differentiated with its mixed ownership of the media and active political debate with vocal positions that may be for or against the regime, yet with overall characteristics that promote government control (Rugh, 2004).

It is apparent that there is a connection between media control and the ability of Arab authoritarian regimes to suppress oppositional political views. While covering traditional media adequately, Rugh's analysis did not include the Internet, which makes it somewhat insufficient on its own to explain the reactions of authoritarian regimes to the use of the Internet and social media. According to Shirky, however, the role of traditional media is starting to weaken as information is increasingly emanating from users through decentralized and distributed networks such as social media (Shirky, 2011). The threat of such social media becomes even more significant when pan-Arab transnational broadcasting media such as Aljazeera use them as an additional resource for their own reporting (Duffy, 2011).

In the political sense, authoritarian Arab regimes are keen on preventing the opposition from gaining any advantage in reaching to potential voters during election campaigns. If election results in Arab states are used as an indicator, then this strategy of media control has indeed been quite successful for many decades.

However, Puppis and d'Haenens warn that rapid technological developments and integration of the Internet into traditional media make it difficult for communication researchers to stay updated in their understanding of the impact of the new technologies on the public (Puppis & d'Haenens, 2013, p. 90). In other words, the seemingly persistent Arab public political apathetic may begin to change if this trend continues.

The economic aspect

One key characteristic that gives authoritarian regimes in the MENA extra leverage compared to other similarly repressive regimes is being rentier states, which is a concept postulated in 1970 by Hossein Mahdavy, who used Iran as a case study. A rentier state is one that mainly sustains itself with revenues generated by renting its national resources such as natural wealth and geographical location to external clients (Mahdavy, 1970).

Libya, Algeria, Arab Gulf countries, and Yemen are examples of rentier states as they rely heavily on selling their natural resources to other countries. Another example is Egypt, which receives fees for passage of ships through the Suez Canal and gets annual military aid from the United

States as part of the peace deal with Israel. With funds flowing from outside, it is possible for those regimes to remain in power and afford paying to keep the public satisfied and politically detached.

In relation to petro states in particular, authoritarianism and oil revenues do appear to have a positive correlation that is more salient in Arab countries. Michael Ross illustrates this clearly by noting that resource wealth may provide governments with funds needed to repress the opposition through internal security, which eventually leads to lower levels of democratic participation (Ross, 2001, p. 335). This suggests a two-sided advantage for authoritarian regimes with oil resources used for repressing the opposition internally on the one hand and with external acceptance from oil-importing countries on the other. The external acceptance aspect is evident in the support of global powers such as the United States and the EU of authoritarian regimes through a strategic decision to prefer stability over democracy in those countries (Sottilotta, 2013).

Meanwhile, Assad's Syria is an interstate recipient of aid from Iran and used to receive aid from Gulf countries in the past. It resembles a distinct case of an authoritarian Arab regime that survived major challenges to its authority through international sanctions and other forms of pressure (Beblawi, 1987, pp. 87–88).

Syria did not have much oil, had no peace treaty with Israel, and did not receive significant amounts of international aid. However, as a populist authoritarian regime, it leveraged a position that confronted Western penetration and the threat of Israel and played the nationalist card while shrinking the income divide between landlords and peasants in a socially more inclusive setting. Furthermore, its heavy-handed approach in dealing with opposition using secret intelligence services (mukhabarat) and other forms of repression helped deter any elements that could pose a threat to the regime or its legitimacy (Hinnebusch, 2006, p. 381).

The cultural aspects

Another issue often raised about Arab authoritarianism is whether culture is seen as a factor in preserving the status quo. Several studies have tried to answer this question with no clear consensus.

As a religion, studies have found that Islam, which has a dominant influence on Arab culture (Obeidat, Shannak, Masa'deh, & Al-Jarrah, 2012), is not incompatible with democracy, and, hence, it is not the reason why Arab countries have remained authoritarian. In fact, there are several Muslim countries such as Bangladesh, Pakistan, Turkey, and Malaysia

that have transformed their systems to electoral democracies (Stepan & Robertson, 2003; Frantz, 2012).

Raymond Hinnebusch contends that the interpretation of Islamic teaching as well as practice and conservative levels vary too widely by region and time, and he argues that the claim that Islam is an obstacle to democratization presents an "essentialist" view that can be compared to assuming that Catholicism was a hindrance to democracy in the past (Hinnebusch, 2006, p. 375).

However, the interpretation of strict Islam can accept authoritarian rule provided that shari'a law is not violated. Shari'a itself remains flexible and is possible to adjust in certain areas. Islam's renowned practice of shura is a form of consultation that resembles an opportunity to extract ideas from the public and feed into the system to amend regulations that do not contradict certain basic Islamic laws, which are clearly identified in the Quran. Shura allows some sort of democratic public participation, making the practice of democratic principles in Islam possible (Al-Hibri, 1992).

Hinnebusch argues that Islam can tolerate a populist form of authoritarianism, but with the leader held accountable and de-legitimatized widely when failing to live up to Islamic standards (Hinnebusch, 2006, p. 376).

On the other hand, another cultural aspect that Hinnebusch considers important is "traditional small group loyalties" that are usually based on kinship, tribalism, or nomadic traditions. These relate to the patriarchal family values found in various cultures around the world. Hinnebusch argued that with those two components of culture taken into account, it would appear that the cultural factor cannot be an independent variable in identifying authoritarianism, but, rather, an intervening variable that can have a partial effect under certain conditions based on the context in question (pp. 376–377).

In several Arab countries, voters could be swayed to vote for a candidate based on his sect (in Iraq or Bahrain) or his tribal affiliation (in Yemen or Kuwait) without much regard to the candidate's merits and qualities. This is where culture has a substantial but relative impact on democracy in the Arab region.

Censorship as an act of social control

From what has been presented so far, one can conclude that authoritarian regimes strive to remain in power for the longest period possible by keeping the public content with the status quo, unorganized, and depoliticized, and by suppressing any potential threat from within its own ranks or from

the opposition. To achieve this, a number of tactics are used, including control of information, which is directly connected to censorship of the media and, consequently, censorship of the Internet. I argue that it may well be possible to consider social control as an aim by the regime to remain in power. Social control theory, which is widely used in criminology studies but has found its way into other disciplines, contends that social systems force individuals to abide by certain social norms through the use of established systems in a way that helps "promote conformity to an established order or a pattern of behaviour" (McQuail, 1987, p. 469). Studying the tendencies of power to penalize dissent or resistance, Foucault stressed the disciplinary nature that modern social control entails (Foucault, 1977). And as social control reinforces authority despite resistance (Grimes, 1978), it could also explain motives behind censorship of theatrical opera plays in the 19th century (Giger, 1999) and movies (Randall, 1968) and the press (Abu-Laban, 1966; Curran, 1978) in the 20th century, and could therefore, also explain the motives behind Internet censorship in the 21st century.

Joel Migdal identified three indicators that can help assess how strong social control is in a particular society. The first is compliance, which resembles how the population conforms to the state's demands. In the case of Internet censorship, I argue that governments try to enforce compliance when making it difficult for people to circumvent censorship of online content they do not agree with. Second, social control can be measured based on the level of participation of others in the society to enforce the state mandate. With Internet censorship, one can conclude that if private sector companies enforce directives and encourage their consumers to avoid using circumvention tools, the state's social control level increases. Finally, legitimacy in the form of accepting the state's rules of the game as a true right is another factor that promotes social control (Migdal, 2001).

In authoritarian states, this would mean that the majority of the population would approve the state's acts of Internet censorship. For example, a study conducted in China showed that the majority of surveyed respondents agreed with restricting access to some online content, citing the government's obligation to defend national unity and sovereignty, and protect the Chinese society from immorality, superstition, violence, pornography, gambling, terrorism, privacy violations, and incompatible cultures or traditions that could emerge from the Internet (Fallows, 2008).

Taking government-imposed Internet censorship of dissident political content as an example, it would be apparent that a desire to achieve con-

formity through social control could prompt—among other things—the issuing of directives to companies providing Internet access to stop the content from being viewed as well as orders or requests to website-hosting companies. The argument here is that through the practice of formal social control, the authority in power will use whatever it has at its disposal to stop information it deems inappropriate from reaching the public domain so as to prevent the deviation from well-established social, cultural and political conformity.

It is important to understand that social control is closely connected to and formed by the particular context in which it is practiced. Jürgen Habermas singled out culture and religion as the two main aspects on which social control could be anchored (Habermas, 1984, p. 159). And so, it would be reasonable for a regime to base its justifications for Internet censorship on religious and cultural grounds as with the case, for example, of pornography and blasphemous content in a traditional conservative society. In other words, states could give the impression that by censoring certain content, they are protecting society from "harm" that may be brought to the country in the form of dangerous online content. What this leads to is an understanding that the particular culture and religion as well as the sociopolitical dynamics in a particular country or region are crucial to understand when trying to interpret the motives behind the blocking of a particular website. The rationale of protecting citizens from terrorism and providing for better security through the use of technology are also means of increasing social control by the state (Eijkman, 2012). Through social control, authoritarian regimes can effectively mobilize the public and monopolize forceful instruments to ensure that certain political or social groups remain in power.

It is important however to note that while authoritarian regimes are more open and straightforward in practicing censorship, Western governments' censorship acts are less obvious, and as noted by Evgeny Morozoy, they act hypocritically when criticizing authoritarian regimes such as Iran and China for tracking and repressing online activists while their law enforcement professionals proceed to "troll" social networking websites (Morozov, 2011, p. 220).

The hypocrisy of the US government is a manifestation of parapolitics[49], which can be described as the conscious planning and execution of actions by elements that later conceal and deny their involvement or responsibility (Scott, 1996, p. 6). An example of parapolitics was stated by Eric Wilson, who described from a dual state theoretical perspective the US War on Terror, which led to the death of civilians and grave abuses of human rights, as merely "a sum total of a series of decisions made by clandestine agencies concerning the identity and presence of the Enemy" (Wilson, 2012, p. 27). It is hence possible to understand why acts that violate free speech, for example, online surveillance, are committed by the United States and other democratic governments while, simultaneously, the very same countries publicly support and advocate for human rights. It also becomes apparent that no state, whether democratic or authoritarian, is immune from practicing some form of control that hampers freedom of speech.

The next section will delve deep into the subject of Internet censorship but will start with a theoretical overview explaining the concept of censorship at large and will thereafter be followed by a close-up look into Internet censorship in particular.

Censorship

Censorship is an ancient practice dating back at least to ancient Greece as illustrated in the case of Socrates and remains active to this very day. Free speech and censorship are two opposite concepts with the former calling for the ability to speak and communicate freely and the latter preventing that very act. In his book Anatomy of Censorship, Harry White referred to censorship as "suppression of certain material" but this definition fell short of including acts of expression. White also pointed to a dilemma in understanding the objectionable material that is being suppressed, because what may be objectionable content at one time, in one country or culture may be perfectly acceptable in another (White, 1997, p. xiii). This dilemma is similar to the one faces when judging if freedom of speech should be legitimately restricted to prevent harm. On the individual level, people practice censorship regularly through self-censorship, which could be quite

[49] While the subject of parapolitics is rather complex and goes beyond the scope of this study, it was used here to point to the need to be skeptical of calls for democratization and free speech by the United States given the history of double standards and hypocrisy demonstrated in the past. See (Wilson, 2012) for more insight.

useful in preventing animosity and conflict in society, particularly in cases when there are frictions, misunderstandings, racism, etc.

Joey Senat used a definition of censorship obtained from *Funk & Wagnalls New World Encyclopedia*, which is more elaborate and comprehensive than that of White:

> Supervision and control of the information and ideas that are circulated among the people within a society. In modern times, censorship refers to the examination of books, periodicals, plays, films, television, and radio programs, news reports, and other communication media for the purpose of altering or suppressing parts thought to be objectionable or offensive. (Senat, 2011)

One way of defining censorship could be in relation to its impact on free speech. Basically, censorship can be described as "the act of restricting free speech." And that implies it would impact all sorts of expressions including oral speech, art, print, and broadcast media, films, theatrical plays, photography, and Internet. From this point, focus will be exclusively on Internet censorship, which is at the core of this study.

Defining Internet censorship

Internet censorship can be understood as one form of censorship that is practiced on the Internet. According to Ronald Deibert, Internet censorship could be understood within the general act of censorship, which is the practice of "suppressing, limiting, or deleting objectionable or any other kind of speech" (Deibert R. J., 2003). In order to avoid the use of the ambiguous "objectionable" term and with the help of the aforementioned definitions of censorship, I formulated the following definition that will be meant as a basis throughout the study:

> Internet censorship is any act or system that suppresses, limits access to, or deletes any other kind of information published or communicated on the Internet.

This is still a broad definition of the concept but is perhaps more comprehensive than classical definitions such as the one by Julie Hersberger, who defined the term "Internet censorship" in the Internet Encyclopedia[50] as "an attempt by anyone to limit access to text or visual media" (Hersberger J. A., 2004, p. 264).

[50] The Internet Encyclopedia is of 3 volumes and is published by John Wiley & Sons.

In order to better understand Internet censorship, it is useful to conceptualize the Internet itself. Henry Perritt Jr. defined the Internet in physical terms as "a worldwide system of interconnected computers and computer networks that use the TCP/IP protocol suite" (Perrit Jr., 1995). Meanwhile, Cannon explicitly indicates that the Internet is not a medium of communication per se, but is a distributed network with interactive capabilities that could also serve as a collection of media with content generated and used by people for very different reasons (Cannon, 2001, p. 32). Scholars in media studies have grappled with Internet-related issues and this is rather expected because the Internet is indeed, "a different animal from other media" due to its decentralized network structure (Croteau, 2006, p. 341).

The decentralized network architecture of the Internet gave it its own unique status, which was notably recognized by Manuel Castells when he gave the title "Opening: The Network Is the Message" to the preface of his Internet galaxy book (Castells, 2002, p. 1).[51] His use of the "Internet galaxy" is meant to resemble the distributed yet interconnected nature of the Internet, which resembles in a way how stars, planets, and other cosmic objects interconnect in a galaxy[52] (p. 294). Furthermore, as a network of distributed nodes, it is quite difficult—if not impossible—to control or govern the Internet centrally (Goldsmith & Wu, 2006).

Mechanisms of Internet censorship

For Internet censorship to happen, there are certain mechanisms that take place. Hersberger (2004) presented several mechanisms of Internet censorship, including the use of filtering software, which can block websites from access by Internet users on a certain level. Filtering can take place on the computer level or on an intranet[53] level through network administrators

[51] In doing so, Castells was mimicking Marshall McLuhan's popular phrase "The medium is the message". McLuhan attempted to show that the form of medium can affect the way the media is understood by audiences by embedding itself in the message . Castells received the baton from McLuhan to take the next evolutionary step in this process of how awareness is formed in a changing society.

[52] The graph on the cover of Castells' book was a map illustrating the topography of the Internet based on trace routes in early 2000. The graph was produced by William Cheswick and Hal Burch of the Bell Labs at the time (Castells, 2002, p. 294).

[53] An intranet is a group of computers linked together in a network that could operate using TCP/IP but without having to be connected to the Internet.

and ISPs, in which case only the portion of users who connect to the Internet through those layers will not be able to view the content (Hersberger J., 2004, p. 266). If the state monopolizes all ISPs or regulates private ISPs, then censorship would be possible to implement on a national level. Apart from filtering, Hersberger indicated that legal obstacles in the form of laws that prohibit publishing or accessing certain content are another form of censorship. In the United States, the CDA was given as an example of an unsuccessful attempt that was made to censor pornographic content through the use of legislation (ibid.). There were also several reported cases of censorship inside the United States, prompting research to shed light on means of protecting free speech in the United States using the First Amendment (Nunziato, 2010).

Bennett, Grothoff, Horozov, and Lindgren (2003) noted that Internet censorship is a weapon used to suppress the dissemination of information and to stifle dissent and could be done through a number of ways including filtering and attacks on websites as well as through the harassment of those who publish information online (Bennett et al., 2003, p. 1). Mechanisms of Internet censorship in the Middle East included filtering, legal restrictions, threats, intimidation, and surveillance (Zarwan, 2005).

The most complete theoretical foundation illustrating Internet censorship mechanisms was found to be the one by Murdoch and Anderson, who describe in detail nine methods used in Internet censorship, which range from technical filtering to domain deregistration and attacks on websites and from surveillance to nontechnical censorship methods (Murdoch & Anderson, 2008, p. 65).

Internet censorship methods, as described by Murdoch and Anderson (2008, pp. 59–65) are as follows:

- **Technical filtering:** There are two methods to prevent access through technical filtering. One is called TCP/IP header filtering, which looks into the address of the website the user wants to access and any queries (keyword searches, etc.) that could be viewable on the URL. If the destination is found to be on a blacklist, the connection is dropped or redirected to a page indicating that access to the destination is denied. Such a measure may result in over-blocking because multiple websites could be hosted on the same server, and if one website on that server is blocked, occasionally, the whole server and all the websites on it would end up being censored as well. The second type of technical filtering is

called TCP/IP content filtering, which goes beyond just looking at the address but checks the actual contents of the page through a mechanism called deep-packet inspection. Through this approach, even if a website's address is not on a blacklist, if it contains keywords that are on a blacklist, the whole website may then be blocked. This method is rather complex and resource hungry and could slow traffic considerably.

- **DNS tampering/hijacking:** Through this method, a request to a particular website would be diverted or fail because the ISP tampers with how the DNS is accessed, and, instead of providing the correct IP address, the ISP may give a false IP address or even drop the connection altogether.
- **HTTP proxy filtering:** In some cases, users are forced to use HTTP proxy servers that are assigned for accessing the Internet. Those proxies may be the only way to reach the Internet and, hence, they can monitor all traffic that goes through them. Such a method is more powerful than TCP/IP header and DNS filtering but usually slows down traffic transfer rates.
- **Hybrid TCP/IP and HTTP proxy:** Because using HTTP proxy filtering is often demanding, a solution was devised to only use HTTP proxy filtering for a list of IP addresses that belong to a blacklist. If any of those IP addresses is accessed, traffic gets redirected to a transparent HTTP proxy, which inspects the transferred stream and filters any banned content.
- **Distributed denial-of-service (DDoS):** In addition to conventional filtering mechanisms, DDoS attacks can cause a server to stop responding by launching an excessive number of simultaneous requests often from many computers often in different countries to that particular server and, hence, overwhelming it with too much traffic, which causes the server and its connection to stall.
- **Server takedown:** Through legal, extralegal, or pressure methods, a company hosting a specific server could take it down and disconnect it from the Internet. The owner of the server, however, may be able to transfer the server's contents—provided that a backup copy existed—to another hosting company within hours.

- **Surveillance:** Constant technical monitoring through logging transfers between the host and the Internet user is another form of Internet censorship. Theoretically, a particular ISP or government could spy on unsecure connections and if they find banned content in the transferred stream, they could take actions, whether legal or extrajudicial, against the user, the host, or both. Such acts trigger a sense of fear, causing that may cause the host to refrain from publishing and the user to hesitate from accessing content. This creates an unhealthy environment of self-censorship.
- **Social techniques:** Apart from technical methods ranging from filtering to surveillance, social methods were also applied. Among them was the requirement to show a photo ID before using public computers at libraries or Internet cafes. Social or religious norms that force Internet users to avoid opening particular content is one form of nontechnical censorship.

Internet filtering was found by Zittrain and Palfrey to be the most common technical means of censorship and can be defined as the "technical blockage of the free flow of information across the Internet" (Zittrain & Palfrey, 2008b, p. 2). But they also complemented the work of Murdoch and Anderson by describing in greater detail the legal and social measures used in Internet censorship. One of such measures they identified was self-censorship online, which, apart from referring to the content producer's own constraint so as to only publish what he/she deems appropriate, is also practiced widely by online discussion forum moderators, who often remove contributions that could lead to the blocking of their own websites. This also applies to news and other websites that have the capability of accepting comments from registered readers or the public (ibid.).

What can be concluded from the described mechanisms is that Internet censorship is practiced through combinations of methods that are not just technical. The area is rather wide and requires continuity as more and new methods of Internet censorship could emerge. Surveillance as a factor that deters users from publishing "objectionable" content is in itself a means of censorship that has received greater attention recently and could directly result in increasing the level of self-censorship, as users would no longer feel safe in expressing their views, fearing that they may be constantly watched. Surveillance has received great attention recently due to NSA's PRISM mass spying program revealed by Edward Snowden (Anton, 2013).

Self-censorship itself has negative considerable impacts on free speech, particularly in preventing the free flow of creative ideas (Williams, 2002).

In the next section, a taxonomy of online censored content is conveyed so as to complete the picture and get the answer to the what question on Internet censorship now that the how and why questions were answered.

Taxonomy of Censored Content

Just as it was important to discuss limits to free speech in general, it is useful to project those limits to cyberspace and see if Internet censorship could at all be justified for the particular content it targets. Given that the Milliam principle by Thomas Scanlon (1972) was developed for a time when citizens were mainly viewed as consumers of information, it would prove rather difficult to use that principle for the Internet without making certain necessary assumptions about the impact that specific "harmful" online content could have in a particular context. But because the Internet is globally accessible, there can be various readings from different parts of the world of what ought to be censored. A more pragmatic approach perhaps is to examine specific cases of censorship and see if their censorship could be justified with the Milliam principle in the given context. Furthermore, just as it is important to understand what content is being censored, it is also useful to understand what factors make circumventing such censorship tolerable. Those two aspects are taken next.

Censored websites

In this section, I establish a theoretical basis on which any blocked website could be categorized based on a taxonomy that, according to Leberknight et al., needs to take into consideration the goal of the censored websites and not merely its content. For example, if the goal of a website is to allow users to publish their own digital content, then it is this very service that needs to be on the top layer of the taxonomy (Leberknight, et al., 2010, p. 4). Hence, I opted to use the website taxonomy developed by Srivastava and Chawla, who have approached the challenge of classifying a website based on a multifaceted approach that takes into account the service a website renders, the general content it provides, and the technology it uses. For the service facet in this taxonomy, Srivastava and Chawla identified four types of services offered by websites: commercial, informational, community based, and interactive. Those service categories are described in more detail as follows:

- **Commercial**: Those are websites that utilize e-commerce interfaces to receive payment information for shopping, banking, and other services.
- **Information:** Those are websites that provide information regardless of the format as it can be multimedia or/and textual. Information can be obtained automatically upon visiting the website and its sections or could be retrieved through queries such as the case with search engines.
- **Community**: Those are websites that provide platforms that allow the creation of communities through socializing, discussions, blogging, networking, sharing, and exchanging videos and other multimedia content, etc.
- **Interactive**: Those are websites that provide services requiring interaction on behalf of the users such as gaming, video conferencing, proxy services, etc.

Website classification based on *content*, however, was divided into two main groups: static and dynamic. As the name suggests, static websites are those that include content that is merely read-only text and images and constitute the minority of today's active websites. Meanwhile, dynamic content websites constitute the majority of the Web as of 2012 as they provide seamless and better communication capabilities between Web users and the website (Jiang, Yan, & Ye, 2012). According to Srivastava and Chawla's taxonomy, dynamic websites are further split into three types, namely, server-managed, user-driven, and query-based.

The categories for content are described in detail as follows:

- **Static:** Those are websites that have a standard format with multimedia and textual content that does not allow interaction and has no dynamic content.[54]
- **Dynamic:** Those websites are further split into three categories:
- **Server-managed:** Those are websites that have a mandate to provide information or services that do not require user response. Those could be in the form of news, entertainment, education,

[54] Dynamic websites require some scripting functions using PHP, Perl, etc. and often require database connectivity. The widespread use of content management systems contributed to the rise in number of dynamic websites.

entertainment, health advice, announcements, etc. They may include interactive functionality in the form of comments by users, polls, etc., but to a limited degree because the primary content is provided by the website managers. Within this category, there will need to be another categorization that is more specific and indicates a genre or topic focus. For example, cnn.com is in this category as it is managed centrally; however, it will need to be assigned one additional category, which could be "news."

- **User-generated:** Those are websites that rely mainly on user-generated content. They include websites meant for social or interactive nature such as social networking, bulletin boards, media-sharing, bookmark sharing, etc. In essence, they rely on users to provide almost all the content as the owners, while managers of the website, are mainly meant to maintain the website. Examples of this category are facebook.com, twitter.com, and youtube.com. Then within each of those categories or platforms, there should also be further categorization. For example, a discussion forum about human rights is user-generated website but could also be placed in the "human rights" category.

- **Query-based:** Those are websites that are predominantly technical or service providing in nature. They can range from communication websites that allow the downloading of software to call online (e.g., skype.com), proxy websites that allow users to bypass censorship (e.g., torproject.org), or e-mail (e.g., gmail.com), to translation (e.g., translate.google.com) or search engines (e.g., yahoo.com). In essence, these websites would have a particular service or technical feature to offer. A proxy website such as guardster.com has a main category of "query-based" and its second-level category of "proxy."

With technology, Srivastava and Chawla refer to one of three technologies: Web 1.0, Web 2.0, and Web 3.0 (Srivastava & Chawla, 2010, p. 481). Web 1.0 is the basic read-only static HTML content that used to be the only option available until the second technology known as Web 2.0 emerged. Web 2.0 is a word coined by Tim O'Reilly to mean websites with functionality that allows users to interact and upload and publish content and perform dynamic queries (O'Reilly, 2009). The third technol-

ogy is known as Web 3.0 and is often called the Semantic Web, which is still in its infancy and is strongly advocated by the creator of the World Wide Web, Tim Berners-Lee, and others as a means of allowing computers to be actively involved in providing suggestions and making decisions instead of merely being passive components that receive and carry out instructions (Berners-Lee, Hendler, & Lassila, 2001).

However, only content and service facets are considered in this study because the technology facet is too technical and is beyond its scope.

So each website would have a service type and a content type assigned. For example, facebook.com's service type would naturally be community, while its content type would be "user-generated." Additionally, its second-level categorization would be "social media." Similarly, google.com's type would be information while its content type will be query-based and its second-level categorization is "search engine." The second-level content category is assigned based on the taxonomy devised by Faris and Villeneuve (2008), who created categories that include search engines, dating, news, proxy tools, etc. The full details of what categories were used are described in details in the Methodology Chapter.

The Role of Technology

As Internet censorship has become a hindrance to free speech, technological solutions trying to defeat it have emerged. The argument here is that while technology could be abused through the practice of censorship to silence dissent for example, technology could also be utilized to combat such practices. The debate on the use of technology dates back several millennia from the era when the wheel was invented. While technology evolved based on need, the debate on whether it is good or bad for society continues.

As the subject of this dissertation revolves around the Internet, it is useful to refer to the debate that Adam Thierer articulated between the two opposite camps of "Internet optimists" and "Internet pessimists" (Thierer, 2010). The Internet optimists group includes scholars such as Nicholas Negroponte (1996), James Surowiecki (2005), and Clay Shirky (2011), who see the Internet in positive light as an open arena for freedom of expression, innovation, liberation, participation, anonymous communication, and empowerment. On the other hand, Internet pessimists such as Neil Postman (1993) and Andrew Keen (2007) view the Internet in negative light as a tool of frequent misuse and abuse with its anonymizing potential serving to debase culture and lead to the lack of accountability.

This study avoids delving in the heated debate revolving around whether Internet is good or bad for society due to time and space constraints. Instead, it focuses on the practice of Internet censorship in authoritarian Arab states and how technology, specifically through censorship circumvention tools, is capable of overcoming it and consequently, promotes freedom of expression.

Can technology be liberating?

One of the techno-optimist views about the use of technology in the age of the Internet was presented by Stanford University Professor Larry Diamond, who coined the term "liberation technology" to mean "any form of information and communication technology (ICT) that can expand political, social, and economic freedom" (Diamond, 2012b, p. 4). In describing why such ICTs ought to be considered liberating, Diamond indicated that it is "because of their demonstrated potential to empower citizens to confront, contain, and hold accountable authoritarian regimes—and even to liberate societies from autocracy" (Diamond, 2012a, p. xi).

A body of literature has emerged in recent years around the use of liberation technology to expand freedom in China (MacKinnon, 2012; Qiang, 2012), the Arab world (Al-Saqaf, 2012), Iran (Yahyanejad & Gheytanchi, 2012), and beyond (Meier, 2012). However, just as there are voices reflecting on the positive liberation aspects of technology, there are certainly voices that highlight the dark side of the very same technology when used for repressive practices (Deibert, 2010; Morozov, 2012), which will be referred to in this chapter.

As a term, "liberation technology" remains hotly contested, with critics saying that it suggests a biased opinion that it is intrinsically "liberating" (Diamond, 2012a, p. xi). So, in order to validate this theory, empirical evidence from various regions and in different contexts was gathered and reflected upon by Diamond, who showcased examples from different regions of the world where liberating technology may have actually lived up to its promise.[55] The debate surrounding the use of technology for liberation was found to be of relevance for this dissertation, particularly as the technology to counter Internet censorship was referred to by Diamond himself as an example of how liberation technology could advance free

[55] In the book "Liberation Technology" edited by Larry Diamond and Marc F. Plattner, there are a number of articles that help describe some uses of liberation technology in several authoritarian countries. See (Diamond, 2012a).

speech while acknowledging the ongoing struggle between two opposing powers: a force trying to extend and refine Internet censorship and another seeking ways to circumvent it (Diamond, 2012a, p. xiii).

Liberation technology has several characteristics that could promote democracy and free speech and are summarized in the following five main points based directly on the work of Diamond (2012b, pp. 4-12):

Empowering citizens:

> enables citizens to report news, expose wrongdoings, express opinions, mobilize protests, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom. (p. 4)

Widening public participation:

> may help to widen the public sphere, creating a more pluralistic and autonomous arena of news, commentary, and information. (p. 5)

Strengthening dissent:

> With the aid of liberation technology, dissident intellectuals have gone from being a loose assortment of individuals with no specific goal or program to forming a vibrant and increasingly visible collaboration force. (p. 9)

Enhancing transparency:

> is also "accountable technology," in that it provides efficient and powerful tools for transparency and monitoring. (p. 10)

Rallying the masses:

> has been instrumental in virtually all of the instances where people have turned out en masse for democracy or political reform. (p. 12)

It is worth noting that Diamond also saw the liberating aspect of ICTs on the economic front through its facilitation of new opportunities to expand markets and improve efficiency that directly benefit the poor[56] (Diamond, 2012a, p. xii). This cyber optimist view is shared by Clay Shirky, who argues that in order to promote political change in undemocratic states, democratic countries such as the United States should promote the use of the Internet and, in particular, social media due to their promise of bringing economic growth so as to serve as an incentive to authoritarian governments (Shirky, 2011, p. 37).

[56] Diamond briefly touched upon ICT4D, where "4D" means for development.

In the political realm, examples that fall into the category of liberation technology are plentiful and range from mobile devices used to document police brutality against peaceful protests to popular social media used to disseminate such information to a large audience (Howard & Hussain, 2012). Examples of liberation technology include traffic encryption tools, which could protect citizens from surveillance and data theft. Social media and blogs could be effective in advocating for human rights and exposing government oppression. Anonymizing tools could help protect the identity of dissidents when they connect to the Internet or publish sensitive data, and so as to protect them from being identified and their character assassinated through smear media campaigns. Such tools would also reduce self-censorship that those activists practice out of the fear of being pursued. Cases of violations committed during mass rallies could be reported and made public through effective mapping tools such as Ushahidi, which was used to report human rights violations (Meier, 2012). Anti-DDoS and anti-malware solutions help protect websites and online services targeted for their dissident or sensitive content. Online petitions and campaigns could be utilized through online platforms such as Avaaz to amass support for issues of common concern such as opposing repressive cyber laws that restrict free speech in the name of security (Kavada, 2012).

Given that expanding the horizons of freedom is one of the key features of liberation technology, one particular example that Diamond referred to in respect to expanding free speech is censorship circumvention, which allows Internet users to break digital firewalls often assembled by authoritarian regimes to prevent access to particular dissident and politically sensitive online content (Al-Saqaf, 2012). The next section will zoom into that particular technology so as to provide an important theoretical foundation for the study.

Censorship Circumvention

Censorship circumvention tools and solutions aim at technically combating Internet censorship by providing users with the power to bypass digital firewalls and access censored websites and content. This makes censorship circumvention at the heart of the definition of what liberation technology is. To understand why censorship circumvention works, it is of value to invoke the early days of the Internet when it was born in 1969 at the US Advanced Research Projects Agency Network (ARPANET) project, which was meant to create a network that cannot be controlled centrally and could withstand major failures or attacks. The architecture and standards

of the Internet were developed by engineers and researchers so as to be fully decentralized to allow researchers to communicate over long distances seamlessly while maintaining a structure robust enough to withstand losses of significant parts of the underlying networks (Brand, 2001).

With the expansion of this Internet outside the United States through standard telecommunication infrastructure used for other forms of communication, it was possible to grow this decentralization globally. The network withstood the test of time and remained true to its original creators by preventing control or obstruction by any particular government or entity. The global usage of the Internet has reached levels that make it indispensable in many countries around the world not only for communication, but also for banking, government, transportation, and various other vital public and private uses (Hoffman, Novak, & Venkatesh, 2004; Varnelis, 2012).

Given the vast size of the Internet, it was useful to device means of storing data at various nodes in the network. And this led to the development of proxies as a concept that emerged well before the launch of the World Wide Web, as it had to do with how bandwidth use is minimized by storing duplicates of the same content on different locations for faster access (Grennan, 2000). The use of proxies is analogous to having to rely on a intermediary agent when exchanging information. When the recipient and the sender of information cannot interact directly, each can interact with a middleman who is not forbidden from communicating with them both individually. Once the middleman becomes forbidden from interaction with either, for example, because the proxy is no longer accessible, there is often an alternative proxy, making total blocking of websites very difficult.[57] For example, for a person in Beijing to access http://facebook.com, which is known to be blocked in China, a circumvention tool could be used to reroute the request to that website via a proxy server based in the United States, for example, and return the data in an encrypted form back to the user. Virtually all circumvention tools use the same method of utilizing proxy servers (Palfrey & Zuckerman, 2011, p. 5), some of which may be predetermined and hard-coded in the circumvention tool, while in other cases they could be fetched dynamically and change to avoid being blocked.

[57] There are increasingly sophisticated ways that can detect whether the user is trying to access a proxy, which makes the list of blocked proxy servers constantly changing.

Although the basic principle of how circumvention tools work is the same, there are several differences in how they operate. Roberts, Zuckerman, and Palfrey of the Berkman Center for Internet and Society identified four groups of circumvention solutions: simple Web proxies, VPN services, HTTP/SOCKS proxies, and "custom" tools (p. 6). While the first three methods are easy to deactivate because they depend on a particular server address, the "custom" tools involve more sophisticated mechanisms, which make them stronger and less prone to being stopped by the government. That is why, in terms of flexibility and blocking-resistance, the fourth group of circumvention solutions, that is, custom tools, is preferred.[58] Each of those groups differs significantly from one another, and each individual tool available today may have its own particularities, pros, and cons.[59] The effectiveness and reliability of various tools vary widely (p. 5), and it is evident from research that governments are keen on studying how censorship circumvention tools work and find ways to deactivate them by disabling access to the proxy servers they rely on and try other tactics to shut access to them, resulting in a steady cat-and-mouse chase like the one witnessed in China (LaFraniere & Barboza, 2011).

It is important to note, however, that despite having the possibility to access such liberation technology, not all users suffering from Internet filtering end up using circumvention tools. Estimates by another Berkman Center study in 2011 indicated that, at best, 3% of all Internet users in countries that practice filtering end up using circumvention techniques, and there is no clear theory explaining the reasons behind this low figure; the study suggests that it is "unrealistic" to expect that those tools would be used by a broad audience due the preference of many users for local content and also due to the poor performance or/and usability of several tools (Roberts, Zuckerman, Faris, York, & Palfrey, 2011, p. 9). Furthermore, Internet filtering could be a means to make accessing the Internet freely more difficult for those without enough motivation or skill to seek a possible way to circumvent censorship, because for a country like China, for example, it may be enough for the government if the majority of the

[58] As described in the methods chapter, Alkasir censorship circumvention solution developed for this study belongs to the "custom" group. You can find details about how it works in the annexed technical report in Appendix A.

[59] The detailed analysis of the particularities, pros and cons of each goes well beyond the scope of this study.

350 million users[60] are discouraged from visiting certain foreign websites when they find that the alternative domestic sites are readily accessible (Chen & Wang, 2010, p. 97). The challenge for circumvention remains difficult, because, as Diamond indicated, there is a "war" between dictators trying to censor and democrats trying to circumvent (Diamond, 2012a, p. xiii), which manifests a grave mismatch in power and resources. Furthermore, circumvention tools require the Internet to be accessible, yet, in times of crisis, some governments could end up killing Internet access altogether, as demonstrated in Myanmar in 2005 (Subramanian, 2012, p. 7) and in Egypt in 2011. Furthermore, a 2010 legislation was proposed in the US senate to give the US President sweeping powers—dubbed the kill switch bill—that would allow him to interfere in the telecommunication operations of the country including those handled by the private sector (Bradbury, 2011, p. 7). Such a development indicates that the threat of having disruptions to the Internet is not limited to authoritarian states.

While noting the importance of circumvention tools for the advancement of free speech in authoritarian countries, authors of the Berkman Center study suggested some steps to limit the impact of Internet control, three of which aim at improving the accessibility and impact of censorship circumvention tools. Those include, first, the focus on specific tools and methods for activists by providing them a pool of resources and local networks to find the most optimal tools to overcome censorship. Second, there should be more support to the minds and projects behind circumvention tools by pulling resources, getting support from other large corporations such as Google and Microsoft, and allocating more funds. Third, there is need for steady and regular monitoring of censorship practices including filtering so as to improve the understanding of what is being blocked and find effective ways to address such practices. Among the most notable recommendations of the study is the introduction of complementary nontechnical approaches to support online free speech in countries suffering from filtering, because technical means alone may not only be insufficient, but could backfire if governments invest resources to aggressively counter every new method of circumvention and potentially use legislation and other forms of pressure (Roberts, Zuckerman, Faris, York, & Palfrey, 2011, pp. 8–10).

While censorship circumvention could indeed be a useful liberating technology, it is also important to understand that the same circumvention

[60] This is an old statistic as used from the 2010 as taken from the cited source.

tools could be used for unlawful activities. For example, there were cases when Tor, which is one of the world's most popular anonymizing and circumventing tools, was used by cybercriminals to launch malicious DDoS attacks (Constantin, 2012). Like any other piece of technology, circumvention tools are conduits that could be used for good or evil. However, as protection is needed for privacy, intellectual property rights, children, and other vulnerable groups from dangers lurking online (Diamond, 2012a, p. xi), it is important that end users read the terms of use to be aware of the risk and understand that they are liable for using the software. This is necessary because no matter how well-intentioned the circumvention tool developers may be, they remain prone to making mistakes and misjudgments when programming, creating security holes and bugs in the process.

It is also important to recognize the right of censorship circumvention tool creators to limit the type of content that they allow to go through their servers. Circumvention tool developers aiming at helping promote free speech online ought to be allowed to restrict the abuse of their server by prohibiting access to websites known, for example, to contain malicious code.

Path Dependence Theory as a Supplementary Tool

Path dependence theory was chosen to help understand what could explain the various developments that occurred in relation to Internet censorship. In this study, it is utilized in analyzing the context and discussing empirical findings regarding online censorship measurements and activities to circumvent such restrictions.

In its broadest meaning, path dependence means that particular decisions taken at critical junctures in the past will have impact on the direction of future development (David, 1985). For social science scholars concerned with path dependence, studying history is of importance to understanding how institutions resist change to sustain the same policies for long periods of times (Pierson, 2004).

Another concept often used in relation to path dependence is "critical junctures," which are events that trigger developments along a particular path. Path dependence establishes an inertia and persistent predictable path that continues steadily until another critical juncture is faced, which changes the path once more (Pierson, 2000, p. 263).

Path dependence is used to identify the occurrence of critical junctures that were considered pivotal for the path that Arab regimes have taken in

relation to free speech and Internet censorship. Those junctures will be identified generally and particularly for Tunisia, Egypt, Yemen, and Syria, which were among the countries that witnessed revolutions and whose regimes have evidently practiced Internet censorship.

Furthermore, the period of this study coincided with the Arab Spring, which is considered a critical juncture for a number of countries where it led to significant developments. However, the particular sequence of events that resulted from this juncture varied by country, and this implies the need to study the different developments online in relation to the events unfolding on the ground, from peaceful protests to violent attacks and from elections to sectarianism. Without having an insight into those developments, it would not be possible to properly analyze the established path that led to patterns of Internet censorship during this period.

Finally, the global context is also important in terms of the growing use of ICTs not only by activists, but also by governments, businesses, and others. Recent technological advancements in mobile connectivity and greater Internet access have affected the way Arab citizens use technology and utilize social media, as will be demonstrated in the next sections. Thus, understanding those aspects in relation to each examined Arab country is of value for the analyses in this study and will hopefully allow a more accurate exploration than would otherwise be possible.

Summary and Theoretical Insights

The theoretical framework presented in this chapter was comprised of elements from four distinct areas, namely, free speech, censorship, technology, and authoritarianism.

Freedom of speech is a valuable right for the individual and society at large, and online freedom of expression should be protected and encouraged. This point resembles the normative standpoint that needs to be prominently placed in the forefront, as it resembles the strongest motivation to start the study in the first place. The right to free speech was defended against oppression and tyranny in many countries over generations to become a recognized human right.

However, the right to free speech should not be unlimited, but is guided by principles that prevent harm, which can only be evaluated with a thorough understanding of the particular circumstantial context in which speech is practiced. This normative theorem directly emerges from free speech theory. An emphasis is made here on the circumstantial context, which is what the study will have to deal with when analyzing the reasons

of why particular content was censored. The Milliam principle by Thomas Scanlon (1972) will serve as a point of departure for each particular case before going deeper into the context.

An attempt to understand how free speech could be practiced on the Internet was manifested in the theory of freedom of expression for an information society of Jack Balkin (2004). Balkin contends that the Internet made some features of free speech more salient. While this is a positive aspect, those features resulted in attempts by governments and other forces such as media conglomerates to limit it. To minimize the threat to free speech online, Balkin suggests legal and administrative measures as well as design of new technology.

While the Milliam principle helps provide a framework or some general guidelines concerning when free speech ought to be limited, this principle was largely violated by authoritarian regimes, which, as described in this chapter, practice censorship mainly to limit threats that could undermine their legitimacy or authority. Furthermore, authoritarian regimes practice social control to enforce conformity and weaken dissent. This is how motives behind censoring political and dissident content could be understood and are connected to the theory of social control. It is in those particular situations where the design of a technology, suggested by Balkin, to protect online freedom of expression comes into play.

To be able to measure censorship on the Internet, it was necessary to understand the different mechanisms of Internet censorship including Internet filtering. Furthermore, understanding how to categorize blocked websites using a clear taxonomy was important to help assess whether blocking of a particular website could be justified based on the Milliam principle.

When authoritarian regimes censor particular dissident websites and such censorship fails to meet the Milliam principle, circumvention tools can be seen as a manifestation of how technology could be liberating for the public. Dissidents can use technology to confront authoritarianism and expand participation through several means, including those that help in combating Internet censorship. The promise of liberation technology in supporting dissent as indicated by Diamond (2012a) needs to be understood within the context of authoritarian rule and motives to censor.

Censorship circumvention could be understood as a method that uses proxy servers to break national firewalls and consequently strengthen free speech. Such tools are taken as one subset of the various ICTs that constitute liberation technology. This is enforced by the suggestion of Balkin

(2004), who highlighted the need to design and deploy such tools for public use. The effectiveness and impact of censorship circumvention tools vary widely, and some tools could be abused by users and restricted by governments. A set of features or factors have been proposed to use as a means of evaluating and improving such tools. As suggested from research around censorship circumvention in particular and liberation technology in general, there can be cases when those tools are abused by users if utilized for harmful causes such as sending malware. Furthermore, those tools are sometimes blocked by governments keen on limiting their ability to bypass censorship. Yet tool creators often find ways to reactivate their tools and resume operation, resulting in a steady cat-and-mouse chase.

When linking the effectiveness of circumvention tools to expanding freedom, it is important to understand how the Internet gained importance in mobilizing a particular community to the level that makes using circumvention tools effective. In an attempt to draw this historical connection and context analysis, path dependence theory was found as a useful approach. While it was not a major component of the theoretical framework, it was found to be a pragmatic method that helped bring the context of the various cases and developments into perspective and connected them to actions taken by regimes when practicing Internet censorship and the reaction by users in circumventing that very censorship.

Chapter 4: Methodology

The methodology adopted in this study mainly uses quantitative methods to answer its research questions. The empirical data collected came through two different channels. The first is the server of Alkasir, which enabled circumvention of censored websites, and the second is the data collected from surveys filled by Alkasir users.

It must be noted that the process of designing and implementing Alkasir should be viewed as an essential part of the study's methodology. However, due to its technical nature, it was placed in Appendix A, which answers questions related to how Alkasir came to be, how it works, and how it was used to collect data. The data gathered from Alkasir's server and the surveys were statistically analyzed with IBM SPSS[61]. In this chapter, I attempt to thoroughly describe materials and data collection processes for both blocks of data and conclude with a section about the methodology's limitations.

Experimental Methods

What makes this study unique is the fact that it is an experimental type of research that involves the construction of an object of study, which is Alkasir as the circumvention software. This was required to examine how technology can be developed and used to grant users the ability to bypass website filtering and enhance democracy as well as create a platform to reach survey respondents.

It is not uncommon in social science research to create the objects of study as in the case of selecting members of focus groups and setting up the place, agenda, and guidelines of the environment where the study takes place. However, this study could be seen as an extreme case where the main tool used for the study was constructed and built from scratch and then used both as a research tool to study how it operated and was used, and to collect a group of survey respondents as another object of study.

This implies that I, as the author of the software, had a dominant and exclusive role in setting up how circumvention took place in terms of regulation, for example, in preventing blocked nude/pornographic websites from being reported; in terms of technology, for example, having the servers centrally located and based in the United States and setting up the speed and hardware specifications; and in terms of sampling by using the

[61] IBM SPSS Statistics software was used for the statistical analysis of data.

software users as survey respondents for the study. The way I have attracted users to using the software from the outset also relied on my own networks and countries of focus, starting from Yemen.[62]

Empirical Data Collection from Alkasir's Server

Parts of the first and second questions require analysis of the data taken from Alkasir's server. The data can be measured consistently and systematically to assess the usage of Internet users when electronically reporting and circumventing Internet censorship. Using this method, I carried out an experiment virtually in cyberspace using Alkasir. These data are of value to understand the behavior of Alkasir users[63] when reporting and accessing censored websites.

The results of this experiment were analyzed by first selecting a subset of Alkasir's global user base and defining a specific duration for the experiment. In the following sections, I go in-depth to explain how and why I derived the sample. I also review how the data extraction process took place and what was used to analyze these data to answer the relevant research questions.

It is important to consider here that the lack of transparency and data by Arab ministries of telecommunication in authoritarian Arab states describing what websites they block and for what reasons made gathering empirical data through Alkasir the next available option understanding the mechanisms of and motives behind Internet filtering.

Materials

By October 2012, when data were gathered and compiled for statistical analysis, Alkasir's database had over 72,000 user records. However, that number is just an estimate, because to preserve the privacy and security of users, Alkasir does not require registration or personal information from users. In other words, it is impossible to know merely from the server data the exact number of individuals that ever used the software. The number of user records can also be referred to as the number of installations,

[62] Limitations that emerge from this methodology are mentioned in the 'Limitations' section towards the end of this chapter

[63] 'user' here does not necessarily mean a particular person, but the application installation used. It might have been the case that there were multiple individuals using the software on the same computer or that the same person used two instances of the software, resulting in an inaccurate count.

which is a number assumed to positively correlate to the number of individuals users. It may well be, however, that the number of installations could be misleading when different copies of different versions are installed on the same computer. For example, if version 1.3 is concurrently used with version 1.4 on the same computer, they are counted as two separate installations, which may lead to an exaggeration of the actual number of users.[64]

As shown in Table 1, for every installation, the software saves a record that includes several fields, of which only a few were used in this study. Each record has a unique installation ID, and a field identifying the number of times that particular installation connected to the server along with the user's interface language, the country and the ISP from which the user is connecting, the operating system used to connect (Windows 7, Windows 8, Windows Vista, etc.), the browser used to access the main page of alkasir.com (such as Firefox, Internet Explorer, or Alkasir's browser), and the last time Alkasir successfully ran and connected to the proxy server.

Variable	Type	Details
User ID	Interval	A serial number is a unique key value that is incremented for every new installation of the software
Connections	Ratio	The number of successful connections (starts) since the first run
Language	Nominal	The language of the user interface of Alkasir (English or Arabic
Country	Nominal	The country where the user is based
ISP	Nominal	The ISP the user used to connect
Operating system	Nominal	The operating system the user connected from (e.g., Win 7, XP)
Browser	Nominal	The Web browser used to connect (e.g., Firefox, IE)
Last access	Ratio	A time stamp indicating when the last successful connection happened

Table 1: Main fields in the installation entry in the server's database

[64] However, this is not naturally the case because Alkasir always checks for updates and users are requested to overwrite the old version.

As for the reported URLs, every database record contains dozens of variables but only a few were indicated in this section as the full list of table variables were not needed to carry out the content analysis needed. Those used are the URL ID as a unique identifier variable, the URL itself and three variables for its taxonomy (service, content, category classifications), the time of reporting for the URL, and the number of times it was visited through Alkasir's internal browser only[65], ISP, the status –if blocked or not- and the moderator's decision. These variables are described in Table 2.

Variable	Type	Details
URL ID	Nominal	This is a unique key composed of text to identify a particular URL submitted from a specific ISP in a particular country
URL	Nominal	The URL that the user reported as blocked
Service	Nominal	The type of service the URL provides
Content	Nominal	The type of content the URL provides
Category	Nominal	The specific category that the URL belongs to (e.g., news, multimedia, social media, religion…)
Country	Nominal	The country from which the URL is reported
ISP	Nominal	The ISP the reporter used to connect
Status	Nominal	Indicates if a URL is found to be blocked or not
Moderator decision	Nominal	Indicates if the URL was approved, was rejected, or remains pending
Number of visits	Ratio	The number of times the URL was accessed using the internal browser by users connecting from the specific ISP in the particular country
Time added	Ratio	This indicates the time and date the URL was first reported

Table 2: Main fields in the URL submission entry in the server's database

[65] It would have been possible to detect the usage of the proxy through other external proxies, but doing so programmatically would have required substantial effort and could violate the privacy of the user. However, through communications with several users, there appears to have been substantial use of external browsers as well.

Sampling

Multistage cluster sampling was applied to identify the cases that will be used in this study. This sampling method was used because, unlike normal cluster sampling, multistage clustering allows one to further define a subgroup out of the original cluster (Borg, & Gall, 1996, p. 227).

It was found useful to apply this sampling method because instead of simply using a particular group of the Internet users based on whether they use Alkasir or not, we can go one further step by refining the cluster and selecting only those users who are based in countries where there is significant degree of Internet censorship. The stages used in this case are described as follows.

First cluster sampling stage

The first cluster only contains, among all the world's Internet users, those who downloaded, installed, and successfully connected Alkasir client application to the Alkasir proxy server.

As of October 2012, there were 72,732 entries representing all Alkasir successful installations in all countries, using any of the available versions. This cluster had cases from 123 different countries from around the world.

Second cluster sampling stage

The second cluster emerges when filtering out all but Arab countries. Here, the cluster was limited to those installations emerging from eighteen Arab countries,[66] which amounted to 32,210 entries from twenty Arab countries.

Third cluster sampling stage

The third and final cluster would prove to be the most critical, because it is assumed that this final chosen cluster would share the common characteristic of being individuals seeking to access filtered online content. If the sample were random, it would have brought countries where Internet censorship is insignificant. As indicated in the chapter detailing previous research, there are disparities in terms of level and intensity of censorship among Arab countries.

Hence, the challenge was to find a way to further refine the cluster to only include the countries where the number of installations, number of

[66] The Arab world is composed of 22 Arab states, but not all of them had consistent usage of Alkasir.

blocked URLs, level of activity, and the period when this happened all need to be taken into account. The number of accesses per installation and number of visits per blocked URL should also be accounted for to arrive at a refined sample that could reflect a group of cases that not only have Internet censorship, but also actively used Alkasir to circumvent it.

To achieve this, a function to calculate Φ (phi), was created as it calculates the a factor evaluating the significance of filtering for a particular country:

$$\Phi = \frac{(\mathrm{N} * \langle S \rangle + \mathrm{U} * \langle V \rangle)}{\tau}$$

where for each country,

- N is the number of Alkasir installations;
- $\langle S \rangle$ is the average number of successful connections S to Alkasir proxy server and is calculated through dividing N by S;
- U is the number of unique reported and approved URLs;
- $\langle V \rangle$ is the average number of visits V for a blocked URL through the internal browser and is calculating through dividing V by U; and
- τ is the interval of time in days during which there was use of Alkasir.

The value of τ for a particular country is calculated by subtracting the date when Alkasir detected user activity for the first time from the date when Alkasir was accessed for the last time, after which there was no longer any activity. The earliest date possible for this calculation would be October 1, 2010, and the latest would be October 1, 2012, as they are the specified interval boundaries for the experiment.

Applying the formula on all Arab countries in the database led to the values indicated in Table 3. It was quite clear that Syria by far was the leader with a factor of 7,378, which was significantly higher than all other countries combined. The factor of the second place holder, Yemen, was 433, followed by Egypt with 379 and Tunisia with 279. All other countries had lower factors in comparison with a total of 450 units.

For the top four countries, additional analysis was carried out as they were given more weight than other countries. In total, the sample represented for the four countries would include a total of 26,264 installations that successfully connected to Alkasir's proxy over 1.14 million times, and

have reported and got approved a total of 1,260 blocked URLs, which were accessed through the internal browser about 4.7 million times during the period from the October 1, 2010, to October 1, 2012.

Country	N	τ	S	$\langle S \rangle$	U	V	$\langle V \rangle$	Φ
Syria	**22,415**	**732**	**958,548**	**43**	**812**	**4,441,849**	**5,470**	**7,378**
Yemen	**3,012**	**732**	**123,120**	**41**	**322**	**193,868**	**602**	**433**
Egypt	**432**	**35**	**11,253**	**26**	**22**	**2,028**	**92**	**379**
Tunisia	**323**	**174**	**47,962**	**148**	**104**	**658**	**6**	**279**
Saudi Arabia	3,012	509	69,710	23	240	53,124	221	241
UAE	924	732	27,170	29	193	29,319	152	77
Libya	220	519	9,929	45	32	16,093	503	50
Bahrain	406	719	10,740	26	72	6,879	96	25
Sudan	271	732	8,578	32	23	664	29	13
Jordan	161	732	5,632	35	17	2,121	125	11
Qatar	225	693	4,766	21	13	239	18	7
Kuwait	227	732	4,753	21	10	446	45	7
Oman	220	675	2,903	13	22	106	5	4
Algeria	98	707	2,658	27	4	212	53	4

Table 3: Internet censorship impact factor (Φ) in Arab states

Identifying Nationwide Filtering

It is important at this point to indicate that in order to arrive to a conclusion about the status of filtering for a particular website in a specific country, it would be necessary to have multiple reports coming from connections using different ISPs. Otherwise, there is a risk of a false positive, which means that a case of censorship would be marked but it was mainly due to filtering by one single ISP while all the others were not blocking it. This could be the case at a public library or primary school, for example, where facebook.com or youtube.com may be blocked based on the terms of use policy set by the library's administration. So if a student trying to visit facebook.com found it blocked and reported it, Alkasir will register one ISP; then, if he or someone else in the country finds that it is blocked and reports the same URL but from another location, such as an Internet

café, that will add to the reliability of the conclusion that the censorship may not be confined to a particular ISP but is nationwide.

It is not possible to ensure that Alkasir will have users using all ISPs and reporting all the websites needed because some of them may use Alkasir for short periods of times, not allowing the program to check the list to verify the status of censorship. While the ideal of having 100% confirmed results is desirable, it is certainly not technically feasible. Hence, there had to be some subjective assessment that would use relative measurements and come up with the most likely hypothesis accordingly. Therefore, a factor was created in the process of this study to help measure how common or distributed the filtering of a particular approved website is. This value is called the filtering confidence level (FCL).

FCL is calculated as follows:

$$\mathbf{FCL} = \frac{\mathrm{ISP}_f(URL) - \mathrm{ISP}_{nf}(URL)}{\mathrm{ISP}}$$

where

- **FCL** is calculated separately for every URL in each country. The higher the value, the more probable that the URL is blocked nationwide.
- $\mathbf{ISP_f}(\boldsymbol{URL})$ is a function that calculates the number of ISPs that have been found to filter, that is, prevent access to, a particular URL in a particular country.
- $\mathbf{ISP_{nf}}(\boldsymbol{URL})$ is a function that calculates the number of ISPs that have been tested and have been found not to filter the provided URL in the country in question.
- **ISP** is simply the total number of ISPs that Alkasir users connected to and used to submit reports in a specified country.

The practice of filtering is sometimes rather dynamic as ISPs could switch their filters on and off for certain periods of time or could put a particular URL or category on or take it off the blacklist for some reason, resulting in changes in the filtering status for the end user.

Alkasir has an internal built-in mechanism that allows it to automatically trigger a process to check the status of websites on all running installations. The URLs on the list are each reported by at least one Alkasir user in the said country. Additionally, there is a method to manually add more

websites for examination. But that feature was not used to allow users themselves to be the creators of the list. This way, the reliability of the data would be enhanced with more users using Alkasir in each particular country. Nationally blocked URLs would then be identified by their relatively high FCL.

Categorizing blocked URLs

Categorization of submitted URLs is a task requiring manual subjective interpretation. This is because it requires a proper understanding of the URLs' content. The categorization process was done based on the general characteristics of the main page of the website and with the use of the "about" section, if any. The time and energy that would have been required to qualitatively analyze and thereafter categorize the thousands of reported URLs made it not feasible to categorize all websites.[67]

Furthermore, the categorization process cannot automatically lead to understanding why a website may have been blocked, particularly if the website in question has multiple uses, in which case it would be virtually impossible using technical measurements alone to pinpoint the particular item or piece of content that triggered a decision by an ISP to condemn the website to be blocked. The complexity of categorizing websites and hypertext material is nothing new, with several authors discussing different approaches to this problem (Mehler, Gleim, & Dehmer, 2006; Zhang, Xie, Wang, Yue, & Ma, 2007).

The process of categorizing was rather straightforward and starts upon receiving an e-mail from Alkasir's server indicating that a particular user had reported a new URL. Thereafter, the URL is opened and examined and thereafter placed in one of the available categories, which have been mainly derived from the categories indicated by Faris and Villeneuve (2008).

But initially, each website is assigned a service type and content type based on the website taxonomy suggested by Srivastava and Chawla (2010).

Once the initial classification of the service and content types is defined, one of the following categories is assigned:

---

[67] A study covering some URLs could utilize part of the collected data and be carried out in the future by doing a qualitative in-depth analysis of each URL to understand how to best interpret the content that may have consequently led to the decision to have those URLs censored.

- News or opinion
- Dissident website (containing news, commentary, etc., from the opposition)
- Reform, legal reform, and governance
- Religious conversion, commentary, and criticism
- Militants, extremists, and separatists
- Human rights
- Foreign relations and military
- Minority rights and ethnic content
- Minority faiths
- Women rights
- Environmental issues
- Economic development
- Sensitive or controversial history, arts, and literature
- Sex education and family planning
- Public health
- Social networking, forums, and groups (Facebook, Tagged, etc.)
- Blogging domains and blogging services
- Multimedia sharing
- Peer-to-peer (P2P)
- Dating
- Free e-mail
- Voice over Internet Protocol (VOIP)
- Search/aggregating engine
- Web hosting sites and portals
- Gaming
- Anonymizers/proxies and circumvention
- Translation
- Commercial sites
- Other
- Uncategorized (not possible to categorize, for example, under construction, etc.)
- Inactive (is no longer in service)

For URLs that do not seem to fit into any particular category, the "other" category is given. And occasionally, there are websites that appear under construction or suffering from a temporary error. Those are marked

as "uncategorized." In cases when the domain has expired and no longer has the content that it used it, it is categorized as "inactive".

All the aforementioned categories are rather self-explanatory except perhaps P2P, which are websites that offer links to downloadable torrents that would allow Internet users to share content. PirateBay.se is an example of P2P websites, which are occasionally legally embattled for allegations of being used to violate intellectual copyright laws by sharing copyrighted content such as movies, games, software, and music (Bridy A., 2009).

Data Extraction for Statistical Analysis

The data sets in the tables mentioned earlier are stored in MySQL[68] databases on the data server where alkasir.com's files are also stored. To extract the required data, the server is sent a series of SQL[69] statements to fetch the relevant data rows. Once obtained, those rows are converted to data that are possible to import to IBM SPSS, which is then used to do the statistical analysis and create tables and graphs and give a concrete picture that could thereafter allow the answering of the first research question.

Designing Surveys and Data Collection

While the content analysis of data retrieved from Alkasir servers was used to answer questions in relation to the visits to blocked websites and number of reported URLs, surveys were used to answer all other questions. Surveys were useful when the aim is to learn about personal experiences, views, and beliefs of a particular population, which is, conventionally, any set of persons that possesses at least one common trait, which is in the case of this study, the fact that they are based in Arab countries.

Out of the different survey formats, it was also natural to use Web surveys due to the need for anonymity, cost effectiveness, short turnaround time, reliability, and ease. Web surveys were chosen for this study as they were naturally found to be generally quite useful for research on populations that use the Internet regularly (Couper, 2000), (Sills & Song, 2002).

---

[68] MySQL is a popular open-source database management system that uses SQL standards and is used widely in Web 2.0 websites.

[69] SQL, which stands for Structured Query Language, helps create, access, and manipulate digital databases.

Survey design and questions

Two Web surveys were created and each allowed respondents to fill them out anonymously. The instructions text at the beginning of each survey emphasized that respondents are not required to provide any personal information such as name, address, or e-mail. The surveys were designed using open-source software called LimeSurvey,[70] which made it possible to actually host the data on Alkasir's server instead of using another third-party application such as SurveyMonkey. The advantages of using LimeSurvey over SurveyMonkey and the like is the security of data, the possibility to use more complex formulas, and the high degree of customization; it also allows exporting the raw data to IBM SPSS and MySQL. The disadvantage is that it requires some level of technical skill in website design and programming. I decided to install LimeSurvey on Alkasir's server and use it to create the surveys and collect the results. The survey questions were available only in English and Arabic, which may be seen as a disadvantage to potential respondents from China and Iran, where many Alkasir users were based. However, as this study focuses only on Arab Internet users, the language aspect was not a major concern.

The first survey was released to the public in May 2010 and remained open until December 2010. The survey had six groups of questions and a total of thirty-two questions. However, as some questions were conditional and dependent on earlier questions, it was not necessary to answer all questions for all respondents. For example, if a particular answer to a question on whether the respondent had a blog was positive, a new question asking him/her to choose the category of the blog would appear. If the answer to the first question was negative, the second question would not appear at all. In most cases, there were notes with extra information to assist in understanding certain words or phrases. Some questions had check boxes, where multiple selections for the same field were allowed, while others were in multiple-choice format, where only one answer is allowed. A few questions were open text so as to give the respondent the ability to add a value that is not available among the options.

The second survey was published in July 2012 on the same page on the website and was closed in December 2012. The new survey had the exact same format and includes all the questions of the first survey in the same order, but an additional group of five questions related to the Arab Spring was added.

[70] See http://www.limesurvey.org.

Once a survey is completed and submitted, the user on the same computer cannot immediately fill it out and submit another without erasing the browser's cookies.[71] This is implemented to prevent accidental double submissions, which could have influenced the results. Furthermore, the surveys start with a warning on the first page not to fill it out more than once. The surveys also had a feature that allows the user to save the session and return at a later time to complete it. This was found necessary due to the length of the surveys and the time it would take to fill them out. Data collected from those surveys may still be used to further advance knowledge in related fields. See Appendix B for the survey questions.

Incentive to increase the response rate

One of the challenges with Web surveys intended for academic research is the difficulty in attaining a high response rate (Dillman & Bowker, 2001). This also applies to the surveys in this study. The survey format ended up being quite long and also included questions that some users may find controversial. If there were no incentives, it would have not been possible to get a high response rate.

So an incentive was offered to those who fill out the survey, and it was in the form of free activation of the new version of Alkasir. Those who already had the old version were invited to fill it out at will, but were not required to. However, those who wished to upgrade to the new version or install a new copy would have needed to fill out the survey to use it. Visitors of alkasir.com who wanted to download and run the new version would have also been requested to fill out the survey to run the software. And it appears that this incentive was quite useful, as it resulted in a relatively high response for both surveys. For the first survey, the number of respondents was 4,212, while the second survey got 1,662 responses.[72]

Sampling

The sampling approach used for the Web survey method in this study is also multistage cluster sampling. However, as survey respondents were either new or returning Alkasir users, this population may not be representative of all Internet users at large but it is explorative in nature and

[71] Cookies refer to a method of passing data from the user's computer to the server to keep for future sessions without having to re-enter the data again.

[72] The reasons behind the lower turnout for the second survey are provided in the General Findings Chapter.

provides an opportunity to reach a subsection of Internet users concerned with Internet censorship and circumvention. A two-stage multistage clustering sampling approach was used to come up with the final sample needed for this method.

First cluster sampling stage

At the first stage, only those surveys that have been completed are taken and the rest are disregarded. The number of respondents who filled out the first and second surveys completely amounted to 4,212 of 5,838 and 1,662 out of 2,576, respectively.

Second cluster sampling stage

The second cluster would then filter out all but respondents from Arab countries. The total number of respondents only from Arab countries was 3,017 respondents for the first survey and 692 for the second survey. In the findings and analysis chapter, those figures will be analyzed further.

Data Extraction and Content Analysis

The data extraction and content analysis for the survey results are identical in terms of technique used for the data extracted from Alkasir's server. The data are fetched from LimeSurvey's MySQL database and exported to IBM SPSS format, and later used for statistical analysis and generate the needed tables and graphs.

On the Use of Quantitative Methods

The five research questions in this doctoral dissertation depended mainly on quantitative methods due to the large size of the data that have been collected for two years. Statistical analysis was heavily used to identify patterns that could be later explained with an eye on relevant theories and previous literature.

It is important to consider the value of the theoretical framework and other chapters that have covered some significant ground using previous studies that utilized qualitative methods. Nonetheless, it would be of value to carry out future research that utilizes qualitative methods to reflect upon and add to the findings of this study. I expect that such research would result in surprising new findings.

Limitations

As Alkasir was used as a research tool and study object, all its software limitations—presented in detail in Appendix A—are essentially inherited as limitations to this study as a whole. Although the degree of their effects may vary, it was important to take that into consideration when interpreting the results.

Given that the software and surveys neither request nor store personal information, the study is unable to match the software usage patterns to the survey answers and cannot verify the validity of certain assumptions about informants and users such as whether all those signaled to be based in an Arab country are indeed Arab and those who are not and don't use Arabic are non-Arab. Those limitations are a natural consequence of the decision to keep survey respondents and software users anonymous by avoiding requesting and storing personal data.

Furthermore, the fact that the software had to be developed in a short period of time and in order to prevent governments from stopping or replicating it, it was decided to keep it closed-source (proprietary). However, this was also a limitation because it meant that it could make it less trustworthy to some users when compared to other open-source software.

The technical and policy choices made when designing and disseminating the software could also be considered limitations as they were driven by some bias particularly when considering that the software was originally aimed to users in Yemen. Furthermore, when I introduced the software publically, I initially reached out to potential users in my own known circles. So it may well be that I had left out other potential users in countries where I do not have substantial marketing.

Another aspect that could be viewed as a limitation is the fact that this type of study is rather unprecedented, which meant that it is not possible to compare it to earlier studies in terms of findings and methods due to its unique nature.

Those limitations had direct consequences on the reliability of the study, as they meant that for a future study using another circumvention solution for a similar purpose to have similar results, it would require having a similar technical structure, terms of usage, and sample. This also means that the generalizability of the study's findings cannot be established beyond the selected sample. Users of Alkasir represent a special subsection of Internet users that were willing to install software to bypass censored websites; this group is not representative of the general Internet user or activist population.

Validity

For the data obtained from Alkasir's server, it is possible to assume a high degree of validity, meaning how well a test measures what it is purported to measure, due to the high degree of accuracy that the technical methods had. Nonetheless, as indicated in the Limitations, challenges, and potentials chapter of Appendix A, there are cases when technical measurements may not be valid due to network interruptions, temporary outages or technical errors on the server side, or some other issues that may result in false positives, for example, indicating that a website is blocked while it was not.[73]

Furthermore, the technical nature of how Alkasir works does not allow verifying if the same user has used the software on another computer or if it was someone else using it. This is a limitation that emerges from the need to protect the anonymity of users, as there is no requirements to provide any unique identification—such as an e-mail address—to use the software.

When it comes to surveys, the questions and multiple-choice answers were clear and available in Arabic and English. Furthermore, in cases where clarifications were needed, an additional note was added, for example, to define what political/security content is. Almost all questions had an additional custom field for respondents to add an answer that may have not been listed among the choices. Those measures were meant to minimize the risk of a misunderstanding or confusion. The anonymity provided by not requesting names or special private information from users allowed for an environment where there is a higher degree of freedom and safety for respondents. The fact that the surveys were on a secure SSL Web page further strengthened the privacy of respondents when submitting their answers. Therefore, the level of anonymity provided sufficient reason to believe that users were frank in their answers.

Reliability

As for the study's reliability, that is, the degree to which its findings can be produced consistently when repeated, I can claim a high degree of reliability if Alkasir were used in similar conditions again. However, if another software program is used, it would require having very similar characteristics to Alkasir, for example, in terms of preventing access to

[73] A more detailed explanation of this particular limitation is in Appendix A under the sub-header 'Potential Inaccuracies in Filtering Detection'.

nude/pornographic websites as well as focusing on the same countries being studied. Furthermore, the conditions of website censorship need to be similar as well, and this may not be possible to achieve given that the conditions have changed during the study, with multiple countries changing their censorship policies suddenly after the Arab Spring.

The statistical analyses of data collected from the use of Alkasir and survey data were done to limit any potential misinterpretation by applying standard statistical procedures through reputable statistical software.

However, there is a concern about the findings obtained from the two surveys because the way Alkasir was marketed resulted in more users from particular countries. For another study to come up with similar results, this distribution needs to be taken into account. Furthermore, some research questions were answered through the combined feedback from the first and second survey together. This would entail bias for the results from the first survey, which had many more respondents than the second survey.

Generalizability

Finally, generalizability is not possible to establish beyond the sample of the study. The results from this study would not have been possible to emerge without individuals who took the initiative to download Alkasir and fill out the surveys. And so, generalizing the results is not possible and was not intended from the start. The aim was to better understand conditions for a particular region during a particular time and so the findings may not be applicable to other cases and regions.

Finally, it is important to note that a significant portion of the statistical analysis in this study is done on combined aggregate data for all Arab countries. In order to minimize the risks of ecological fallacy[74], however, an analysis is carried out in the seventh chapter specifically for the four case studies, namely, Tunisia, Egypt, Yemen, and Syria.

[74] Ecological fallacy emerges when inferences about individual members of a society are derived from the aggregate findings gained from the society they belong to.

Part II

The Scene

Chapter 5: Background and Contextual Analysis

This chapter is a crucial part of the study because it sets the scene by providing a general picture of the social and political context in the Arab world and particularly the four case studies: Tunisia, Egypt, Syria, and Yemen. This chapter thematically and chronologically presents some relevant background information about free speech and Internet censorship in Arab states. Path dependence is used to a limited extent in this context analysis as an additional approach to understand how Internet censorship and circumvention emerged in general terms and within the Arab context. It will also be used to analyze some of the empirical findings in the next chapter.

Free Speech in the Arab World

As described in the theoretical chapter, several factors have led to the success of authoritarian regimes in the Arab world in resisting political change and having a strong grip on power. This has led to a consistent long period of repressive practices targeting the freedom of speech. International organizations, advocacy groups, and some democratic nations have expressed grave concerns about human rights and democracy in the region for decades. Yet Arab heads of states have remained in power for decades without being challenged and with any potential political opposition being marginalized or crushed. On the specific front of freedom of speech, the picture is quite dismal. There was evidence of an uneven battle between ruling elites and dissidents because the former had a tight grip on information by controlling the mass media. For generations, Arab regimes have systematically prevented citizens from practicing free speech by limiting the freedom of the press through regulations. The seemingly persistent authoritarian characteristics of Arab regimes have hindered progress in the area of free speech for generations.

Over time, the poor free speech conditions and limited access to information in the region have contributed to a knowledge deficit, which was highlighted by the United Nations Development Programme (UNDP) in the first Arab Human Development Report released in 2002. The report emphasized the value of ICTs for shrinking the knowledge gap through openness and liberalization (UNDP, 2002) and the need to end information monopoly and start serious steps toward "building a knowledge society" (UNDP, 2003).

Those calls by the UNDP could be viewed in light of the fact that informed citizenry's contribution to democracy has been well documented in many studies such as those by Milner (2002), Schindley (1997), and Bimber (2003), which have shown that well-informed citizens can take decisions that promote democracy and challenge the status quo.

And when considering 'knowledgeable' to mean "the status of being aware or informed"[75], one would find that Arab citizens were uninformed about many key aspects of their lives and lacked the freedom to seek and exchange information, which resulted in a chronic deficiency in the diversity of views and opinions.

In a report on press freedom issued by the International Federation of Journalists in 2010, several measures taken by Arab states contributed to limiting free speech, including using criminal law against journalists and media, restrictive press and media laws, use of anti-terror laws to stifle legitimate political and social protest, restrictive Internet regulations, and the lack of a right to freedom of information framework (IFJ, 2010, pp. 5–6).

Using the path dependence theory, it is possible to conclude that the critical juncture that established this authoritarian system emerges when the regime in question takes power either through revolution followed by military coups, for example, Syria, Libya, and Tunisia, or through a negotiated agreement to hand over rule from a foreign power to an oligarchic royal family, for example, Gulf countries, Morocco, and Jordan. In both cases, political legitimacy was not obtained democratically through elections. The authoritarian path helped eliminate any challenge to that legitimacy by suppressing the opposition and keeping citizens depoliticized and content with the regime. Various human rights violations in suppressing voices calling for regime change were attempted to prevent any significant challenges to the regimes. The persistent internal and external factors continued to give Arab regimes, particularly the petro states, the edge in maintaining the status quo.

Internet and the End of Information Monopoly

As Arab governments started to provide Internet access to the general public in the 1990s, they ensured that ISPs remained directly run by them

[75] In this context, information is not meant to be equal to knowledge. However, taking in and interpreting information from different sides is required for the attainment of knowledge.

through the monopolization of services, such as in the case of Yemen, or by regulating private companies that offer the service, such as the case in Egypt. When Arab regimes started allowing public access to the Internet, they may have not been aware of the potential loss of information control.

Internet penetration continued to rise significantly across the Arab world, and, as of June 2012, it was said to have risen to over 31% of the population, marking an increase of over 4,000% since 2000 (Internet World Stats, 2013a). If this growth continues unabated, the penetration rate by 2014 would have exceeded 40%.

The rise of Internet penetration in the region was also largely attributed to the simultaneous increasing spread of mobile connectivity and 3G networks, which allowed affordable wireless access in most Arab states (Zuehlke, 2012). Furthermore, when information was published online, satellite TV channels such as Aljazeera, which allowed citizens to upload their photos and videos directly online for broadcasting, allowed those messages to reach people who may have never used the Internet (Hamdy, 2009, p. 104).

The advent of the Internet has in some ways limited the powers of regimes to regulate the flow of political and social information and has effectively broken the monopoly imposed by many governments in the region. Furthermore, many activists in the Arab world utilized the ability of remaining anonymous online to submit sensitive content freely without having to reveal their identity. The Internet has therefore led to a new sense of freedom (Noman & Zarwan, 2008). This led to having the regime lose the most important traditional weapon it had in its arsenal to control the flow of information, the weapon of "selective information feeding" (Al-Jassem, 2006, p. 180).

Gender and Financial Disparities

There are, however, several challenges that remain to have a more inclusive Internet access in the Arab world. Among the most pressing are the financial and gender disparities. While Gulf countries have high per capita income levels and affordable and high-speed broadband connections, poor countries such as Yemen and Djibouti have relatively expensive and low-quality Internet services (Zuehlke, 2012). Similarly, Arab countries, as a whole, suffer from a significant gender divide compared to other regions in the world, with some countries such as Kuwait and Saudi Arabia having up to two times more men than women connected to the Internet using mobile phones in 2012–2013 (BCDD, 2013).

The digital gender divide has been signaled as a challenge to Internet usage in the region since many years (see: Wheeler, 2007; Warf & Vincent, 2007). And while the Internet could be seen as a means of liberation and free speech, it was seen as a potential key factor in *empowerment* rather than liberation of women (Wheeler, 2007). Furthermore, the disparities among Arab countries themselves in the gender divide were quite visible as well, with some countries such as Egypt being more progressive than Gulf countries (BCDD, 2013). But even before the Arab Spring, activists of both genders used the Internet to generate political pressure due to its inherently democratic nature that fosters populist participation (Seib, 2007, p. 5).

Authoritarian Governments Pushing Back

Inspired by their success in restricting traditional media, authoritarian regimes in the region have been eager to control the Internet by setting up firewalls. Some regimes have even gone to the level of trying to regulate the Internet through cyber laws.[76] For example, cybercrime decrees were used to target online activists and restrict free speech in Iraq (Sutton, 2012) and the UAE (Gradstein, 2012). Most Arab regimes resorted to Internet censorship, which includes Internet filtering plus a variety of other methods described here by Noman (2009):

> Internet censorship in the MENA is multilayered, relying on a number of complementary strategies in addition to technical filtering; arrest, intimidation, and a variety of legal measures are used to regulate the posting and viewing of Internet content. (Noman, 2009, p. 3)

To fully understand why Internet censorship has evolved globally as well as in the Arab world, path dependence can be used to invoke the founding of the ARPANET, which created the Internet as a decentralized network that uses TCP/IP for communication in a way that cannot be controlled or governed centrally. However, the natural consequence of forming such a network was the inability of any single governments, or even group of governments for that matter, to fully control it (Brand, 2001).

[76] Some states have indeed enacted legislation, often referred to as 'cyber laws', regulating the Internet. Through those laws, users and website managers may be required to register and get a license from the local authorities.

After the success of the ARPANET network model, the growth of the Internet led to the creation of the Internet Corporation for Assigned Names and Numbers (ICANN) in 1998 as a nonprofit private organization that coordinates domain name systems for websites and allocated IP addresses through a division within ICANN named the Internet Assigned Numbers Authority (IANA). Although ICANN is based in California, its mandate was global and had long-reaching implications on all users of the Internet (Klein, 2002).

Apart from ICANN, the Internet Society (ISOC) is another international, nongovernmental, nonprofit organization based in the United States. Since its creation in 1992, it has been a key leader in promoting open and efficient standards for the Internet and aims at improving citizens' accessibility to the Internet around the world. ISOC is also the parent corporation of the Internet Engineering Task Force (IETF), which creates Internet standards to improve the usability and efficiency of the Internet (Castells, 2002, p. 30). Furthermore, the largest corporations that develop global Internet solutions that the world relies on for disseminating, exchanging and producing content on the Internet are also based in the United States, for example, VeriSign, Google, Facebook, Twitter, Microsoft, Apple.

The opportunities that the Internet brought to developing the national economies encouraged countries across the world to embrace it and offer it to the public. That was also the case in the Arab world, where governments introduced Internet services to their citizens and widely promoted the use of this new technology. Populations in those countries became increasingly dependent on it for communication, education, information, and other services, making it increasingly important for day-to-day activities. But by doing so, Arab regimes may have inadvertently created their own critical juncture, which signaled an increased dependence on this distributed network and weakened the government's central control of information due to a high volume of unmonitored exchange of data flowing freely and exchanged widely within the country and with the rest of the world. Furthermore, the Internet's efficient utilization of infrastructure made it quite affordable and accessible to citizens, resulting in thriving social networking and online content publishing.

Meanwhile, this very open, decentralized, and empowering nature of the Internet made it a magnet for opposition movements, dissident and other anti-regime groups to use for their own campaigns against their authoritarian regimes.

The way communication is made on the Internet is no longer possible to change unless fundamental modifications to the architecture and design of the Internet are made. Hence, unlike other forms of media, the Internet defied attempts of being controlled because unlike other forms of media, such as print media and even satellite TV, governments do not have a direct way of controlling what goes online and what doesn't. And eventually, Internet censorship in its various forms, as illustrated in the theoretical chapter of this study, emerged as desperate and fallible methods to try to control information flow and stop the global network from being used by dissidents to target the authorities. Those methods were insufficient, particularly as circumvention tools such as Alkasir could be used to circumvent technical filtering. Nontechnical forms of censorship were used to suppress online free speech as well. But the possibility to leak information and publish content anonymously was also possible due to the Internet's inherent decentralized structure, making it difficult to stop the flow of content from and to authoritarian states.

However, government control over the Internet could be enhanced by converting the global network to national intranets that are each controlled nationally just like regular telephone networks. Furthermore and as indicated earlier, most of the global institutions and corporations that could have a significant influence on the way the Internet is governed are based in the United States. Another option, therefore, is to reduce the influence of the United States by establishing international treaties and conventions that build a global Internet governance regime that follows national government directives perhaps through the UN.

The dominant role that United States corporations and institutions have in Internet governance issues and its growing power and impact of the Internet have indeed made some governments around the world call for establishing a new global Internet governance model. Therefore, the United Nations initiated steps towards creating a multistakeholder[77] model that would prevent any group of countries, interest groups or governments within countries from having a dominant influence on the Internet. Consequently, the first phase of the World Summit on the Information Society (WSIS) started in Geneva in December 2003 and triggered consultations

[77] 'Multistakeholderism' in the Internet governance context often refers to the participation of different Internet stakeholders including civil society, academia, technical community, the business community, in addition to governments when discussing Internet governance issues.

for a couple of years that culminated in the creation of the Internet Governance Forum (IGF) as one of the inputs of the second phase of the WSIS held in Tunis in 2005. The Summit approved the creation of the IGF as an annual event where global multistakeholder interaction and cooperation is achieved in order to address worldwide Internet governance developmental and public policies (Mueller, 2010, p. 107).

Following the creation of the IGF and the apparent inability of governments to dominate Internet governments nationally or internationally due to the multistakeholder model required, several Arab governments opted for unilaterally suppressing online speech within their own borders. Among the four case studies addressed in this dissertation, namely Tunisia, Egypt, Syria, and Yemen, all except the latter were considered "enemies of the Internet" in a 2010 report by RSF, as will be described in detail in later sections (RSF, 2010).

Yet governments did find it more difficult to suppress the flow of information due to the fact that the content being viewed is not locally stored and the Internet itself is not centrally controlled. Furthermore, tools to circumvent governmental censorship of news websites and social media have remained an option for citizens who wish to get information that traditional media cannot deliver. For the Arab world as a region, Internet access has established itself and reached the critical mass that made it indispensable to businesses, governments, and citizens, particularly the young generation (Hofheinz, 2005). And hence, shutting down Internet access in most Arab countries would prove to be an ineffective strategy and would not last long due to the cost to the economy and reputation of the regime (Stepanova, 2011, p. 2).

The Emergence of the Arab Spring

With the Internet becoming a relatively accessible means of voicing opinions and receiving information, it was the natural place for many Arabs to vent their frustration by their governments, citing economic hardships and many societal and political problems. Out of a total population of around 360 million, more than 60 million Arabs were estimated in 2010 to be living below the national poverty in the twenty-two Arab states (Ismail & Jondi, 2011). Additionally, most Arab countries were labeled "not free" by Freedom House in 2010. While the biggest wave of democratizations happened in the 1990s, raising the number of electoral democracies from 69 in 1989 to 116 in 2009 (Freedom House, 2010a), it was evident that the Arab world remained in a state of stagnancy.

Political acts of repression combined with economic difficulties and indifference and sometimes support to authoritarian regimes by Western powers (Sottilotta, 2013) have collectively reached critical levels in several Arab states. However, the level of economic hardships was not uniform across Arab countries, with some Gulf states enjoying a much higher level of income compared to poorer states such as Egypt and Yemen.

This excessive repression and disregard to human rights combined with economic hardships were just too much for a Tunisian soul to bear. Tunisian street vendor Mohamed Bouazizi took the decision to set himself alight in the poverty-stricken town of Sidi Bouzid on December 17, 2010, igniting several Arab revolutions and creating history. His act contributed to the downfall of four Arab leaders known for their repression against their people in Tunisia, Egypt, Libya, and Yemen. It also caused tremors that were felt by the leaders of other countries such as Morocco and Jordan, leaving them no choice but to put together some reforms to avert a similar scenario (Boukhars, 2011). Syria was a country that was perhaps the most unfortunate, as it slipped into civil war, leading to thousands of deaths and more than a million displaced citizens. Meanwhile, Bahrain's uprising held promise at the beginning, but was severely suppressed by the state using help from other Gulf countries (Jacinto, 2011).

The Arab Spring can be considered a critical juncture that not only altered the path of several Arab states, but also resulted in adjustments to foreign policies of major global powers such as the United States and the EU (Sottilotta, 2013). The critical juncture started with Tunisia first and then moved to other Arab countries, creating a chain reaction. As will be described in the next chapters, the new path taken was not uniform for all Arab states, with some countries moving closer to democracy, for example, Tunisia, and others becoming even more repressive, for example, Syria. Furthermore, it is not possible to predict the outcome path that will be settled, because, in some way, the critical juncture has not yet completed its phase and an ultimate clear path is still not yet possible to define.

While the public motivation for those leading the Arab uprisings resembled commonsense demands such as better living conditions, more freedom, and justice, it is important to consider that the Internet allowed the frustrations of Arab citizens to be expressed more vocally and globally. Online platforms such as social media and critical dissident websites have served as a breathing space in many Arab countries where governments initially had an open attitude to investing in ICTs and allowing public access to basic Internet services.

The critical juncture in Tunisia along with the one in Egypt may have shared the same motivations, because both countries had a relatively low per capita income level, yet their governments decided to invest heavily in telecommunication and connectivity infrastructure and services, which allowed their Internet penetration to thrive and surpass the average for the Arab world as a whole (Internet World Stats, 2013b).

If economic hardships alone were behind the revolutions in the Arab world, then only poor Arab states would have had revolutions. Nonetheless, Libya was an oil-rich country with a per capita annual income exceeding $15,000 and Bahrain's income was even higher, exceeding $22,000 (The World Bank, 2010). So political oppression could be considered a conditional explanatory factor leading to significant and steady popular uprisings that, if maintained, could in combination with poverty and suppressed opposition constitute a critical juncture capable of changing the course of history in a given context. This is supported by the fact that Tunisia, Egypt, and Yemen all had political repression and per capita income levels of less than $5,000 (ibid.).

As I noted in my earlier argument, the moment the Internet became indispensable for countries was a critical juncture signaling that the Internet has become part of daily routine for communication, business, and other uses. And hence, it was a strategically opportune moment for opposition and activist forces to use social media platforms such as Facebook and Twitter during the Arab Spring for disseminating anti-government content and for mobilizing street protests particularly in countries that had a relatively high Internet penetration such as Egypt and Tunisia (Huang, 2011).

The use of social media also picked up pace in other Arab countries, with the number of Facebook users growing tremendously throughout the region. As of June 2012,[78] there were over 45 million Arab Facebook users, which reflected an increase of about 300% since June 2010, with 70% being between 15 and 29 years old. It was also found that Arabic is the fastest growing language on Facebook since 2010 (Mourtada & Salem, 2012, p. 7).

As this study aims at analyzing empirical data obtained from observing Internet censorship patterns and reactions to censorship by Alkasir users during the critical period that preceded and followed the Arab Spring, being aware of the tremendous rise in popularity of the Internet and social

[78] It is worth noting that by October 2013, the total number of Arab Facebook users had in fact reached over 56 million.

media is helpful when drawing conclusions and discussing results. The sociopolitical dynamics of the Arab Spring and the use of social media make it specifically important to understand the potential motives behind governments' actions to filter types of websites and how users reacted to such filtering.

In this study, I give special attention to four Arab Spring countries: Tunisia, Egypt, Syria, and Yemen. The next four sections will be used to provide an exploratory perspective through contextual analysis for those countries.

Diachronic and Synchronic Developments in Four Arab States

The earlier analysis has shown how the Arab Spring, which started with the Tunisian revolution, was a critical juncture for the Arab world as a whole with various degrees and directions of change in path. The described historical sequence of events reflects a diachronic development across time and geography. It also reflects a diachronic development within Tunisia itself, with the first spark of the revolution being triggered in Sidi Bouzid first and later moving to other parts of the country.

A good understanding of the sequence of events that connected the uprisings in the different Arab countries is useful in understanding how Arab regimes dealt with the flow of digital data during the Arab Spring and how citizens may have shared common interests in confronting such censorship using circumvention tools to find a way to break free from government-imposed information monopoly during each country's critical juncture.

However, the moment a new critical juncture in the form of a popular uprising started in a particular Arab country, the direction it took did not necessarily have to be linked to the preceding revolution in the other Arab state. This reflected synchronic developments, with each country now independently seeking to achieve the goals of the revolution on its own.

This section has four sub-sections each covering one of the four case studies (Tunisia, Egypt, Yemen, and Syria) with the aim of analyzing the context in the Arab world diachronically as well as having each of the four case studies independently analyzed synchronically.

I wish to emphasize at this point that to meet the study's goals, understanding contexts is important, mainly because censorship practices are connected to motives that often differ from one country to the other and from certain circumstances to others. Context in this study refers mainly to events linked to the Arab uprisings, but it also could be understood as the political situation in question, with each state having its own political

history and developments. An overarching context that differentiates Arab states as a whole from non-Arab states is culture, which is a rich subject but one that goes well beyond the scope of this study. However, references to the cultural context were made in the preceding Theoretical Framework Chapter in connection to authoritarianism. Those perspectives will be important in analyzing some of the empirical findings in the following chapters.

Generally speaking, the synchronic developments in relation to censorship practices could be understood within the event/political angles and are vital for the analysis in the empirical findings in relation to why a particular government blocked a political website because such decisions relate to the developments happening on the ground in the concerned state.

And while Arab regimes started suppressing free speech on the Internet domestically through Internet censorship before and during the Arab Spring, in 2012 they attempted to push for greater governmental influence on the global arena in order to alter the multistakeholder model adopted for the IGF, which effectively limited the role that Internet Telecommunication Union (ITU)[79] could have had in controlling content on the Internet. Saudi Arabia, Sudan, UAE, Algeria, and Russia had their name on a drafted proposal to the 2012 World Conference on International Telecommunications (WCIT) held in Dubai to strengthen the role of national governments in the Internet governance model.[80] The proposal called for Internet governance to be developed and applied by governments representing ITU member states and emphasized their sovereign right to establish and implement public policy on the national and international levels on matters related to Internet governance (Gayathri, 2012). This effectively meant that those governments wish to take over the bulk of Internet governance tasks from the other multistakeholders. Although the proposal was eventually discarded after being opposed by many other countries and advocacy groups, it demonstrated that Arab regimes are willing to openly use international bodies such as the ITU to expand their role in Internet governance and consequently, have better means to control online content.

---

[79] The ITU is a UN agency represented by government officials, mostly ministers of telecommunication, and is responsible for coordinating the shared global resources used for international communication through radio, satellite, telephone networks, international submarine, land cables, and other infrastructure components.

[80] Egypt's name was also on the document but the head of the Egyptian delegation issued a statement denying his country's involvement (Gayathri, 2012).

Tunisia

A history of repression

When Zine El Abidine Ben Ali seized power from his predecessor Habib Bourguiba through a bloodless military coup in 1987, he promised his people democratic reforms that would guarantee free and fair elections to choose their next government. However, he backed away from his earlier democratization promises when nonviolent Islamist movements started to grow in Tunisia and neighboring Algeria. The 1989 elections could be considered the critical juncture that led to an authoritarian type of government lasting for well over two decades. Given that the elections were not reported to be free and fair, Ben Ali's political legitimacy to rule was questioned by the opposition Ennahda Islamic movement, which was repressed and whose leaders were exiled. During Ben Ali's rule, political repression, election fraud, and severe restrictions on freedom of expression took place while a high degree of secularism was maintained (Dalacoura, 2006, p. 16).

During Ben Ali's reign, the Tunisian constitution guaranteed freedom of opinion and expression but allowed legislators to establish restrictions, which were included in the 1975 Press Law and amended three times. Among the restrictive laws was one that could lead to imprisonment for up to five years and impose up to 2,000 dinars in fines on anyone insulting the head of state through any form of media including the Internet. Just before the Arab Spring, the situation of free speech in Tunisia had reached its worst years since the country's independence, with harassment of journalists reaching unprecedented levels, particularly after the October 2009 presidential elections, which gave President Ben Ali a fifth term in office. Police brutality against journalists manifested itself in various forms, ranging from arrests to personal threats and from fabricated allegations to intimidation and physical assault (IFJ, 2010, pp. 5–6).

Despite the poor human rights record, many developed countries, including the United States and EU member states, had formed strong political and economic ties with Ben Ali's regime, which was often praised for its cooperation in confronting Islamist fundamentalism and for its strong tendency to develop a secular, stable, and modern state (Durac & Cavatorta, 2009; Mullin & Shahshahani, 2012).

Following Ben Ali's reelection in 2009, the pace of repression increased, with restrictions on free speech being one of many human rights violations that were committed at an accelerating rate throughout the country. Ac-

cording to a 2010 report by Amnesty International, hundreds of people were convicted without fair trials using anti-terror regulations. Furthermore, practices of torture and harsh conditions in prisons continued to be reported. Among those who suffered the most during that time were political prisoners and defenders of human rights (Amnesty International, 2010). Free speech was never a priority for the Ben Ali regime, which has taken a steady and consistent approach on repressing the opposition and tightening its grip on information.

Pervasive Internet censorship as is the norm

Tunisia was the first Arab country to link to the Internet in 1991 and, by June 2012, out of the total population of 10.7 million, 34% had Internet access (Internet World Stats, 2013a). From its outset, the Internet was tightly controlled by the state-run Tunisian Internet Agency (ATI),[81] which was responsible for spreading the technology to encourage foreign investment while strictly censoring content through Internet filtering (Mellor, Rinnawi, & Dajani, 2011, p. 126). While ATI allowed private companies to provide Internet services, it had indirect control over what users were allowed to access through a set of agreements with those companies on what content is to be accessed and what should be blocked. Furthermore, ATI is responsible for surveillance in cooperation with the National Information Security Agency, whose mandate is to ensure cybersecurity but which has transformed to an agency responsible for spying on Internet traffic generated by users (RSF, 2010, p. 30).

The Tunisian regime's focus on providing the public with affordable and high-quality Internet services is in itself a critical juncture that set the country on the path toward more connectivity and routine use of the Internet for various purposes. It could be concluded that as time passed, the reliance on the Internet by all parts of the community, including the government, had reached a point of no return. In other words, shutting access down to prevent it from being accessed by activists and dissidents to mobilize the masses and communicate was not a viable option.

Tunisian authorities combined Internet filtering as a means to prevent access to dissident and social networking content with other more brutal forms of oppression including intimidation, harassment, threats, and imprisonment of critical and outspoken bloggers and online journalists. Those restrictions escalated over time and reached their climax in 2010,

[81] Abbreviation stands for the formal French name Agence Tunisienne d'Internet.

when Tunisia was placed on the "enemies of the Internet" list in a report issued by RSF (pp. 29–31). Despite filtering, however, online activists found ways to bypass the firewall through a combination of anticensorship tools and methods. They also launched campaigns exposing corruption and other ill practices by the Tunisian regime through websites such as TuniLeaks, which was blocked in Tunisia for inciting hate against the wife of the President (Black, 2010).

Yet human rights violations, corruption, and other ill doings of the regime started to reach the public not only via the Internet, but also through satellite TV, which meant that the Tunisian regime was beginning to lose its control over information that was reaching the public (Eko, 2012, p. 130). Social networks including Facebook were actively used by the public and helped Tunisian activists in mobilizing protests and launching campaigns, particularly with the wide use of mobile phones and social assemblies (Stepanova, 2011). By the beginning of 2011, Facebook had about two million users in Tunisia, which accounts for about a fifth of the population (Preston, 2011).

The Jasmine Revolution sparks the Arab Spring

The second major political juncture in Tunisia's recent history was the "Jasmine Revolution," which was sparked on December 17, 2010, with Mohamed Bouazizi's self-immolation in Sidi Bouzid. The inability of the Tunisian regime to prevent images from being taken by mobile phones and distributed online to reach international and terrestrial satellite TV made it impossible to conceal the large masses of protestors flooding the streets (Eko, 2012, p. 130).

The radical act of Bouazizi, according to his mother, was not in reaction to the confiscation of his goods, but rather because of the humiliating treatment by a female police officer[82] (The Independent, 2011). However, it turned out that Bouazizi was not the only Tunisian who had committed suicide to protest harsh treatment or for economic conditions. But this time it was different because the case gained enough attention to reach a critical mass through mobile phones, social media, websites, and the rebroadcasts by satellite TV channels such as Aljazeera and others (Ryan,

[82] The family of Bouazizi claimed that Faida Hamdi, a 45-year-old female municipal official, slapped him in the face, spat at him, and insulted his deceased father. Faida, however, denied those claims. Furthermore, there were no eyewitnesses that claimed to have seen her slap Bouazizi. See: (The Independent, 2011).

2011). The viral effect had taken the Tunisian regime by surprise because the old repressive practices to cover up what was going on in the country were useless as Tunisians were able to see massive protestors roaming the streets throughout the country. It was a revolution that was broadcast online and through terrestrial TV.

On January 14, 2011, successive and massive protests throughout Tunisia resulted in having President Zine El Abidine Ben Ali give in to the mounting pressure, ending his 24-year rule and marking the first time in recent history for an Arab leader to leave power mainly due to public protests and because the small apolitical Tunisian army did not take sides but it stuck to its professional duties in protecting the county's sovereignty (Lutterbeck, 2013, p. 34). Starting in 2012, January 14 became an official national holiday, as it marked the day the Tunisian revolution toppled the head of the regime (Amara, 2012). And while the question of whether the Internet and social media were vital for the success of the Tunisian revolution remains contested, it was evident that the images taken by mobile phones and published online had a role to play in highlighting the uprisings. It can also be concluded that the revolution was the critical juncture that started setting Tunisia on the path toward forming a democratic system of government (McCarthy, 2012).

The fruits of the revolution started to be noticed with the banning of former ruling party members from participating in senior positions and with the formation of a government led by the once exiled leader of Ennahda Islamic movement Mohamed Ghannouchi (Bouderbala, 2011). Later on, the long-feared political police, which prosecuted and intimidated dissidents and activists, was also banned, allowing the human rights record of the country to improve and move from the "not free" to the "partly free" status in Freedom House's 2012 press freedom report (Freedom House, 2012). Tunisia moved on to have its first democratic elections, which resulted in giving ninety out of 217 parliamentary seats to the Ennahda Party, which was formerly banned under the Ben Ali regime. And on December 12, 2011, the former exiled human rights activist Moncef Marzouki was elected President, and the moderate Islamic Ennahda Party announced that it would keep the secular nature of the state and will not refer to Islamic law in the constitution, resulting in some tensions with some hard-line Islamists (Fahim, 2012). By the end of 2012, Tunisia had already achieved a number of major reforms and appears on a steady course of political reform toward achieving the goals of the January 14 revolution (McCarthy, 2012).

Egypt

Challenges for free speech in a state of emergency

When Hosni Mubarak took over power as President of Egypt in 1981 following the assassination of Anwar Sadat, he did not create a critical juncture, as he continued along the path that was drawn by the military regimes that preceded him. His rule had merely continued along the same general lines set by his predecessor, particularly in connection to the 1979 peace treaty with Israel and the military's cooperation with the United States, which continued to provide billions of US dollars in annual financial aid to the military in return for the peace deal it signed. Similarly, the practices of former military leaders, particularly those targeting the Islamic Muslim Brotherhood movement, continued and the military remained active in interfering in politics and consolidating its influence and power in various important sectors while having no one to account to (Kienle, 2001). Hence, there appears to have been no major political change throughout Mubarak's rule, particularly as Mubarak started to groom his son Gamal to succeed him (Arafat, 2009).

Generally speaking, the Egyptian 1971 constitution, which remained in effect until late 2012, had acknowledged basic rights of citizens including the freedom of expression, press, and publications among other rights. However, those rights were regulated by the Press Law, the Publications law, the Penal Code, and, most importantly, the Emergency Law, which has been continuously extended every three years since 1981. The law was last extended in 2010 and officially ended without extension in June 2012 (Chick, 2012). However, human rights advocates expressed concern that a tough anti-terrorism law kept in the drawer since 2007 could potentially be enacted in the near future and warned that, once implemented, the new law could serve as a replacement of the long-feared Emergency Law (Waterman, 2007).

Egypt's free speech record has been marred with violations against journalists ranging from confiscation of cameras and equipment to severe financial penalties and from military trials to abductions and brutal attacks that are sometimes committed by police but other times by thugs hired by the National Security[83] (Shukrallah, 2011). During the Nasserite era in the 1950s and 1960s, Egypt developed a censorial culture in the practice of journalism, resulting in an environment of overt and self-

[83] They are commonly referred to as 'Baltageya' (singular, 'baltagy') by Egyptians.

censorship (Amin, 2002). Financial penalties were a measure that was used widely to suppress free speech and promote self-censorship due to the limited income of Egyptian journalists compared to the issued fines (ANHRI, 2009, p. 14).

Reporting about violations of human rights against citizens in police custody has been picking up pace in recent years but has also resulted in casualties among the reporters themselves (p. 16). The internationally renowned Egyptian blogger and human rights activist Wael Abbas had published on his blog "Misr Digital" many documented videotapes of cases of torture and abuse against Egyptians in prison cells. In 2009 and upon his return to Cairo coming from Sweden, where he showcased his work in defending human rights, he was harassed and detained by airport authorities (p. 38).

The Emergency Law gave impunity to security forces, intelligence apparatuses, and policemen to detain and interrogate individuals without being accountable, triggering calls by Amnesty International to end it (Amnesty International, 2012). And while the Emergency Law was lifted in 2012, the situation of freedom of expression continued to suffer after the Arab Spring, with many of the old practices that security forces were known for such as abductions, crackdowns, assaults, harassments, and confiscation of equipment continuing and even intensifying (Freedom House, 2012).

Internet as an emerging power

In 1993, Egypt became the second Arab country after Tunisia to be linked with the Internet. The government had ambitious aims to expand Web access considerably (ONI, 2008). The state-run Information and Decision Support Center was the first body to be hooked to the global network, and in 1997, it started giving licenses to private ISPs that were then able to sell the service to the general public. As of 2010, Egypt already had over 200 private ISPs and created healthy competition, which resulted in significant growth (Mellor, Rinnawi, & Dajani, 2011, p. 126). By mid-June 2012, Egypt had about 29.9 million Internet users out of a total population of about 83.7 million, giving it the first position among Arab countries in terms of sheer numbers and the second in the continent of Africa[84] (Internet World Stats, 2013a).

Internet growth in Egypt was quite significant and reflected the importance given to the ICT development policy that was supported directly

[84] The first being Nigeria with about 48 million users.

by Mubarak since the Ministry of Communication and Information Technology was established in 1999 (Stahl, 2008). The high Internet penetration levels were attributed largely to the affordable services and widespread use of wireless 3G mobile phones mainly to access social media, which had a significant role in the Arab Spring through online activism mainly relying on Facebook's capacity to help in recruiting, mobilizing, networking, and campaigning (Stepanova, 2011).

Just like the case of Tunisia, Egypt reached the critical juncture where the Internet became indispensable to many sectors and to most young Egyptians in urban areas, who constituted the bulk of Internet users in Egypt. It meant that the Internet would become an essential means of communication, business, and a variety of other usages (Mourtada & Salem, 2011).

It was as early as 2005 when Egyptians started utilizing social networking platforms to mobilize the public through movements such as Kefaya ("Enough") with a mandate to call for combating corruption and driving serious reforms (Shorbagy, 2007). Kefaya was followed years later by youth movements such as the April 6 Youth Coalition, which utilized Facebook effectively to call upon a labor strike (ibid.). But Egyptian authorities started tracking down online activists and used various means of harassment, intimidation, and prosecution along with orders to shut down websites to silence them, which gave Egypt a place on the 2010 "enemies of the Internet" list (RSF, 2010). Despite those measures, however, social media continued to be the main platform to discuss politically sensitive topics openly and express dissident views to the public and the world (Tufekci & Wilson, 2012, p. 364).

A Facebook page dedicated to a young computer programmer Khaled Saeed was set up in June 2010 under the title "We Are All Khaled Saeed" in protest of his brutal death by the hands of the Egyptian police. According to eyewitnesses, the 28-year-old Khaled was severely beaten up by policemen, who later denied all allegations and claimed that he committed suicide by swallowing cigarettes containing drugs (Chick, 2010). The Facebook page, which was later found to have been created by Wael Ghonim, was used as a platform to disseminate images of Khaled's shattered face[85] and mobilize protests against police brutality. Over time, the

[85] The graphic picture shows Khaled's jaw twisted, skull cracked and face severely bruised. [Graphic warning] http://en.wikipedia.org/wiki/File:Khalid-Saeed.jpg.

page gained tremendous popularity, and by late September 2012, it had over 2.5 million subscribers (Rashwan, 2012).

Twitter was also quite powerful in spreading information during the weeks and months of the Egyptian revolution with hash tags such as #Egypt having 1.4 million mentions and #Jan25 having 1.2 million in the first three months of 2012 (Huang, 2011). While Facebook was mainly used to mobilize groups on the ground, Twitter played a significant role in reaching out to the international community because much of the breaking news flashes from inside the protest camps used to come from activists that are recognized internationally and could help focus the attention of global media to Tahrir Square, where the main protest camp was located (Tufekci & Wilson, 2012, p. 366).

Until 2011 and unlike most other Arab states, Egypt was not found to practice Internet filtering to censor the Internet. However, that changed on January 25, when reports started to emerge claiming that Facebook and Twitter were blocked and were reported by multiple users to be inaccessible (Schonfeld, 2011). However, the regime took one more radical step by shutting down access to the Internet by having the different ISPs disconnect their networks from the Internet for most of their users and jammed mobile network traffic on January 27 and remained so until February 2, when Egypt was brought back online (Cowie, 2011).

But as noted earlier, the level of Internet use in the country had already arrived to a point where its path is already set and cannot be easily reversed. Taking a path dependence approach, this meant that the institutions and society at large have already become dependent on Internet services to a degree that makes reversing that course too expensive to succeed.

Although the attempt to shut down the Internet was made, the uproar and strong reaction it caused was quite overwhelming and the response was manifested in greater numbers of people flooding the streets. The act of shutting down Internet access backfired, leading to stronger anti-government movements on the ground (Khamis & Vaughn, 2011, p. 15). The cost the regime had paid was quite high, because when the Internet was resumed, it took just over a week of rallies and extensive use of social networks to fuel the protests that eventually led to Mubarak's resignation on February 11 (McGreal & Shenker, 2011). Since then, Internet usage in Egypt has continued to rise (Internet World Stats, 2013a).

A revolution that captivated the global media

Several days after the Tunisian revolution succeeded, demonstrators flooded Egyptian streets on the so-called "Day of Wrath" on January 25, 2011. Inspired by the Tunisian revolution, protestors rallied in peaceful demonstrations in most Egyptian cities, chanting for the end of President Hosni Mubarak's three-decade-long rule.

Despite the Internet outage during January 25–February 2, calls had already been made to walk to and occupy the Tahrir Square on the "Friday of Rage" on January 28, which was a milestone that marked the day when anti-Mubarak protestors succeeded in occupying the Tahrir Square after bloody confrontations with riot police, resulting in dozens of deaths and hundreds of injuries (Rashed & El Azzazi, 2011). Attacks by pro-Mubarak gangs and police against protestors continued for a few days, raising the number of fatalities, but this failed to empty the square. The mass rallies were widely and thoroughly covered by the world's biggest media houses. Thereafter, the US administration led by President Barack Obama called upon Mubarak to leave power without delay and called Egyptian protests an "inspiration" (Amanpour, Tapper, Khan, & Radia, 2011).

In a televised address on the first day of February, Mubarak committed not to run for another term and just remain in office for a few more months until the September elections (Fleishman & Parker, 2011). However, just after this message, the "Incident of the Camel" took place on February 2, in which Mubarak supporters rode horses and camels into Tahrir Square, wielding sticks to chase the protestors out of the square in a display of excessive violence, which infuriated the crowds and increased support among the Egyptian public to the cause of the revolution (Eleiba, 2011). Following a few days of increased protest momentum and with a multi-faith Sunday mass held on February 6, the Egyptian army started assuming greater responsibility to maintain order and protect the Egyptian Museum of Antiquities and other vital facilities (McElroy, 2011).

Just as the public was waiting for a resignation announcement, Mubarak came out with yet another address asserting his intention to stay in power, triggering greater numbers of protests and unprecedented escalation in demands to overthrow the regime (Rashed & El Azzazi, 2011). The momentum increased steadily until the "Friday of Departure" on February 11, when Mubarak finally resigned, allowing the Supreme Council of Egyptian Armed Forces to take charge temporarily (McGreal & Shenker, 2011).

The Supreme Council thereafter dissolved the parliament and assumed power for six months (Shadid, 2011). A constitutional referendum to adjust the constitution and open the way for parliamentary and presidential elections was held on March 19 and passed with over 77% (Michael, 2011). On April 16, the former ruling National Democratic Party was dissolved by a court verdict (Bradley, 2011) and, soon afterward, Mubarak was arrested and following a long trial was handed a life sentence (Kirkpatrick, 2012a). On November 28, 2011, and January 11, 2012, parliamentary elections took place, yielding considerable gains, with about 37%, for the Freedom and Justice Party, which is the political entity representing the formerly banned Muslim Brotherhood (Fahmy, 2012). The first democratic and free presidential election took place in two rounds, one during May 23–24 and the other during June 16–17. It ended up with a win for the Muslim Brotherhood candidate Mohamed Morsi, who was sworn in as President on June 30 (Yeranian, 2012).

The downfall of Mubarak could be considered a critical juncture in the history of Egypt for setting the country on a path that allowed Egyptians to vote for the first time in history in a free and fair presidential election. It also marked the first time in the Arab world when a former head of state was brought to trial.

As of 2012, however, this new path the country will remained unpredictable as the situation in Egypt was uncertain due to tensions that emerged between Morsi and a large subsection of the liberal and secular groups in the country, particularly after he issued in November a declaration immunizing his decrees from being challenged and granting himself powers "to protect the revolution" (Samaan, 2012).

Tensions between the Muslim Brotherhood supporters and secular groups increased significantly upon news that the constitution-drafting assembly that Morsi had appointed planned to include references to shari'a in the new constitution (Kirkpatrick, 2012b). In a mass protest held in November 2012, clashes erupted leading to several casualties and international condemnation from human rights organizations and local advocacy groups (Hussein & Black, 2012). Upon approving the new constitution with a majority vote in the referendum, several secular anti-Morsi groups accused the government of rigging the vote and vowed to overturn it, which consequently led to more tensions and instability (Tait, 2012).

Given the uncertainty that ensued after Morsi's election, it is difficult to conclude that the new path toward democratization is fully established. It

might well be that Egypt will remain in a critical juncture while gaining confidence in the direction it will take.

It is important to understand that while the diachronic nature of developments from Tunisia to Egypt was quite evident, with many of the same chants used in Tunisia heard in the squares and streets of Cairo, the nature of the political regime in Egypt was quite different, which meant that the outcomes should not be expected to be the same. While Tunisia had a smaller and more professional military that was relatively disconnected from politics (Lutterbeck, 2013, p. 34), in Egypt, the military was quite powerful and resourceful and has deeper and stronger political roles nationally locally and regionally, particularly as it receives financial aid from the United States in relation to the peace deal with Israel (Anderson, 2011).

Morsi's agreement to honor Egypt's commitments based on treaties signed by his predecessors came after Israel expressed its fear in that a power transition could threaten the treaty (Black, 2011). Annulling the treaty could lead to intervention by the United States, Israel or even the Egyptian military itself. This is a situation not shared by any other Arab country except Jordan.

Yemen

Free speech abridged, democracy obstructed

Yemen is also the only Arab country that witnessed a reunification after decades of tension and wars between former North Yemen and former South Yemen. Using the path dependence theory, I argue that the reunification of the two Yemens in May 1990 was perhaps one of the most significant critical junctures that the country had witnessed in recent history.

After unification, the country started adopting an electoral democracy system to transform Yemen from a state of a single-party authoritarian rule under Saleh's regime in the north and a state under the socialist party rule in the south to one republic with a multiparty political system that allowed some degree of press freedom. The country continued along that promising path until another critical juncture occurred in 1994, when a civil war erupted between the southern and northern armies, which at the time were not yet fully unified. The victory of the northern forces led by Saleh resulted in a new path of authoritarianism under his rule, which was enforced through repression, election fraud, and a series of other violations (Carapico, 2001).

During Saleh's rule, Yemen's constitution provided for free speech conditionally with the familiar "within the limits of the law" clause. The 1990 Press and Publications law is full of restrictions and criminal sanctions for various issues ranging from criticism of the head of state and goals of the Yemeni revolution to false information and defamation of religion or foreign relations. Punishments against violators would be based on the 1994 Penal Code, which criminalizes inciting of public peace and lays down a range of other restrictions. Penalties can range from a simple fine up to two years in prison. The vague language used in these laws made it possible for abuse by the government, which set up the Special Court for Journalists in 2009, receiving several local and international condemnations (IFJ, 2010, pp. 16–17).

Being among the least developed countries in the world, Yemen had multiple challenges on several fronts ranging from food shortage to security and from corruption to social disparities. Human rights violations started to escalate and reach unprecedented levels after the 2006 presidential elections, which renewed Saleh's term after winning the majority of votes over his contender representing the opposition coalition, Faisal bin Shamlan. The results of the elections were strongly contested by the opposition, citing evidence of election fraud (Saleh, 2006).

The presidential elections seem to have given Saleh all the power he needed to continue restricting free speech and suppressing the opposition. Human rights violations continued to be reported and ranged from enforced disappearances to arbitrary arrests and detentions and from denial of free trial to abuses of anti-terrorism laws to prosecute journalist and activists (FIDH, 2010). Meanwhile, the opposition intensified its calls upon Saleh to step down and save the country from total collapse due to the numerous economic and security problems it was facing. Yemen had three major fronts to deal with: an ongoing war with the Shi'ite Houthi rebellion in the north, a growing resistance movement calling for secession in the south, and Islamic extremism led by al-Qaeda in the Arabian Peninsula, which had strongholds mainly in the south and southeast of the country (Brown S., 2011).

Furthermore, Yemen faced a severe economic crisis fueled by unprecedented high unemployment rates and acute water shortage in several cities, which pushed Yemen to the verge of collapse (Boucek, 2009). However, Saleh held on to power relentlessly while getting bogged down in many of those unresolved crises. He was supported by the various military, financial, and governmental institutions that were controlled by his sons, neph-

ews, and loyalists (Erlanger, 2010). In 2010, it was revealed through one of the WikiLeaks cables that Saleh had offered the United States an open door to attack alleged al-Qaeda elements on its soil using military drones. Simultaneously, however, he insisted on maintaining the status quo in publicly denying any US involvement even when civilian casualties were caused by US drone attacks (Booth & Black, 2010). Those indicators pointed to the lack of political will in performing deeply and urgently needed political and economic reforms.

Internet: low penetration, indirect impact

While TV and radio remain the most popular method for the Yemeni public to consume news, Internet's share has started to increase since Yemen was first linked to the Internet in 1996 by the Ministry of Telecommunication's Public Telecommunications Corporation (PTC) and Teleyemen, which was formed in 1990 as a joint company owned by PTC and UK's Cable and Wireless Plc. By the end of 2003, PTC bought out all Cable and Wireless shares and signed a management contract with France Telecom to manage the company until June 11 (Teleyemen, n.d.). Teleyemen initially provided Internet services starting only with very few subscribers due to poor infrastructure, low literacy rates, and lack of personal computer affordability (ANHRI, 2004). However, Teleyemen's monopoly ended in 2002 when the Ministry of Telecommunication established Yemen Net as the country's largest ISP. So far, no private ISP was allowed to operate, keeping competition relatively limited.

Nonetheless, the rate of Internet subscribers has been steadily rising. The number of Internet users surged from 15,000 in 2000 to around 3.7 million in 2012 out of a total population of more than 24 million (Internet World Stats, 2013b). Despite having one of the lowest penetration ratios in the region, Yemen's news websites have been quite active and diverse. By 2008, many news websites have become useful sources for national mainstream media and started presenting critical views and news items that are often ignored or underreported. This growing influence was seen as a factor behind significant Internet censorship (Al-Saqaf W., 2008). By 2010, Internet censorship was reported to have been substantial in targeting political content, while filtering of social content such as pornography was found to be pervasive (ONI, 2013).

Despite the evident growth in penetration, the Internet in Yemen remained backward and has not attained a status similar to that in Tunisia, Egypt, or Gulf countries for it was mainly accessed by the youth that live

in main cities while it remained off reach for the majority of the population due to high costs, poor service, or inaccessibility (Al-Saqaf, 2013). And, hence, I argue that the usage of the Internet in Yemen has not yet reached the state that makes it indispensable as the global network remains largely underutilized. That being said, the Internet did play a noticeable role during 2011–2012 in feeding the mainstream media with content related to the popular uprising and street activities. Aljazeera, which was one of the most-watched terrestrial TV channels in actively following developments in Yemen, allowed Internet users to upload content directly to its website (Hamdy, 2009, p. 104). The extensive coverage of Aljazeera resulted in attacks by security forces against some members of the channel's Sana'a bureau, and some equipment was confiscated (The Global Report, 2011). And while Internet censorship continued sporadically and inconsistently during 2010-2012, an official at the Ministry of Telecommunication in the newly formed government that took over after Saleh's departure has indicated that previously filtered websites were gradually being unfiltered and the very practice of filtering dissident and anti-government websites was no longer taking place based on instructions from the Minister in March 2012 (Saleh, 2013).

Yemen's revolution: slow and steady

When the Tunisian and Egyptian revolutions erupted, Yemen's own revolution followed, but its results were coming at a slower pace than the rest. From the outset, Yemenis had lower ambitions when they started their first protest, which was mainly calling for improved economic conditions, and for tackling corruption and unemployment. The first large-scale protest took place in Sana'a on January 27, when thousands of Yemenis marched through the streets of the capital Sana'a, followed by even bigger protests a week later on February 3 (Hatem & Salam, 2011). Those protests triggered Yemen's own critical juncture, which started setting the country on a different path than the one set by the authoritarian regime of Saleh.

One of the key events marking this critical juncture occurred on March 18 in 2011, when a sniper attack in Tagheer Square in Sana'a' killed over 50 peaceful protestors including children and led to a state of emergency. The assault resulted in the first serious cracks in the Saleh regime with the defection of major military commanders including second-in-command General Ali Mohsin, who broke ranks with Saleh citing violence against unarmed protestors (Boone, 2011). The rift within the army weakened

Saleh considerably and led to clashes between pro-Saleh Republican Guard units and Central Security Forces on the one hand and armed groups loyal to Mohsin and other pro-revolution tribal factions on the other (Zirulnick, 2011).

The downward spiral in Saleh's grip on power continued steadily until on June 3, 2011, Saleh was severely injured and many of his aides killed in an attack at the mosque inside the presidential palace in Sana'a. While receiving medical treatment in Saudi Arabia, Vice President Abd Rabbuh Mansur Hadi served as Acting President (Bakr, 2011).

Despite surviving the explosion, Saleh was considerably weaker and under pressure from the Gulf Cooperation Council (GCC) and strengthening protests. So he eventually succumbed and signed a GCC-sponsored power transfer deal in Jeddah on November 23, 2011 (Rashad, 2011). Saleh officially handed over the presidency to Hadi on February 27 after the latter won a symbolic one-man presidential election on February 21, 2012, with a relatively high turnout of 6.6 million (Jamjoom & Almasmari, 2012).

I argue, however, that this internationally backed power transfer deal may have set the country on a path away from dictatorship and toward building an electoral democracy. The degree of free speech and political debate has increased significantly since then while it remains to be seen whether this path will continue to produce more democratic participation or would change course just as what happened in Egypt.

Since leaving power, Saleh largely faded away from the political scene with occasional appearances in his capacity as head of the former ruling party, the General People's Congress. Since the transfer of power took place, some steps were taken in a long thoroughly planned transformation to a full electoral democracy with decentralized rule. By the end of 2012, the coordination committee of the National Dialogue Conference had established its mandate to start discussions in relation to the shape of the future state and draft the constitution (Al-Kibsi, 2012). The implementation of the GCC initiative has thus far continued with no serious flaws (MacFarquhar, 2013) and is planned to continue well into 2014 when parliamentary and presidential elections are expected to take place (Al-Samei, 2012).

Syria

Ba'athist Syria: where repression is the norm

When Bashar Assad inherited Syria from his father Hafez Assad in 2000, he also inherited a complex and deeply rooted set of apparatuses known for their brutality and violence committed in notorious prisons (Halaby, 2012) or in undisclosed less-known underground torture chambers (Mcdonald-Gibson, 2012). Since the 1963 coup d'état, the Arab Socialist Ba'ath Party has ruled the country with an iron fist based on a socialist, secularist, and pan-Arab nationalist ideology and depending mainly on the religious Alawi minority (Pipes, 1989). Upon seizing power, the Assad regime imposed an emergency rule, which justified arbitrary arrests, prosecutions and detentions targeting activists and opposition figures and entities (Moiles, 2012).

While human rights were mostly disregarded by Syria prior to the Arab Spring, the situation has reached unprecedented levels since March 2011, with a study revealing that torture and human rights violations against civilian men, women, and even children have been carried out in a widespread and systematic manner (Black, 2012). Bashar's rule was already on the authoritarian path set by his father and the Ba'ath Party since 1970. As the Assad family's attaining of power did not come through a democratic process, their political legitimacy was questioned by various opposition groups, which mostly had to operate in exile due to the oppressive nature of the regime with some subjected to assassination attempts even abroad (Zahler, 2009, p. 66). There were no critical junctures that could be identified to have changed the political direction of the country even after the Arab Spring.

Despite having over 22 mentions of the word "freedom," the Syrian constitution has not created any adequate levels of freedom on the ground (Heller, 1974). Freedom of speech had been heavily restricted before the Arab Spring and became yet more restricted afterward. The 2001 Press Law gave Syrian authorities the right to arbitrarily deny, revoke publishing licenses or enforce pre-censorship on newspapers. Crackdowns on journalists have been repeated on the grounds of protecting national security, and a ban of newspapers coming from certain countries reflected a strong tendency of censorship (Freedom House, 2010c). Although Assad had ordered the lifting of the state of emergency that was in force for about fifty years and initiated the constitutional amendments to allow political pluralism to emerge, those steps were not expected to improve the conditions of

freedom in the country, nor were they expected to end the numerous human rights violations (Macleod H., 2011a). And, similarly, the new Press Law that was approved in 2011 following the Syrian uprising did nothing but increase the number of journalists that were harassed or detained (Zein, 2011).

The culture of fear created in Syria made strong self-censorship the norm, particularly with the many restrictions in the 2001 Press Law. Some the law's articles imposed fines that could go up to one million Syrian pounds as well as a jail term that could range from one to three years. Under the Press Law, any speech challenging national sovereignty or security or offending public morality is punishable regardless of the medium used (Freedom House, 2010c). Lawsuits for defamation are filed frequently and criticism of the government could lead to fines, harassment, and even dismissal from public sector positions. Among the most severe forms of free speech repression, however, are those that specifically target minorities such as Kurds, who are prohibited from importing Kurdish-language publications (Ziadeh, 2009).

As most publishing houses are owned by the ruling Ba'ath Party, the ability of dissident voices to challenge the government through the media is not possible. Democratic debate about government policy is rare and does not include sensitive topics in relation to the president or the Ba'ath Party. Security agencies, which are immune from judicial prosecution and operate independently of the judiciary, are known for torturing suspects to extract information and admissions or targeting relatives including family members (Freedom House, 2010c). And since they are not easily identifiable among crowds, secret agents create a sense of fear in society and prevent open public debate about political issues, which is exactly what happened in May 2011 when secret police swarmed Damascus ("A Correspondent in Syria," 2011).

Cultural restrictions against Kurdish minority are particularly salient due to the nationalistic orientation of the Ba'ath Party, which has also established a norm of excluding Kurdish leaders and their families from public sector employment, and many Kurds lack necessary documents for travel outside the country (Ziadeh, 2009). Human rights activists and relatives of exiled dissidents are also prevented from traveling abroad. The Syrian regime's systematic weakening of internal opposition resulted in having a predominantly exiled dissident movement, which has failed to unite itself due to several competing factions including Kurds, Islamists, liberals, moderate Sunnis, and others (Lund, 2012). The opposition re-

mains weak in the face of a repressive Syrian regime that maintains a strong grip on the media and economy, particularly with its economic alliance with Iran and Russia (Landis & Pace, 2007).

Using the Internet in an oppressed society

Syria was very slow in introducing the Internet to the public after the country got hooked on the global network in 1997. The main concerns cited at the time included security issues, which made the service initially get to a very limited number of state institutions, and even then, the service was highly restricted (Goldstein, 1999, pp. 55–56). It was only after Bashar Assad inherited the presidency from his father in 2000 that the Internet started to boom, as it grew from having just around 30,000 users in 2000 to over five million in 2012, which represented about 22.5% of the Syrian population (Internet World Stats, 2013c).

For Syria, the Internet grew by leaps and bounds since Bashar started his policy of developing communication infrastructure and services, a strategic move meant to develop the economy and research community. The growth of the Internet in such a short period of time has contributed to giving it a status of importance that I argue is on par with Egypt for a significant number of sectors, including the Syrian government itself, which uses the Internet to reach to the masses and prop up its information propaganda and targets is opponents in a virtual cyberwar (Watson, 2011). And, hence, it is plausible to consider that the country has indeed undergone the critical juncture that made reversing the growth of the Internet unlikely.

Despite this growth, however, Syria remained the most regulated country in MENA as the network infrastructure remained under the control of the Ministry of Telecommunications and Technology through its Syrian Telecommunications Establishment (ONI, 2009). Although the Syrian regime did invest in the telecommunication infrastructure and allowed Internet services to be provided by private companies, it indirectly controlled those operators through restrictive regulations depriving those private ISPs from being independent. Rami Makhlouf, who owns of the biggest Syrian ISPs, SyriaTel, which is a private company that operates a wireless 3G GSM network, is in fact the first cousin of President Assad (US Department of Treasury, 2008). Overall, the country remained in a state of corruption and inefficiency, signaling a missed opportunity for reform (Schmidt, 2006).

With the rise in Internet penetration, the level of restrictions on freedom on the Internet also rose and manifested itself in the pervasive Internet filtering practiced by the state, which has blocked numerous dissident and anti-Assad websites as well as globally renowned platforms such as Facebook and YouTube (ONI, 2009). The Syrian regime intensified its repression on the Internet and found its place on RSF's "enemies of the Internet" list along with Tunisia and Egypt. The international media-freedom-monitoring watchdog labeled Syria as an Internet enemy for its pervasive Internet filtering as well as for measures it was regularly taking against bloggers and activists through arrest, harassment, and other repressive practices (RSF, 2010). Syria was also engaged in surveillance and prosecution of online activists such as the blogger Tariq Biassi, who was sentenced in May 2008 for three years for posting an article criticizing security agencies and for allegedly "spreading false information" and "weakening national sentiment" (p. 27).

Nonetheless, Syrian activists were able to formulate pressure groups and use campaigns via the Internet despite censorship because of their ability to master the use of censorship circumvention tools including open proxies. By using proxies located in other countries, activists were able to bypass the firewall and reach blocked social networking websites such as Facebook and media-sharing websites like YouTube so as to publish content on behalf of imprisoned bloggers, to campaign for boycotting some mobile operators and to reject proposed repressive laws (pp. 26–27).

The harassments that online bloggers suffered from prior to the Arab Spring were insignificant compared to the atrocities committed against citizen journalists and bloggers after the Syrian uprising and throughout the civil war. While 2011 witnessed the killing of at least ten citizen journalists and online activists, the number surged to almost fivefold in 2012 with the killing of at least 49 (RSF, 2013). This is in addition to unnumbered cases of imprisoned, wounded, or kidnapped online journalists. The sudden rise was mainly attributed to the fact that traditional journalists were banned from going into Syria for reporting, which meant that most news reports had to come from citizen journalists (Arnold, 2012). It was also reported that Syrians who communicate with foreign news media may be detained, tortured, or even killed. So it was often necessary to ensure that devices used to send news content are clean from malware and that data transfers are made with strong encryption. Otherwise, local sources may run the risk of being identified, tracked, and targeted (Galperin, 2012).

From a potential revolution to an all-out civil war

Following the fleeing of Ben Ali of Tunisia and resignation of Mubarak of Egypt, Syrians took to the streets in Daraa in March 2011 protesting the arrest of schoolboys between the ages of 10 and 15 who had used graffiti cans to write political statements similar to those that Egyptians and Tunisians had been using in their calls for the end of the regimes in their countries. Hundreds of protestors were gunned down by government forces. But that did not stop protests from growing exponentially mainly to call for saving the residents of Dara'a, the release of political prisoners, and the end the state of emergency. Mourners in funerals of killed protestors were also targeted and killed by snipers. This resulted in an ongoing vicious cycle that promised continued violence. Along with using force, the government issued a decree on March 24 to cut taxes and raise state salaries by 1,500 Syrian pounds per month (Macleod H., 2011b).

With protests starting to pick up pace and confronted with gunfire from snipers and police forces across Syria, chants started to call for bigger demands including the end of the Ba'athist regime, which were followed by a decree from Assad on April 21 ending the state of emergency for the first time since 1963. His decree also regulated the right to peaceful protest, and dissolved a state security court known by lawyers to have violated the rule of law and prevented fair trial (Oweis, 2011). However, violence continued with an intensified wave of defections of military and government personnel followed by mounting international pressure in May and August when the United States imposed sanctions and froze Syrian government assets (Myers, 2011). Meanwhile, the number of dissident military officers reached a critical mass, which resulted in forming the "Free Syrian Army" in July and, hence, transforming the popular uprising from an unarmed peaceful revolution like those that took place in Tunisia, Egypt, and Yemen to an all-out civil war similar to the one that developed in Libya (Karam & Kennedy, 2011).

The Syrian regime became more isolated when Saudi Arabia, Kuwait, and Bahrain recalled their ambassadors to Syria in August 2011 citing escalating violence (Derhally & Abu-Nasr, 2011). Additionally, the EU took a decision to ban oil imports and impose additional sanctions in September 2011 (LaFranchi, 2011). After receiving support from several countries, the Syrian National Council was formed in Istanbul in September as the formal body representing Syrian opposition and was meant to coordinate with opposition rebels on the ground to secure a transfer of power from the Assad regime, which warned against recognizing the new

council (Carey & Peker, 2011). However, as rebels fighting the Assad forces were not united, it was quite difficult to find consensus on how to represent the entire opposition before the international community (Lund, 2012).

The Arab League members voted in November to suspend Syria's membership and freeze assets belonging to the Syrian regime and impose sanctions and travel bans (Fielding-Smith, 2011). The Arab League-imposed sanctions were also adopted by neighboring Turkey, which has been accused by the Syrian regime of allying with the opposition to overthrow Assad (Yanatma, 2011). Despite holding Syrian local council elections in December, violence continued to escalate amid dismissals of the elections by opposition groups (Zavis & Sandels, 2011). Initiatives to reduce violence by sending Arab League monitors to Syria in January 2012 failed as casualties continued to climb to unprecedented levels, reaching more than 5,400 fatalities according to the United Nations (Fahim & Bakri, 2012).

The Syrian regime's isolation was eased when Russia and China vetoed in February a UN Security Council resolution condemning the Assad regime's violence against civilians and highlighting an international rift that made handling the rapidly deteriorating situation very difficult (Lynch & Fordham, 2012). As another attempt to ease the situation, Assad then initiated constitutional amendments to convert the political system in Syria to a political pluralist system with direct popular voting and with a presidential term of seven years and a one-time reelection possibility (Chulov, 2012). Assad removed articles in the old 1973 constitution that gave absolute powers to the Arab Socialist Ba'ath Party, and which gave the party the right to nominate a presidential candidate and have him elected in an uncontested popular referendum (Heller, 1974). The amendments eventually passed with an overwhelming majority in an unmonitored referendum held on February 26, 2012 (Chulov, 2012).

Through a mission spearheaded by former UN General Secretary Kofi Annan, who brokered a UN-sponsored cease-fire agreement, UN monitors arrived in Syria in April to ensure the implementation of the deal by Assad and the opposition forces (Weaver M., 2012). However, the deal did not last long as violence escalated to reach its peak when over 100 civilians including fifty children in Houla were killed in a massacre that resulted in international condemnation and the expelling of Syrian diplomats from several European countries as well as the United States, Australia, and Canada (Charlton, 2012).

With the civil war escalating and with the international rift continuing, the level of violence and destruction continued to rise, and by January 2, 2013, the death toll, according to the UN, had exceeded 60,000 with over half a million internally displaced (Hubbard & Jordans, 2013). Furthermore, while hundreds of thousands of Syrian refugees were struggling to survive amid cold winters on the borders with Turkey, Jordan, and Lebanon, a further influx of hundreds of thousands was expected, which was expected to lead to over one million refugees in the first half of 2013 (Sweis, 2013).

It is worth mentioning that the Syrian situation has a higher potential—compared to the other three countries studied—of turning into a sectarian internal or regional conflict due to the fact that the Assad family belongs to the Alawi Shiite sect while the majority of the Syrian population is Sunni. This could also trigger support for the regime from Shiite forces in the region including Iran and Hezbollah and could equally result in sectarianism being a motivating factor for some Sunni radical religious factions to fight Assad forces, Hezbollah, and Iranian bases or camps that may come into the country (Sherlock, 2012).

It remains to be said that despite all these internal and external factors, the Syrian regime—as of late 2012—proved to be more resilient than the other three case studies. It was apparent that its choices were limited, particularly if the crimes it committed are to be considered war crimes or crimes against humanity. Indeed, the level of atrocities the Syrian regime had committed raised the possibility of having it tried by an international tribunal, which may have been a strong motive for not handing over power to a transitional government (Walt, 2012).

Part III

The Findings

Chapter 6: General Findings

The findings presented in this chapter help answer all questions by treating Arab countries as a unit. To answer the second question concerning patterns of censorship and circumvention, however, a deeper analysis is provided in the next chapter dealing individually and comparatively with the four case studies of Tunisia, Egypt, Syria, and Yemen.

This chapter starts with general observations about Alkasir's usage, followed by more detailed sections that include the findings necessary to answer all the five research questions.

Observations of Alkasir Usage

When I wrote my first PhD proposal in 2008, the situation regarding Internet censorship in the Arab world was quite troubling as shown from research done by the findings by Deibert, Palfrey, Rohozinski, and Zittrain (2008). It was apparent that authoritarian Arab states, which are known to practice various forms of repression in the physical world, started to clamp down on activism in the virtual cyberspace. Therefore, it was found useful to give an overview of the situation when Alkasir started operating and how it was perceived and used during 2010–2012.

Global overview

While I had already understood that by late 2010, over a couple hundred Tunisians were using Alkasir to bypass censorship of Facebook and other Tunisian dissident websites, the real breakthrough was in Egypt when for just a couple of days, specifically during February 25–27, the Egyptian government filtered a few websites. After the start of the Arab Spring in early 2011, Alkasir usage had surged, and part of the reason behind that may have been wider media coverage[86] of the software such as when it was mentioned in a brief story on CNN, highlighting it as a tool used by Egyptian activists to bypass governmental digital firewalls during the initial stage of the uprising (Dougherty, 2011). With this new fame established, the number of users of Alkasir rose steadily; this occasionally brought too many simultaneous users, straining the Web and proxy servers, which were originally not meant to handle a high number of users.

[86] Find some links to online resources that Alkasir received in the 'Links for reference' section at the end of Appendix A.

By 2012, Alkasir had become a well-established circumvention tool with international recognition and had a Wikipedia page created in April 2011 (Wikipedia, 2011). With a higher number of users, it was also possible to get more empirical data for this study, as users of Alkasir came from 123 countries. Figure 1 shows a map reflecting where Alkasir users came from as of October 2012,[87] which is the last month for data collection from Alkasir's data server in relation to this study. The number signaled a significant increase from the sixty-four countries represented when data collection started in October 2010. The map corresponds to those countries where users had to download, install, and successfully run the program.

Figure 1: Countries (in gray) where Alkasir users come from (October 2012)

It is to be noted that while users came from many countries around the world, there were particular countries that had many more Alkasir users than others. This is expected, because some countries had higher levels of censorship than others, and while in some countries such as the United States, Alkasir can be useful for users who attempt to bypass filters at particular institutions, for example, libraries and schools, such usage dif-

[87] More users from an additional 15 countries have been added by December 2013.

fers in objective and scope compared to usage in countries with nationwide censorship. Table 4 provides some general information about the users' location (whether in an Arab country or not), the interface language used (Arabic or English), the total number of websites submitted so they could be accessible, the total number of unique URLs that were approved, and the total number of times approved URLs were accessed using the internal browser.[88]

	Arabic interface	English interface	URL submissions	Approved URLs	Visits
Arab countries	18,368	13,842	34,216	1,594	4,747,986
Non-Arab countries	1,509	39,013	121,717	2,005	2,507,049

Table 4: General overview of Alkasir's global usage as of October 1, 2012

Given that Alkasir was originally established as a solution aimed at helping Arab citizens access blocked content, it was no surprise to see that 19,877 (27.2%) out of the total of 72,732 users, used the Arabic interface. Despite being only 44.3% (32,210) of the total, users in Arab countries used the internal built-in browser to access blocked websites almost twice as much as users in non-Arab countries, who used external browsers for that purpose. I believe this as a natural consequence of having the software developed by an Arab activist and researcher and providing native support for Arabic language both in the client's interface and the website in addition to answering questions sent through the website or by email in Arabic when the original questions came in Arabic.

Furthermore, while it was predictable to find the majority of users in Arab countries going for the Arabic interface of Alkasir, it was interesting to notice 1,509 users from outside the Arab world, who constitute 3.7% of the total, deciding to use the Arabic interface. While the available data do not explain why this was the case, one explanation could be that the Arabic interface may have swayed Arab expatriates to use it to circumvent censorship in non-Arab countries. And given that Alkasir was intrinsically created for Arab users, this hypothesis appears to have some merit. Anoth-

[88] This number of visits only corresponds to those visiting blocked websites using the internal browser and does not include those using external browsers.

er explanation could be that Alkasir may have been running on top of another circumvention tool, such as a VPN that is based in another country. When this occurs, Alkasir cannot tell if the user is using a VPN, and so it simply assumes that he/she is located in the in that country where the connection comes from.[89]

Changing usage dynamics

During the two-year period when Alkasir's usage was examined, access to Alkasir's website varied widely as shown in Table 5, which identifies the top ten countries in terms of user accesses, with every access considered a successful start of a new session on Alkasir. Those numbers are cumulative, meaning that they are incremented for every new access, and so they will constantly grow. A major factor behind those changes is the changing dynamics of censorship in the country in question. An example of that is Tunisia, which witnessed the lifting of censorship in early 2011.

By October 2010			By October 2012			
Rank	Country	Accesses	Rank	Country	Accesses	Change
1	Saudi Arabia	46,406	1	**Iran**	**1,471,088**	↑ **+8**
2	Tunisia	34,113	2	**Syria**	**958,548**	↑ **+3**
3	Yemen	32,107	3	**USA**	**151,164**	↑ **+5**
4	China	18,164	4	Yemen	123,120	↓ **-1**
5	Syria	13,826	5	Saudi Arabia	69,710	↓ **-4**
6	Bahrain	4,322	6	China	48,740	↓ **-2**
7	UAE	4,075	7	Tunisia	47,962	↓ **-5**
8	USA	2,986	8	UAE	27,170	↓ **-1**
9	Iran	2,774	9	**UK**	**23,830**	↑ new
10	Libya	2,740	10	**Germany**	**15,756**	↑new

Table 5: The changing dynamics of Alkasir's usage during 2010-2012

[89] I have received feedback from several users who have been using HotSpot Shield VPN software among other circumvention tools and occasionally, this leads to confusion concerning the actual location of the user.

In 2010, however, Tunisia was known to be one of the most restrictive governments when it comes to Internet filtering. As can be seen on the table, this meant that its usage has dropped after censorship ended in 2012 because users no longer needed to use the software in Tunisia.

It is important to note here that while the United States does not have nationwide censorship, Alkasir continued to be of value throughout this period to users interested in overcoming specific restrictions at the ISP level throughout the United States. And given that the United States does not block alkasir.com and because it does not restrict the use of censorship circumvention tools on the national level, the availability of Alkasir among other tools made it accessible and usable freely. Furthermore, some users may have used Alkasir on top of a VPN that is usually based in the United States, giving Alkasir the IP address and geo-location of the VPN instead of the real country. Nonetheless, the United States is still ranked a distant third, far behind the first two countries, Iran and Syria. Similarly, the UK and Germany do have a place on the list, but their usage is dwarfed in comparison to the top two.

On the other hand, the reason why Saudi Arabia and China have dropped significantly in October 2012 despite having the top two positions in October 2010 is mainly due to intervention by ISPs in those countries to block access to Alkasir's website and/or proxy servers. The interrupted access to Alkasir was meant to limit the possibility of having the software work in those countries.

One way of restricting access to Alkasir is by blocking access to alkasir.com, and it was verified through Alkasir itself that multiple ISPs in Iran, China, Syria, Yemen, Columbia, and Nigeria have resorted to that option. In countries where alkasir.com is blocked, it is categorized as a circumvention/proxy solution by filtering software such as Websense, which considers alkasir.com as one of many proxy websites "that provide information about how to bypass proxy server features or to gain access to URLs in any way that bypasses the proxy server" (Websense, n.d.). This prevented users from accessing the website from the outset. And while this is bad news for potential users in those countries, it is a testimony to the effectiveness of Alkasir in challenging technical Internet filtering regimes.

To grant access to users affected by those measures, a workaround was devised in a way that would allow Internet users to download Alkasir despite the website's inaccessibility. It was still possible to obtain the software by sending an e-mail to get@alkasir.com, which will send back an automatic response containing a secure and accessible link to the package

along with English instructions. Similarly, sending an e-mail to get-ar@alkasir.com would result in Alkasir's server to automatically send a reply with a link along with Arabic instructions. This mechanism is effective because Web-based e-mail transactions, such as Gmail, Yahoo, and others, are processed on the secure webmail servers and not by the local ISPs. This makes it extremely difficult to block e-mails from being sent and received. Furthermore, e-mail requests are handled on Alkasir's server, which allows modifying the links to send in the auto-respondent mode if needed. Furthermore, alkasir.com had a membership base of over 10,000 subscribers, who could be informed at any moment by a mass notification e-mail that could include a newsletter or announcements. For those subscribers who can no longer access alkasir.com because of censorship, it is still useful to keep this membership as a bridge to exchange information and advice on the best methods to circumvent censorship and to get steady feedback from users.

Besides blocking access to alkasir.com, two countries, namely, Saudi Arabia and China, went the distance and blocked Alkasir's proxy servers, on which the software relies to provide users with access to censored content. This meant that even if the software is already running in those countries, it would not be able to connect to the proxy servers, which may render Alkasir useless in such situations. Trying to overcome the blocking of Alkasir's proxy servers, however, was a more difficult task, as it required providing users with a special encrypted code through which they could plug into Alkasir to grant them access to a private proxy server that the authorities have not yet blocked and do not know about. Although this alternative method is less prone to being disabled by governments, it does require manual intervention from both sides, that is, Alkasir and the affected user, which has proven to be an extra step that almost all users in those affected countries were not prepared to take.[90]

As shown in the last table (Table 5), when the governments of China and Saudi Arabia created those obstacles to access Alkasir, they succeeded in limiting the number of users from those countries significantly. Perhaps what triggered their move was the fact that users in those countries started to successfully use Alkasir widely, and there are documented cases where instructions on how to use Alkasir were written in foreign languages by

[90] More information about how the private proxy works is available in the technical report (Appendix A).

users in those countries, which helped further expand the software's reach.[91]

Those developments confirmed the findings of the study by Palfrey, Roberts, and Zuckerman (2011), who highlighted the difficulties that circumvention tool developers were increasingly facing because of the more vigilant and aggressive government steps to try to disable such tools from functioning. However, as the table shows, there was a simultaneous expansion of Alkasir's user base in countries that did not yet impose any forms of censorship on alkasir.com or its proxy servers. By far, Iran and Syria are the two countries with the largest share of Alkasir users and have a wide margin between them and the other countries. Iranian users have been particularly keen on providing tips and instructions in Farsi to others who wish to install the software and use it to circumvent censorship in Iran.[92] However, it may be just a matter of time before those countries too end up following the footsteps of Saudi Arabia and China, emphasizing the need to develop better blocking-resistant mechanisms.

Internet Filtering

From the theoretical framework and literature review, it was identified that Internet censorship could be technical mainly in the form of Internet filtering or nontechnical censorship methods such as harassment and server takedowns. As the first question of this study asked about the forms and mechanisms of Internet censorship in the Arab world, it is useful to start with the practice of Internet filtering because it was said to be the most dominant form of technical censorship. Measuring this form of censorship can give a general picture of what websites were found to be blocked at least once during the period of this study.

URL submissions and approvals

Alkasir's data identified significant level of Internet censorship in most Arab countries, with some countries being more pervasive than others. Table 6 shows those countries sorted by the number of unique URLs found to have been blocked at least once by one ISP, and those URLs were found to not be of nudity/pornographic content, so they were approved.

---

[91] See https://www.google.com/search?as_epq=alkasir+com&lr=lang_zh-CN for a list of Chinese pages that refer to alkasir.com's use.

[92] See https://www.google.com/search?as_epq=alkasir+com&lr=lang_fa for Farsi pages referring to alkasir.com

The value of FCL is not taken into account in this table, which also shows those URLs that were rejected because they belonged to the nudity/pornography category. The higher the approval rate, the more aggressive ISPs and users in the country are in focusing on political and informative content rather than on adult content.

The countries with approval ratios that did not exceed 50%, namely, Oman, Iraq, Qatar, and Egypt, have all, except for Egypt, not had substantial activity through Alkasir. Egypt is an exception because its usage was concentrated during the specific period of January 25–27, 2011.

Despite very clear instructions stating that Alkasir does not accept submissions of pornography and nudity websites, as they do not meet its policy,[93] many users still submitted such websites. While Alkasir had to reject those websites, it was able to collect raw data that were used to conclude that censoring content that the society may find inappropriate, such as pornography, was practiced in all examined countries except Algeria and Palestine.

Country	Approved URLs	Rejected URLs	Approval rate	Blocking ISPs	Transparency level
Syria	654	42	94%	61	54%
Saudi Arabia	182	83	69%	64	81%
UAE	100	93	52%	30	53%
Yemen	95	53	64%	13	1%
Tunisia	70	22	76%	5	0%
Bahrain	59	27	69%	21	87%
Sudan	18	16	53%	14	4%
Libya	15	6	71%	3	0%
Jordan	12	10	55%	36	29%
Kuwait	10	1	91%	20	34%
Oman	9	62	13%	7	78%
Qatar	8	12	40%	10	0%
Egypt	7	29	18%	14	45%
Palestine	5	1	83%	1	100%
Algeria	1	0	100%	2	0%

Table 6: Arab countries with detected Internet filtering

[93] See Alkasir's submission policy here: https://alkasir.com/policy

The transparency level indicated on the table corresponds to the percentage of cases where access to a URL is clearly identified by the ISP to be forbidden with a page that usually includes a message describing why the URL is blocked.[94] While some Arab countries toward the top of the list have shown considerable Internet filtering, those at the bottom did not.

Furthermore, there are some countries with higher transparency as they provided the rationale behind censorship, for example, Saudi Arabia, Palestine, Bahrain, Oman, and, to some extent, Syria, while the others with lower transparency appear to have consciously decided to confuse the viewer so he/she would not know for sure if the website was blocked or was unavailable for some other—perhaps technical—reason, for example, technical problems or server time-out. Furthermore, countries with very few ISPs such as Mauritania, Palestine, Algeria, Libya, and Iraq make verifying filtering in those countries challenging due to the limited number of users. Therefore, it was important to give more weight to countries that had more ISPs than others that had few.

Nationwide filtering

When it comes to assessing the possibility of nationwide filtering of websites, the number of URLs starts to drop as we seek higher FCL values as shown in Table 7. For countries that have high numbers of ISPs, this is particularly challenging, as it means that Alkasir needs to run on computers connected to most if not all ISPs in the country to increase the confidence in nationwide filtering. On the other hands, having a small ISP number is also problematic, because even if the value of FCL is high, it cannot give a proper assessment of national censorship due to the small sample size.

The best approach to identify the likelihood of nationwide filtering is to start by filtering out the countries that do not have at least two ISPs. This would result in eliminating Palestine and Mauritania from our data.

[94] When accessing a filtered website in some countries, it was possible to get a clear 'Access Forbidden' page, which is technically called a 403 page. On other occasions however, the page would not indicate if the website was intentionally blocked or if there was some other reason, e.g., server timeout, technical error, missing page, etc., that prevented the website from appearing. The table identifies this as 'transparency' and the more transparent a country is when filtering, the higher the number of transparent responses. Notwithstanding, this data may not be 100% accurate but serve as an estimate because there may be cases where the response was not obtained properly, e.g., a real technical issue.

Thereafter, we need to also consider the period when Alkasir was quite active. The shorter the period, the more difficult it would be to guarantee a high FCL value.

To take the case of Egypt, for example, we see that the period was quite short and the act of filtering started and ended within a few days. Even if users were to verify censorship by February 28, they would have been unable to do so because the Internet itself was cut off that day. So it would still be reasonable to consider a value of FCL higher than 25% and lower than 50% to represent the minimum threshold to consider possible nationwide censorship. This would also naturally require that the number of ISPs taken into account is at least two.

Country	FCL < 25%	FCL ≥ 25%	FCL ≥ 50%	FCL ≥ 75%	ISPs
Saudi Arabia	38	144	127	40	64
Syria	447	207	129	26	61
Jordan	11	1	1	1	36
UAE	49	51	28	1	30
Bahrain	14	45	42	28	21
Kuwait	7	3	1	1	20
Sudan	13	5	4	1	14
Egypt	5	2	0	0	14
Yemen	23	72	39	9	13
Qatar	2	6	6	3	10
Oman	5	4	1	1	7
Tunisia	1	69	66	64	5
Libya	0	15	6	0	3
Algeria	0	1	2	1	2
Palestine	0	5	5	5	1

Table 7: Number of filtered URLs and FCL levels for Arab states

Syria, Bahrain, Tunisia, and Yemen had dozens of blocked URLs that had FCL values over 50%, which is quite reasonable to assume as a threshold in identifying which of those websites were probably blocked across the country.

There is certainly a margin of error involved particularly with cases that Alkasir may have mistakenly assumed a website blocked while it was the

website management itself that was responsible for the blocking. This is, however, an infrequent occurrence and should not affect the overall reliability of the data, particularly for the countries with many ISPs and high FCL values. The four example countries that have been studied in this project, that is, Syria, Tunisia, Egypt, and Yemen, all had significant FCL values, which made statistical analysis of their filtering data quite productive and rewarding.

Commonly blocked websites

Although Internet filtering is best understood when taking into account the context and specific conditions of the country in question, the available data did reveal some websites that were interestingly blocked in more than one Arab country. By far, the most commonly blocked websites were pornography websites. However, because Alkasir does not allow the use of its servers for accessing pornography, they will not be described in this study. Table 8 lists the ten websites that were filtered in more than one country.

#	Website	Number of countries where filtering was detected		Individual ISPs blocking it
		FCL>0	FCL ≥ 0.25	
1	facebook.com	8	3	51
2	youtube.com	6	4	70
3	arabtimes.com	5	5	147
4	hotspotshield.com	4	3	83
5	skype.com	4	4	71
6	metacafe.com	4	2	45
7	oovoo.com	4	3	31
8	ultrareach.com	4	3	26
9	el7ad.com	3	3	99
10	anhri.net	3	2	83

Table 8: The most commonly blocked websites in the Arab world

The number of countries does not necessarily imply that they were censored nationally but it might have been an individual decision by a particular ISP. In addition, when the value of FCL ≥ 0.25, it means that at least a quarter of all of the ISPs that were used to connect to Alkasir servers in the country have blocked it, which indicates that it has indeed captured the attention of the government. The number of individual ISPs that carried out the filtering is useful to get an idea of how aggressive filtering was for each site.

I hereby provide some description of each of those websites and a context to help highlight potential reasons[95] behind their censorship:

1) **facebook.com**

   Eight countries—Syria, Egypt, Libya, Yemen, Mauritania, Jordan, Algeria, and Palestine—had at least one ISP that filtered Facebook at least once during the period of this study. The filtering may have not been nationwide for all countries. However, Syria and Egypt have confirmed evidence that filtering happened nationally, while in the other countries, the filtering was limited to a particular set of ISPs. As the world's leading social networking platform, Facebook's role in the Arab Spring was significant in mobilizing anti-government activities as highlighted in earlier chapters. It is therefore of no surprise to have the website targeted by some Arab regimes. This action could be attributed to the fear of the authoritarian regimes of having their political legitimacy continuously challenged or undermined through anti-government content that is published by anonymous sources using pseudonyms. For most countries, however, blocking Facebook would prove costly and unproductive in the long run due to its prominent position as one of the most widely visited websites in the world based on the Alexa[96] rankings and because both government and activist camps are keen to utilize it for their own goals.

2) **youtube.com**

   Cases of filtering of youtube.com were found in Syria, Libya, Saudi Arabia, Jordan, Sudan, and Tunisia. The website has been a

[95] The reasons provided are tentative and are based on the reviewed literature and theoretical framework as well as on personal understandings of the context and should not be seen as definitive.

[96] Alexa is a website ranking service provided by Amazon that utilizes its browser plug-in to track website traffic.

major source of information about atrocities, protests, and various other important events during the Arab Spring. Motives behind blocking access to YouTube.com could be seen in similar light to the blocking of Facebook.com as it has a complementary role in providing the audiovisual content that is often shared on social networks. Just like facebook.com, this website's content is created by users, making it difficult to track down the original producer and preventing replicating the content, which could be dissident in nature.

3) **arabtimes.com**

Having been found to be blocked in Saudi Arabia, the UAE, Oman, Syria, and Jordan, arabtimes.com is a satirical and scandalous online news website mainly targeting royal Gulf families and Arab leaders. It has also been the most aggressively targeted website given the large number of ISPs that blocked it (147 in total). Being based in the United States gives its owners protection from being targeted by those regimes, which eventually resort to blocking access to prevent the public from viewing stories that may undermine the regimes' legitimacy, particularly as the website often includes content that exposes corruption and other issues that the regimes would not want their citizens to know about. It also boasts on its website of being "The only known website to be censored in Jordan" (Arab Times, 2003).

4) **hotspotshield.com**

As the website of the US company AnchorFree, hotspotshield.com provides free VPN services to the public to bypass Internet censorship and was found to be blocked in Syria, Qatar, Saudi Arabia, and the UAE. The VPN software that is downloaded from this website has been in operation for a long time and gained a strong following. This study has found that their VPN software is indeed among the most commonly used in the Arab world.[97] It is obvious that Arab regimes that practice censorship strived to also block proxy avoidance websites in general to prevent the public from reaching forbidden content.

5) **skype.com**

As one of the most popular VOIP solutions for communication over the Internet, Skype's website was found to be blocked in Syr-

[97] More about this is available in the survey findings section.

ia, the UAE, Kuwait, and Oman. Apart from Syria, only Gulf countries appeared concerned about the use of Skype, and this can be understood within the commercial and security aspects, because accessing Skype to call internationally allows the bypassing of the international telephone carrier and results in losses, as well as the bypassing of potential spying and eavesdropping that some authorities could use for security purposes or to monitor some activists.

6) **metacafe.com**

This is another video-sharing platform similar to youtube.com but it has an additional section that contains pornographic content but in a well-marked part of the website. Metacafe.com was found to be blocked in Saudi Arabia, Syria, Egypt, and Tunisia. Given that it has both a standard generic video-sharing platform and one that allows the dissemination of adult content suggests the protection of cultural and religious values to be the rationale, which is a relevant justification in Saudi Arabia. However, its potential in promoting dissident and oppositional content could be seen as another motive that enticed the authoritarian regimes of Tunisia and Syria to block it.

7) **oovoo.com**

This is the website of the popular ooVoo video chatting cross-platform application that can be downloaded and used for international communication. It was found to be blocked in Yemen, Syria, Oman, and the UAE, and while it is similar to Skype in function, it is more oriented toward mobile devices. The motives to block it are similar to those for Skype.

8) **ultrareach.com**

This website is filtered in Qatar, Syria, Tunisia, and Yemen, and was the gateway to gaining access to free censorship circumvention software Ultrasurf, which is a popular circumvention tool—like hotspotshield.com—in many Arab countries. The rationale behind blocking it is the same as for other circumvention websites. Governments work relentlessly to ensure that proxy avoidance tools are restricted to prevent them from reaching too many Internet users, as that could spell the end of the effectiveness of the national firewall.

9) **el7ad.com**

The word "el7ad" is إلحاد, the Arabic transliteration of "atheism," and serves as the website of the self-proclaimed "Arab Atheists Network," which promotes and discusses atheism and other controversial religious issues through an open discussion forum. Given its outright conflict with religious rule in Arab countries, it was blocked by Saudi Arabia, the UAE, and Syria. Along with arabtimes.com, the website appears specifically targeted to Arab audiences. Another atheist website, ladeenyon.net[98], is also blocked by multiple countries, indicating that it has become a policy by a few Arab states to block some anti-religion websites.

10) **anhri.net**

As the official website of the Cairo-based Arab Network of Human Rights Information, anhri.net is known for its strong advocacy of human rights issues through regular reports exposing human rights violations in the Arab world. The website was blocked in Bahrain, Syria, and Saudi Arabia, three countries with dismal human rights records. This shows that some Arab regimes are uneasy about critical reports about their human rights records and are willing to block access to such websites to prevent their public from learning about those violations.

It is worth noting that the websites mentioned above may well be blocked in other Arab countries not mentioned in the table because the data are limited by the activity of Alkasir users in reporting blocked websites. For the 1,594 URLs reported and approved during this period, it means that users were motivated enough to take the effort and report them using Alkasir's built-in submission interface so they could become accessible. Limits to free speech, as argued in the Theoretical Framework Chapter, can be legitimately imposed if the speech in question meets the conditions set by the Milliam principle, which require imminent direct danger. However, I argue that none of the ten websites are inherently dangerous to society, and while context in each specific country is important to consider, the blocking of those websites is not justifiable purely based on the potential harm they could bring to the general public or the country. Therefore, their censorship is indeed a violation of free speech. This makes Alkasir's mission in enabling users to reach them a step toward upholding free speech.

[98] Ladeenyon is the transliteration of 'لا دينيون', which means 'those with no religion'.

Censorship tendencies based on category

Upon compiling the websites that have been blocked in more than one Arab country, those websites were then categorized based on the taxonomy described in the Theoretical Framework Chapter. Each website was given three categories. The first defines what service the website provides and this could be one of four: commercial, information, community, and interactive. The second identifies the general type of content and could be static, server-managed, user-driven, or query-based. The last step involves a deeper level of classification that requires selecting one of the categories identified in the Methodology Chapter. By identifying the taxonomy of each of those websites and aggregating the results, an interesting pattern starts to emerge. Figure 2 shows the number of countries that were involved in censoring websites based on the service those websites provided and with a value for FCL greater or equal to 0.25.

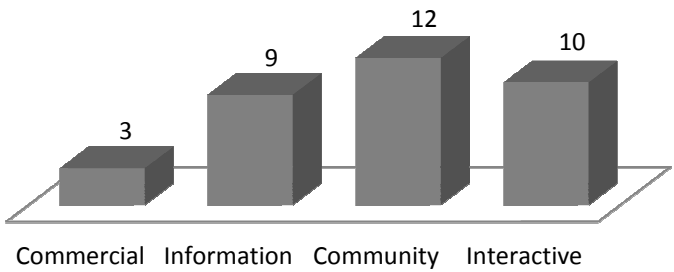

Figure 2: Arab countries blocking common websites categorized by type of service (FCL ≥ 0.25)

Websites providing services for building and encouraging online communities such as social networking websites were found to be the most commonly blocked content, with twelve countries blocking them. As indicated in the top ten most commonly blocked websites, Facebook stands as a clear example that Arab regimes are willing to limit access to such platforms. This further solidifies the conclusion that authoritarian regimes are uneasy about websites that allow communities to share and exchange content publicly as they do not have any control over such content.

Coming second with ten countries were interactive websites with their capacity to empower the public by providing new means of communication such as VOIP services that allow citizens to eliminate the need to use public telephony services and proxies that allow users to overcome censorship. Those tools are powerful for coordinating among activists without

governmental oversight. In an authoritarian system, not knowing what activists, dissidents, and others are up to is a grave vulnerability. When such communication tools come along, they eliminate the possibility for monitoring, which is a strong enough reason to have them blocked. This is in addition to the financial loss a state could incur due to the shying away of citizens from using public long-distance calling services in favor of free online alternatives. A close second with nine countries was information websites, which include those such as anhri.net and other news, oppositional or dissident websites, which provide information that the governments may not want the public to view. Meanwhile, websites providing commercial types of services such as shopping websites were apparently not seen of a grave threat.

While the earlier figure showed what service the blocked websites were meant to deliver, the general content category explains who is responsible for the creation of the content. Figure 3 shows the number of Arab countries that blocked common websites based on the main content type.

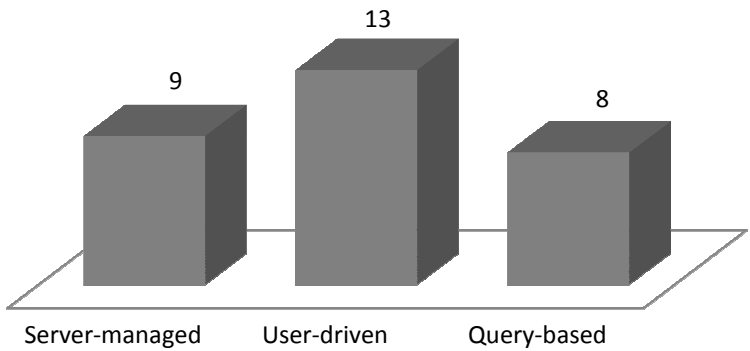

Figure 3: Arab countries blocking common websites categorized by type of content (FCL ≥ 0.25)

Websites with user-driven content types such as Facebook, YouTube, discussion groups, etc., were blocked by thirteen countries, which is by far more than any other content type. Server-managed websites including those by critical opposition websites or human rights groups came second with nine. The last group of query-based websites such as circumvention tools and communication websites gained considerable attention, making it a close third. What this implies is that Arab governments are eager to stop access to websites with content that is generated by the public. The

attention paid to user-driven media was apparently greater in comparison to the other two groups, that is, server-managed and query-based.

The final stage of classification involved probing deeper into each individual website to see what the content is all about. Upon combining websites into common categories and measuring how many countries block each category, Figure 4 emerges with fascinating results, showing that social networking websites lead the way with thirteen countries.

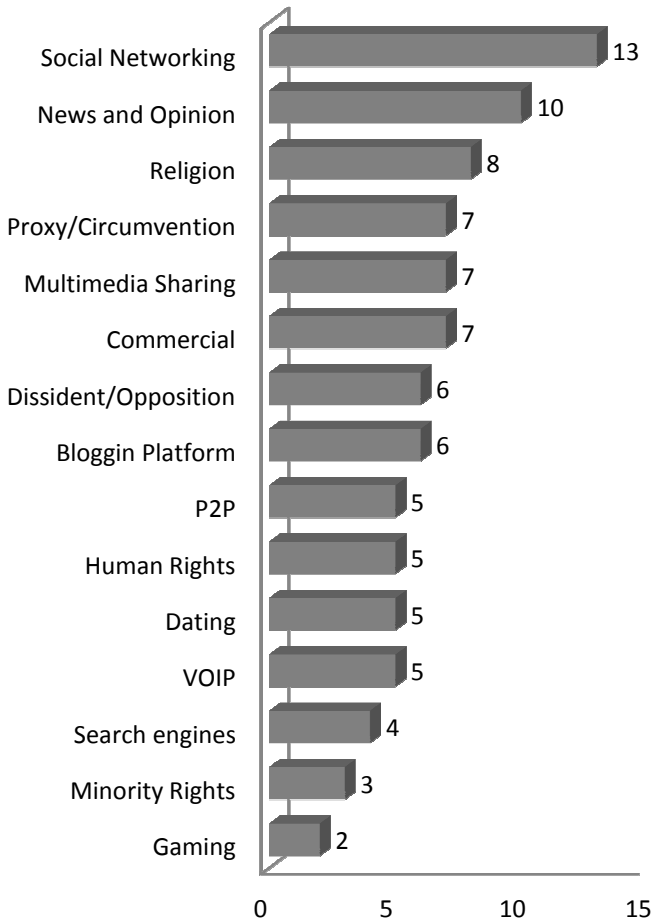

Figure 4: Blocking categories based on number of countries

They are followed by news and opinion websites, which often include critical content that goes a long way. Thereafter, anti-religion or religiously fundamental websites come third, followed by proxy and circumvention websites, followed by commercial and multimedia sharing websites such as youtube.com. The other categories have fewer countries so analyzing them would be best done on the country level.

The next section attempts to put the pieces together in order to better understand what those findings entail particularly to the question of motives behind censorship.

One Common Nemesis of Arab Authoritarian Regimes

From the earlier section that analyzed the most common blocked content in terms of URLs, service, content type, and content categories, it became apparent that some Arab regimes share some common fears, and although each of those countries may not have coordinated what websites they are blocking, they ended up blocking similar categories of websites. And the most censored websites they were eager to censor were not those managed by exiled dissidents, nor were they the vocal human rights websites exposing governments' poor records, nor were they the providers of various query services such as VOIP or even circumvention tools. What the data show is that governments see the biggest threat as their own citizens, who are active on user-driven websites.

This finding would appear natural given the booming social media, the increasing ability of users to mobilize campaigns, the anonymous posting of critical content, the exposing of corruption, and the publishing of other revealing information the regimes do not want to be known. The main problem for regimes supposedly is that user-generated content is produced by individuals with elusive or anonymous virtual identities. When an online user is not identified, he/she cannot be held targeted through prosecution or other forms of pressure. We can contrast them to managers of server-managed websites, who are formally responsible for the websites' content and who could easily be targeted and silenced through judicial and extrajudicial measures. It is somewhat similar to summoning the editor of a news website to remove content, or otherwise he/she would face a diverse set of possible penalties that governments can pick and choose from.

But when it is an open platform for users from various directions, authoritarian Arab regimes cannot always find whom to target and how to stop particular online content from being published. So they eventually go for blocking the particular URL that is causing problems or the whole

server where it is hosted. This shows that regimes are worried about getting dissident content out to the masses without prior approval. And hence, citizen journalism content, for example, in the form of a blog post or a Facebook page post or a tweet are deemed more dangerous to authoritarian regimes than any other form of online content. And if we can just imagine a time when government censorship of user-driven content becomes ineffective due to strong circumvention tools, this power of active cyber activists or dissidents may well turn into a threat to those authoritarian regimes. In some ways, it may well become a game changer in terms of the governments' ability to control what citizens publish or access.

When Arab states took the decision to invest in telecommunication infrastructures and expand Internet connectivity for all sectors of the population, including regular citizens, those steps were aligned with the recognition by the UN that the digital content industry contributes heavily to produce a knowledge-based economy that could support Arab national economies tremendously (ESCWA, 2012).

The governments effectively encouraged the use of the Internet in areas of crucial importance such as telecommunications, health, education, business, and government services. This meant that reversing the growth and influence of the Internet no longer was a viable option. And so, when the social media started to become effective in distributing anti-regime content, governments resorted to Internet censorship instead.

In the next section, I present some of the findings in relation to the technical and nontechnical Internet censorship that Arab governments utilized.

Technical and Nontechnical Internet Censorship

In this section, I examine the various technical and nontechnical Internet censorship mechanisms that Arab content producers were exposed to during the period of the study. I started in the last section by using Alkasir's own data, which helped shed light on one of those methods, namely, Internet filtering. However, to identify the other forms of technical and nontechnical filtering, the two surveys deployed during the period of this study were used.

The first survey was put online before the Arab Spring, as respondents were able to access it during May–December 2010. The second survey was accessible during July–December 2012, which is well after the Arab Spring started. The two surveys contain the same questions except that the second has additional questions related to the Arab Spring. Some of the questions

were formulated with help from literature by Murdoch and Anderson (2008), who have indicated that prosecution, intimidation, threats, malware attacks, surveillance, and other forms of acts were meant to censor publishers of content. One could also call such acts pre-Internet forms of censorship as they have been used well before the Internet came to be. But governments simply applied them to bloggers and other online activists, resulting in the notion of nontechnical censorship.

There are two groups which authorities can target to suppress free speech on the Net. One is Internet users at large and who could be dealt by limiting their access to particular content using Internet filtering, which may affect large communities and cause particular harm to content publishers whose content was censored. And the second group would be content producers living in the country in question, and they would include website managers, bloggers, and citizen journalists. Targeting the latter group would be accomplished through various technical and nontechnical methods ranging from sending malware to legal prosecution.

The two surveys combined had a total of 4,212 responses, out of which 3,017 or around 72% were from the Arab world. As this study deals with the Arab world, only the 3,017 cases were considered. Given that the context in December 2010, when the first survey was closed, has changed drastically compared to the context in October 2012, which marked the end of the second survey, I have decided to take each survey results independently for some of the questions and analyzed the combined results for others. The rationales behind those decisions are explained as appropriate.

Results from the first survey (pre Arab Spring)

When the first survey was released in May 2010, Alkasir had just started gaining publicity and was working quite smoothly in many countries, allowing it to gather a significant number of respondents during May–December 2010. When the survey was closed, it had already collected responses from 3,017 respondents in 21 Arab countries, that is, all the twenty-two Arab countries except Mauritania.

It is important to note at this stage that among the 3,017 respondents that are based in the Arab world, the highest number of respondents come from Yemen. This is attributed to the fact that Alkasir was originally, as noted in Appendix A, aimed at assisting Internet users in Yemen to access my website http://yemenportal.net. From the initial look at the cases of the second survey, this appears to have changed dramatically, with Syria tak-

ing the lead, leaving Yemen far behind as a distant second. This reflects the change that occurred in the user base of Alkasir from 2010 to 2012.

Table 9 shows[99] that the absolute bulk of the respondents were men (91%), which is a stark reminder of the digital gender divide discussed in the Background Chapter. It came as no surprise that there would be more men than women respondents, but one possible explanation of this sheer gap between the two may be because using Internet censorship circumvention tools—such as Alkasir—could be seen as an act that combines activism, Internet usage, as well as some limited technical skills needed to identify, install, and use such tools. The intersection of those three areas, which are male-dominated in the Arab world, is what could explain this large gap. This divide could be understandable, given that men in the Arab world are more likely to use software and connect to the Internet (Neagle, 2013). While delving into the reasons behind this gender gap is important for the development of free speech on the Internet, it is beyond the scope of this particular study.

Age	20 or under	**168**	6%
	21-30	**1,157**	41%
	31-40	**996**	35%
	41-50	**340**	12%
	over 50	**176**	6%
	No answer	162	6%
Gender	Female	**257**	9%
	Male	**2,714**	91%
Place of most frequent Internet access	Home	**1,564**	60%
	Work	**505**	19%
	School/Institute	**22**	1%
	Café	**263**	10%
	Mobile	**31**	1%
	Laptop (wireless)	**236**	9%
	No answer	297	11%
	Other	35	1%
Average Internet usage		**27.3 hours/week**	

Table 9: Characteristics of the first survey respondents (2010)

Furthermore, most participants were between 20 and 50 years and most accessed the Internet from home (60%). The average use of the Internet was 27.3 hours per week, which indicates an average of just around four hours daily. Among those respondents, there were 940 who managed a

[99] Not all fields are compulsory so the total may not necessarily add up to the same number as some respondents decided to fill some questions while skipping others.

blog, a website, or some other form of online content. The breakdown of the types of websites they managed is shown in Table 10.

Country	Blog	Dissident	News	HR/activism	Forum	Aggregator	Other	Total websites	Total managers	*N*	Ratio
Algeria	7	0	1	0	0	0	6	14	13	37	35%
Bahrain	35	4	6	4	2	9	37	97	71	222	32%
Comoros	0	0	0	0	0	0	0	0	0	1	0%
Djibouti	2	0	0	0	0	0	2	4	4	6	67%
Egypt	11	5	8	4	5	5	21	59	38	120	32%
Iraq	2	1	0	0	2	1	1	7	4	14	29%
Jordan	15	2	2	4	2	2	9	36	22	57	39%
Kuwait	11	4	3	3	4	4	13	42	24	56	43%
Lebanon	0	0	0	0	0	0	5	5	5	7	71%
Libya	13	1	0	0	0	0	0	14	14	63	22%
Morocco	9	0	0	1	1	0	9	20	18	48	38%
Oman	7	0	0	2	2	2	8	21	19	66	29%
Palestine	3	0	0	0	0	0	2	5	5	10	50%
Qatar	11	6	2	2	0	0	11	32	27	68	40%
Saudi Arabia	73	9	17	11	7	8	54	179	131	489	27%
Somalia	2	0	0	0	0	0	0	2	2	6	33%
Sudan	12	0	0	2	0	0	5	19	19	50	38%
Syria	67	3	16	3	3	10	57	159	141	406	35%
Tunisia	20	4	6	9	7	4	19	69	41	108	38%
UAE	12	0	3	3	1	9	37	65	58	193	30%
Yemen	118	23	38	24	44	29	122	398	284	990	29%
Total	**430**	**62**	**102**	**72**	**80**	**83**	**418**	**1,247**	**940**	**3,017**	**31%**

Table 10: Website managers who responded to the 2010 survey

Among the most important questions asked to survey respondents was if they managed a website[100] or blog. In response to that question, almost a third (31%) said they did, which illustrates that a significant portion of Alkasir's users appear to be using it to manage websites and upload con-

[100] The definition here is not meant to be a domain. A website can be a page on a domain containing millions of pages. For example, a Facebook page administrator is also a website manager as he/she controls material on a Web page and produces content.

tent to blogs or Facebook pages. Furthermore, the fact that there were 1,247 websites managed by the 940 respondents indicates that some managers managed multiple websites. This has also been verified through a number of personal communications with some users.

When breaking down answers to see what types of websites the respondents were managing, it became apparent that the largest and most dominant group was blogs. And a "blog" here could be a website with its own domain name or one that is hosted on blogging or social networking platforms (blogspot.com) or a page on a social networking platform (a Facebook page). Those are the user-driven websites of which some authoritarian Arab governments are wary because they are not institutionalized and can often be quite critical. The second largest group was news websites covering local and other events as well as providing opinion articles.

A significant number of eighty-three aggregators were also managed by respondents, and those are websites that collect news and articles—sometimes automatically—from other websites and serve as a place where a variety of perspectives are allowed to be published. Respondents managed eighty discussion forum websites, which are easy to set up and can be quite engaging but usually require heavy moderating especially for popular ones.

Human rights and activism websites managed were seventy-two and, in general, they are websites that promote the rights to access to fair trial, freedom of expression, rights of minorities, mobilizing the masses for campaigns to release prisoners, etc.

There were also sixty-two websites identified as dissident, meaning that they promote anti-government content and aim at challenging the regime. Although this is the smallest group, it remains one of the most actively pursued by Arab governments, as indicated in the earlier section. It is to be noted, however, that a high number of websites was categorized as "other," and this is probably because their managers did not find any of the categories suitable, which may be the case for websites such as sport, file-sharing, P2P, etc. Another reason could simply be privacy or security concerns, which is understandable.

When it comes to exposure to censorship, results, and shown in Table 11, indicate that out of the 940 respondents, 377 indicated that they were exposed to some sort of nontechnical censorship ranging from attacks to legal prosecution and from surveillance to kidnapping.

Nontechnical censorship

	Occurred	At risk	No answer	Don't remember	Not at risk
Legal prosecution	72 (24%)	29 (10%)	66 (22%)	46 (15%)	86 (29%)
Kidnapping or illegal detention	58 (19%)	27 (9%)	78 (26%)	49 (16%)	87 (29%)
Harassment, threats, and hostility	67 (22%)	36 (12%)	70 (23%)	50 (17%)	76 (25%)
Torture of physical violence	52 (17%)	41 (14%)	72 (24%)	52 (17%)	82 (27%)
Surveillance (wiretapping, etc.)	64 (21%)	40 (13%)	70 (23%)	59 (20%)	66 (22%)
Other forms of pressure	64 (21%)	31 (10%)	76 (25%)	59 (20%)	69 (23%)
Total	377	204	432	315	466

Technical censorship

Internet filtering	110 (37%)	31 (10%)	61 (20%)	54 (18%)	43 (14%)
Traffic attacks (DDoS, etc.)	79 (26%)	36 (12%)	59 (20%)	69 (23%)	56 (19%)
Virus, Trojan, worm, etc.	82 (27%)	37 (12%)	55 (18%)	63 (21%)	62 (21%)
Compromised login information	80 (27%)	26 (9%)	59 (20%)	83 (28%)	51 (17%)
Domain taken over	62 (21%)	24 (8%)	73 (24%)	87 (29%)	53 (18%)
Other forms of technical pressure	58 (19%)	22 (7%)	75 (25%)	73 (24%)	71 (24%)
Total	471	176	382	429	336

Table 11: Responses on nontechnical and technical censorship (2010)

Additionally, 471 responses indicated that they have at least once in the last 12 months suffered from some form of technical censorship ranging from filtering to viruses and from domain takeover to compromised credentials. What is also of concern is the fact that there were other respondents who have not suffered from some of those practices but said they felt threatened and at risk of being exposed to one of those forms of censorship. The highest form of censorship was torture or physical violence.

These results confirm previous research and highlight the difficult situation of free speech on the Internet in the Arab world. While these numbers are not possible to verify individually due to the fact that the survey was filled out anonymously, they provide empirical data that help contribute to the available body of literature.

The dismal image of free speech indicated in the context analysis chapter of this study has been verified empirically with these findings, pointing to the authoritarian tendencies of regimes actively suppressing content they regard as threatening, and they do so using technical and nontechnical methods.

Furthermore, an interesting additional finding was the correlation spotted between the level of technical and nontechnical censorship in Arab countries. To calculate this correlation, two independent variables were computed using the data from the survey. The variables were called censorship levels, and one corresponded to technical censorship while the other corresponded to nontechnical censorship, and the value for each was calculated as follows:

$$\textbf{\textit{Censorship level}} = 2 * \left(\sum_{i=0}^{6} c_i \right) + \sum_{i=0}^{6} t_i$$

where (ci) corresponds to the affirmative answer to the question of having been exposed to the particular form of censorship and there are six types of censorship, while (ti) corresponds to the affirmative answer indicating the risk of being censored. The first value is multiplied by two to give it double the weight of the risk.

For the thirteen countries examined, the overall results in Table 12 showed a stronger degree of technical censorship compared to nontechnical censorship in all countries except Qatar and the UAE. However, a number of countries still had a high level of nontechnical censorship such as Bahrain, Egypt, Tunisia, and Yemen, which does correspond to a large degree of repression and prosecutions happening in those countries prior to the Arab Spring.

And as the correlation appears rather strong, it shows that Arab regimes generally tend to take a comprehensive offline and online approach when restricting speech online. One other major question asked was whether those forms of censorship that a particular respondent suffered from or is at risk of may be attributed to the political[101] or security[102] con-

[101] Political content is meant to be news or views on the regime or government, human rights, freedom of expression, corruption, elections, minority rights, religious movements, etc.

[102] Security content is often that which deals with war reports, inner conflicts, rebel movements, separatists, militants, resistance movements, etc.

tent that he/she was publishing online. Just over half (54%) of the 119 persons who answered this question believed it is definitely or probably true that they were victimized because of their political writing, while less than 9% believed that they were not.

Country	Technical censorship level	Nontechnical censorship level
Yemen	981	734
Tunisia	243	143
Bahrain	199	118
Egypt	125	104
Syria	89	28
UAE	86	100
Oman	78	62
Kuwait	76	20
Saudi Arabia	60	47
Djibouti	60	10
Libya	30	12
Iraq	30	8
Qatar	22	64
Pearson's correlation coefficient $r = 0.989$, correlation significant at the 0.001 level ($n = 13$)		

Table 12: Technical and nontechnical censorship in Arab countries and their correlation (2010)

All the 940 were also asked how frequently they published political or security content. And a correlation analysis was done in 299 cases between the frequency of publishing political content and the overall level of censorship, which is calculated by adding the technical and nontechnical censorship levels. The analysis resulted in a Pearson's correlation r value of 0.212 and a two-tailed significance value of less than 0.001, indicating a statistically significant positive correlation. This in fact verifies from two independent variables answered by the respondent that the more political content is published, the more likely that producers of content will be exposed to censorship. An additional Pearson's chi-square association analysis has shown that the degree of censorship that a website manager is exposed to is directly associated with the type of website he/she manages.

Although the association as shown in Table 13 is significant for all types ($p < 0.001$), the highest association was in the case of managers of dissident content, which is another way to verify that governments are targeting opposition websites through Internet filtering or DDoS attacks and their managers through intimidation, legal prosecution, or other nontechnical pressure more than any other website.

Although this was to be expected, these data give empirical evidence from website managers themselves. However, when it comes to websites containing critical news content, it appears that website managers were targeted directly through nontechnical censorship rather than filtering. On the other hand, discussion forum websites ended up being the victim of technical filtering more than news websites. This result could be interpreted in light of the distributed liability of a discussion forum, which is user-driven and open to all those willing to post critical or controversial political views, and so there is no single responsible individual for those views. The forum administrator does have a moderator role, however, which explains that he/she is also targeted through nontechnical censorship. But filtering is the easiest method to block access altogether. On the other hand, news websites are server-managed and, hence, the sole liability and responsibility falls on the website manager. In other words, the news website manager is under the spotlight, and when a critical article angers an Arab authoritarian regime, it is easy to know whom it will pursue in order to remove the objectionable content willingly or suffer the consequences.

Type of website	Nontechnical censorship level (df: 20)	Technical censorship level (df: 19)
Blog	225.0*	187.6*
Dissident	441.4*	370.2*
News	351.0*	261.9*
HR/activism	285.0*	260.8*
Forum	321.9*	337.0*
Aggregator	285.8*	254.7*
Other	103.5*	109.4*

(*$p < 0.001$)

Table 13: Pearson's chi-square analysis for the level of censorship and type of website (2010)

This could be understood when considering that repressive practices against traditional media were done routinely in Arab states, and so the structures that regimes are eager to control are those whose management is known and easily identifiable, putting greater risk on news websites that do not deploy any anonymity advantage that the Internet provides to hide their identity. In cases where the government is able to pursue the owner of a website, nontechnical methods of censorship—such as prosecution and threats—are more effective. But in cases when the ability to use nontechnical methods is limited, due to having the website manager in exile or when the content providers are anonymous, then the more effective method to suppress the content would be through technical censorship.

What is interesting to note at this point is that the second least targeted type of websites appears to be blogs. Initially, this may appear odd, given that bloggers are targeted constantly in many countries. However, it is also important to take into consideration that it too is being targeted but not as urgently or strongly as the other groups. There are reasons that could explain this. The first is that bloggers have the ability to mask their identity and use pseudonyms while news and other popular websites have known individuals behind them. Furthermore, the outreach of personal blogs and potential readership may be seen as lower than established news websites. Finally, blogs can be hosted on powerful servers such as Google's blogspot.com blogging platform, or as a Facebook page. Those give additional protection to the blogger from being targeted technically, because blocking or launching a DDoS attack on a and popular domain like Facebook is too costly in return for blocking access to a page on it.

Censorship as a Result of Political/Security Content

When it comes to the impact caused by nontechnical Internet censorship, survey results, shown in Figure 5, indicate that among the 119 respondents, about 54% said they believe that the nontechnical censorship they were exposed to was definitely or probably due to the political/security content they published. In contrast, just around 9% said their political contributions surely or probably were not the cause of the censorship they have been exposed to.

What this demonstrates is the belief among a significant portion of website managers in the causality between the political commentary, news, and other forms of content they publish on their website and harassment, intimidation, lawsuits, and other forms of nontechnical pressure.

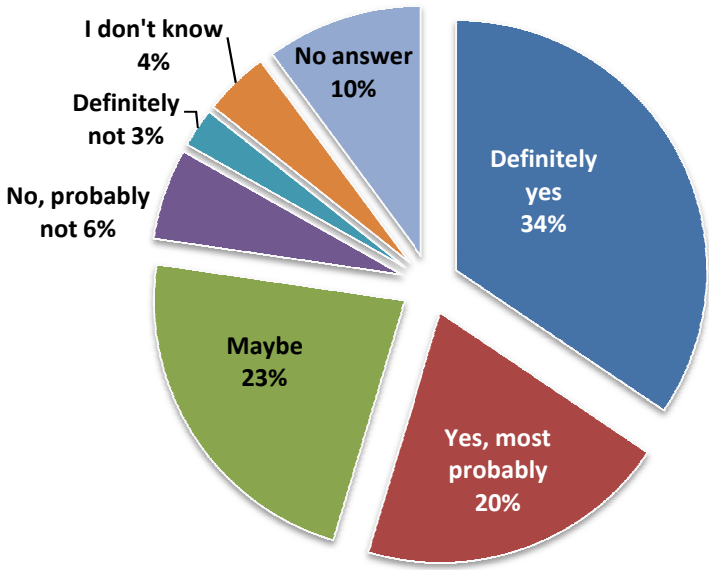

Figure 5: Survey responses to the question on whether nontechnical censorship was caused by political/security content (n = *119) (2010)*

A remarkably similar result, reflected in Figure 6, emerged upon analyzing answers from 145 respondents, of whom just over half (74) indicated their belief that technical censorship in the form of Internet filtering, targeted attacks, etc., was due to the political content they published. However, a significant portion exceeding 28% was unsure about the reason behind such censorship.

This is quite predictable as cases of harassment, lawsuits, and physical violence usually always result in identifying the cause behind such acts, while motives behind censoring websites and sending viruses may not be clear to the victim, particularly if he/she is not fully aware of the technology used and lacks the motivation to do more research and explore what those technical attacks could be caused by.

The results further verify the theoretical stance that authoritarian regimes are mostly concerned about content that has a political implication, something that could affect their political legitimacy negatively even if it contains content from other sources. When contrasted to traditional me-

dia, it is apparent that the lack of meaningful national jurisdictions on the Internet gives websites an advantage in not having to meet any of the rigid conditions that apply to political/security content based on penal and press laws. In several Arab countries, it is possible to establish private audiovisual media, but while they are largely free to broadcast various types of content, they are prohibited from broadcasting news or political content, and even when they are allowed to do so, they need to abide by rigid restrictions (Karlekar, 2009, p. 15). This policy allowed authoritarian regimes in the region to control information on press and broadcast media, but appear to be less successful on the Internet.

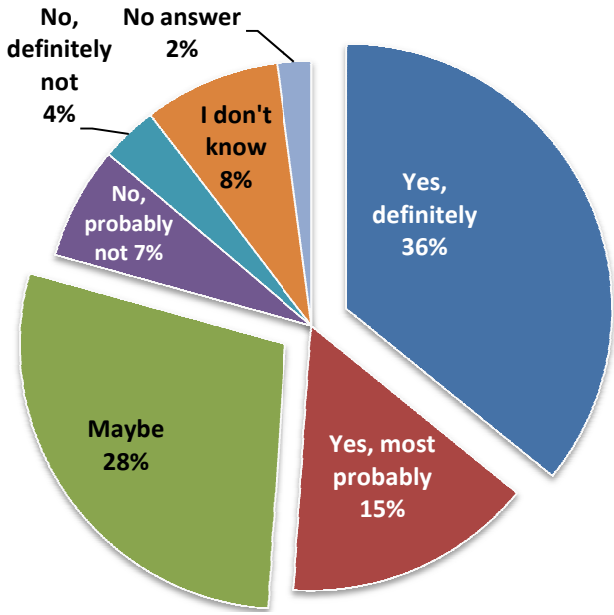

Figure 6: Responses to whether technical censorship was caused by political/security content (n = *145) (2010)*

This suggests an important role that cybersecurity and technical education plays for website managers. Cybersecurity risks to website managers are constantly increasing. But they are not because of government targeting alone, but also because malware and other cyber attacks are on the rise in the Middle East and around the entire world (Faris, Roberts, Heacock, Zuckerman, & Gasser, 2011).

When asked if those blocked sites included dissident content, the results shown in Table 14 indicated that only 20% indicated that the blocked websites had no dissident content while 16% of the total indicated that all websites blocked in their country included dissident content.

All blocked websites have dissident content	184	16%
Most blocked websites have dissident content	207	19%
Some blocked websites have dissident content	271	24%
A few blocked websites have dissident content	229	21%
None of the blocked websites have dissident content	225	20%

Table 14: Responses to the question on the share of websites containing dissident content (2010)

Those figures, albeit from the user's perspective, reflect an awareness of dissident content in the websites they know are blocked. The fact that 35% of the respondents indicated that the majority or all websites blocked had dissident content further solidifies the conclusion that governments are indeed targeting content that aims at criticizing them and, consequently, undermining their authority or legitimacy.

Effects of Internet censorship on users

Among the questions that were addressed by the survey was that about the impact that censorship has on website managers. Out of all respondents who answered that question, only about 29% (52 out of 179) and 21% (44 out of 210), did not see any effect by nontechnical censorship and technical censorship, respectively.

While fear and self-censorship, as shown in Figure 7, took the lead as the most devastating effect caused by censorship in both modes, what is noticeable is that nontechnical censorship was more effective than technical censorship in reducing the activity of the victims. When putting this into perspective, it does make sense for a blogger who has been prosecuted, beaten up, or threatened to reduce the volume of activity compared to a case when his/her website is blocked.

These results, albeit interesting, only give part of the story, because they portray the effects from the website content provider's point of view. To

get the perspective of the Arab user in general including those who do not produce content, the survey asked about the impact that Internet filtering in particular had on their experience when using the Internet. Out of 3,017 respondents, 1,116 (37%) indicated that they have indeed witnessed some kind of Internet filtering.

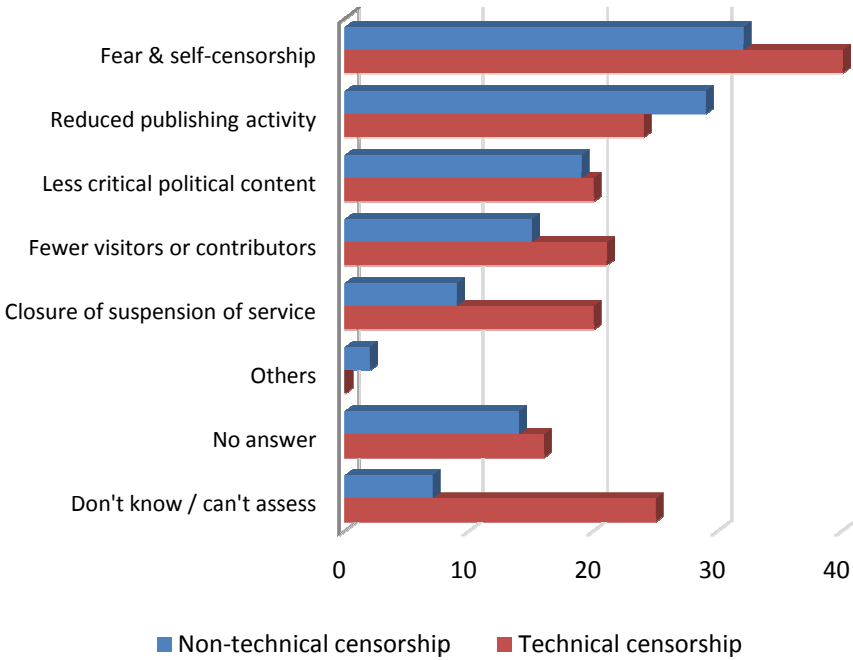

Figure 7: Nontechnical and technical censorship effects on content producers (2010)
(N = 179 for nontechnical censorship, N = 210 for technical censorship)

As shown in Figure 8, most respondents said that freedom of expression as well as access to information were the two rights most severely affected by restricting their access to websites. The third negative effect was on their ability to engage in social networking, limiting their community building abilities.

It is, however, information to consider that blocking a social networking website does affect the user's ability to express an opinion, get information, and socialize all at the same time.

While using the Internet for educational, entertainment, and other purposes was also negatively impacted, the results of this survey confirm the need for solutions to end censorship due to those negative effects. A circumvention solution such as Alkasir could partially help by allowing users to access news, social networking, and information websites, and, if possible, also allowing access to entertainment and other content. In the case of Alkasir, all those categories were allowed access to except pornography, which could be viewed as "adult entertainment," but given that Alkasir did not make it a priority, its sacrifice is not likely to adversely affect the freedom of users.

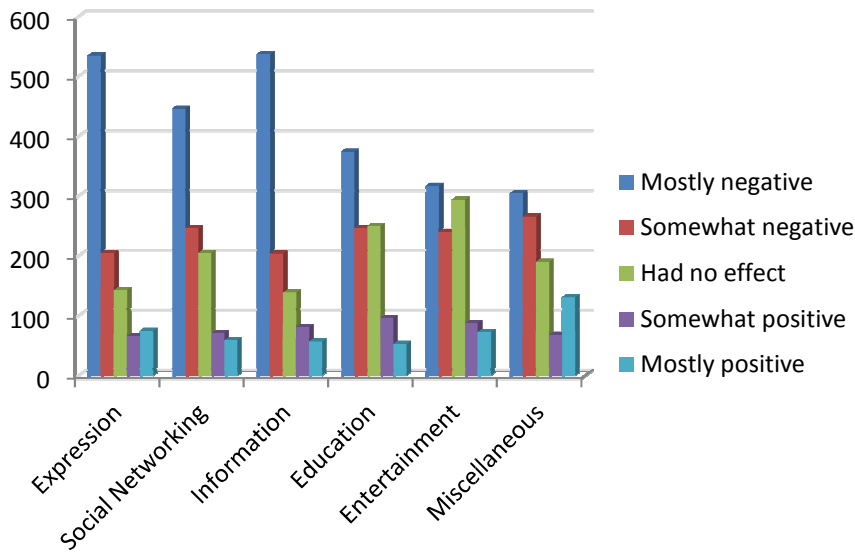

Figure 8: Survey results showing the level of impact of blocking websites that contain political/security content (2010)

Combined with earlier findings from the perspective of content producers, the lack of free speech on the Internet is hindering democratic participation, which prompts the need to support all efforts to end technical as well as nontechnical censorship.

This empirical finding indicates that governments violated citizens' ability to acquire information, which should be protected universally with

Article 19 of the UDHR. This connects directly to the arguments of the importance of free speech as a fundamental human right, as demonstrated in the theoretical framework. The lack of free speech could be perceived as a direct consequence of censorship, and the end result is depriving the public from the empowering benefits that free speech brings and which were articulated by many liberal thinkers that helped promote the universal values of free speech.

Results from the second survey (post Arab Spring)

While the first survey helped shed light on the situation of Internet censorship based on the perspective of Arab users and content producers before the Arab Spring, the second survey was meant to assess the situation after the Arab Spring had swept through the region, toppling four heads of state and shaking several others. The starting point is to emphasize that there were significant changes in the user base of Alkasir due to three main factors. First, Saudi Arabia had restricted access to Alkasir, as indicated earlier. Second, Tunisia and Yemen no longer practiced Internet censorship as they did in the past. Third, Alkasir was outpaced by a growing censorship circumvention market that offered a wider variety and more blocking-resistant solutions. Those factors resulted in a much smaller section of Alkasir that have responded to the survey. In fact, compared to 3,017 Arab respondents that responded to the first survey, only 692 responded, which is less than 25% of the first.

The characteristics of respondents, as illustrated in Table 15, were quite similar to the first survey. The majority of respondents in this survey also were men (85%), with

Age	20 or under	**78**	12%
	21–30	**279**	42%
	31–40	**186**	28%
	41–50	**80**	12%
	over 50	**36**	5%
	No answer	**6**	1%
Gender	Female	**102**	15%
	Male	**568**	85%
	No answer	**22**	
Place of most frequent Internet access	Home	**315**	47%
	Work	**119**	18%
	School/institute	**9**	1%
	Cafe	**45**	7%
	Mobile	**17**	3%
	Laptop (wireless)	**59**	9%
	No answer	**103**	15%
	Other	**8**	1%
Average Internet usage		**41 hours/week**	

Table 15: Characteristics of the second survey respondents (2012)

those between 21 and 50 years old constituting 82% of the total, and 47% accessing the Internet from home.

While there was a modest improvement of 6% in the number of female participants in the new survey, to be 15% of the total, it is quite telling that the area of censorship circumvention is male dominated. The gender divide identified in this survey remains wide but it has decreased by over

50%, which appears to be representative of the overall decreasing gender divide among Arab citizens in other areas such as literacy and tertiary education (Filali Adib, Driouchi, & Achehboune, 2013). This shrinking gap has also been documented when analyzing women's active participation in the protest movement as well as cyber activism during the Arab Spring (Kuhlow, 2013), which is supported by the findings that emerged from analyzing responses to this survey.

Furthermore, the survey results show a significant rise during 2010-2012 in terms of average Internet usage with 41 hours per week compared to twenty-seven in the first survey, marking a considerable 52% rise. Coupled with higher Internet penetration, the higher frequency of usage highlights a greater potential for the Internet to be used for mobilization political and social campaigns.

One other relevant finding was that a sizable percentage (15%) of respondents refused to identify where they access the Internet most frequently. Given the developments during the Arab Spring, this is understandable, as users may have become more aware of the need for protection from surveillance and to not be identified even though the electronic survey introduction made it clear that their data will remain private. Another observation is that there was a threefold increase in the usage of mobile phones for accessing the Internet. However, the ratio—of 3%—remains quite low and this may be attributed to the fact that running Alkasir and filling the survey required using a computer, and hence, it was likely that users without computers would not constitute a significant percentage of the respondents.

In The rise in frequency of Internet usage indicates an increase in connectivity using wired and wireless networks, which came at a time when strategic decision were taken by several Arab states to develop their telecommunication services and consequently expand Internet access to the public. And in accordance to path dependence theory, this suggests that the chosen path will not be easy to leave, suggesting that Internet penetration rates are destined to continue rising.

Table 16 lists the number of respondents in Arab countries that had at least one respondent. The table shows that the survey had no respondents from Somalia and Comoros, but had four from Mauritania, which had none in the last survey. Despite having a lower number of respondents compared to the first survey, the second survey still had 291 respondents who were managing at least one website.

When comparing the two survey results, the major difference that one can see from the outset is the significant drop in the number of respondents from Saudi Arabia, Yemen, and Tunisia as illustrated in Figure 9. As explained earlier, the drop in the number of users is probably due to Internet filtering practices being abandoned in Tunisia and diminished considerably in Yemen. On the other hand, Saudi Arabia's blocking of Alkasir resulted in a plummeting in the number of users.

Country	Blog	Dissident	News	HR/activism	Forum	Aggregator	Other	Total websites	Total managers	*N*	% with website management roles
Algeria	9	1	2	2	2	1	6	23	15	27	56%
Bahrain	2	0	0	1	1	0	2	6	6	15	40%
Djibouti	0	0	0	0	0	0	0	0	0	1	0%
Egypt	7	1	3	4	3	4	5	27	19	38	50%
Iraq	9	5	5	4	3	5	11	42	24	40	60%
Jordan	2	2	0	0	2	0	2	8	8	21	38%
Kuwait	0	0	0	0	0	0	1	1	1	6	17%
Lebanon	5	0	1	0	0	0	1	7	7	8	88%
Libya	2	1	0	0	1	0	2	6	6	13	46%
Mauritania	0	0	1	0	1	1	1	4	3	4	75%
Morocco	3	0	0	0	1	0	2	6	6	9	67%
Oman	1	1	1	0	0	0	1	4	2	9	22%
Palestine	1	0	0	0	0	2	5	8	8	19	42%
Qatar	4	0	0	0	0	2	2	8	6	10	60%
Saudi Arabia	6	2	1	1	2	1	7	20	15	32	47%
Sudan	2	0	0	0	0	1	0	3	3	16	19%
Syria	43	9	8	9	4	12	62	147	130	339	38%
Tunisia	1	0	0	0	0	0	1	2	1	2	50%
UAE	5	0	0	0	1	1	1	8	8	26	31%
Yemen	9	2	3	4	4	3	12	37	23	56	41%
Total	111	24	25	25	25	33	124	367	291	692	44%

Table 16: Website managers that responded to the 2012 survey

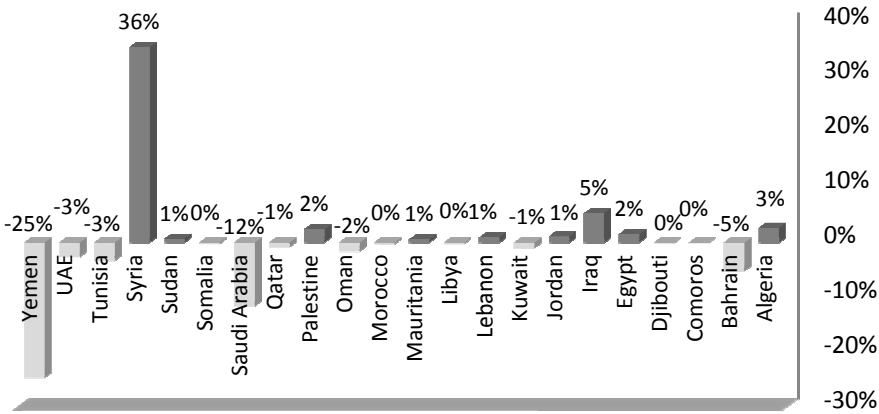

Figure 9: Change in the level of response from Arab respondents comparing the 2010 and 2012 surveys

However, the most significant change is perhaps the very high number of respondents from Syria, who constituted almost half of all cases. While it was possible to interpret the reasons behind the lower response rates for Saudi Arabia, Yemen, and Tunisia, the rise in number of Syrian respondents can be attributed to the increased level of Internet filtering practiced by the regime amid significant developments on the ground. This made Alkasir and other circumvention tools an important asset that could be utilized by activists and online content producers to access their censored websites during tense and critical periods of the country's ongoing civil war. As will be described in the next chapter concerning the specific case of Syria, not only was there a direct role for Alkasir in facilitating communication and publishing content about unfolding events and campaigns, but the software had also helped save lives in the most critical of moments when various online communication tools were blocked.

Meanwhile, the relatively lower response rate for the second survey compared to the first made the representation of Syria in the new survey stronger than all other countries. And while this may suggest that the response from Syrian activists would affect the reliability of the survey results, I have verified by taking a Pearson's chi-square association test that there was in fact no systematic difference between answers from a Syrian or a non-Syrian respondent to most of the questions concerning censorship practices. This was proven by doing the analysis for all technical and non-technical censorship questions, with the lowest p value being 0.082 for the

surveillance censorship tactic that Syrians appear to be most worried about. And so, this actually supports the conclusion that while different in their level of repression and system of government, Arab authoritarian regimes have cross-national similarities. Monarchs in the Gulf, Jordan, or Morocco as well as presidents in the rest of the Arab world have practiced at least one form of technical or nontechnical Internet censorship.

Similarly, Arab online activists and content producers of political content in different Arab countries also had cross-national similarities. Given the observations attained from this study's Literature Review and Background Chapters, one could conclude that online activists, whether in Syria, Egypt, the UAE, or other countries, do have common aspirations to rid themselves of decades of oppression, and that could be what motivated a significant number to go online, search for circumvention solutions, and use them to access political blogs, Facebook groups, and dissident websites.

Hence, by comparing results of the 2012 and in 2010 surveys about Internet censorship, one could still get a reasonably relatable snapshot of progress or decline after the Arab Spring. And, as shown in Table 17, upon doing a Pearson's chi-square comparison between the intensity of technical and nontechnical censorship in 2010 and 2012, the situation in 2012 appears to have deteriorated significantly.

Statistically, the higher the Pearson's (r) value when comparing two independent variables, the stronger the association is. In this case, a comparison was made between each of the censorship acts and the year the survey was taken. The values were quite high, indicating that there was a consistent change in patterns from 2010 to 2012. When looking at the number of reported cases, we can see that as a percentage, there was a rise in Internet censorship practices committed against respondents to the 2012 survey (25% nontechnical and 36% technical) compared to those answering the 2010 survey (12% nontechnical and 16% technical)[103].

The table identifies the number of victims who had said they were subjected to the indicated censorship methods and indicates the number of respondents saying that they felt insecure and threatened of potentially

[103] It is worth mentioning that informants, as shown in Appendix B, were asked about cases of censorship that occurred within one year so that the information would remain relatively recent and relevant. This suggests that those answering the 2010 survey may refer to cases in 2009 in addition to 2010 and those answering the 2012 survey may refer to cases in 2011 in addition to 2012.

being exposed to those methods. Like 2010, legal prosecution and harassment continued to be among the main censorship methods that were used against Web content producers. Generally speaking, the noticeable surge was not only in the rate for those exposed to censorship but also in the rate of those feeling at risk of being subjected to one of the nontechnical methods such as kidnapping, legal prosecution, and other technical pressure. This reflects a situation of instability and, arguably, a consequence of the Arab Spring as a whole.

			2010		2012	
Nontechnical censorship	*r*	*p*	**Victim**	**At risk**	**Victim**	**At risk**
Legal prosecution	21.4	0.001	72	29	36	27
Kidnapping or illegal detention	14.0	0.015	58	27	33	19
Harassment, threats, hostility	14.0	0.016	67	36	36	23
Torture of physical violence	15.2	0.009	52	41	18	24
Surveillance (wiretapping, etc.)	14.7	0.01	64	40	31	29
Other forms of pressure	18.2	0.003	64	31	19	23
		Total	**377 (12%)**	**204 (7%)**	**173 (25%)**	**145 (21%)**
Technical censorship						
Internet filtering	**6.2**	**0.285**	**110**	**31**	**57**	**16**
Traffic attacks (DDoS, etc.)	12.0	0.035	79	36	48	18
Virus, Trojan, worm, etc.	18.5	0.002	82	37	50	24
Compromised login info (e-mail, admin)	17.0	0.005	80	26	43	18
Domain taken over	22.9	0.000	62	24	26	30
Other forms of technical pressure	11.8	0.038	58	22	27	15
		Total	**471 (16%)**	**176 (6%)**	**251 (36%)**	**121 (17%)**
N (2010) = 3,017 *N* (2012) = 692						

Table 17: Comparing Internet censorship responses between 2010 and 2012 based on survey feedback

Furthermore, surveillance was indicated to be a risk by twenty-nine respondents, which resembles the greatest of all risks in the nontechnical censorship category. This is a sign of increased distrust and concern against their regimes and possibly the ISPs they use to connect. Interestingly enough, these data were gathered well before the 2013 reports emerged

exposing the NSA mass surveillance and some other regional and national spying programs.

Similarly, technical censorship appears to have increased in relative terms, with seventy-four respondents saying that they were either exposed to or were at risk of being subjected to malware attacks. This is a major change compared to 2010, when Internet filtering was the greatest concern. In other words, users in 2012 were concerned more about their own data and cybersecurity than about the blocking of websites. It might well be that circumvention tools were not the ultimate solution for censorship if this trend continued because governments may then revert to sending viruses and worms to spy on activists' online activities or simply compromise and destroy their data. This finding confirms what had been indicated in the earlier Background Chapter about the cyberwar escalating in Syria and in which activists were targeted by the government using malware and other cyber attack methods (Watson, 2011).

In essence, the battle between freedom and repression online has not dwindled, but intensified, and survey results show that content producers in the region are aware and concerned about this. It is therefore important to not be limited to anticensorship effort using circumvention and proxy tools. But better cybersecurity through encryption, anonymity, software updates, and other good security practices will be crucial in any fight against online repression in the region.

Retrospectively, it was rather wise that a set of additional questions were added toward the end of the second survey to get respondents' perspectives in relation to the uprisings during the Arab Spring. The questions were helpful in getting their views about the potential motives behind censorship. In the next section, responses to those questions are discussed.

Motives behind Internet Censorship

Respondents were asked what they considered the most important motive behind website filtering were and five potential factors were provided, each with its own Likert scale. Respondents had to rate each of the following as a factor that motivated censoring websites containing political/security content:

1. To prevent raising public awareness of corruption and malpractices of the regime
2. To prevent helping organize rallies, protests, and sit-ins
3. To prevent causing dissent within the army or prominent officials

4. To prevent providing content to other traditional media (e.g., aljazeera.net)
5. To prevent encouraging strikes in the public or economic sectors
6. Other factors

Apart from the sixth factor (other), respondents actively ranked each of the other factors. The order of the factors in accordance to importance based on respondents' feedback was 1, 2, 4, 3, and 5, as shown in Figure 10. The data reflect considerable attention to preventing the raising of awareness about the regime's wrongdoings as the main motive. This was followed by mobilizing protests against the regime and preventing online content from reaching the media.

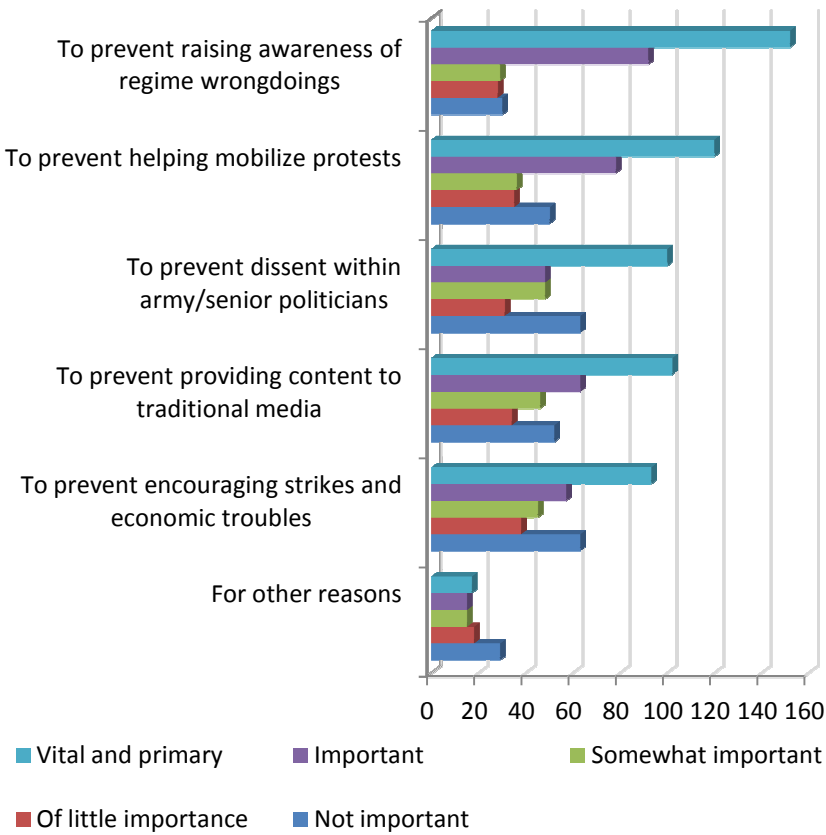

Figure 10: Motives behind Internet filtering (2012)

When zooming in to see the factors for the two dominant factors (1 and 2), it was apparent that individual characteristics of Arab countries start to emerge. As can be seen in Figure 11 and Figure 12, the standard deviation for both the first and second factors was quite small, as they were 7% and 6%, respectively.

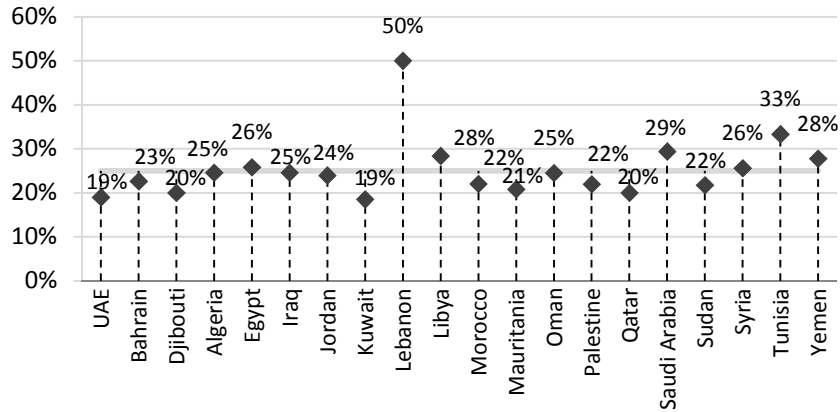

*Figure 11: Significance (as a ratio) of exposing government wrongdoings as a motive (*N = *20,* M = *25%,* s = *7%) (2012)*

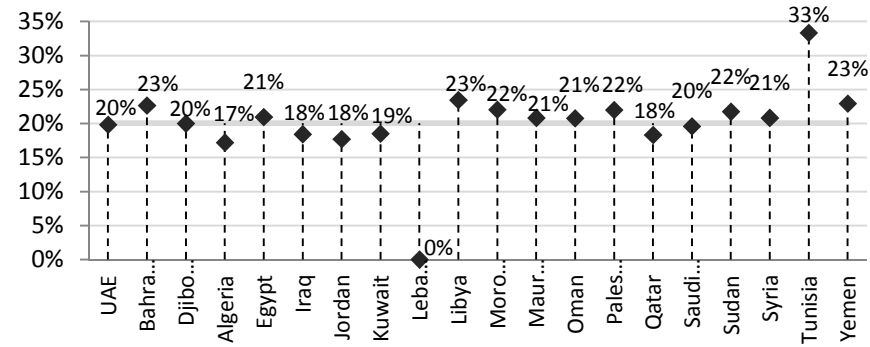

*Figure 12: Significance of supporting anti-government protest mobilization as a motive (*N = *20,* M = *25%,* s = *6%) (2012)*

For the factor about exposing wrongdoings, it is interesting to note that all Arab Spring countries have had a higher than average rating for this factor. This highlights the frustration they had with their governments' performances. On the other hand, countries better off economically, such as Gulf countries, with the exception of Saudi Arabia, have done very well.

Lebanon appears to have been the odd one in this set, and this could be attributed to the low number of responses, i.e., small sample, from that country.

When coming to the second most rated factor, which is supporting anti-government protests, respondents from Tunisia, the birthplace of the Arab Spring, gave it the highest rating compared to the other countries. Yemen, Syria, Libya, Bahrain, and Egypt also were all higher than the mean, indicating how publishing information about protests and using the Web for mobilizing the crowds is a strong factor that could result in a governmental decision to censor. Most Gulf countries have shown a lower than average rating in this category as well. The other three factors had a yet lower standard deviation, suggesting that there were no statistically significant findings connected to those countries.

How Successful Was Internet Censorship?

The second natural question to ask now that the motives were acknowledged was about the effectiveness of censorship practices carried out by the authorities to achieve their goals. Respondents were given a 5-point Likert scale to identify how successful censorship was in causing the intended impact, and the results were rather similar to those for the earlier question, with the majority seeing substantial to complete effectiveness of Internet censorship in achieving the governments' objectives.

However, the response rate was rather dismal, with only about half of the respondents answering the question, and within this group, a substantial portion answered with "I don't know" or "no answer," as shown in Table 18. This illustrated the difficulty for a regular user to answer such a question. It is also understandable, as it requires a broad and in-depth understanding of the causality between censorship and events on the ground.

Nonetheless, the lack of awareness is natural for many respondents given that they too are part of the public and they cannot know what they are prevented from seeing. For example, if the only popular sources about government corruption and scandals are online and if those websites are all blocked, it might not occur to the user that the government's aim may in fact be to limit content that exposes government corruption, which he/she cannot learn about from the Internet if all such online content is censored. Nonetheless, there is still a substantial view within this modest sample that believes the effects are manageable and not devastating.

	Completely effective	Substantial, but not devastating	Moderate	Little effect	No effect	Don't know	No answer	*N*
Raising awareness about wrongdoings	104 (18%)	76 (13%)	77 (14%)	40 (7%)	47 (8%)	82 (14%)	140 (25%)	566
Helping mobilize protests	71 (13%)	74 (13%)	77 (14%)	44 (8%)	52 (9%)	83 (15%)	153 (28%)	554
Causing dissent within the army/officials	61 (11%)	42 (8%)	64 (11%)	59 (11%)	64 (11%)	110 (20%)	160 (29%)	560
Providing content to traditional media	73 (13%)	30 (5%)	89 (16%)	56 (10%)	54 (10%)	102 (18%)	157 (28%)	561
Encouraging strikes/economic troubles	59 (11%)	46 (8%)	80 (14%)	41 (7%)	68 (12%)	110 (20%)	153 (27%)	557
Others	12 (2%)	15 (3%)	17 (4%)	21 (4%)	30 (6%)	147 (30%)	242 (50%)	484

Table 18: Success rating of Internet censorship in achieving its goals for governments (2012)

When summed together, the views that see that the effects of censorship were moderate to none would prevail with the exception of the first factor. In other words, Arab governments have not yet successfully controlled the flow of information on the Internet in a way that is as effective as the methods used to control traditional media. But they have achieved some success. When factoring in the growth trends of social media usage in the region, it is likely that the states' grip on information would continue to loosen. And this would accelerate if human rights advocates, reformists and dissidents promote more means of distributing information about government failures and corruption through multiple means that may not be easily censored.

What liberation technologies do, as illustrated in the theoretical framework, is offer that possibility, allowing the public to receive and impart information in ways that governments may not have the power to control. This will be dealt with in more detail in the later part about censorship circumvention.

When Can Online Speech Be Limited?

Perhaps the most controversial question that comes to mind at this stage is about what Arab Internet users think when it comes to limits of free speech. The Milliam principle by Scanlon (1972) and how it could help identify when speech should be censored to prevent harm were discussed rather comprehensively in the Theoretical Framework Chapter. However, this is the time to reflect on what survey respondents thought those limits, if any, should be. Both surveys asked of the content that is appropriate to censor online. The first survey had a higher number of respondents than the second survey. In this section, I present the aggregated combined findings for the two surveys while in the next section, I present an analysis of notable key changes in the second survey compared to the first.

When asked if it was appropriate to censor certain types of online content, respondents based in Arab countries demonstrated a strong opposition to censoring politically critical content. Among Arab respondents answering the question about the appropriateness of censoring politically critical content, 1,625 indicated that they believed it was totally or mostly inappropriate to block access to politically critical content targeting the regime, while 1,086 agreed to censoring such content but varying degrees. This result demonstrates that most users found the Internet as the window through which critical anti-government views could be expressed freely on political matters. After all, this is what sets the Internet apart from traditional media, which are strongly restricted in the region. The value of free speech to bring government to account has been advocated strongly in the free speech theory. Arab respondents demonstrated through these results that they too strongly support their right to freely express their political views and grievances against a government.

Figure 13 and Figure 14 compare the views between Arabs and non-Arabs. Remarkably, Arab respondents appeared more passionate than non-Arabs in opposing the restriction of critical political views.

Another type of websites that Arab respondents thought should not be censored is circumvention or proxy websites. When a regime practices filtering of websites, including those that contain politically critical content, it becomes apparent that users will have to rely on means to circumvent a firewall. This is done mostly by accessing websites of censorship circumvention tools and services such as Alkasir (https://alkasir.com) and others that are available on the Web. And it was rather expected that Arab respondents who oppose blocking political content would also oppose blocking the tools that allow them to access such content.

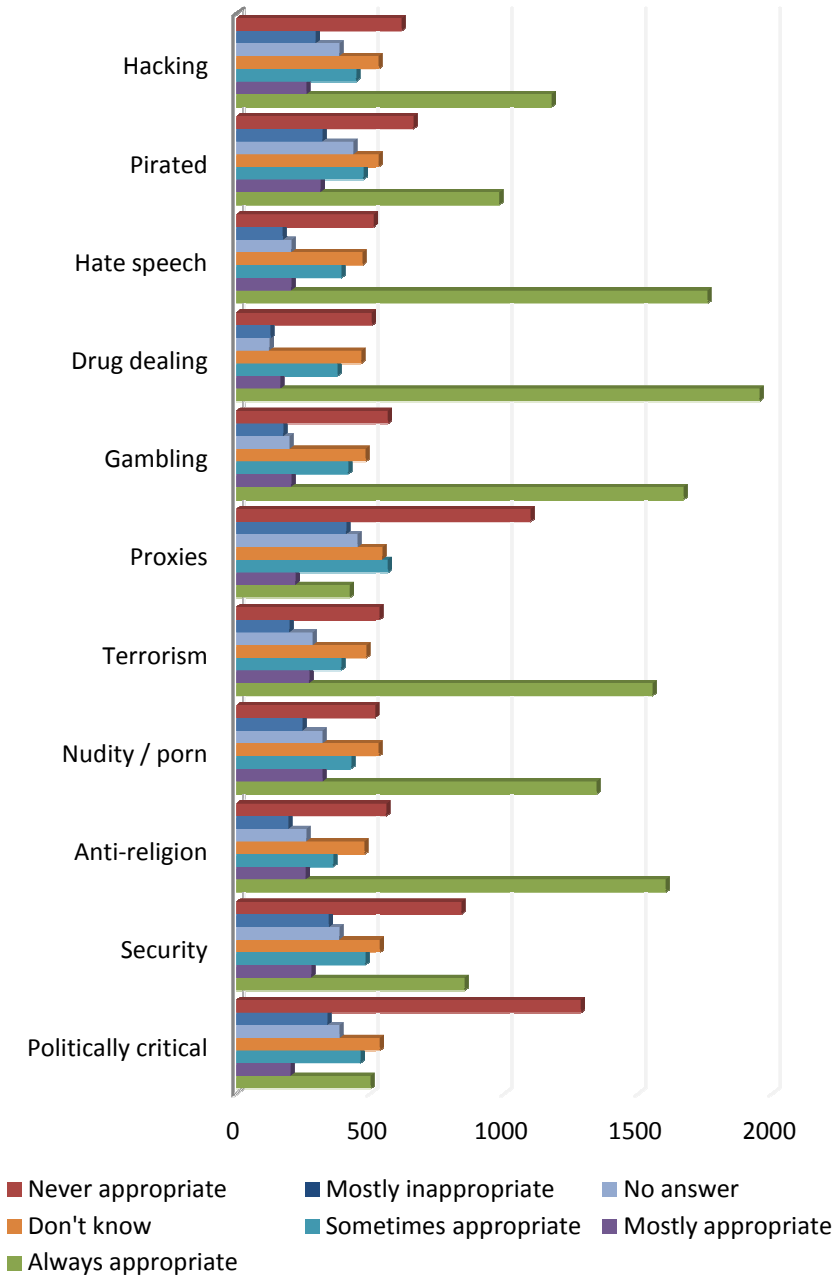

Figure 13: Appropriateness of censoring in Arab countries (2010 and 2012)

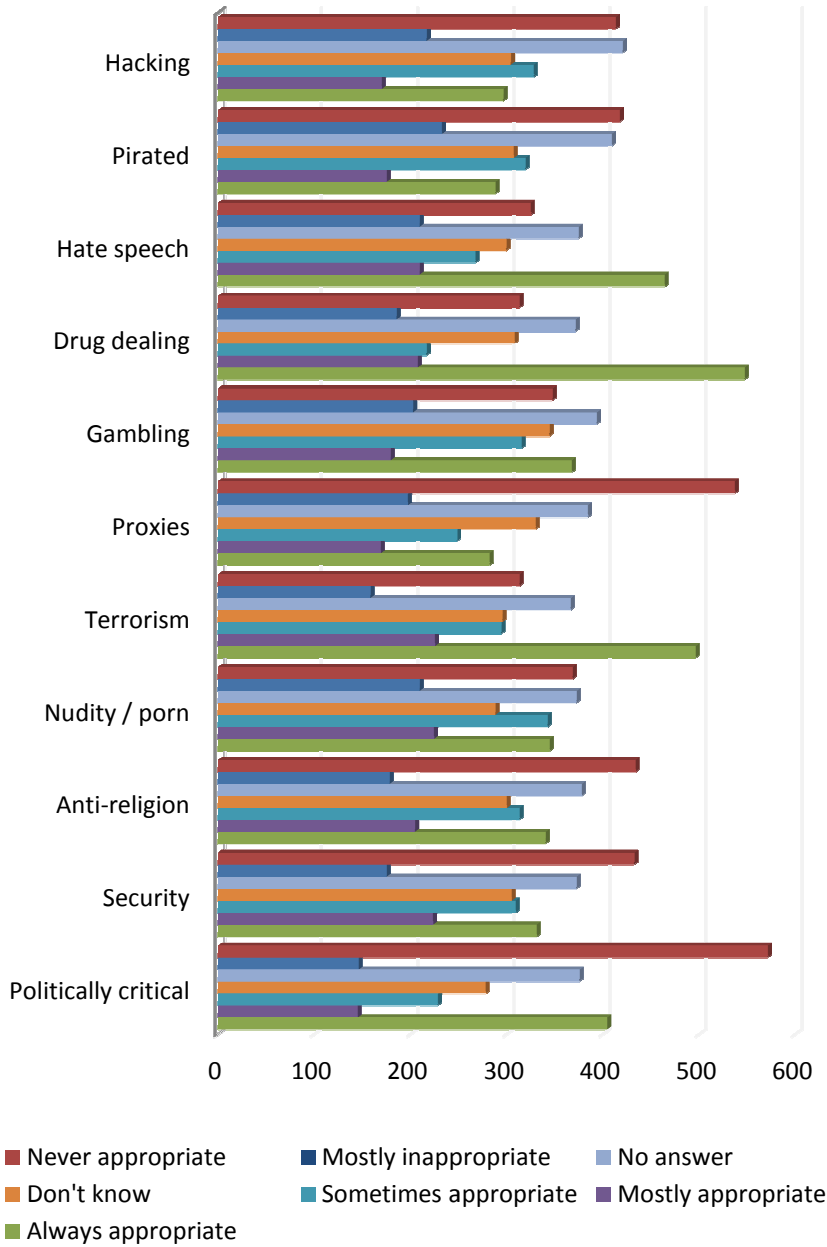

Figure 14: Appropriateness of censoring in non-Arab countries (2010 and 2012)

This result was also predictable given the fact that survey informants have accessed Alkasir's website to reach to the survey itself. If Alkasir had its website blocked, they would not have been able to use it to access political content. But when it came to the other categories of online content, results started to change dramatically and with major differences of opinion between Arabs and non-Arabs clearly emerging.

While most Arab respondents supported censoring all categories except those that have politically critical content or offer proxy and circumvention solutions, the majority of non-Arab respondents, on the other hand, opposed blocking everything except those promoting terrorism, illegal drug dealing, and hate speech.

The irony of this result is allowing proxy websites to be accessible would make it possible to overcome censorship of all those categories that Arab respondents said should be censored. One possible explanation would be because Alkasir users are already biased in their view that pornography should be censored because Alkasir's terms of use restrict access to such content from the outset. Furthermore, it might also reflect a desire by respondents to issue a statement that they agree with governments blocking what they deem culturally offensive while keeping a window open for those wishing to use circumvention tools to access them. In such a way, they took a middle ground between the extremes.

I argue, however, that Arabs' and non-Arabs' diverging opinions on pornography, gambling, and anti-religion content stem from the cultural context of each. This brings us back to the theoretical questions of where free speech limits are drawn and what is the basis on which a regime formulates those limits. The Milliam principle states that an imminent danger is the only condition to restrict speech. For many of these categories, however, it is very difficult to stipulate what could satisfy that condition and what could not. This opens the way for authoritarian regimes to abuse cultural and religious beliefs and use them as a justification to practice censorship widely, as demonstrated in the study by Fallows (2008).

As indicated in the Theoretical Framework Chapter, free speech's limits are often constrained by other fundamental rights that may end up being violated. It then becomes a matter of judgment as to when free speech is to be limited; a decision would be required to decide which of the human rights need to be given higher priority in a given context by measuring the consequences of unrestrained speech.

While this debate is philosophical in nature and may not lead to any answers except perhaps 'it depends on the context', this issue does raise several important legal and ethical dilemmas particularly when dealing with the right to life, right to freedom of religion, right to privacy, etc. It is apparent that at this stage, the results do not provide answers to these complex questions, but rather introduce opportunities to examine views from new angles and contexts and invite further studies in this area.

To further simplify what these results mean, Table 19 aggregates the ratio of those who indicated that it is either totally or mostly appropriate to block certain content to those who think it is completely or mostly inappropriate to do so.

	Arab respondents		Non-Arab respondents		
	Agree to censor	Don't agree	Agree to censor	Don't agree	*r* (df = 6)
Politically critical	**30%**	70%	43%	57%	**74.9***
Security	**49%**	51%	48%	52%	**77.1***
Anti-religion	**71%**	29%	47%	53%	**338.9***
Nudity/porn	**69%**	31%	50%	50%	**214.6***
Terrorism	**71%**	29%	60%	40%	**190.6***
Proxies	**30%**	70%	38%	62%	**42.1***
Gambling	**72%**	28%	50%	50%	**385.5***
Drug dealing	**77%**	23%	60%	40%	**377.7***
Hate speech	**74%**	26%	56%	44%	**331.2***
Pirated/copyright	**57%**	43%	42%	58%	**127.1***
Hacking	**61%**	39%	43%	57%	**169.6***

*$p < 0.001$

Table 19: Percentages of respondents in Arab countries finding filtering appropriate (2010 and 2012)

A Pearson's chi-square association analysis was also carried out to identify the strength of the association between views on censorship and being

an Arab.[104] The analysis shows all categories reflected some degree of association ($p < 0.001$) but with some content representing a more vocal view than others. While Arabs agreed with censoring eight categories of content, non-Arabs agreed to censor only three.

However, the biggest difference as shown on the table was for the gambling ($r = 385.5$) and drug dealing ($r = 377.7$) categories. The results appear to confirm the argument by Hinnebusch (2006), who indicated that in the Arab context, culture could be seen as an intervening variable through religion and tradition (Hinnebusch, pp. 376–377). This could also be understood by acknowledging Islam's prominent influence on Arab culture (Obeidat, Shannak, Masa'deh, & Al-Jarrah, 2012), and by noting that Islam does indeed strictly prohibit gambling and drugs except those used for medical purposes (Mayled, 1999, p. 61). Islam also strictly prohibits nudity and pornographic literature and even obscene songs (al Qaradawi, 2013, p. 21), which entails forbidding all sorts of such content on the Internet. Taking that into account, it becomes clear and understandable why most Arab survey respondents would want to have such content blocked.

The third strongest association ($r = 338.9$) was with anti-religious or defamatory content, which is no surprise if we recall the uproar in many Arab countries against the anti-Mohamed cartoons and videos published on the Internet (Akiner, 2011). And although the fourth strongest association was with hate speech ($r = 331.2$), the blocking of content in this category is supported, albeit mildly, by non-Arabs as well.

The other interesting diverging view was in the pornography category ($r = 214.6$), which reflected greater support for blocking among Arabs compared to non-Arabs, who were split as to whether it should be blocked or not. This also stems from traditional conservative norms and traditions in Arab societies and can be understood within a religious context, particularly in Arab countries that are quite conservative in nature, for example, Saudi Arabia and Yemen. The issue of pornography/nudity is a bit problematic to assess in this study because, as indicated earlier, users have agreed not to access pornographic content using Alkasir so they are already at a biased position in that respect.

Websites containing information on hacking and others with pirated and copyrighted content were only seen as appropriate to block by the

[104] It is assumed that those who used the Arabic interface or identified their country being an Arab state to be Arab and everyone else to being a non-Arab.

Arab respondents, but to a much lesser extent compared to anti-religion and pornography. Respondents in both camps, however, indicated that it was not appropriate to block websites that could be security-related such as those calling for rebellion against the state or secession.

Changed perceptions on censorship during the Arab Spring

The results of the two surveys in terms of level of support of censoring a particular category were for the most part the same for the second survey compared to the first. The most significant difference however was in the security category. While most respondents in the 2010 survey said that they agreed that it was appropriate for at least some security-related content to be blocked, the survey respondents of the 2012 survey that took place after the Arab Spring reversed this position, with the majority of 2012 survey respondents opposing the censoring of security content. The turnaround was so strong that it also tipped the scale in favor of the view that opposes the censoring of security content in the combined aggregated data for the two surveys.

Furthermore, another notable difference was that while there was somewhat of a disagreement between respondents from individual Arab countries in 2010 about whether it was appropriate to block political content, in the second survey, they all collectively agreed that political content should not be blocked. In 2010, respondents from some Arab countries were in strong opposition to censorship of political and security content while respondents from other countries agreed with such censorship. I take here the cases of Yemen and Syria out of the four selected cases because they had a significantly higher number of respondents compared to Egypt and Tunisia, whose respondent rate were not enough to do a meaningful statistical analysis.

As shown in Table 20, Syrian respondents in 2010 agreed with censoring political and security content but made a remarkable U-turn in 2012, when they strongly opposed such censorship. This suggests that this change in opinion may have been a reaction following the Arab Spring wave of new filtering practices and other repressive practices committed by the Assad regime under the pretext of maintaining security.

While it is not possible to immediately interpret this change as a consequence of the Arab Spring, the fact that the strongest shift in opinion happened in Syria, which witnessed severe suppression of demonstrations and on-the-ground violent confrontations gives reason to consider the Arab Spring as a contributing factor leading to this change.

	Agree with censorship of		2010 survey	2012 survey
Syria	Political content	No	83 (33%)	133 (70%)
		Yes	171 (67%)	58 (30%)
	Security content	No	61 (23%)	112 (61%)
		Yes	199 (77%)	73 (39%)
Yemen	Political content	No	641 (75%)	35 (80%)
		Yes	219 (25%)	9 (20%)
	Security content	No	457 (55%)	26 (62%)
		Yes	378 (45%)	16 (38%)

Table 20: Positions of respondents in Syria and Yemen concerning censoring political and security content

It is worth noting that it was not only Syria and Yemen that have developed stronger views against censoring political and security content in 2012 compared to 2010, but almost all Arab countries have shown this as well. However, only the opposition to censoring political and security content and circumvention (proxy) websites has increased noticeably in 2012. There was no significant change in respondents' views regarding the other categories such as nudity, anti-religion, and drugs.

Limits to free speech in Arab eyes

It is useful to pause here and reflect on whether the liberal principles of free speech often advocated in the West are what Arab respondents think are appropriate to apply in their own contexts and countries. I believe this presents two problems. The first is the difficulty in classifying a particular type of content. There is indeed immense difficulty to identify where a content category begins and where it ends. For example, sexual educational online material could indeed include nude photographs of female and male bodies for educational purposes. Should such content be blocked merely because they contain nudity? The issue gets even more complex when it relates to anti-religious commentary. As demonstrated earlier, one of the most widely blocked websites in the Arab world is el7ad.com, which advocates for atheism and calls upon Arabs to abandon the Islamic faith and spread atheism in the Arab world. A question that emerges is whether there can be a global standardized method to identify if and when any particular online content could be censored.

The second problem is about the methods to use in order to restrict the content that is, hypothetically speaking, agreed universally to be harmful. As it has been indicated before, blocking websites is not technically feasible because circumvention and proxy websites, which should not be blocked as respondents suggested, are often capable of bypassing such restrictions. Theoretically, this means that they could be used to access illegal content such as child pornography. Technical filtering is not a bulletproof method of blocking. While liberation technologies are meant to be helpful to access content that is blocked, they can certainly be abused.

Finally, I wish to reemphasize a point that Arab governments could easily exploit when looking at these data. By interpreting the majority's view that blocking some content is appropriate, governments could abuse this by suppressing freedom of expression online with the justification of serving the public and restricting culturally insensitive or immoral material. It is already being done in China, where the government filters the Internet on the grounds of protecting public interest and in response to the demands of the people, who, according to the study by Fallows (2008), mostly trust their government to do what is right and filter the content that could be harmful.

Those results illustrate that the discussion around where free speech limits are will remain controversial and with no clear conclusion. It will also continue to be affected by the cultural and religious affiliation of the involved groups, communities, and countries. This study is not meant to give the ultimate recipe of where to draw the line and indicate what is appropriate to block and what is not. But it aims at providing empirical data pointing to what some people in the Arab world think when it comes to those limits.

The results add to the body of literature related to limits of free speech online and are an invitation to scholars and policy makers to use these data for their own research and studies.

Findings on Censorship Circumvention

In this section, a comprehensive discussion and analysis of the survey findings in relation to censorship circumvention is provided. It is meant to answer the research questions related to the appropriateness, effectiveness, and desired features in circumvention tools according to Arab survey respondents. The section also raises the question on whether circumvention is enough in combating Internet censorship or what could be done to supplement it.

In many Arab states, there was an evident drive toward establishing stronger communication infrastructure to achieve greater Internet accessibility. Such a move was deemed important for integration into the global economy and for overall developmental growth in various sectors, including government services. With the increasing dependency on the Internet, it became apparent that regimes would not likely close down the Internet permanently or even reverse its growth.

Consequently, Internet censorship, whether technical or nontechnical, would remain one option to control information access online. Yet, as demonstrated with the use of Alkasir, for those willing to gain access to overcoming website filtering, circumvention tools would also remain a viable solution. This confirms the perspective noted in the Theoretical Framework Chapter of this study in the technology's potential use as a means of liberation from repression, albeit by confronting only one form of Internet censorship, namely, Internet filtering.

Usage of censorship circumvention solutions

Survey respondents were asked what circumvention methods or tools, if any, they used in the last 12 months. Given that almost all respondents were users of Alkasir anyway, they were not given Alkasir as one of those solutions shown in Table 21. The results indicated that out of the 1,858 respondents answering the question (1,505 in the first survey and 321 in the second), Hotspot Shield came on top with 27.7% of the total, followed by Ultrasurf with 18.2% and Web-based proxies as third with 16.8%. The other circumvention solutions were much lower in usage.

Between 2010 and 2012, however, there were some interesting changes resembled in the halving of responses indicating the use of Web-based proxies. In the past, Web-based proxies used to be the easiest way to get around censorship. But ISPs have become more aggressive in their filtering techniques (Palfrey, Roberts, & Zuckerman, 2011). Additionally, those proxies may not be able to efficiently handle the increasingly bandwidth-demanding multimedia content available on social networks or video-sharing websites. They also cannot be used for non-Web-based uses such as VOIP or P2P applications.

Furthermore, usage of Ultrasurf dropped significantly while DynaWeb gained a considerable number of users. Both solutions are free of charge but are often slow and may not open all websites in all countries due to bandwidth restrictions. In the new 2012 survey, Ultrasurf was by far the biggest loser as it lost 75% of its usage in the Arab world.

Circumvention method	2010	2012	Combined
Web-based proxy[105]	18.5%	9.3%	16.8%
Ultrasurf	21.1%	5.7%	18.2%
Hotspot Shield	28.6%	21.2%	27.2%
Tor	2.7%	26.1%	7.2%
DynaWeb	1.8%	9.1%	3.2%
GPass and FirePhoenix	1.4%	2.8%	1.7%
JonDo	2.5%	2.0%	2.4%
Your-Freedom	1.1%	2.8%	1.5%
A VPN service (free or paid)	4.5%	6.2%	4.8%
Other	8.1%	8.8%	8.2%
No answer	7.4%	2.3%	6.4%
I don't remember	2.3%	3.7%	2.5%
Total respondents (*N*)	**1,505**	**321**	**1,858**

Table 21: Circumvention tools used by Arab survey respondents

Meanwhile, Hotspot Shield is a VPN software package and remains one of the most widely used circumvention methods as indicated in both surveys. It was developed by an American company named AnchorFree and offers the service free of charge but with several advertisement windows popping up throughout the Web surfing experience.

While many users reduced their reliance on Web-based proxies and on Ultrasurf, the biggest winner in 2012 was Tor, an open-source software package known for its robust, strong encryption and anonymity features. Given that Web-based proxies are known to be the least safe circumvention method and Tor is often praised to be the safest (Palfrey, Roberts, &

[105] Web-based proxies are those that can be accessed directly via a browser. All the user needs to do is find one of those websites and enter the URL he/she needs to visit directly into its field and it will fetch the website and display it within the internal web-based proxy window.

Zuckerman, 2011), this finding points to a rise in awareness of cybersecurity demands among Arab respondents. In the last few years and during the Arab Spring, many activists reported cases of online traffic monitoring, surveillance, spying malware attacks and other forms of tracking (Silver, 2012). By choosing to use Tor, respondents were giving themselves better protection for their anonymity while surfing the Web.

Gaining access to circumvention solutions

When asked about how respondents were able to get to know about and download the circumvention tool or method they used, those who used Web-based proxies said they found about them mainly through search engines (39.9%) followed by word of mouth (26.4%), while 14.5% said they learned about them by reading discussion forums, of which many exist in Arabic language and often also exist on social networking platforms such as Facebook.

These findings, shown in Table 22, indicate that a proactive approach was taken by users in deliberately going about the Web in search for such solutions. But personal communication directly through word of mouth and indirectly through social networks together amounted to 40.9%, which is close to the percentage of those who found them through search engines (39.9%). While the first survey was done in 2010 when social networking was steadily growing, the use of blogs and discussion forums has witnessed a noticeable increase in 2012, which explains why the rate of those using them to learn about Web-based proxies has increased from 13.8% to 24.2%. Such forums are generally useful to learn about censorship evasion tools and tricks.

When it comes to downloading the actual circumvention software, the majority of the combined total (62.1%) had either downloaded them from the official website of the solution provider (29.6%) or from another website (32.5%). The third most popular method was to get the software from another person (21.3%), while just 7.2% got it via external physical means such as memory sticks or CDs.

This finding illustrates that users have shown great keenness in getting the software from trusted sources, be it the official website, a popular download site, or a person whom the respondent trusts. Downloading circumvention software through P2P applications or by e-mail is generally more risk-prone, and, unsurprisingly, only a small portion used such a method (2.4%).

Users' reasoning for not using circumvention tools

Because not all respondents were familiar with Alkasir and because even those who did use Alkasir may have done so reluctantly, it would then be natural for some respondents, who were not familiar with circumvention tools before, to indicate that before using Alkasir, they had not at all used any circumvention tool. An important question that this study addresses is what the reasons that prompt users to use or not use circumvention tools were.

How did you learn about the Web-based proxy service?	2010	2012	Combined
I read about them on a blog or discussion forum	13.8%	24.2%	14.5%
I found them through the use of a search engine	40.0%	39.4%	39.9%
I was told by another person	26.3%	27.3%	26.4%
I saw them on an advertisement or e-mail	5.4%	0.0%	5.0%
I learned about them through traditional media	1.7%	3.0%	1.8%
I found them on a specialized circumvention website	11.7%	3.0%	11.1%
I don't remember	0.2%	3.0%	0.4%
No answer	0.9%	0.0%	0.8%
Total respondents (*N*)	**463**	**33**	**496**

How did you obtain the circumvention software?	2010	2012	Combined
I downloaded it from another website	34.4%	24.2%	32.5%
I downloaded it from its official website	28.6%	34.0%	29.6%
I got it from another person	20.6%	24.2%	21.3%
I got it through external storage (CD, USB, etc.)	6.4%	10.2%	7.2%
I received it by e-mail	4.3%	1.4%	3.8%
I got it through a P2P connection	2.4%	2.3%	2.4%
Don't remember	2.3%	2.3%	2.3%
No answer	1.1%	1.4%	1.1%
Total respondents (*N*)	**931**	**215**	**1,146**

Table 22: How respondents learned about Web proxies and downloaded circumvention software

A combined total of 209 respondents, constituting just over 5.6% of the studied population, said they never used a circumvention method before. In answering why they never used such tools, almost half of the re-

spondents (47.4%) said they did not know how to get or use them, which is a strong indicator that lack of knowledge about circumvention tools is perhaps the biggest challenge in advancing the use of such tools. This ignorance factor is perhaps good news for the authorities that wish to maintain their grip on information flow. This may be enough to justify the censorship of websites containing circumvention solutions and tools, because, otherwise, Internet users would easily be informed of ways to bypass the government's digital firewall.

The second most cited reason indicated by 14.8% was their lack of trust in those solutions or their developers, indicating that faith is a significant factor behind winning users and having them download and use such products. Perhaps a way to go about this is to establish a transparent mechanism to verify the credibility and legitimacy of the software by providing the developers' address, real name, etc.

The third most selected reason indicated by 12.9% was their suspicion in the reliability and effectiveness of such tools. In other words, they did not have confidence in the ability of circumvention tools to bypass censorship effectively. This would be best addressed by allowing the solution to go open-source, for example, or be checked by a third party through a code audit to verify its safety, competence, and reliability.

It is noteworthy that only 0.4% of all Arab respondents (15 cases) refrained from using circumvention tools because of fear from government, family, or society. It may be considered a indication that governmental or societal pressure is, thus far, limited. Finally, 7 of the 209 respondents said that they did not use such software before because they believe that accessing blocked content was generally inappropriate. It is difficult to come up with any concrete reasoning why they thought so despite the fact that they were filling a survey on a website providing censorship circumvention services. Most of those who filled out the survey have already downloaded and installed Alkasir and filled out the survey to be able to use it. It means that they have obviously passed the threshold of anxiety, doubt, or fear of using circumvention tools, unless they were not committed to using the service after the survey is sent.

How important are circumvention tools for free speech?

An optional question asked to respondents answering the second survey in 2012 was if they thought that circumvention tools could indeed be of any importance in reducing the effects caused by Internet censorship and promoting free speech. Despite having a relatively small population from

thirteen countries answering this question (N = 409), as shown in Table 23, the results appear to confirm the view that censorship circumvention could indeed be liberating, as the data show a strong view in favor of the suggestion that such tools have been important in confronting censorship in the Arab world.

	Vital/ primary	Important	Somewhat important	Of little importance	Not important	I don't know
Algeria	4	5	2	1	1	2
Bahrain	3	2	4	1	0	1
Egypt	11	11	2	1	1	2
Iraq	7	5	5	4	1	3
Jordan	4	7	2	1	0	2
Kuwait	0	2	0	2	0	0
Oman	2	4	0	0	0	0
Palestine	6	6	2	2	0	2
Qatar	1	3	0	0	0	1
Saudi Arabia	9	4	1	1	3	6
Syria	94	57	12	8	2	21
UAE	6	6	1	2	0	2
Yemen	15	19	6	4	2	0
Total	162	131	37	27	10	42
Total (%)	39.6%	32.0%	9.0%	6.6%	2.4%	10.3%

Table 23: The importance of circumvention solutions to limit the effects of Internet censorship (2012)

Those who indicated that circumvention tools were important or vital reached around 62% of the total cases, besides about 10% who have indicated that they do not know the answer. It is important to consider those results in relation to the Arab Spring during which the Egyptian regime, as demonstrated in the earlier Background Chapter, restricted access to Facebook and Twitter and the Syrian regime has steadily increased its level of Internet filtering.

Figure 15 shows the results in terms of percentage for each country to be able to compare across states. Out of the four countries examined in

this study, respondents in Syria, Egypt, and Yemen have given significant weight to the value of circumvention tools. But so did respondents in countries that have not witnessed revolutions, such as Kuwait, Oman, Qatar, and Jordan.

All countries in the region to varying degrees have assessed the importance of circumvention tools positively. Recalling the role Alkasir had in Egypt, Syria, Yemen, and Tunisia, it was quite evident that tools like Alkasir were useful in promoting free speech, particularly during times of crises.

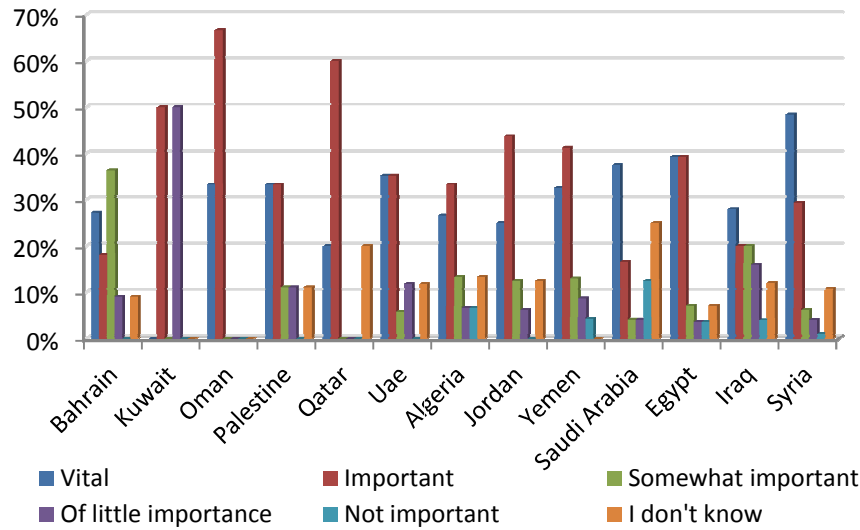

Figure 15: Answers to the question of circumvention tools' importance to combat censorship (2012)

However, it would be immature to use this finding to conclude that circumvention tools will totally erase the effects of Internet because, as demonstrated in the case of China, a government could set up a firewall just so the majority of the population gives up trying and instead, use the available alternatives (Chen & Wang, 2010, p. 97). In such a situation, governments care more about ratios. So even if a small portion of a population is able to use censorship circumvention methods, the authorities may not be terribly concerned, because they would have achieved their goal in preventing the majority from accessing censored Web.

When asked if censorship circumvention tools are only for use in cases where there is Internet censorship already in place, 233 out of 555 respondents (42%) said it is important to be aware of such tools even when there is no censorship because they would become handy if and when the Internet is censored. This is a precautionary measure that could have helped Egyptian activists a lot had they known about such tools beforehand. The frantic requests for advice on Twitter showcase the lack of awareness at the time of such tools which were rarely taken into account until censorship became a reality, subjecting users to delays in using their social media platforms or updating their websites due to the lack of the necessary know-hows.

When asked if one could use such tools merely for anonymity and privacy protection purposes, a significant percentage (22%) agreed with some comments indicating how important it is for them to protect their traffic from surveillance. One anonymous respondent added a comment saying:

> I never like the fact that ISPs track and record your history, I'm sure most Internet users agree too.

This illustrates that the importance of censorship circumvention tools could go beyond simply gaining access, but also encrypting or hiding traffic when suspecting that the ISP is eavesdropping on the connection. A Syrian answered by indicating that some websites may not be blocked but are monitored by the authorities, so it is important to use such tools to avoid being tracked and attacked.

Additionally, other answers suggested the usefulness of such tools for faster access to some websites. This is an added benefit in the case of fast and reliable proxies because, often times, those proxies have caching capacities that improve the speed of browsing websites located in the same country where the proxy is. Improving the surfing experience is always desired by users regardless of whether they are accessing a censored or uncensored website.

Given those benefits to users living in authoritarian countries or even in countries that do not practice censorship, the use of reliable censorship circumvention tools is encouraged based on those survey results. But what is required is not merely to introduce such tools to the public, but to find ways of encouraging the public to be informed about them and have them develop enough motivation and know-hows to get and use them in convenient and safe ways. Given that free and effective tools are already available, the next step is to find ways to support the tool developers so

they could help make them more visible to their target users to be useful for the advancement of free speech, particularly in oppressed societies.

Generally speaking, the value of circumvention tools for liberating users from repression has been demonstrated clearly in those results. The findings therefore verify the applicability of the term "liberating technology" on Alkasir as one example of a diverse set of solutions that could allow overcoming Internet filtering. Yet, as will be demonstrated later, circumvention tools are not sufficient to overcome the different forms of Internet censorship.

Getting the word out about circumvention tools

As demonstrated earlier, the majority of respondents do see censorship circumvention solutions as a form of liberation technology, that is, as a means of advancing democratic practices and freedom of expression. However, the lack of awareness and understanding of what they are and how they work is a hindrance.

Survey respondents that have used circumvention tools successfully gave their perspective on how to get the word out about those tools by ranking the following six approaches meant to make those tools more accessible:

- Personal coaching by having users themselves help educate others
- Discreet distribution to small groups with all needed information
- Workshops and seminars that are available for those in need
- Advertisements on traditional media such as TV and newspapers
- Internet advertising (in the form of banners, Google ads, etc.)
- Simple distribution on CDs and flash drives

The results shown in Figure 16 illustrate a strong tendency to act away from the public eye as demonstrated by the opposition to the use of mainstream media or even workshops and public seminars. Those approaches, albeit good for public relations and mingling, may not be the best approach to get the solutions into the hands of the people who need them, particularly those living in authoritarian states.

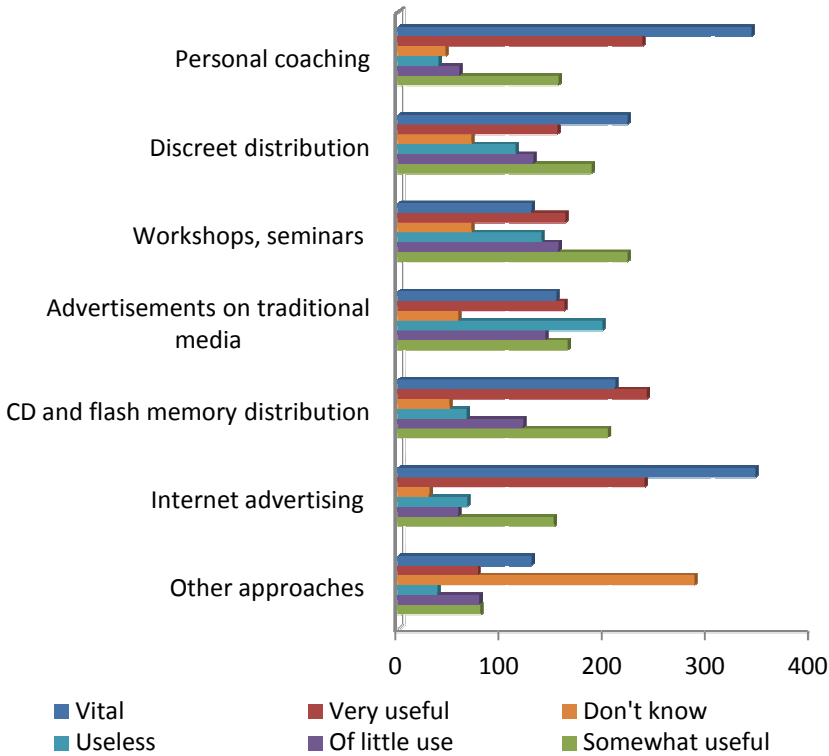

Figure 16: Assessment of approaches to raise awareness about circumvention tools (N = 891) (combined 2010 and 2012 surveys)

Respondents' preference was for personal coaching as the best approach and one that involves a one-to-one interaction with a person who is trusted and who could provide hands-on training and guidance in a safe environment. The second best approach was Internet advertising and is meant to capture the attention of new users. Doing so is quite commonsense as it will reach greater numbers of individuals in need, and with the use of marketing solutions on Google or Facebook, for example, it is possible to target the ads based on geography, gender, and other characteristics.

Discreet distribution is also preferred because it helps maintain confidentiality and have people share the know-how and software programs without getting much attention from the authorities. Respondents also suggested additional ways that were not considered in the question, name-

ly, mailing lists, Google Reader, discussion groups, social networking websites, and P2P torrents. This shows that Arab users want diversity in accessing tools and not limit themselves to one single source. Recalling the continuous cat-and-mouse chase between developers and governments as indicated in the theory part on censorship and circumvention, having such a diverse set of alternative methods is quite important.

In a personal reflection as an educator in the areas of social activism and using technology, I have had the opportunity to train many youths on how to use circumvention tools in the past, but it never occurred to me that workshops and public training events were not the preferred method. These findings have opened my eyes and have given me a useful insight into this aspect. They could also be useful for guiding the work of donors and international advocacy groups engaged in promoting the use of circumvention tools in particular and liberation technologies in general.

A particular type of action that could also be useful when considering training users on how to utilize circumvention tools is to provide training to women by women trainers, which could help increase the usability of tools generally as well as limit the gender divide when considering that such tools are liberating. Training could also be used as a general means of empowerment of women as suggested by Wheeler (2007). Targeted training for women in Arab countries would be more beneficial given that the overwhelming majority of respondents were men. A priority to training women could be a solid recommendation that emerges from this study.

What makes circumvention tools effective?

The answer to the question of which circumvention solutions respondents use the most could provide useful hints on what matters to the end users. The ease of usage, overall reliability, and relatively high speed are three characteristics that the most widely used circumvention solutions have in common. However, to have a more adequate and reliable conclusion, further questions were asked about the factors that respondents considered as important for effective and regular utilization of circumvention solutions.

There were ten different factors that were provided for survey respondents to choose from when assessing their importance for an effective circumvention tool. These were as follows:

- Speed and stability of the connection so as to be reliable and not get interrupted often and be not too slow

- Being free or charge because some tools do require payment
- Blocking-resistance, which is the ability to resist attempts by ISPs to have them inaccessible
- Privacy and secure communication to ensure that the data exchange is not saved or kept on the device in ways that expose the security of the user or have him spied upon
- Robustness refers to the ability of the tool to deal with various forms of content ranging from simple pages to bandwidth-consuming 3D games
- Accessibility refers to the ability to find the software easily
- Anonymity is to ensure that the person using the service is not traceable and it is not possible for the websites accessed to know where the user is located
- User-friendliness means that the interface is easy enough to get around to do all the basic tasks
- Cross-platform compatibility refers to the availability of different versions of the software to use on different operating systems (e.g., Windows, Mac) and mobile devices
- A small file size for download and requirement for storage on the computer

The results, shown in Figure 17, illustrate how the ten different factors were assessed by respondents of both the 2010 and 2012 surveys. Respondents were given a Likert scale to choose from, and the results were aggregated by adding up those who indicated that a factor is vital or very important and those that selected "somewhat or not important" on the other. Respondents were allowed to select multiple factors. The results were then tallied as percentages for each factor so as to be able to compare the two surveys, because otherwise the large difference in the size of the two populations would have made direct comparison cumbersome.

As shown in the graph, speed and stability were seen as the top most important factor in both surveys, which is understandable given that the quality of the connection is important for a pleasant and productive browsing experience. The second most important factor was also the same for both surveys and represented the need for the service to be free of charge and not for a fee. Payment-based services are less attractive because

apart from being an additional economic cost, they often require personal and credit card or other payment information, which is a major vulnerability, particularly for activists who wish to remain anonymous. This will certainly keep most users from accessing commercial VPN and other circumvention tools.

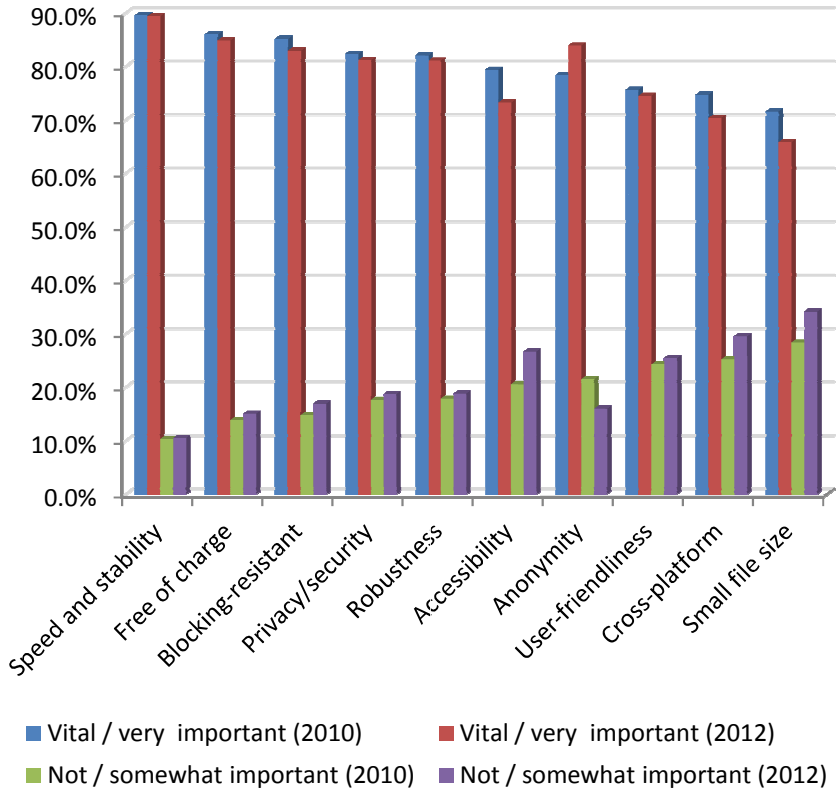

Figure 17: Importance of factors for effective circumvention based on the 2010 and 2012 surveys

Coming to the third priority, however, there was an interesting shift in priorities for survey respondents, because before the Arab Spring, users were not much concerned about their anonymity, which was given the seventh priority in the 2010 survey.

This trend was also demonstrated by the lower number of users in 2010 of Tor, which is the only available circumvention tool that provides high-level privacy protection. The anonymity factor jumped from seventh position in 2010 to third in 2012 as shown in Table 24.

	Change (%)	Priority (2012)	Priority (2010)	Change (priority)
Speed and stability	-0.2%	1	1	0
Free of charge	-1.2%	2	2	0
Anonymity	5.5%	3	7	4
Blocking-resistant	-2.2%	4	3	-1
Privacy/security	-1.1%	5	4	-1
Robustness	-1.0%	6	5	-1
User-friendliness	-1.1%	7	8	1
Accessibility	-6.1%	8	6	-2
Cross-platform	-4.3%	9	9	0
Small file size	-5.8%	10	10	0

Table 24: Comparing factors for better circumvention (2010 and 2012)

Taking these results into account, it is important for developers of circumvention tools to consider using methods that provide users with anonymity. This is not an easy task but it might be useful to consider models similar to Tor to achieve this.

Another interesting finding was the importance that respondents gave to the blocking-resistant factor, which implies that the software should have an ability to dynamically change its settings or servers so it will not be blocked by the authorities. This was an important factor for both 2010 and 2012 surveys and will probably remain for a while given that governments are trying to find ways to disable circumvention solutions.

The battle between developers and governments is on multiple fronts. First, there is surveillance, which could be addressed by anonymity. Second, ISPs may try to disable or throttle the service, which could be dealt with through a strong blocking-resistant approach. Tor has a built-in mechanism through which users can manually find 'bridges' that allow them to overcome most cases of IP blocking. Some tools do better than others when it comes to resisting being blocked. Alkasir lacked the blocking-resistance capacity, which is why it was blocked in Saudi Arabia and China. Future plans to improve it would require integrating a more sophis-

ticated mechanism that can detect an attempt by an ISP to block its proxy servers and take measures accordingly.

Privacy and security were the next important factor in the answers to both surveys, as users do not want their computers to be damaged or their personal information or data to be stolen. The security factor in ensuring that logs of users are not kept is important because of the potential risk of revealing users' behavior with their associated IP addresses, which may put some users at risk if this information is sold or abused. It is worth noting that some circumvention tools were reported to have sold the information of the users to authorities (Donovan, 2009).

The next important factor was robustness in its ability to confront all types of content from flash videos to demanding 3D gaming systems and VOIP protocols. This is an added value that Alkasir has, because it can be used with a number of applications in addition to the Web browser.

The other remaining factors were somewhat of similar importance, with user-friendliness becoming a greater priority for 2012 respondents, and this may be considered a tip for developers to ensure that their interfaces are in fact easy to navigate and are localized in the language of the users. Alkasir's biggest contribution perhaps is that it came out with an Arabic / English dual-language interface, making it easy for Arabs to use effectively.

Having cross-platform compatibility received a low rating, which is surprising given the booming mobile and tablet market industry that will require applications to run on different platforms. It is to be noted, however, that the growth in the mobile sector is exponential, so as time progresses, there will probably be a rise in importance of cross-platform applications, and that is to be taken into consideration.

Through personal communications with some of Alkasir users, there were several requests to have a mobile app that can circumvent censorship on Android phones. This is a priority for the future stage of Alkasir's development.

The file size, on the other hand, was ranked least in terms of importance, which is a reasonable outcome given that the software is downloaded only once and users may end up taking the effort and pain to download it even if it is a relatively large file as long as the other factors are met. Furthermore, with improving bandwidth services in the region and the world, the issue of file sizes would no longer be a concern.

It was also of interest to see if the frequent users of Tor were in fact interested in anonymity, and so a Pearson's chi-square analysis was done for

all circumvention tool choices and the answers to the factor of anonymity, and, indeed, the results, shown in Table 25, confirmed the expectation that users of Tor were the ones with the highest value (r = 32.6); so the association between the usage of Tor and the importance of anonymity to users has been empirically established in the survey's data.

	Web-based proxy	Ultrasurf	Hotspot Shield	Tor	Dyna Web	Gpass & FirePhoenix	JonDo	Your-Freedom	VPN
r	18.1*	5.6	21.3**	32.6***	5.3	7.8	15.6*	8.7	8.99
p	0.006	0.469	0.002	0.000	0.5	0.252	0.016	0.191	0.174

* $p < 0.05$, ** $p < 0.01$, *** $p < 0.001$

Table 25: Pearson's chi-square analysis of the association between usage of a tool and anonymity

Circumvention seen as insufficient

The study has thus far empirically demonstrated how Internet censorship is practiced in the Arab world and how circumvention is used and how it can be improved for the use of content producers as well as regular users. However, the question that presents itself is how the international community and foreign actors could help in the face of growing Internet censorship in the region.

An impressive combined number (from the 2010 and 2012 surveys) exceeding 2,500 respondents from the Arab world decided to give their perspective and answer this important question in the form of ranking one of the following actions that the world could do to limit Internet censorship in the Arab world:

- Pressurize governments to end censorship
- Support activist efforts financially and morally
- Support circumvention software developers financially and morally
- Help victims of censorship take legal action against the government
- Encourage reforms of laws dealing with Internet usage
- Others (open comment)

Supporting circumvention software developers financially and morally was given a high rank, with 1,030 saying it is always appropriate for the international community to do so and an additional 435 seeing it as mostly appropriate. However, this turned out to be the second most important step. The first, however, was encouraging reforms of laws dealing with Internet usage. The word "encouraging" here is key as it suggests a soft approach. This was also consistent with the fact that the highest disapproval was for the first option in pressurizing government to end censorship. This is a rather interesting finding because it reflects something that not many would consider important in an Arab setting, that is, using force is not as productive as using other persuasive approaches. Sanctions, wars, condemnations, and other similar measures meant to pressurize a country to give in to the demands of the international community have been ranked lowest by respondents in this survey and considered the least preferable approach to combat Internet censorship.

Figure 18 shows a snapshot of responses in addressing the problem of Internet censorship with an international effort. Helping victims of censorship take legal action has also been viewed as an important step by a healthy 1,368 who said it was always or mostly appropriate to do so. Although supporting activists' efforts on the ground to combat Internet censorship was somewhat supported, it was the second least preferred step, which indicates that a significant portion sees it as less beneficial than the other steps.

If we take the Arab context into account, having activists receive foreign funding to confront their government even in the court of law is not always preferred. Egypt is an example of a country where several donor agencies and international offices were raided many months after the removal of Mubarak from power (Beaumont, 2011). This shows how sensitive Arab governments are when it comes to having activists receive support from abroad. One of the respondents explicitly expressed an objection to this option by saying:

> Generally I don't support outside support, but if it is for global peace, then education is key.

This implies a preference of education and training from international actors over outright intervention in the form of paying legal fees or other forms of pressure.

Respondents also suggested additional methods of which the most prominent was having foreign governments stop selling filtering software

to authoritarian Arab states, which is indeed a point raised by earlier mentioned literature and confirmed by several respondent comments on this matter. One respondent indicated that legal reforms were needed, not in Arab states, but in Western governments so that they could introduce laws to stop their own companies from selling tools that suppress free speech elsewhere around the world.

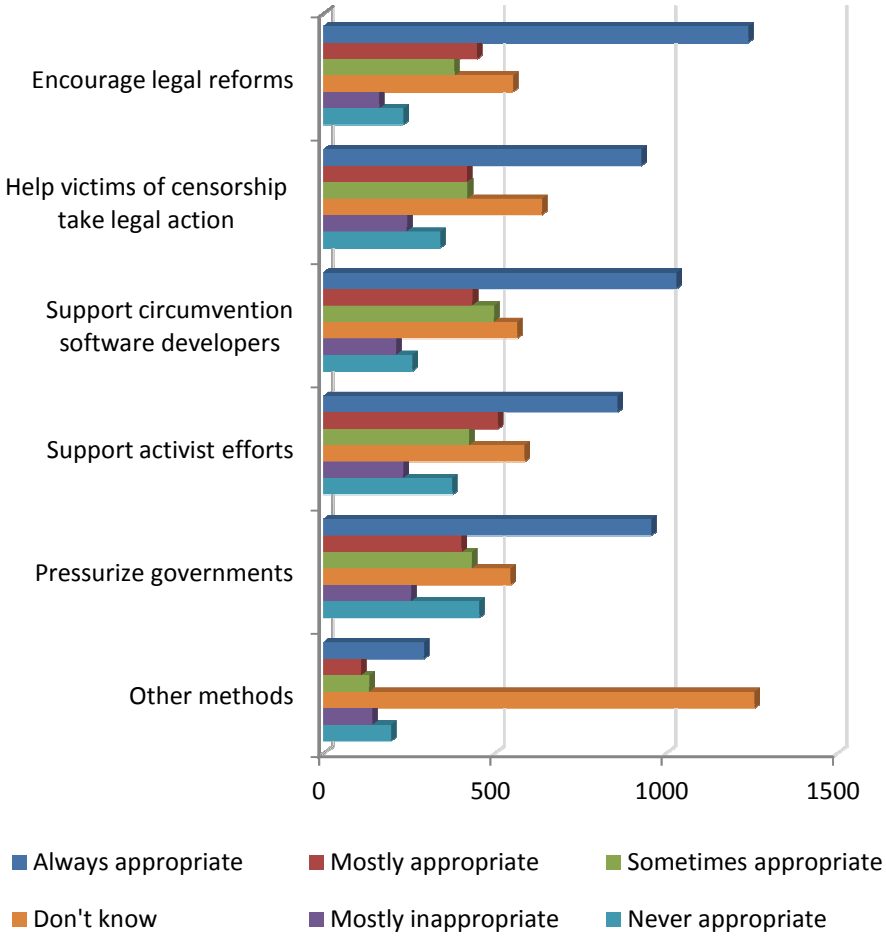

Figure 18: Suggestions to the international community on how to help in limiting Internet censorship

In summary, there were calls for a comprehensive program to combat Internet censorship that includes developing censorship circumvention tools and supporting developers and programmers to create more robust and efficient solutions. But there is also need to encompass a series of other measures from legal reforms both in the West and in Arab countries, by supporting educational programs that highlight the importance of free speech on the Internet to government and societal representatives and to support victims by raising their awareness about their rights based on the UN conventions. Imposing a solution was not suggested by most respondents and is hardly the right approach, particularly in a region that had already suffered a lot from foreign intervention.

In the next chapter, a thorough analysis for each of the four case studies—Tunisia, Egypt, Yemen, and Syria—will be made with an emphasis on the context and events unfolding on the ground and how they affected the level of filtering and uses of Alkasir. The aim is to address the second research question by comparing what censored content users were interested in vis-à-vis what governments were censoring to better understand the practice and motivations behind censorship in the different contexts.

Chapter 7: Case Study Findings

Database entries for Alkasir users in the four sampled countries Egypt, Syria, Tunisia, and Yemen were analyzed and findings revealed interesting differences between the four in terms of the intensity and response of users to Internet censorship in their countries. This chapter addresses the first and second research questions that aim at understanding the mechanisms of censorship and how activists tried to overcome them. In this chapter, I present four cases, each corresponding to one of the four countries.

These cases were suggested as an easy way to identify patterns that may exist in particular periods of time for particular countries. They are not meant for generalization to other countries or even for the same countries outside the period covered by the study (2010–2012). Furthermore, as they only deal with Internet filtering, they should not be considered a representation of all forms of Internet censorship. They correspond to the levels of URL submissions by Alkasir users and visits to approved websites through the internal browser. There are no guarantees that the submitted URLs include all the blocked URLs because it may well be that there were censored websites that were not reported by Alkasir users.

The four case studies on Tunisia, Egypt, Syria, and Yemen have resulted in findings that presented four distinct models of Internet filtering. Each of those models was named metaphorically based on the shape its graph represented: cliff, peak, mountain range, and slope.

Tunisia: The Cliff Model

Tunisia was one of those countries that had a relatively good number of Alkasir users since the program was launched in 2009 till January 2011 (Al-Saqaf, 2010). By the time former President of Tunisia Zine El Abidine Ben Ali fled the country on January 13, 2011, there were 277 installations and 466 reports of 102 censored unique URLs that were visited over 623 times through the internal browser of Alkasir. As shown in Table 26, the number of reporting unique URLs started with fifty-two in October 2010, going down to thirty-one in November, and then growing much higher to eighty in December. Several Tunisian Alkasir

Month	URL reports	Unique URLs
2010-10	65	52
2010-11	33	31
2010-12	85	80
2011-01	16	9

Table 26: The number of reported URLs in Tunisia

users often reported censored URLs actively, verifying that they were using the program to report and circumvent censorship.

On the day Ben Ali left Tunisia, Alkasir detected what could be perceived as having the censorship switch turned off, leading to a sudden plummeting in the number of new reported URLs.

The server detected that URLs that used to be blocked were no longer filtered and, hence, Alkasir server did not allow access to them through the proxy server and the number of reports of censored URLs has taken a nosedive, resulting in a graph that looks like a cliff as shown in Figure 19. When zooming in further to see when the highest reports happened in December, they were found to have occurred on 21 December, when seventy unique URLs were reported. That was four days after the street vendor Mohamed Bouazizi self-immolated. One could reasonably assume that it may have taken several days before there would be a strong reaction by Alkasir users and an attempt to report those blocked URLs in reaction to what had happened.

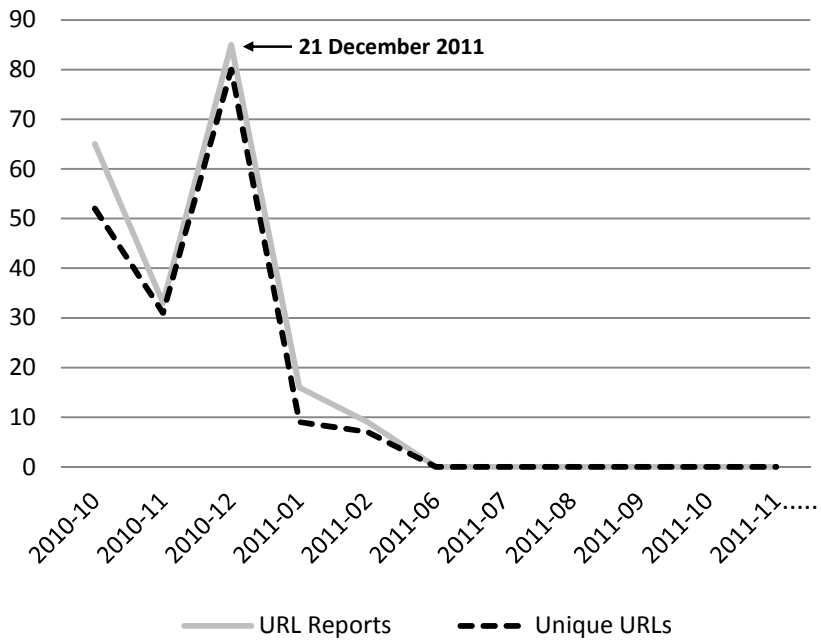

Figure 19: User censorship reporting activity reporting in Tunisia (cliff model)

To put it into context, it is important to note that Tunisians reached the tipping point when the street vendor Mohamed Bouazizi set himself ablaze on December 17, 2010, in the small poverty-stricken town of Sidi Bouzid. One could argue that the action taken by Bouazizi may have not merely been because of the frequent confiscation of the fruits he used to sell. It was rather because he was unable to have his plight heard by the governor of Sidi Bouzid, as documented by multiple sources (De Soto, 2011).

In other words, technical censorship of websites was merely another form of the censorship that prevented Bouazizi and others from expressing their views about the harsh treatment of police and the hard living conditions, which led to his dramatic suicide, resulting in Ben Ali fleeing Tunisia and the subsequent lifting of Internet censorship (Ghannam, 2011).

Until mid-January 2011, the reporting of censored websites was relatively high and included various categories of content. Data extracted from old records of Alkasir when censorship was at its peak reflected a focus on websites that contained news and opinion content, including Aljazeera's website. When taking a look at the service category of the websites blocked in Tunisia, we find a rather interesting divergence between the priorities of the government compared to those of users. The service categorization of censored content, shown in Figure 20, demonstrates that the government focused on adding to the blacklist as many information websites as possible, including those with dissident content, human rights reports, and a variety of other informational websites.

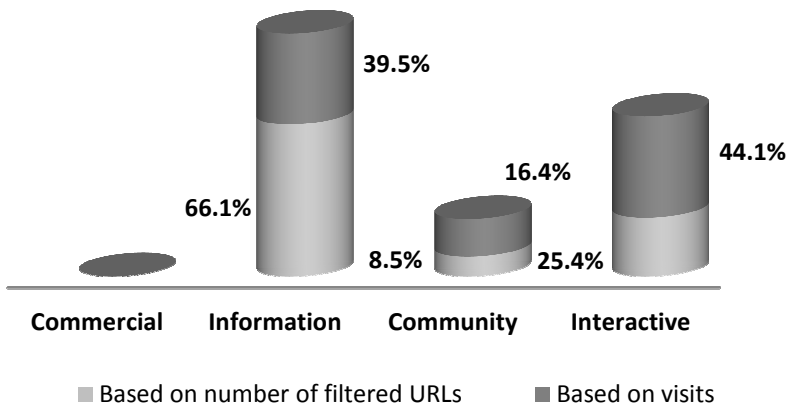

Figure 20: Service category for blocked URLs in Tunisia

Meanwhile, users were more interested to access interactive, service-oriented websites that would allow them to communicate through means other than telephones. Among the most popular interactive websites that were accessed were those allowing users to open censored websites through proxies and circumvention tools. This reflects shrewdness on the part of Tunisian users to evade censorship through additional circumvention tools apart from Alkasir.

In 2010, social media were picking up pace, and because Facebook was not blocked in Tunisia at the time, there was no need to use Alkasir to access it. Blocked websites that provided community-forming and -engaging services were still not popular enough at the time compared to blocked news and other information websites. The general content categorization shown in Figure 21 further confirms that the authorities have slightly misjudged what the users were after as they have been building up longer blacklists of server-managed websites while it was query-based sites such as search engines, communication sites, and proxies that were of more interest to the users.

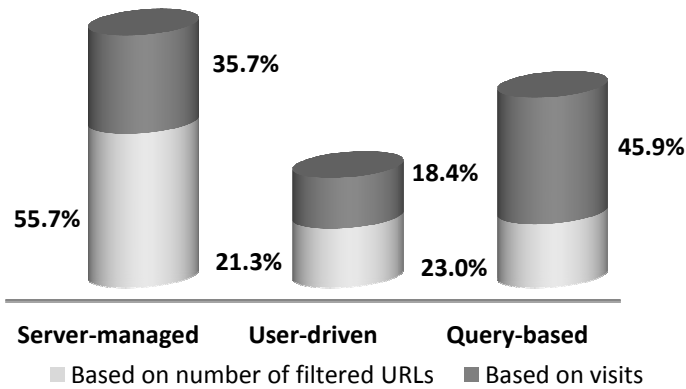

Figure 21: Content category for blocked URLs in Tunisia

The top categories of censored URLs[106] is shown in the pie chart in Figure 22, which clearly indicate that the regime was focusing mostly on news and opinion websites and not on social networking. However, less-known social networking websites were also blocked.

[106] Not all URLs were categorized as some were not possible to fit into any category and were left out.

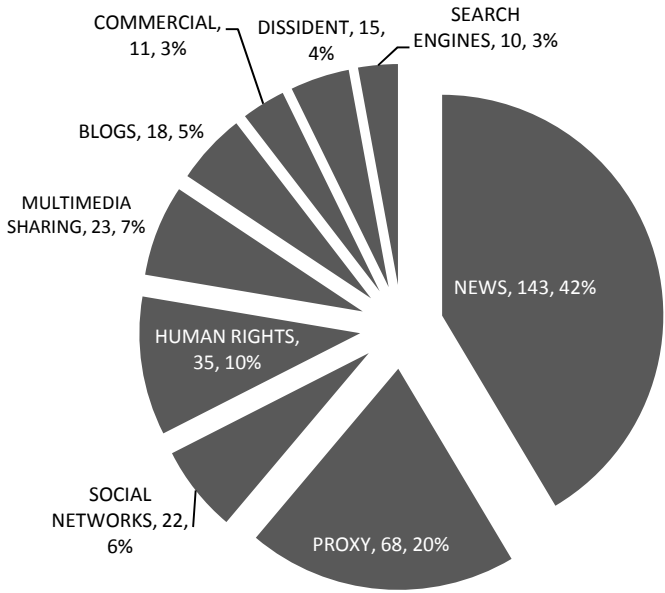

Figure 22: Categorized censored URLs in Tunisia based on submissions

Proxy sites appear to have been reported widely, indicating that some users used Alkasir to access other circumvention tools that were later utilized instead. This meant while Alkasir may have not ended up being the ultimate tool of choice, it did serve an important role in granting users access to the preferred circumvention tool. Human rights websites were the third target, which shows that several users may have been human rights advocates or activists. Such websites could be a source of information as well as a means to send complaints about human rights violations.

News websites were on top of the requested content followed by multimedia and proxy websites. In fourth place come dissident websites. There was also strong appeal for critical and dissident websites targeting the Ben Ali regime (e.g., pdpinfo.org, albadil.com). Those results confirm findings of previous research by ONI, which pointed out that Tunisia was one of those countries where censorship of political and news online content and

some social network and multimedia websites was extremely pervasive, well before the revolution started (ONI, 2010).

The top-ten list of blocked websites based on the number of visits via Alkasir's internal browser is as follows:

Website	Category
3. aljazeera.net	News and Opinion
4. fsurf.com	Proxy/Circumvention
5. youtube.com	Multimedia Sharing
6. multiproxy.org	Proxy/Circumvention
7. proxytools.sourceforge.net	Proxy/Circumvention
8. kalima-tunisie.info	News and Opinion
9. ultrareach.com	Proxy/Circumvention
10. rrdb.org (defunct)	Proxy/Circumvention
11. anchorfree.com	Proxy/Circumvention
12. dailymotion.com	Multimedia Sharing

The most visited website through the internal browser was aljazeera.net, which is the official website of Aljazeera pan-Arab news channel. It had already been blocked months before the December protests started but the number of visits and reports increased after the protests. This could be attributed to the fact that the website had a feature that allowed Tunisian activists to have any raw videos and photos taken with mobile phones uploaded directly for screening and potentially appearing on the news broadcast of the TV channel.

Aljazeera's role in the Arab Spring is well-documented (e.g., Sultan, 2013; Filiu, 2011, p. 53) and the fact that its website took the leading position among all blocked websites in terms of number of visits via Alkasir confirms its relevance and appeal to users on the ground during the peak of the revolution.

The second most visited website was fsurf.com, which was a Web-based proxy that allowed accessing other censored website. Tunisian users have apparently developed the competence and skills that allowed them to identify a working proxy website that would then allow them to open other censored websites without the need to report them via Alkasir. It was a shrewd move because Alkasir only allows access to blocked websites and if a blocked website is a proxy website, then effectively, users can use Alkasir to access all websites through that proxy.

As indicated earlier, apart from Aljazeera, and the prominent outspoken news radio website Kalima (kalima-tunisie.info), all the other websites on the top ten list are either proxy or multimedia websites, which highlights the interest of Tunisian users in bypassing the firewall. But censorship in Tunisia was not only practiced online. Peaceful protests were often confronted with violence, as in the case when security forces sporadically clashed in 2008 with hundreds of nonviolent protestors in the mining town of Gafsa, arresting and charging dozens (Freedom House, 2010b).

While many websites were censored for years before the Tunisian revolution began, the number of activists who had been able to use circumvention tools such as Alkasir had reached a point where information about the mass protests obtained from blocked websites was circulated through non-blocked websites and through some mainstream media portals, which in turn presented the information to the public domain (Garcia Marin, 2011, p. 7).

Furthermore, the relatively high Internet penetration ratio of 39% (Internet World Stats, 2012) and the wide use of ICTs were found to be instrumental for the success of the Tunisian revolution (Lang & De Sterck, 2012). This high penetration level may have been a strong motive for the Tunisian regime to practice this aggressive form of censorship, particularly as it clearly targeted political and news content as demonstrated by the data extracted from Alkasir's server.

However, once Ben Ali fled the country and censorship stopped, Alkasir became of no immediate value for users in that country. The cliff model represents a case when significant censorship is reduced to almost zero overnight, creating a cliff-like graph as shown earlier in Figure 19.

Egypt: The Peak Model

Unlike all the other four Arab countries examined, previous research indicated that Egypt did not have a history of nationwide Internet censorship (ONI, 2009) and not many Alkasir users were found to be based in Egypt. Even when there were users, they were mostly accessing websites censored by a particular ISP and not nationally. But in January 2011, suddenly, Alkasir servers received dozens of reported URLs, as shown in Table 27. And as demonstrated by the graph in Figure 23, this led to a sudden spike forming a peak in the number of reports from users eager to report censored URLs.

Month	URL reports	Unique URLs
2010-10	5	2
2010-11	8	4
2010-12	2	1
2011-01	55	13
2011-02	36	14
2011-03	15	4
2011-04	1	1
2011-05	2	2
2012-07	1	1
2012-08	15	7
2012-09	3	3

Table 27: The number of reported URLs in Egypt

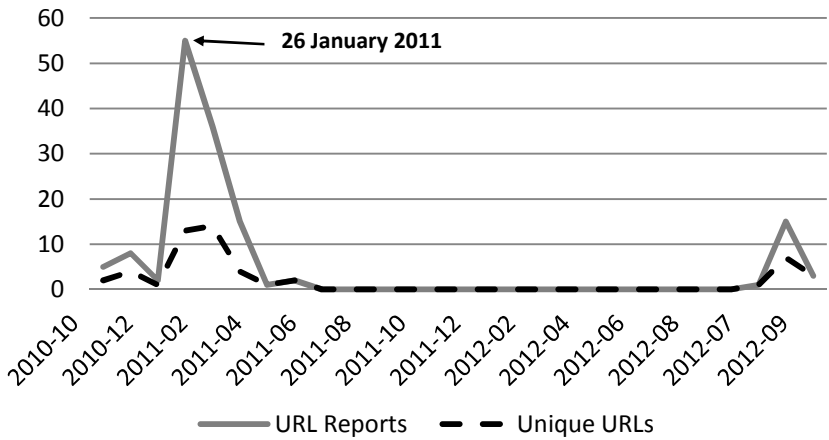

Figure 23: URL reports and unique URLs in Egypt (peak model)

When examining the data up close, and upon analyzing the days of January 2011, which witnessed the spike, it was revealed that twitter.com got the highest number of requests for that month with 1,595 accesses, separated by a large gap from the second and third most accessed websites: facebook.com and dostor.org, which is the website of an opposition newspaper critical of the Mubarak regime.

The only websites that were ever confirmed to have been blocked were very limited in the case of Egypt, which is in total contrast to the other three Arab countries. This meant that the mapping of Internet censorship based and services, categories and content of Egypt is not useful as there was no censorship to speak of except for the aforementioned spike that was caused mainly by the blocking of twitter.com.

The main category that appears to have been censored in Egypt is social networking websites, which implies that user-driven content has been perceived as a threat to the regime's control of information at a time when social media websites were actively used to mobilize public opinion against it. The data have shown that among all URLs reported, twitter.com received the highest with over 1,500 reports on January 26, followed by facebook.com with seventy-three reports, while dostor.org was reported forty-seven times.

As the developer of Alkasir, I got contacted by several Egyptian activists on January 26, telling me that they were initially unsuccessful in reaching twitter.com because when they used the program, it was possible to circumvent it. The news about Alkasir's usage for accessing Twitter spread quickly, perhaps with the help of a CNN report mentioning the software (Dougherty, 2011), resulting in the shown spike. On January 26 and January 28, some users reported Facebook and dostor.org as blocked and started using Alkasir to reach them. But the traffic from Egypt seemed to have dropped suddenly starting on January 28 because ISPs started shutting down their services and users were prevented from connecting to the Internet altogether.

The relatively high Internet penetration in Egypt of 26% (Internet World Stats, 2013b) meant that Internet could be a useful tool for mobilizing crowds and starting protests in major cities. But that did not last long because ISPs were ordered to cut off access to the whole population (Singel, 2011), leading to a situation where neither Alkasir nor any other circumvention tool could be helpful. The Internet was reconnected again on February 2 (ibid.), and, based on Alkasir records, the websites that were blocked a few days earlier were also unblocked.

It is true that Alkasir's use in Egypt was very short and limited. Nonetheless, the messages that were sent using the software as well as other circumvention tools were able to make a difference and facilitated the delivery of timely content to Facebook and Twitter despite the government-imposed filtering. Such content was also available for access by international media such as Aljazeera, which in turn helped spread the mes-

sages further (Filiu, 2011, p. 53). Ultimately, the public protests led to the resignation of Mubarak and the clearing of the way to a change in the regime.

The sudden censorship in Egypt of a popular website such as Twitter, which may have not necessarily been used only for political protest and spreading dissident messages, appears to have triggered a strong reaction verified by Alkasir's usage patterns. The desire to break free from online restrictions could be a motivator for proactive and aggressive action in times of crises, and people will work very hard and very fast to get access to the online resources they were restricted from reaching.

The two blocked websites (facebook.com and twitter.com) belong to the community service category because they are both meant to have users engage with each other actively. Furthermore, the websites were user-driven as a main content classification as their content is produced by the end users with little involvement from the website owners or managers. So if we take those into account, we could confidently conclude that the main motive behind suppressing those websites was restricting users' capacity to produce content and engage others, hence eliminating the social interaction and mobilization that social media are known to provide.

Meanwhile, dostor.org belongs to the information category, as it is a newspaper website known for its critical views and articles targeting the authorities. It is a server-managed website with a central administration that is not user-generated. It was interesting to see that the website was only reported to be blocked by four ISPs while eight ISPs blocked facebook.com and nine blocked twitter.com. The number of ISPs in the database helped measure the pervasiveness of censorship as well as the dedication of Alkasir users to report the specific URL in question.

The fact that Egypt had no earlier record of censorship prevents the possibility of doing a further analysis similar to the one done for Tunisia, Syria, and Yemen. Nonetheless, the level of impact created by censoring three websites, facebook.com, twitter.com, and dostor.org, have shown how powerfully devastating Internet filtering could be, particularly at a very critical historic moment for the country. As it has happened once, Internet filtering could happen again, and it is a good lesson for many activists on the ground in Egypt to be well-prepared in advance for any potential censorship of a major website. Circumvention tools are available and could be used regardless if there is censorship or not. Hence, getting sufficient training and know-how is crucial for the next possible wave of Internet filtering.

Syria: The Mountain Range Model

Syria was by far the Arab country with the highest number of Alkasir users. As of October 1, 2012, the number of installations was 22,460, which constituted over 85% of all installations coming from the four sampled countries.

Syria even ranked high globally, as it only came second only to Iran in terms of the number of Alkasir installations. The increase in the usage of Alkasir in Syria was particularly noticeable after the fall of the Ben Ali presidency in Tunisia and the number continued to rise after the Egyptian revolution picked pace and lead to the toppling of Mubarak.

After this sudden rise in the number of reports in January, as shown in Figure 24, the situation appeared to calm down until users started reported again in July 2011, which was the period when the number of defections from the army reached critical levels, culminating in the creation of the Free Syrian Army (AFP, 2011).

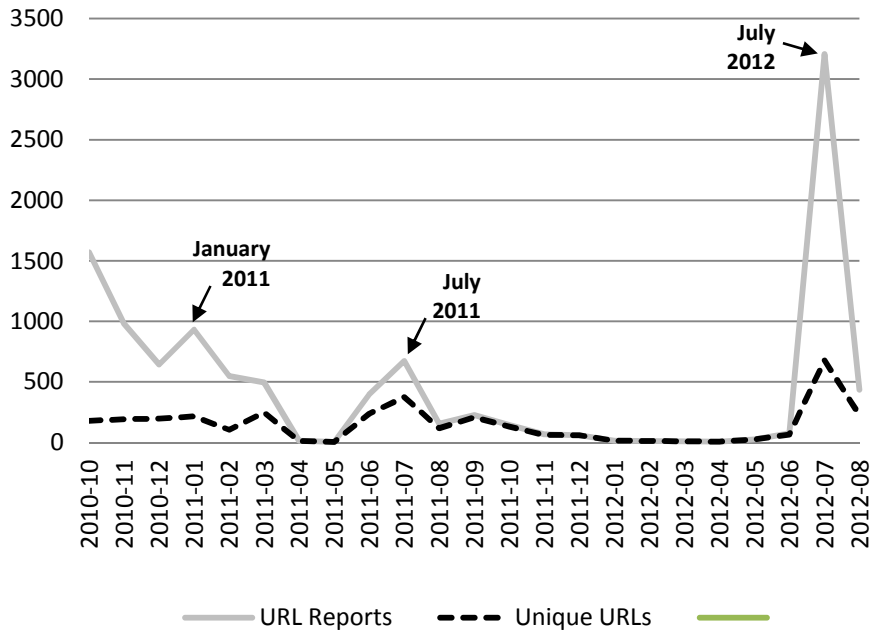

Figure 24: Level of user activity in reporting blocked URLs in Syria (mountain range model)

This has triggered an influx of censorship reports by Alkasir users. A few months later, it was reported that the Syrian government used sophisticated US-produced software named Blue Coat Filtering to censor and practice surveillance of the Web, which raised the question of whether the American company Blue Coat violated the trade ban by the US trade embargo (Valentino-Devries, Sonne, & Malas, 2011).

After July 2011, the activity on Alkasir server once again subsided gradually, until the highest level of reports of censored URLs was recorded in mid-2012, when a spike was witnessed, as shown in Table 28. As will be described in-depth later, those influxes were triggered in parallel with developments on the ground. Unlike reports in Egypt and Tunisia, which were in the hundreds, in the case of Syria, they were in the thousands.

It is possible to conclude from this that there was an information control war between the government in the form of censorship reflected in the number of unique blocked URLs and netizens using circumvention tools including Alkasir. Users of the software tried to resist by submitting any new URLs they could confirm to be censored, so all Alkasir users in the country could also get access to them.

While there were bursts happening every once in a while over the long period from October 2010 to September 2012, when zooming to a particular period where there were noticeable increases in reports such as during July 2012, similar influxes in that micro level would still appear as clearly demonstrated in Figure 25.

Month	URL reports	Unique URLs
2010-10	1,571	178
2010-11	983	192
2010-12	645	197
2011-01	933	216
2011-02	550	105
2011-03	496	247
2011-04	14	13
2011-05	4	4
2011-06	395	236
2011-07	674	374
2011-08	154	118
2011-09	227	207
2011-10	144	131
2011-11	67	63
2011-12	61	60
2012-01	16	16
2012-02	12	12
2012-03	9	9
2012-04	7	7
2012-05	25	25
2012-06	76	65
2012-07	3,207	677
2012-08	435	226
2012-09	393	270

Table 28: The number of reported URLs in Syria

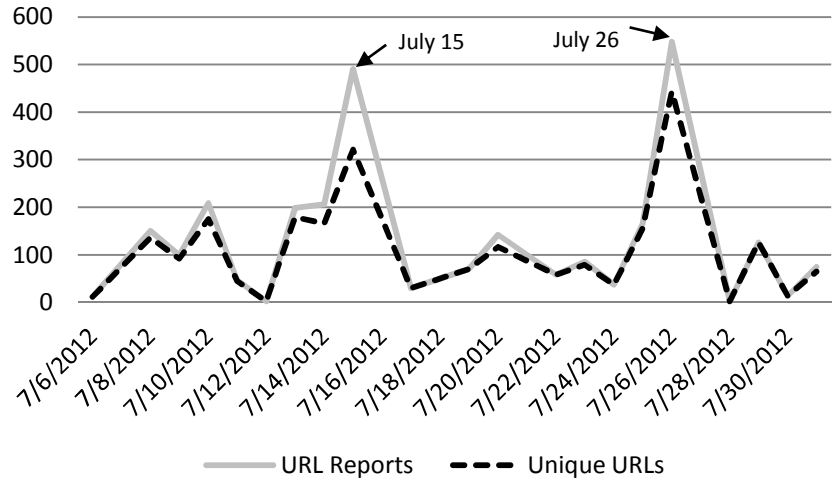

Figure 25: User activity in reporting blocked URLs in Syria in July 2012

Metaphorically, this resembles a mountain range that is not easily predictable as it may depend on other developments on the ground. They demonstrate a state of restlessness from both sides: the government in maintaining a grip on freedom of expression on the Internet, on the one hand, and Alkasir users, who appear to have mobilized themselves to use the software more effectively, on the other.

It would be important at this stage to know when URLs were reported the most during the period of this study as that could help understand whether censoring websites was potentially caused by the developments on the ground.

The highest level of any number of URLs reported in one month in all four sampled countries was in Syria in July 2012 when 677 unique URLs were reported a total of 3,207 times. To understand what may have triggered this influx of reports in July, we can zoom into that month to find that the highest number of reports came mainly on two occasions, as Figure 25 shows. The first was on July 15, when the Free Syrian Army announced that it had started operation "Damascus Volcano and Syrian Earthquake" to liberate the capital Damascus (Karouny, 2012), and the other was on July 26, which was one of the bloodiest days of the war with over 200 killed as per the revolutionary sources (Abeer, 2012). Although it

is not possible to verify the direct connection between those events with the decisions by the government, the hypothesis of a connection is what emerges from the available data.

Upon examining the general service category of the blocked websites in Syria, a remarkably different image appears compared to Tunisia. As shown in Figure 26, the authorities have been heavy-handed on information websites ranging from those containing dissident content, news, and human rights reports to various other websites with no interactive or community services. But those websites information websites were rarely visited through Alkasir. In fact, the software was mostly used to access websites with a community orientation. Facebook dominated not only the social networking category, but all categories, as well.

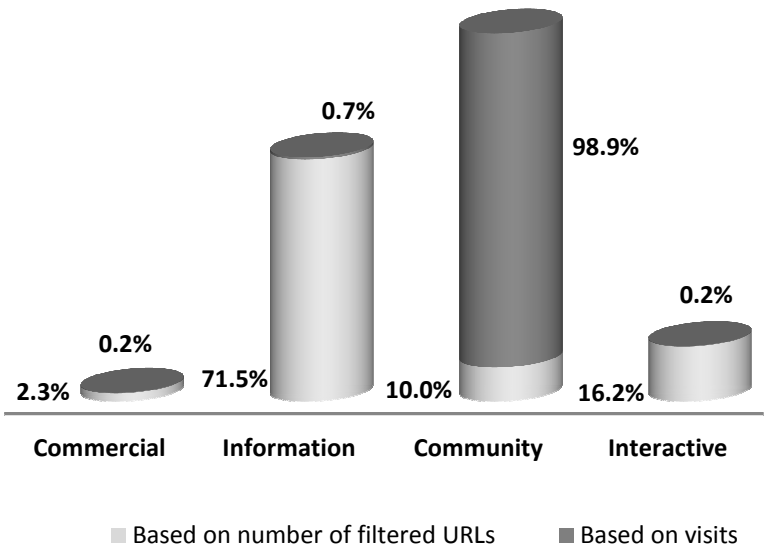

Figure 26: Service category for blocked URLs in Syria

As can be seen, the views this category received were almost 99% of all visits. As these data were collected toward the end of 2012, it shows that users were increasingly eager to access community websites vis-à-vis the case of Tunisia in 2010 when most visits were to information and interactive websites.

In essence, while the Tunisian authorities appear to have lacked clarity about what blocked content users were pursuing, the Syrian regime seems to have understood that community content is what needed to be blocked, so it blocked Facebook in an attempt to limit the possibilities of activists and dissidents from mobilizing themselves as they did in Tunisia and Egypt. However, that did not stop the authorities from also piling up tens of news websites on blacklists as well. However, those websites appear to have not been appealing to the majority of users, who were instead seeking social networking websites and were trying to reach them through circumvention tools such as Alkasir.

Also unlike Tunisia, Syrian users used Alkasir's internal browser more actively, and this may be attributed to the improvements that new versions of Alkasir brought to the browsing experience in 2011 and 2012 in addition to the possibility to use it with Facebook with relative ease. Interactive services were also accessed but mainly to download programs such as Skype.

When it comes to the general content of the blocked websites, the situation becomes even clearer; as shown in Figure 27, over 99% of all traffic was going to user-driven websites. It illustrates the understanding by the government of the dangers of user-driven websites compared to others, which is perhaps why Facebook was blocked. However, this also meant that users in Syria would be increasingly reliant on circumvention tools to gain access.

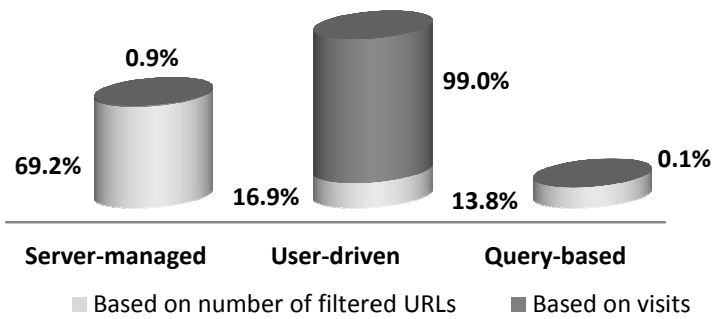

Figure 27: Content-type category for blocked URLs in Syria

Figure 28 represents a breakdown of the second-stage categories of accessed websites.[107] In terms of sheer number of times URLs were reported, it was found that the news category received the highest number of reports followed by social networking, proxy, and multimedia URLs. This indicates that there was tremendous interest by users to report the inaccessibility of news websites. What would be interesting at this stage is to see if the interest in reporting blocked URLs in certain categories correlates to the number of visits to those blocked websites.

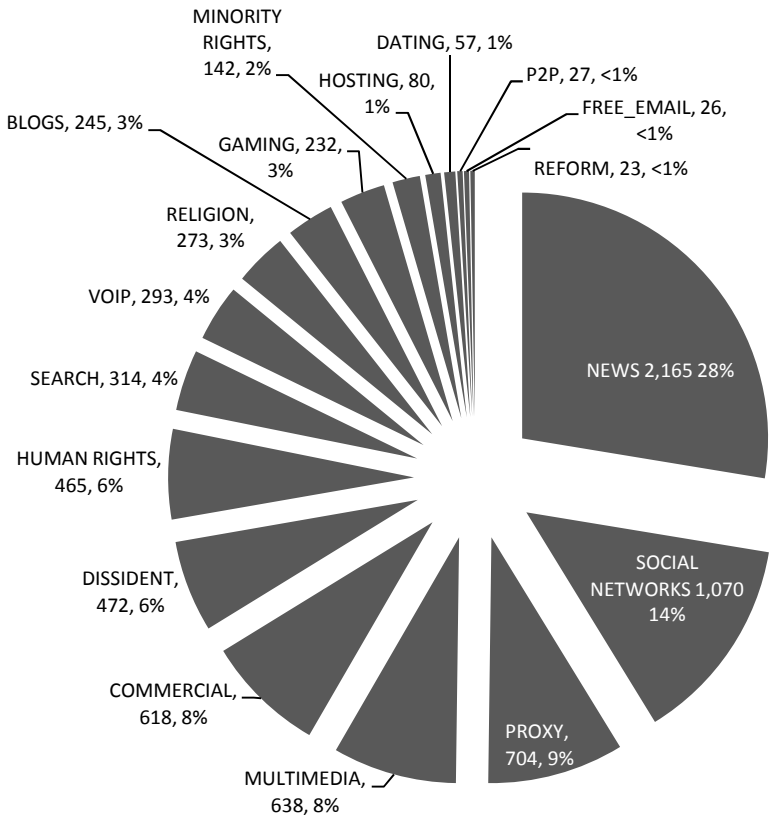

Figure 28: Categorized blocked URLs based on times reported in Syria

[107] This only takes into account URLs that were found to have a clear category. Those websites that were not categorized were left out of this data.

Taking a look at the very same URLs but from the perspective of the visits by users, a different picture emerges. As shown in Figure 29, social networking websites received around 92% of the accesses to all blocked URLs. And within that category, it was found that facebook.com constituted 97% of all visits.

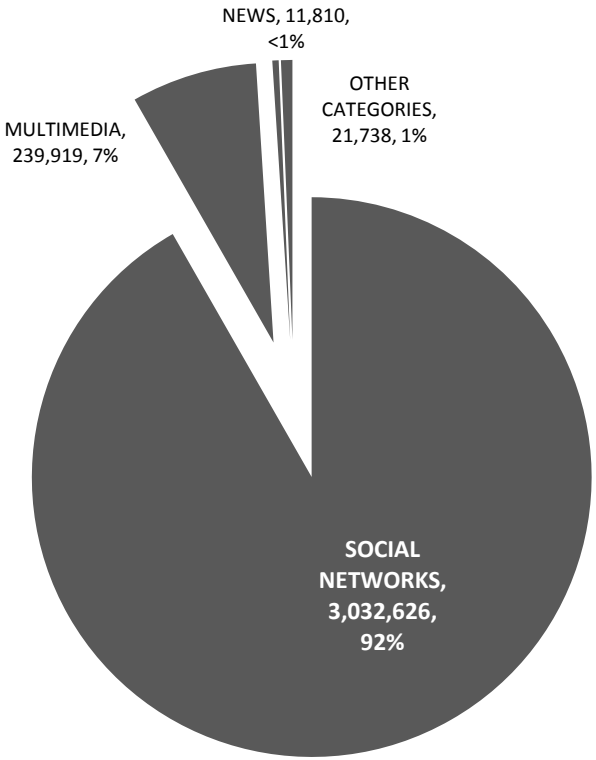

Figure 29: Visits of blocked URLs based via internal browser in Syria

Furthermore, the second place went to multimedia sharing websites, with youtube.com having the whole multimedia sharing-category almost exclusively to itself with over 99.6% of the visits. The other categories had much lower ratios, including news, which just had less than 1%, signaling a dominant presence of Facebook on the social networking cluster and YouTube on the multimedia sharing cluster. This indicates that users were mostly interested in accessing facebook.com and not in the frequently reported blocked news items.

It is important to note that those Alkasir users who report blocked websites are a small fraction of the total number of users, many of whom may have never reported of blocked of websites, but who use the software exclusively to access blocked content.

Data revealed that facebook.com received over 2.5 million visits while youtube.com came a distant second with just over a quarter million. All other websites received very little attention in comparison.

The top-ten list of blocked websites based on the number of visits was as follows:

Website	Category
1. facebook.com	Social Networking
2. youtube.com	Multimedia Sharing
3. tagged.com	Social Networking
4. mig33.com	Social Networking
5. all4syria.info	Dissident
6. aawsat.com	News and Opinion
7. netlog.com	Social Networking
8. store.ovi.com	Commercial
9. skype.com	VOIP
10. adobe.com	Commercial

Facebook has become almost the exclusive destination for Alkasir Syrian users. It is worth noting that only Syria is blocking it persistently while Tunisia, Yemen, and Egypt only blocked it for short periods of time, making meaningful comparisons difficult. This may have been expected given that Facebook, according to Alexa ranking service, is among the two most visited websites in the world, the other being google.com. And although one can suggest that Facebook was used intensively for publishing news and mobilizing campaigns against the Syrian regime, it is not possible to decisively say that Alkasir users were using Facebook for such purposes given that the platform is for general purpose and is not confined to activism.

All first four websites are global and do not target Syria specifically. However, All for Syria (all4syria.info) is a dissident website with a strong anti-regime and pro-revolution tone. It presents news from the battlefield and is the only Syrian website on the top ten in terms of visits. Alsharq Al-

Awsat (aawsat.com) is a Saudi-affiliated London-based daily that often reports about developments in the country. Given the fact that Saudi Arabia had had suspended its diplomatic ties to Syria and called for the transfer of power from Assad (Derhally & Abu-Nasr, 2011), it was not surprising to see its affiliated media websites blocked. The top-ten list of the most accessed URLs also includes commercial, VOIP, and social networking websites that are, as indicated earlier, commonly blocked in Arab countries.

In summary, with the regime's unabated and persistent efforts to restrict free speech online using Internet filtering, the data have shown an equally persistent resilience on behalf of the software users who have continuously reported inaccessible URLs to have them added to Alkasir's database and thereafter accessible to other users living in Syria. This intense activity from both sides is what created the impulses that were reflected in the graphs of Figures 24 and 25 that resemble the mountain range model.

Finally, I wish to include in this section concerning findings about Alkasir usage in Syria one additional aspect that puts a human face to the big data that I presented through tables and graphs. On several occasions, I have received feedback from users in Syria indicating how important it was for them to use Alkasir as a circumvention tool that allowed them to publish videos and images reflecting what was going on the ground. Furthermore, I also learned that Alkasir was useful in acquiring access to Skype's voice chatting service because the website and its servers are blocked by the regime.

One user sent an e-mail describing how the use of Alkasir helped save lives by allowing him to send a warning to a particular neighborhood to leave the area due to an imminent attack by government forces. On another occasion, he indicated that the software was used to call humanitarian organizations asking for urgent relief, which consequently resulted in the delivery of badly needed assistance.

These findings and experiences reflect an important aspect of liberation technology that confirm the theoretical stance of the use of circumvention tools as a piece of technology that could be of positive value to individuals living in oppressed conditions and being subjected to unjust censorship.

What can be added, based on the above testimonials, is that such technologies, resembled in this case in circumvention technology, could occasionally be life-saving when regular communication channels and means are cut off during a conflict or civil war.

Yemen: The Slope Model

Despite its considerably pervasive level of Internet censorship, Yemen is rather peculiar compared to the other three Arab countries because it has a rather low Internet penetration of 14% (Internet World Stats, 2012). Yet despite that the Yemeni government seems to have been determined to stop access to websites that criticized the regime along with many others.

Internet censorship reports were received well before the Arab Spring. However, there was an apparent steady increase, as shown in Table 29, until the number of reports peaked in March 2011 and thereafter declined considerably until July 2012 when reports of filtering resumed but at a lower rate, indicating a dwindling or diminishing effect. When connecting the two peaks of 2011 and 2012, it becomes apparent that a *slope* emerges as illustrated in Figure 30.

Month	URL reports	Unique URLs
2010-10	81	35
2010-11	73	37
2010-12	63	42
2011-01	53	34
2011-02	89	32
2011-03	150	81
2011-04	75	74
2011-05	33	32
2011-06	8	8
2011-07	9	9
2011-08	5	5
2011-09	1	1
2011-10	3	3
2012-01	3	3
2012-03	2	2
2012-05	1	1
2012-06	2	2
2012-07	97	97
2012-08	1	1
2012-09	38	38

Table 29: The number of reported URLs in Yemen

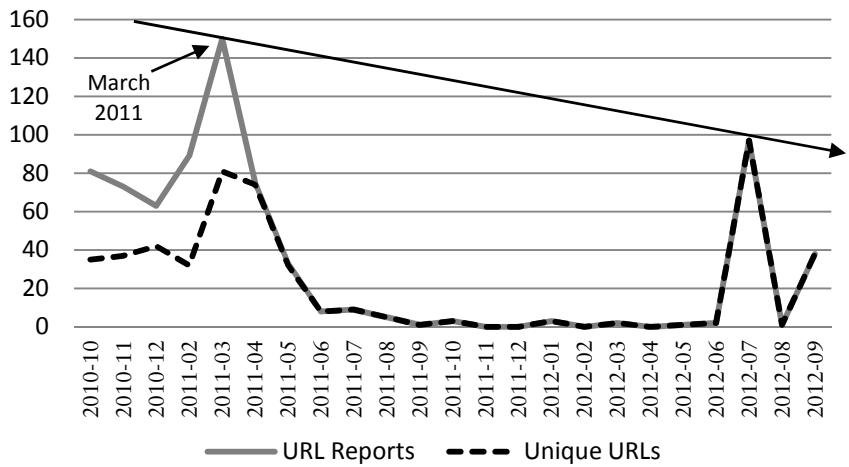

Figure 30: User activity in reporting blocked URLs in Yemen (slope model)

A quick look at the graph illustrates that the highest number of reports was in March 2011 that marked the bloodiest month of the Yemeni uprising as it witnessed the sniper attack that killed dozens of protestors, consequently leading to major defections in the army and to the significant weakening Saleh's regime (Boone, 2011). It is hence understandable why Alkasir users were reporting blocked URLs intensely during that month. When the situation started to get out of Saleh's control amid national and international pressure to relinquish power, the regime signalled fewer attempts to censor the Internet. As pressure on Saleh continued to mount, he eventually abandoned power through a GCC-brokered agreement signed in Jeddah in November 2011. Since March 2011, it looks like there was very low reporting activity, which would have resembled a scenario similar to that of Tunisia. However, unlike Tunisia, it was apparent that the authorities did not stop censorship totally because another reporting wave emerged in July 2012. However, it was much smaller in scale and was followed by a third yet smaller wave in September. With every new wave, the number of reports got smaller and weaker, creating a downward trend represented with the slope shown earlier in Figure 30. It appears that the slow and steady decline in censorship mirrored the slow and steady political transfer of power from Saleh to Hadi.

When it comes to service categorization of blocked websites, it was found, as shown in Figure 31, that over 70% of blocked URLs were providing informational services. Those websites ranged from dissident portals that called for the overthrow of the regime to news websites that often had extremely critical anti-regime opinions.

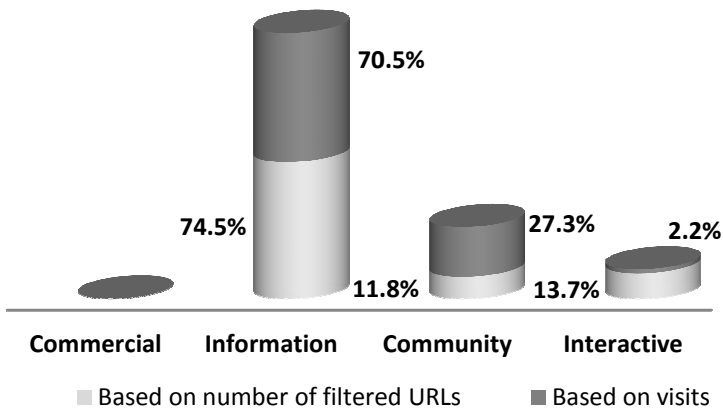

Figure 31: Service category for blocked URLs in Yemen

Within a context of an authoritarian regime where press laws prohibit criticizing the head of state, the first option would have been to close down a website containing prohibited content. However, many of those websites were managed by exiled individuals and hence, the government cannot pursue them legally nor can it close down their websites. Hence, the only other option was to block access to them using Internet filtering.

By 2012, Yemenis remained behind all other countries in the region in terms of accessing social networking websites. Nonetheless, users appeared to be ahead of the government at the time as their access to blocked websites offering online community-engaging services have had a significant share of the visits (27.3%). The interactive service websites, however, have not garnered attention compared to Tunisia.

Similarly, the general content categorization of filtered websites in Yemen, as shown in Figure 32, reveals greater interest in gaining access to readily available server-managed websites instead of user-driven platforms such as social networking websites. This may be attributed to the fact that Facebook was not blocked nationally and hence, there was no reason to use Alkasir to access it. However, a third of all visits did target blocked user-driven websites, which mainly included discussion forums that often included hotly debated national issues (e.g., ye22.com).

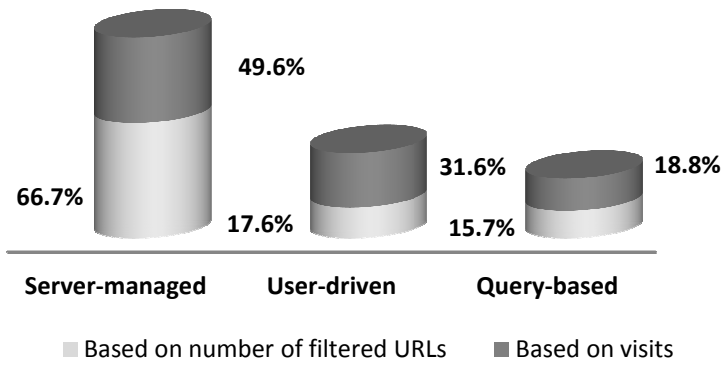

Figure 32: Content category for blocked URLs in Yemen

Going one additional layer deeper in analyzing what sort of websites were censored in Yemen during the period of this study, it was found, as shown in Figure 33, that the most often reported URLs were of news and

opinion content. They were then followed by social media and closely followed by dissident websites, which were known to publish harsh critical articles targeting the regime. The most aggressively pursued websites in the dissident group, however, were those calling for secession of the south of Yemen, which prior to the 1990 unity, was named the Democratic Republic of Yemen. Content on those websites could be labeled as 'harmful to national unity' and so such content would typically be reason for prosecution if published in regular print media.

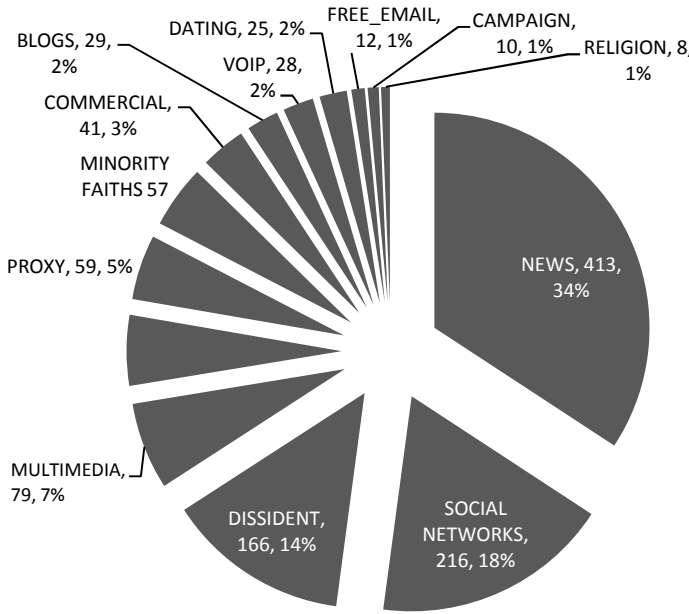

Figure 33: Categorized URLs based on times reported in Yemen

Unlike Tunisians, users of Alkasir in Yemen were, to some degree, keen on using the internal browser, which resulted in significant numbers that allowed an overall assessment of which websites were the most visited.

The top-ten list of blocked websites based on the number of visits was as follows:

Website	Category
1. yemenportal.net	Search Engine/Aggregator
2. dhal3.com	Dissident
3. ye22.com	Social Networking
4. almasdaronline.com	News and Opinion
5. sadaaden.com	Dissident
6. adenpress.com	Dissident
7. al-teef.com	News and Opinion
8. wikimapia.org	Other
9. adengulf.net	Dissident
10. forum.sh3bwah.maktoob.com	Dissident

It was natural for my own website (yemenportal.net) to be on top of the list of the most accessed in Yemen given that my motivation behind building Alkasir was partially based on my desire to help Yemenis access it. It is of value to point out, however, that the contents on the website were a diverse set of news, opinion, blog posts, and videos mostly focusing on Yemen. However, much of the content that appeared on the website contained anti-government and, in fact, anti-Saleh views, which I did not filter out despite requests from the Yemeni authorities. This led to the website being blocked and Alkasir to be born.[108]

On the other hand, dhal3.com is a popular dissident discussion forum that openly promotes discussions around secession from the north to reestablish the former Democratic Republic of Yemen. It was not identified as a social networking websites because its inclination was to have discussions purely around dissident issues connected to the Southern struggle for independence.

The most popular discussion forum on Yemen affairs is ye22.com, which came third for its reputation as a totally unfiltered and open platform. It had repeatedly been blocked and unblocked, showing that the authorities were keeping an eye on it for a while. The fact that almasdaronline.com was also blocked despite it being an independent news website could be attributed to its critical and often factual and deep investigative reporting about corruption cases connected to the Saleh regime. The website was affiliated to a weekly newspaper that was also in

[108] Find more about the link between Alkasir and yemenportal.net in Appendix A.

trouble with the authorities on more than one occasion. This shows that the regime did not recognize or care whether criticism is offline and online as both would be confronted and suppressed, albeit using different means.

The others on the list were dissident and news websites except Wikimapia, which is put in the "other" category as it provides interactive maps. There is no definitive answer as to why it was blocked, but when it first emerged, it was rather controversial as it allowed users to pinpoint the geographical coordinates of President Saleh's palaces, and other military installations due to its user-driven nature. Posts about those locations were shared on social media to identify and expose the real estate properties that Saleh and his cronies owned. This capacity of Wikimapia was probably enough to prompt the regime to block it.

Unlike Syria, Yemen did not block Facebook permanently, nor was there evidence that it blocked it nationally. But when it did block it, it took the top position in terms of visits through the internal Web browser.

It was found that the news category had a total of about 19,000 visits, with no single website totally dominating over the others. The most visited news websites were almasdaronline.com, and al-teef.com, which often published corruption-exposing articles targeting the regime. Dissident content came second, with over 16,000 visits representing websites that had a clear stance opposing the former regime of Ali Abdullah Saleh. This significant appeal to dissident content has actually set Yemen apart from the other three sampled countries and suggests that Yemen has a more politically diverse cyber sphere with a presence of a significant divide particularly between the south-oriented websites and the others. While more in-depth empirical research will be needed to understand why dissident websites have a significant appeal in Yemen,[109] the typology of authoritarian Arab states presented by Rugh (2004) categorized Yemen as a diverse state when it comes to press and broadcast media. The results demonstrated in this section appear to support to some extent the possibility of applying the theory to the cyber sphere given the diverse set of blocked dissident websites that were managed from within Yemen during the period of this study.

Generally speaking, Internet censorship remained evident despite the fact that Saleh left office in February 2012. To understand why this has

[109] This may be attributed partly to the fact that tensions between the northern and southern populations are reflected in some of the dissident websites that Alkasir users reported.

happened, one could consider that unlike Egypt and Tunisia, which resulted in the removal of the ruling party from power, when the deal was reached through the GCC initiative to have Ali Abdullah Saleh leave power, he remained in charge of the ruling party, which was in charge of 50% of the government. Among those loyal to Saleh who remained after the power transfer deal was the minister of telecommunication (Al-Qadhi, 2011), who has the power to make the ultimate decisions on website filtering. On the one hand, there was an evident easing of restrictions to a significant degree. If this trend continues, it is expected that censorship of websites that do not include nudity content would be lifted completely.

It is timely at this stage to recall that while repression, unemployment, corruption, injustice, poverty, and other hardships were leading factors behind the Tunisians' and Egyptians' uprisings, those very factors, especially the economic ones, were even more prevalent in Yemen. Yet, the limited impact of Internet censorship in Yemen can be attributed to low Internet penetration of around 14% at the time, which singled out the country from the other three. Nonetheless, Internet's role was amplified, as was the case with Tunisia and Egypt, through Aljazeera and other satellite TV channels, which were fought rather vigorously by the Saleh regime (Sharqieh, 2011). This suggests that authorities in Yemen were more concerned about traditional media than about the Internet or social media for that matter.

Emerging Patterns

It was apparent from the reviewed four countries that users responded actively in reporting blocked URLs. Furthermore, news and opinion content appear to have dominated in terms of number of submitted URLs. Yet it was also evident that social networking websites were what most users wanted. The case of Syria is a good example of a country where social networking has become quite popular, as demonstrated by Alkasir's usage patterns. With millions of visits only through the internal Web browser, this is a strong indication of the role Alkasir may have played in connecting Syrians with each other during the period of this study.

However, Alkasir users in Tunisia did not utilize the internal Web browser mainly due to the fact that censorship in that country ended a few months after the study started. Hence, only visits recorded to blocked websites in Egypt, Syria, and Yemen made it possible to carry out meaningful empirical measurements and show the usage of Alkasir users.

Earlier sections about the four countries indicated a huge gap between levels of Alkasir usage in Syria compared to the other countries. But, on the other hand, the most accessed website through Alkasir overall is facebook.com, which is a strong indicator that social networking is a desired activity by users in these countries. Yemen emerged as the country where users accessed news and dissident content the most, setting it apart from the others in that respect. One important observation that emerged from analyzing usage of Alkasir both in reporting and in accessing blocked websites during various periods during October 2010-October 2012 was that there was similarity among the four countries in the apparent connection between the intensity of political developments happening on the ground in each country and the level of reported Internet censorship.

The highest level of reporting activity in Tunisia occurred just after the initial protests that started in Sidi Bouzid. However, Tunisians also used Alkasir well before that critical juncture. The increasing levels of Internet filtering prior to December 2010 were telltale signs of a growing level of anxiety by the Tunisian regime of the impact of the Internet. But when Ben Ali fled the country, it moved all the way from a pervasively censoring country to no censorship at all. This is why the graphs showing levels of activity represent a cliff, as the usual filtering practices were suspended.

In the Egyptian case, a spike in activity was noticed at a particular period of time when the regime took a hasty decision to block two of the most widely used websites in the country, namely, facebook.com and twitter.com, before the major rally planned for Friday January 28. This action resulted in a strong reaction by users who used Alkasir in a very limited, albeit effective way. Egyptian Alkasir users intensified their reporting of the censorship of those two websites until the Internet itself was disrupted.

The Syrian case was by far the more serious and relevant with thousands of reported URLs. The level of usage in Tunisia, Egypt, and Yemen is dwarfed in comparison to Syria, as demonstrated in Figure 34, which combines the four models together in terms of URL reports.

Censorship in Syria illustrated how URL-reporting efforts from Alkasir users came in waves and not in linear patterns due to the needs and developments on the ground. Syrian activists have continuously been using Alkasir to report and access blocked content throughout the period of the study but had—as shown earlier—some significantly higher levels of use during major developments on the ground, for example, when the Free Syrian Army was officially formed in July 2011.

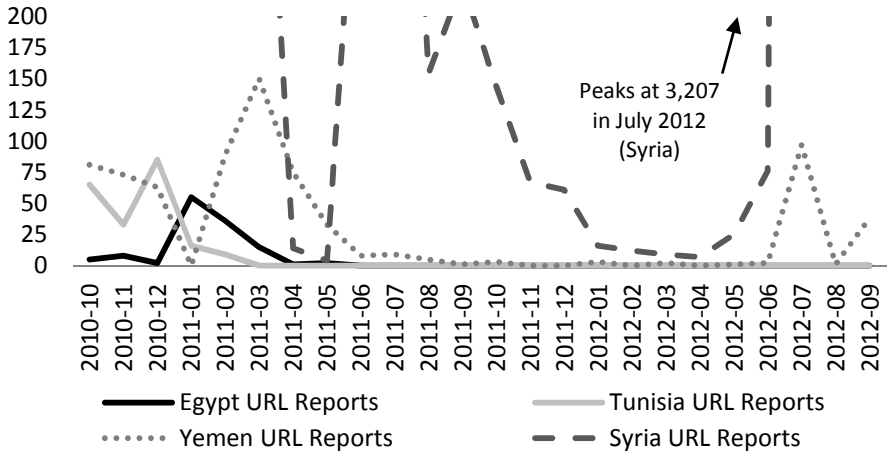

Figure 34: A combined graph showing the number of URL reports for the four case studies (Tunisia, Egypt, Yemen, and Syria)

Yemeni Alkasir users, on the other hand, submitted reports intensely when popular protests started to grow in number and size during the first months in 2011 after a period of systematic use of Alkasir in 2010. As the political situation started to change, a diminishing pattern of usage in terms of reporting blocked websites emerged. With the new regime taking charge in 2012, the enthusiasm to block websites subsided to some degree.

This established connection between actual developments on the ground and the level of Internet filtering as demonstrated by Alkasir usage highlights the threat perceived by authoritarian Arab states of the role that Internet in general and social networking in particular can play to undermine their legitimacy and ability to influence public opinion during times of crises. The findings suggest that while this perceived threat resulted in having them practice censorship in the form of Internet filtering, tools such as Alkasir allowed users to identify cases of filtering as they happened and use the software to overcome such censorship.

While Internet censorship targeting popular social networks such as Twitter and Facebook may have not been enough to stop activists from uploading and sharing content using circumvention tools, the number of users that utilize circumvention tools remains negligible when compared to the total number of Internet users in those countries, which indicates a strong need to promote the use of circumvention technology.

Chapter 8: Summary and Conclusion

This study is a pioneering attempt set out to explore how Arab regimes practiced Internet censorship and how users used technology to fight back. It also is an attempt to explore the view of Arab Internet users about censorship and circumvention. The study aimed at answering the following five questions:

- *Q1. Why do regimes use Internet censorship practices and how do those practices affect users in the Arab world?*
- *Q2. What usage patterns emerge when users are provided with a technology that can be used to report and circumvent Internet filtering?*
- *Q3. How do Arab users view the appropriateness of blocking access to websites containing particular types of content and what could explain those views?*
- *Q4. Why do users in the Arab world use circumvention tools and how can such tools improve their effectiveness?*
- *Q5. How can the international and foreign actors help limit the effects of Internet censorship?*

The aim of the study is to fill a knowledge gap pertaining to the experiences and struggles of Arab Internet content producers and users when trying to express political/security views on accessing content freely on the Web. As the study covered the period of the Arab Spring (from late 2010 to the end of 2012), it had a unique position in studying the use and importance of Internet censorship and circumvention tools in the context of the developments during the Arab Spring. And while this very uniqueness makes the results of this study context-bound and not readily generalizable, they contribute to the understanding of how technology could be used to empower users during times of crises in authoritarian states.

Much of the previous research around Internet censorship was focused on either specific countries such as China, the United States, and Iran or had an empirical overview of the world, including the MENA. However, neither of those studies seemed to have captured the particularities of Arab activists seeking to overcome censorship just prior to and during the Arab Spring. Furthermore, none of those studies used a crowdsourcing approach to allow regular Internet users to verify the accessibility of websites.

This study is unique in that it resulted in creating Alkasir, which is a software program that helps on two fronts. First, it empowers Arab users, providing them with an ability to overcome censorship of political content. Second, it creates an opportunity to gather data about cases of website filtering in countries where the program is active. Furthermore, by establishing Alkasir firmly as a global censorship circumvention tool, the study's impact is continuous, with possibilities to extract and use data about censorship patterns from across the globe for future research.

This research is interdisciplinary with elements from computer science in the creation of a software solution that helps overcome censorship of websites and elements from media and communication in analyzing access to and control of information on the Internet. Simultaneously, it is a media and communication study that provides new perspectives on the use of technology in confronting censorship of speech in an information society. It would have been difficult if not impossible to come up with the data this study has produced if it had not taken this interdisciplinary approach because of several reasons, including the inability to cover so much ground in the field in those countries to identify patterns of censorship as well as the improbability of having government agencies granting interviews and providing data revealing their censorship policies.

Alkasir was fundamental for the study because it was used to get data from twenty Arab countries through users who were willing to install the program after accepting its terms of use, run it, and voluntarily submit links of websites they suspect had been blocked. The software verifies the status of the submitted websites and grants users the right to access them if they were found to be censored and if the websites are not of nudity/pornographic content.

The other important contribution of the software was its ability to attract a large number of Arab users to answer a survey that was considerably lengthy and detailed but which had key questions that help in the understanding of various aspects of Internet censorship. With the large number of collected responses—exceeding 5,000—in a combined set of two surveys two years apart, the study has contributed to the field by providing empirical relevant data directly from thousands of users. To my knowledge, this was an endeavor that no other research project managed to do.

The empirical findings of this dissertation have shown that Internet users in Arab countries took the initiative in downloading, installing, and running Alkasir and, thereafter, reporting censorship and accessing cen-

sored URLs. Significant differences in usage levels and patterns from country to country in the Arab world were evident, and with the four Arab countries Egypt, Tunisia, Syria, and Yemen examined up close, it was quite apparent that the level of censorship during different periods of time had close connections to the level of political turmoil and activity in each of those countries. This illustrates that governments are aware of the power of the Internet and are trying to stop this power from being used by dissidents for opposition and mobilization. And yet, by censoring the Internet, governments are also affecting citizens' ability to use it for information seeking and sharing purposes.

The next five sections present answers to the five research questions posed in the study. They also include a discussion along with some reflections. Together, they sum up the contribution of this dissertation.

Internet's Transformation from a Growth Agent to a Threat

When comparing the four models that emerged from plotting the number of URL reports of blocked websites in Tunisia, Egypt, Syria, and Yemen during 2010–2012, it was possible to identify a diachronic relationship that had a domino effect on the ground in those four countries.

It all started with Tunisia, which by December 2010 already had strong Internet filtering practices as shown in Alkasir's data. However, Tunisia had at the time already taken a decision to invest and expand digital literacy and Internet accessibility to allow users to connect and use the Internet for competence building and economic growth. Although censorship of websites was pervasive, facebook.com was not among the blocked websites and was a major online platform through which users mobilized the masses to protest near vital government buildings in Tunis and other major cities. I argue that at that point, the Tunisian regime was caught off guard and realized that shutting down the Internet was too high a cost to bear. After all, a long-term strategy was already formulated by the government to expand access to the Internet, on which the country would rely for economic growth. Ben Ali had to flee the country on January 21, 2011, and, consequently, the era of Internet censorship ended, leading to a sharp fall in the number of reported blocked websites through Alkasir to zero. This development was illustrated by the cliff model shown in Figure 19.

Following the developments in Tunisia, the momentum of public protests increased and reached other Arab states including Egypt, whose Mubarak regime did end up blocking facebook.com as well as twitter.com on January 25, which was three days away from the major protest planned

for Friday, January 28 to occupy Tahrir Square in the heart of Cairo. Almost instantly, requests to download Alkasir grew sharply and reports of blocked websites spiked, resulting in the peak model shown in Figure 23. This was unprecedented given Egypt's open Internet policy and because in comparison, Mubarak's regime was not known to practice Internet filtering before. Unlike Syria, Tunisia, and Yemen, where outright website filtering was the norm, Egypt's regime sufficed with nontechnical means of censorship through prosecution and incarceration of some anti-regime activists. Not blocking websites could have been a strategic decision to encourage investment in the Internet, because interruptions and suspension of online websites in an economy increasingly relying on the Internet will not be helpful.

It was only after the fall of Ben Ali that Internet filtering was attempted in Egypt, which explains the sudden peak in usage of Alkasir. The regime apparently intervened to block websites only when all other options failed. But it proved ineffective, perhaps due to the Internet's decentralized nature, which allows accessing blocked websites through circumvention tools such as Alkasir. The regime then took the drastic measure of shutting down the Internet altogether. This meant that the power of the Internet in the hands of cyber freedom fighters appeared to pose a serious threat to the regime. But it was already too late because as interpreted from the perspective of the path dependence theory, maintaining an Internet blackout for too long was too costly given the strategic decision taken years ago to expand the Internet and have it as one of the major pillars of the economy. Without Internet access, many more people joined the protests in Tahrir Square, leading to Hosni Mubarak's resignation, which in turn resulted in a regional shock affecting other countries in the region.

In Syria, Internet filtering had already been in place for years, and in January 2011, there was a noticeable escalation of such censorship with facebook.com becoming inaccessible. Alkasir was used to access facebook.com and many other dissident and social networking websites. However, the Assad regime proved resilient and did not let go of power while maintaining a strong grip on the Internet. The complex political situation of Syria and the regional connections Assad had were enough to have him hold on to power. Meanwhile, the influxes shown in Alkasir's data during 2011–2012 support a possible association between website filtering practices and some of the major developments that happened on the ground. For example, the regime resorted to a new wave of filtering in July 2011 when many members of the regime defected and in July 2012

when the Free Syrian Army started a major operation against the regime's forces. The continuous Internet filtering practices in Syria have expanded Alkasir's usage in the country with frequent bursts of activity in reporting blocked websites, reflecting a pattern that is represented by the mountain range model shown in Figures 24 and 25.

Finally, Yemen's situation was different from the other three given its inferior Internet service sector and low Internet penetration, making the Internet less instrumental to the economy. However, Internet filtering was still practiced frequently by the government for years well before the Arab Spring. Following the fall of the regimes in Tunisia, Egypt, and Libya, Saleh's decision to peacefully transfer power resulted in a gradual decline of Internet filtering, leading to the slope model shown in Figure 30. The new transitional government in Yemen had admitted that censorship of websites was a mistake and expressed strong intentions to limit filtering to socially "inappropriate" content such as pornography.

These results confirm earlier studies suggesting the potential use of the Internet by dissidents and opposition to undermine authoritarian regimes' authority and reputation (Bowman & Camp, 2013, p. 11). They further support the view that authoritarian regimes in the Arab world limit the free flow of information, particularly during election campaigns and at critical political junctures, to minimize the advantage they could give to opposition and dissident forces and to maintain the status quo. Such a strategy has been used on traditional media and contributed to the success of keeping oligarchies ruling for several generations often with the justification of maintaining security and stability. The findings of this study point to an eagerness by those regimes to practice similar forms of censorship to establish social control and punish those websites that deviate from the social norms by having them blocked. However, and as it could be concluded from the ability of users to circumvent Internet filtering, such efforts are not fully successful.

Mechanisms and Effects of Internet Censorship

It is important to acknowledge that Internet filtering referred to in the earlier section is but one method of censorship. Mechanisms of Internet censorship have been identified to range from nontechnical to technical methods with many Arab Web content producers indicating that they have suffered from or feel at risk of being exposed to such pressure. Furthermore, the Arab Spring, which initially started to rid citizens from restrictions on freedom, has not, at least until the end of 2012, done so.

In fact, respondents to the second survey, which ran from mid-2012 to the end of the year, have clearly indicated that they were still subjected to the same mechanisms of website filtering and have in fact witnessed an escalation of nontechnical and technical censorship. It was interesting to see that it was the degree of fear and the feeling of being at risk that had surged in the 2012 survey. This can be understood within the context of a region undergoing turmoil and transformations with governments uneasy about increasing calls for liberation, and so it was natural for activists to feel afraid, anxious, and cautious. This explains the higher percentage of respondents in 2012 compared to 2010 who said that they were directly exposed to surveillance or felt at risk.

As shown clearly in the Background and Introduction chapters, the Arab world has long suffered from repressive practices on many levels, and so the fear expressed by these bloggers and Web content producers is reasonable, particularly at a time of instability.

And while nationwide Internet filtering had ended in Tunisia, and did not return to Egypt since January 2011 and has largely diminished in Yemen, it was still evident in several Arab countries including Syria, where censorship of websites escalated noticeably during the period of the study.

Viruses and malware are perhaps the most worrisome mechanism of technical censorship as indicated by the 2012 respondents. It also marks an important trend as indicated by the survey responses with users feeling threatened by technical attacks, which could effectively steal data or create security vulnerabilities. That is why the use of anonymity and encryption tools would be crucial in the future. This also demonstrates the need to do more than just rely on circumvention technology to overcome Internet censorship.

The study took an approach of surveying Internet users to get their views and experiences when it comes to censorship. A significant number of Arab content producers such as blog and website administrators have indicated that their websites were filtered at least once in the last 12 months before they filled out the survey. The existence of such censorship confirmed empirical findings obtained from Alkasir servers and validated the fact that censorship in some Arab countries was pervasive.

Although the motives behind the censorship of political/security content are not possible to establish with absolute certainty as that would require insider information from the Arab ministries of telecommunication, yet it was possible to conclude both from the data obtained from the servers of Alkasir as well as from the respondents' answers to questions about mo-

tives that political/security content is often targeted when it dealt with anti-government news and commentary or information that could undermine the reputation or legitimacy of the state.

Several studies examined in the Literature Review Chapter have shown that Arab authoritarian states often justify censorship to protect national security, religion, or morality. However, the data obtained through this study have repeatedly shown that ISPs blocked dissident websites that contained political speech that was critical of the regime. Censoring such content as a means to protect religious or moral values does not qualify as a valid argument because many of those websites do not contain religious or morally offensive content. Furthermore, the other argument that blocking websites is needed to protect national security is also rather fuzzy and could hence be abused to block virtually any news or opinion website such as arabtimes.com, which is blocked by multiple Arab states.

Hence, I argue that while such justifications are given as a rationale to censor, the main motive is most likely the regimes' desire to hold on to power by limiting any content that could undermine or question their legitimacy before the public.

The motives can also be connected to the effects of censorship as seen by Web content producers. Effects of censorship were widely felt by respondents, with the worst being a limited ability to access information and practicing freedom of expression. Those two qualities that many developed countries cherish dearly were taken away from Arab Internet users with Internet censorship practices, as verified by the data.

The adverse influences of Internet censorship affect users and Web content producers alike. From the perspective of an authoritarian regime, however, working on multiple fronts to limit any threat to its legitimacy is most effective. While Internet filtering is a prevalent censorship approach to limit recipients' access to anti-government content, other nontechnical methods targeting producers of such content could also have similar results. These approaches include targeting bloggers and content producers with prosecution, harassment, and other means of pressure. According to survey respondents, such practices have led to a reduction of the intensity and frequency of critical content.

Hence, it can be concluded that governments' declared rationale behind censorship is highly disputable, as it seems they used it mainly to retain power and push back any potential threat to their legitimacy in the public eyes. Limits to free speech based on such motives do not conform to the Milliam principle discussed in the Theoretical Framework Chapter. Such

practices are illegitimate violations of human rights as indicated in the theoretical chapter. They violate Article 19 of the UDHR, which guarantees the freedom to receive and impart information. Free speech theoreticians have expressively indicated how free speech is helpful for a deliberative democracy, and so it is only natural that efforts are made to combat those types of censorship if democratic conditions in Arab states are to be improved.

Circumvention Usage: Liberating for Users, Troubling for States

According to the server data, website filtering happened and intensified during political turbulent times. Despite the potential risks to users of circumvention tools, particularly because of surveillance and other practices, Alkasir continued to gain more users from the region, and it appears that the Arab Spring had actually given them more motivation to bypass censorship.

During the period of this study, Syria had witnessed a devastating civil war that affected large parts of the population. Yet it still had the highest number of Alkasir users among all Arab countries. It also dominated in terms of number of blocked URLs. This indicates that the level of oppression in a particular country does not necessarily mean a more passive population that would surrender and give up. On the contrary, the high influx of Syrian users onto Alkasir is an indication that the more oppressive a regime, the more likely it is that its people would seek and find new ways to overcome this oppression. In the case of Syria, Alkasir was found useful to overcome the censorship of critically important websites such as Facebook, which had over four million accesses through Alkasir's internal Web browser alone.

Egyptian, Tunisian, and Yemeni Alkasir users were also active in using the function that allowed them to report censored URLs. This allowed the mapping of censorship in the region by comparing local and remote contents of URLs and by checking to see if those URLs were blocked by multiple ISPs in the country to identify cases of nationwide censorship.

However, what was quite remarkable to see the aggressiveness of Arab governments to collectively target user-driven websites that provide free space for citizens to voice their views and criticize the state freely. Citizens have long been deprived from their right to criticize the government in traditional media, so the Internet became their refuge, and this resulted in reactions by the state, which imposed strong restrictions.

Yet users kept on finding ways to break the firewall and get their voices heard. The upward trend in targeting user-driven content is undoubtedly a serious and unmistakable indication that governments in the Arab world are increasingly fearful of their own citizens. This is a confidence and a legitimacy crisis because governments are aware of the frustrations and aspirations of the youth in changing the regimes, whose legitimacy was not obtained through free and fair elections. But as this will spell their end, those regimes resorted to Internet filtering as a temporary remedy. While governments kept adding more websites to the blacklists, users kept on finding new and innovative ways through circumvention technology to access social media platforms, which, over time, got bigger and more powerful. This is not a trend in favor of authoritarian states. The study's results have proven that circumvention technology can indeed be liberating by helping eliminate one of the major obstacles to free speech online in the Arab world, that is, website filtering.

Perhaps realizing that technical filtering alone is insufficient to control the flow of information online, some Arab governments have shown interest in using the UN to have a more dominant say on Internet governance issues as revealed during the WCIT12 meeting in Dubai. The fact that Internet filtering is unsustainable could motivate Arab governments to continue seeking ways to control the national Internet governance process from a macro level. The threat of having the ITU or any UN body that is represented by governments take over the administrative tasks from ICANN is very real and could spell trouble to Internet freedom and may change the Internet as we know it.

Arabs' Views: There are Limits to Free Speech on the Internet

One of the research questions required that survey respondents express their views about the appropriateness of blocking content that belongs to one of eleven categories: politically critical, security, anti-religion, nudity/porn, terrorism, proxy, gambling, drug dealing, hate speech, pirated, and hacking content. The findings revealed that Arab respondents differed from non-Arabs on the limits of free speech. While non-Arabs disapproved censoring anti-religious content and were split on nudity/pornography, Arab respondents overwhelmingly supported their censorship. But on the flip side, their opposition to censoring critical political speech was stronger than that by non-Arabs.

It is known that political speech in the Arab world had been suppressed for so long because whenever a new form of media emerges, governments

quickly use legislations and tough press laws to limit any potential of true free speech. However, when the Internet opened a new window of opportunity for free speech and when this window was, unlike the other traditional media, not possible to fully control by authorities, Arab users have shown a desire to protect their newly found freedom to criticize their government—sometimes anonymously— and express their minds freely in ways that are not possible in traditional media. This may explain why they were more assertive in protecting their political speech online and refusing to have it censored. This illustrates a degree of frustration with the past and a desire not to close the door again on their opportunity to breathe some freedom. Critical political content against the government was the only area that had strong anti-censorship ratings out of all the categories.

The fact that there was a rise in opposition to censorship of political/security content as well as proxy and circumvention websites in 2012 compared to 2010 could be attributed to the developments during the Arab Spring. After all, this was a development that shook the whole region and allowed people to go out to the streets to express their grievances against their governments, perhaps for the first time in generations. The data indicated a change in dynamics with more Arabs believing in their right to protest and speak out.

Non-Arabs opposed censorship of seven of the eleven categories and approved the censorship of only three: terrorism, hate speech, and illegal drug dealing. Arab respondents, on the other hand, went on to approve the blocking of anti-religion, nudity/porn, terrorism, gambling, drug dealing, hate speech, pirated, and hacking, that is, all categories except for three: critical political speech, security-related content, and proxy/circumvention.

These results could be explained in terms of the influence of Islam on most aspects of Arab culture. Supporting the opposition of anti-religion content is directly related to the revered value of Islamic symbols to Muslims. The documented protests of Arabs in the streets against the "Innocence of Muslims" controversial anti-Islam YouTube video, and the issued campaigns calling for the boycotting of Danish products on social media due to the *Jyllands-Posten* Mohamed cartoons are a couple of examples illustrating how religion is central to Arab culture. And so, the limits of free speech for religious reasons will remain a contentious issue whether on the Internet or on any other form of media.

Nudity, gambling, and the other categories whose censorship was approved by most Arab respondents are also connected to Islamic influence

on Arab culture. However, this brings us back to the theory of free speech and its limitations. Scanlon's Milliam principle has been argued to help find a way to define when and how a particular form of speech could be restricted. In the case with the Arab world, however, the bar is much higher due to religious and cultural factors.

Looking back to the time when I decided not to allow Alkasir to be used to access pornography, I believe that by taking such a decision, I reduced the chances of being attacked by Arab users, which would have resulted in greater personal risk and a reputation problem for users who are using the software for activism and other non-pornography-related activities.

Problems with Circumvention Tools

Although the concept of liberation technology has been manifested in the use of Alkasir, the software as it is, remains vulnerable as demonstrated by the actions by Saudi Arabia, for example, in blocking access to its proxy servers within the country. If Alkasir had built a stronger blocking-resistant mechanism, it could have remained actively used in China and Saudi Arabia. This illustrates the persistent and continuous struggle between circumvention tool developers on the one hand and authoritarian governments on the other. This study confirmed the validity of the findings of a 2011 study by the Berkman Center that indicated an increasingly more difficult environment for the successful operation of circumvention tools.

And therefore, for circumvention tools to remain effective, they need to improve their blocking-resistance. In addition, speed, stability, and being freely available were indicated by survey respondents to be of utmost importance for tools to be used widely. What is noticeable, however, is the rise of the importance of anonymity. Allowing users to be anonymous when connecting was not of much concern in the 2010 survey, but in 2012, it gained significant attention. It was closely followed by privacy and security. The aforementioned three factors could be seen as a unit to help protect users and their safety. After the Arab Spring, it has become apparent that surveillance, monitoring, and tracking of activists and users who publish politically critical content could be pursued. Having a circumvention tool that would prevent such surveillance is of immense value for activists at risk. Nonetheless, anonymity, as mentioned in the Literature Review Chapter, can be abused by cybercriminals, which needs to be taken into consideration.

Awareness of Circumvention Tools and the Gender Divide

The study has found that the percentage of Arab circumvention tool users compared to the general Internet user population is still quite low. If this is to change, there will be need to raise awareness about circumvention tools and methods. The strongest message that one could conclude from the survey results concerning the best ways to raise awareness about such tools is that confidentiality and trust are crucial. Respondents have indicated that training novices on the use of circumvention technologies is done best in a discreet and closed environment of trust and through face-to-face communication with other users who could provide guidance and hands-on training in a secure setting.

The study has found that the majority of Alkasir users –as can be concluded from the survey responses- were men, which is a stark reminder of the gender divide in the use of ICTs in the Arab world. Hence, specialized training for Arab women to use liberation technologies such as circumvention tools is quite important and could help create a positive impact in limiting the gender divide as well as empowering women to have greater skills to overcome censorship of their own blogs and websites.

Reordering Priorities in the Fight against Internet Censorship

As I have started this whole study with a normative view about the need to protect free speech based on human rights principles, it was therefore plausible to have the study address the question that connects the international community when all options to fix a broken free speech status caused by Internet censorship in a particular country are off the table. In such a situation, the question posed was about the steps that the international community should take to help.

A lesson that one can draw from this study is to listen first and know the Arab mindset without prejudgments or assumptions. Survey respondents indicated that their preference is not to apply external pressure on Arab regimes to abide by international human rights principles and stop filtering political speech. In fact, they preferred taking a soft persuasive step in encouraging Arab governments to apply legal reforms that would help ease Internet censorship measures. This to me was an indicator of the wisdom of Arab Internet users, who have seen that external pressure through the threat of sanctions, for example, or even mild condemnation could backfire, resulting in yet more censorship.

What also caught my attention was the deep understanding of the Internet censorship industry that some respondents have shown when they pointed their fingers at the global corporations for providing Arab authoritarian states with the filtering software used to block websites and repress free speech. They openly condemned such practices and called for taking the fight against censorship back to the democratic countries where those corporations are based.

Insights on the Future of Internet Censorship Research

While this dissertation helped shed light on the processes that were involved in Internet censorship and circumvention in the Arab world, it remains not fully comprehensive with findings that do not represent all online activism during the Arab Spring. Among the most notable problems was the inability to cover all Arab countries such as Saudi Arabia. It means that Alkasir needs to improve so it could withstand government restrictions. It also validates the respondents' note on the importance of being blocking-resistant for circumvention solutions.

The other limitation is the methodology is caused by the surveys' dependency on the software, particularly with regard to questions about circumvention and censorship. The sample would have been more representative of Arab Internet users at large if the surveys were answered by a cross section of the whole Arab Internet user base and not only by users of a circumvention tool.

However, the findings open the door to researching something even more exciting, that is, the future of social media in a world where governments will have little control over information and when censorship becomes more difficult to implement. I personally believe that Internet filtering will become a thing of the past, especially as new and more efficient circumvention tools are being constantly developed and improved. This means that governments may increasingly focus on Internet governance as an approach to hack the system from the top. It is a possible scenario that researchers and activists should be ready for.

Nonetheless, I believe that Internet studies should continue to be interdisciplinary in nature with social science scholars cooperating with applied scientists particularly as the use of technology in media studies is expected to grow due to the increasing reliance on the Internet to receive and distribute media content.

I wish here to evoke Amara's law about our tendency as humans to overestimating the short-term effects of technology while underestimating

the long-term effects. We should indeed not consider circumvention technologies as the ultimate Holy Grail that will fix the problem of Internet censorship. Circumvention tools, albeit helpful, have not been given the highest priority by survey respondents when asked about ways to fight censorship. And this is no coincidence. Internet censorship may change and transform, and hence, solutions need to be more long-term and less situational. A case in point is the mass surveillance committed by the US government as uncovered by Edward Snowden. That program along with other similar surveillance techniques adopted by authoritarian states, albeit on a smaller scale, reflect the willingness of states to practice more covert information control mechanisms compared to traditional forms of outright website blocking.

However, even if Internet filtering and surveillance are defeated using anonymizing circumvention tools, there are numerous others battlegrounds where censorship methods will probably continue to be used by repressive regimes. Among them are DDoS attacks, malware attacks, throttling of services, and many other technical methods.

One should also not to forget that repressive regimes will probably also continue with their old-fashioned traditions of information control and various other technical and nontechnical methods such as harassment, threats, legal prosecution, kidnappings, and even murder.

On the Internet governance front, it is expected that authoritarian regimes would be willing to cooperate with other similar regimes to establish alliances that may want to change the way the Internet is governed worldwide and so future studies should take that into account.

The bottom line is that this study is merely scratching the surface, and much more can be done to study Internet censorship and in parallel, promote free speech online. I firmly believe that academia and activism need not be mutually exclusive, and this very study stands in support for that argument, because it is indeed possible to have a positive supporting role for freedom of expression while maintaining high degrees of academic integrity and professionalism. The challenge of tackling Internet censorship is no longer a local domestic issue because the Internet is a global network that connects humans across borders and where geographical and national jurisdiction does not apply and where boundaries are an illusion.

I believe it is of value to take the recommendations of the respondents to heart and encourage future research to study the legal implications of Internet censorship. Studies could also try to identify means of applying necessary global, regional, and national reforms to address the issue and

ease restrictions on political speech online. Furthermore, future research could be carried out to identify to what extent the findings of this dissertation can be extrapolated beyond the studied sample.

Finally, the data that Alkasir gathered and continues to gather could be of value to cover more territory and new areas. There is also a possibility to have Alkasir users fill in future surveys as they did for this study. The software is free for users to utilize. But, in return, users can be invited to fill out future surveys and get updates about the situation of censorship in the Arab world and beyond.

An Additional Lesson Drawn

What this study illustrates is that there is something every human holds dearly and often citizens in developed countries take for granted: something that generations living under oppression always aspired to have and what young activists fought and died for; it is what many in the Arab world had long lost and have in recent years started to consider regaining again. It is the ability to speak freely without fear of repercussion.

From the early works of playwright Euripides in the 5th century BC to the Arab Spring in 2011 and beyond, censorship of speech has always existed, but so have ideas and efforts to defeat it. History is full of examples when men and women fought against censorship with a conviction that humans were born free and are entitled to express their grievances regardless of time and place.

The six years spent on this study have culminated in one additional lesson about human nature. By witnessing how Internet users openly challenged government repression and sought ways to break free from and defeat Internet censorship, they have clearly demonstrated that humans are willing to fight for freedom in creative ways regardless of time, place, and medium. And while in the past, traditional media was where much of the struggle took place, today's struggle is being fought online.

The Internet may be a new and different battlefield, but the battle remains the same. It is the battle to be *free*.

Bibliography

A Correspondent in Syria. (2011, May 24). *Fear and trembling in damascus: A pretense of calm in Syria's capital*. Retrieved November 13, 2013, from TIME: http://content.time.com/time/world/article/0,8599,2073623,00.html

Abeer. (2012, July 26). *200 Martyrs in Syria today 26-7-2012*. Retrieved November 10, 2012, from Local Coordination Committees: http://www.lccsyria.org/9595

Abu-Laban, B. (1966). Factors in social control of the press in Lebanon. *Journalism and Mass Communication Quarterly, 43*(3), 510-518.

AFP. (2011, July 30). *Syrian colonel claims big defection*. Retrieved November 10, 2012, from News24: http://www.news24.com/World/News/Syrian-colonel-claims-big-defection-20110730

Ahluwalia, P., & Miller, T. (2012). The politics of free speech. *Social Identities, 18*(6), 627-628.

Akiner, N. (207). The Jyllands-Posten Prophet Muhammad cartoons controversy: Freedom of expression or clashing of stereotypes? *Istanbul Universitesi Ileticim Fakultesi Hakemli Dergisi*(29), 7-25.

al Qaradawi, Y. (2013). *The lawful and the prohibited in Islam*. Selangor, Malaysia: The Other Press.

Alexander, L. (2005). *Is there a right of freedom of expression?* Cambridge: Cambridge University Press.

Al-Hajery, E. S. (2000, January 12). Evaluating Web filters: A practical approach. *INET 2000*. Yokohama, Japan: Internet Society. Retrieved November 10, 2012, from Internet Society: http://www.isoc.org/inet2000/cdproceedings/8k/8k_5.htm

Al-Hibri, A. Y. (1992). Islamic constitutionalism and the concept of democracy. *Case W. Res. J. Int'l L., 24*(1), 1-27.

Al-Jassem, M. (2006). The impact of the electronic media on Arab socio-political development. In *Arab media in the information age* (pp. 169-182). Abu Dhabi: Emirates Center for Strategic Studies.

Al-Kibsi, A. (2012, November 18). *No shortage of challenges for national dialogue's success.* Retrieved December 2, 2013, from National Yemen: http://nationalyemen.com/2012/11/18/no-shortage-of-challenges-for-national-dialogues-success/

Al-Qadhi, M. (2011, December 8). *Yemen's new government takes shape.* Retrieved March 5, 2014, from TheNational: http://www.thenational.ae/news/world/middle-east/yemens-new-government-takes-shape

Al-Samei, M. (2012, November 22). *In surprise visit, UN, GCC Secretary-Generals celebrate Gulf initiative anniversary in Sana'a.* Retrieved December 3, 2013, from Yemen Times: http://www.yementimes.com/en/1627/report/1647/In-surprise-visit-UN-GCC-secretary-generals-celebrate-Gulf-Initiative-anniversary-in-Sana%E2%80%99a.htm

Al-Saqaf, W. (2008). *Unstoppable trends: The impact, role, and ideology of Yemeni news Websites.* (Master's thesis). Orebro: Orebro University. Retrieved November 10, 2012, from Örebro University: http://oru.se/Extern/English/Schools/HumUS/GJC/MAGJ-student-works/Walid%20Al%20Saqaf.pdf

Al-Saqaf, W. (2010). Internet censorship challenged. In C. Strand (Ed.), *Increasing transparency and fighting corruption through ICT* (pp. 71-93). Stockholm, Sweden: SPIDER.

Al-Saqaf, W. (2012). Circumventing Internet censorship in the Arab World. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 124-138). Baltimore, MD: The Johns Hopkins University Press.

Al-Saqaf, W. (2013, November 25). *The Internet as a catalyst for change in Yemen.* Retrieved February 12, 2014, from Global Voices Online - Advocacy : https://advocacy.globalvoicesonline.org/2013/11/25/the-internet-catalyst-for-change-development-ict4d-transparency-in-yemen/

Amanpour, C., Tapper, J., Khan, H., & Radia, K. (2011, February 1). *Barak Obama urges Hosni Mubarak's departure, calls Egyptian protestors 'inspiration'.* Retrieved December 10, 2013, from ABC News: http://abcnews.go.com/International/egypt-uprising-jordan-king-abdullah-sacks-cabinet-cairo/story?id=12809623

Amar, A. R. (1991). The Bill of Rights as a Constitution. *Yale Law Journal, 100*(5), 1131-1210.

Amara, T. (2012, January 14). *Tunisians celebrate their revolution one year on.* Retrieved December 10, 2013, from Reuters: http://www.reuters.com/article/2012/01/14/us-tunisia-revolution-anniversary-idUSTRE80D0LV20120114

Amin, H. (2002). Freedom as a value in Arab media: Perceptions and attitudes among journalists. *Political Communication, 19*(2), 125-135.

Ammori, M., & Poellet, K. (2010). " Security versus Freedom" on the Internet: Cybersecurity and Net Neutrality. *SAIS Review, 30*(2), 51-65.

Amnesty International. (2010). *Tunisia - Amnesty International Report 2010: Human Rights in Republic of Tunisia.* Retrieved December 14, 2013, from Amnesty International: http://www.amnesty.org/en/region/tunisia/report-2010

Amnesty International. (2012, June 1). *Egypt must return to rule of law as state of emergency ends.* Retrieved November 5, 2013, from Amnesty International: http://www.amnesty.org/en/news/egypt-must-return-rule-law-state-emergency-ends-2012-06-01

Anderson, L. (2011). Demystifying the Arab Spring: parsing the differences between Tunisia, Egypt, and Libya. *Foreign Affairs, 90*(3), 2-7.

Ang, P. H., & Nadarajan, B. (1996). Censorship and the Internet: A Singapore perspective. *Communications of the ACM, 39*(6), 72-78.

ANHRI. (2004). *Yemen: All roads lead backwards.* Retrieved December 10, 2013, from The Arab Network for Human Rights Information: http://www.anhri.net/en/reports/net2004/yemen.shtml

ANHRI. (2009). *Freedom of expression in Egypt 2009.* Retrieved December 5, 2013, from The Arabic Network for human Rights Information: http://www.anhri.net/en/wp-content/uploads/2012/02/Freedom-of-Expression-in-Egypt-2009.pdf

Anton, D. K. (2013, June 14). *The dark days of NSA indiscriminate data surveillance.* Retrieved December 10, 2013, from http://www.canberratimes.com.au/comment/dark-days-of-data-collection-20130613-2o6yl.html

Arab Times. (2003, January 27). *Arabtimes*. Retrieved December 4, 2013, from Arab Times: http://www.arabtimes.com/englishv/english/

Arafat, A. A.-D. (2009). *The Mubarak leadership and future of democracy in Egypt*. Hampshire: Palgrave Macmillan.

Arnold, D. (2012, June 29). *Syria: A war reported by citizen-journalists, social media*. Retrieved June 29, 2013, from Middle East Voices - VOA News: http://middleeastvoices.voanews.com/2012/06/syria-a-war-reported-by-citizen-journalists-social-media-41863/

Bakr, A. (2011, June 26). *Yemen's Saleh injured by planted bomb - source*. Retrieved December 3, 2013, from Reuters - UK: http://uk.reuters.com/article/2011/06/26/uk-yemen-president-idUKTRE75P0NO20110626

Balkin, J. M. (2004). Digital speech and democratic culture: A theory of freedom of expression for the information society. *New York University Law Review, 79*(1), 1-55.

Ball, J. (2013, October 25). *NSA monitored calls of 35 world leaders after US official handed over contacts*. Retrieved November 5, 2013, from The Guardian: http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls

Bambauer, D. E. (2012). Orwell's armchair. *University of Chicago Law Review, 79*(3), 863-944.

Barendt, E. (2007). *Freedom of speech*. Oxford: Oxford University Press, Incorporated.

Barton, J. (2008). *Backdoor censorship: How media giants' copyright protection policies collide with the First Amendment*. (Doctoral dissertation). Lawrence, KS: University of Kansas.

BCDD. (2013). *Doubling digital opportunities: enhancing the inclusion of women and girls in the information society*. Geneva: ITU & UNESCO.

Beaumont, P. (2011, December 29). *Egypt police raid offices of human rights groups in Cairo*. Retrieved December 6, 2013, from The Guardian: http://www.theguardian.com/world/2011/dec/29/egypt-police-raid-human-rights-groups

Beblawi, H. (1987). The rentier state in the Arab world. *Arab Studies Quarterly, 9*(4), 383-398.

Bennett, K., Grothoff, C., Horozov, T., & Lindgren, J. (2003). *An encoding for censorship-resistant sharing.* GNUnet.

Berners-Lee, T., Hendler, J., & Lassila, O. (2001). The semantic web. *Scientific american, 284*(5), 28-37.

Bimber, B. (2003). *Information and American democracy: technology in the evolution of political power.* Cambridge: Cambridge University Press.

Black, I. (2010, December 7). *WikiLeaks cables: Tunisia blocks site reporting 'hatred' of first lady.* Retrieved December 10, 2013, from The Guardian: http://www.theguardian.com/world/2010/dec/07/wikileaks-tunisia-first-lady

Black, I. (2011, January 31). *Egypt protests: Israel fears unrest may threaten peace treaty.* Retrieved February 12, 2014, from The Guardian: http://www.theguardian.com/world/2011/jan/31/israel-egypt-mubarak-peace-treaty-fears

Black, I. (2012, July 3). *Syrian regime engages in systematic torture, says report.* Retrieved December 6, 2013, from The Guardian: http://www.theguardian.com/world/2012/jul/03/syria-torture-human-rights-watch

Blasi, V. (2010, October 23). The eclectic objective. *University of Virginia Law School's Free Speech Symposium.* Charlottesville, VA, USA: University of Virginia.

Boone, J. (2011, March 21). *Top general defects in Yemen.* Retrieved December 7, 2013, from Global Post: http://www.globalpost.com/dispatch/news/regions/middle-east/110321/yemen-general-defects-sanaa-saleh

Booth, R., & Black, I. (2010, December 3). *WikiLeaks cables: Yemen offered US 'open door' to attack al-Qaida on its soil.* Retrieved December 15, 2013, from The Guardian: http://www.theguardian.com/world/2010/dec/03/wikileaks-yemen-us-attack-al-qaida

Borg, W. R., & Gall, M. D. (1996). *Educational research: An introduction.* New York, NY: Longman Publishing.

Boucek, C. (2009). *Yemen: Avoiding a downward spiral* (Vol. 102). Washington, DC: Carnegie Endowment for International Peace.

Bouderbala, S. (2011, October 26). *Once a dissident, Tunisia's Ghannouchi now a kingmaker*. Retrieved December 8, 2013, from The Daily Start Lebanon: http://www.dailystar.com.lb/Article.aspx?id=152227

Boukhars, A. (2011, September 1). *The Lesson from Morocco and Jordan: Reform or Perish*. Retrieved December 3, 2013, from Middle East Institute: http://www.mei.edu/content/lesson-morocco-and-jordan-reform-or-perish

Bowman, W., & Camp, L. J. (2013). Protecting the Internet from Dictators: Technical and Policy Solutions to Ensure Online Freedoms. (A. Dawoody, Ed.) *The Innovation Journal: The Public Sector Innovation Journal (Special Issue on the Middle East), 18*(1), 1-23.

Bradbury, D. (2011). Routing around censorship. *Network Security, 2011*(5), 5-8.

Bradley, M. (2011, April 18). *Egypt's former ruling party dissolved—but not defunct*. Retrieved November 4, 2013, from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424052748703702004576269172473506278

Brand, S. (2001, March 3). *Founding father*. Retrieved February 12, 2014, from Wired: http://www.wired.com/wired/archive/9.03/baran.html

Brett, A. (2009). Law warp. *Index on Censorship, 38*(2), 89-95.

Bridy, A. (2009). Why pirates (still) won't behave: Regulating P2P in the decade after Napster. *Rutgers Law Journal, 40*(3), 565-611.

Brown, B. (2008). fortifying the safe harbors: reevaluating the DMCA in a Web 2.0 world. *Berkeley Technology Law Journal, 23*, 441-47.

Brown, S. (2011, April 5). *Losing Yemen*. Retrieved December 10, 2012, from FrontPage Mag: http://www.frontpagemag.com/2011/stephenbrown/losing-yemen/

Cairo, A., & Wilken, R. (2012). The Australian government Internet filter: Its scope, and its potential civil liberties implications. *Telecommunications Journal of Australia, 62*(2), 25.1-25.15.

Cannici Jr., W. J. (2007). The Global Online Freedom Act: a critique of its objectives, methods, and ultimate effectiveness combating American businesses that facilitate Internet censorship in the People's Republic of China. *Seton Hall Legislative Journal, 32*(1), 123.

Cannon, H. M. (2001). Addressing new media with conventional media planning. *Journal of Interactive Advertising, 1*(2), 28-42.

Carapico, S. (2001). Yemen between civility and civil war. *Civil society in the Middle East. 2 (2001), 2*, 287.

Carey, G., & Peker, E. (2011, October 2). *Syria opposition forms anti-assad transitional council, warns of civil war.* Retrieved November 4, 2013, from Bloomberg: http://www.bloomberg.com/news/2011-10-02/syria-opposition-forms-anti-assad-transitional-council-warns-of-civil-war.html

Casper, G. (1995). *Fragile democracies: the legacies of authoritarian rule.* Pittsburgh, PA: University of Pittsburgh Press.

Castells, M. (2002). *The Internet galaxy: Reflections on the Internet, business, and society.* Oxford: Oxford University Press.

Charlton, A. (2012, May 29). *Syria diplomats expelled by governments around the world.* Retrieved December 4, 2013, from The Huffington Post: http://www.huffingtonpost.com/2012/05/29/syria-diplomats-expelled-_n_1552189.html

Chen, T. M., & Wang, V. (2010). Web filtering and censoring. *Computer, 43*(3), 94-97.

Chick, K. (2010, June 24). *Egypt's denial of police brutality in Khalid Said death spurs fresh protest.* Retrieved December 13, 2013, from The Christian Science Monitor: http://www.csmonitor.com/World/Middle-East/2010/0624/Egypt-s-denial-of-police-brutality-in-Khalid-Said-death-spurs-fresh-protest

Chick, K. (2012, January 25). *Egypt's military lifts emergency law – with one big loophole.* Retrieved December 17, 2013, from The Science Christian Monitor: http://www.france24.com/en/20131112-egypt-lifts-state-emergency-curfew/

Chulov, M. (2012, February 27). *Syria claims 90% of voters backed reforms in referendum.* Retrieved December 6, 2013, from The

Guardian: http://www.theguardian.com/world/2012/feb/27/syria-bashar-al-assad

Cisco. (2011, June 1). *Global Internet traffic projected to quadruple by 2015*. Retrieved Nov 10, 2012, from The Network: Cisco's Technology News Site: http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003

Clemente, D. (2013). Compelled to control. *Special Report - Australian Strategic Policy Institute - International Cyber Policy Centre, October*, 1-8.

Constantin, L. (2012, December 10). *Tor network used to command Skynet botnet*. Retrieved November 3, 2013, from TECHWORLD: http://news.techworld.com/security/3415592/tor-network-used-to-command-skynet-botnet/

Couper, M. P. (2000). Review: Web surveys: A review of issues and approaches. *Public opinion quarterly, 64*(4), 464-494.

Cowie, J. (2011, January 27). *Egypt leaves the Internet*. Retrieved December 4, 2013, from Renesys: http://www.renesys.com/2011/01/egypt-leaves-the-internet/

Croteau, D. (2006). The growth of self-produced media content and the challenge to media studies. *Critical studies in media communication, 23*(4), 340-344.

Curran, J. (1978). The press as an agency of social control: an historical perspective. In J. Curran, G. Boyce, & P. Wingate (Eds.), *Newspaper history from the seventeenth century to the present Day* (pp. 51-75). London: Constable.

Dalacoura, K. (2006). Islamist terrorism and the Middle East democratic deficit: Political exclusion, repression and the causes of extremism. *Democratization, 13*(3), 508-525.

David, P. A. (1985). Clio and the economics of QWERTY. *The American Economic Review, 75*(2), 332-337.

De Soto, H. (2011, December 16). *The Real Mohamed Bouazizi*. Retrieved November 4, 2013, from Foreign Policy: http://www.foreignpolicy.com/articles/2011/12/16/the_real_mohamed_bouazizi?page=full

Deibert, R. J. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium-Journal of International Studies, 32*(3), 501-530.

Deibert, R. J. (2010). *China's cyberspace control strategy: an overview and consideration of issues for Canadian policy.* Toronto: Canadian International Council.

Deibert, R. J., & Rohozinski, R. (2008). Good for liberty, bad for security? Global civil society and the securitization of the Internet. In R. Deibert, J. Palfrey, & R. a. Rohozinski (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 123-149). Cambridge, MA: MIT Press .

Deibert, R. J., Palfrey, J. G., Rohozinski, R., & Zittrain, J. (Ed.) (2008). *Access denied: The practice and policy of global internet filtering.* Cambridge, MA: MIT Press.

Depken, I., & Craig, A. (2006, September 4). *Who supports Internet censorship?* Retrieved December 12, 2013, from First Monday: http://firstmonday.org/ojs/index.php/fm/article/viewArticle/1390/1308

Derhally, M., & Abu-Nasr, D. (2011, August 8). *Syria deaths spur growing condemnation as Saudi envoy pulled.* Retrieved December 1, 2013, from Business Week: http://www.businessweek.com/news/2011-08-08/syria-deaths-spur-growing-condemnation-as-saudi-envoy-pulled.html

Diamond, L. (2012a). Introduction. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. ix-xxvii). Baltimore, MD: The Johns Hopkins University Press.

Diamond, L. (2012b). Liberation technology. In L. Diamond, & M. F. Plattner (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 3-17). Baltimore, MD: The Johns Hopkins University Press.

Dillman, D. A., & Bowker, D. (2001). The Web questionnaire challenge to survey methodologists. In U. B. Reips (Ed.), *Dimensions of Internet science* (pp. 159-178). Lengerich: Pabst Science Publishers.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium* (pp. 303-320). San Diego, CA: USENIX Association.

Donnelly, T. (2010). A popular approach to popular constitutionalism: the First Amendment, civic education, and constitutional change. *Quinnipiac Law Review, 28*(2), 321-384.

Donovan, K. (2009, January 12). *Surprise! Net censorship circumvention tools sell user data.* Retrieved November 10, 2012, from Techdirt: http://www.techdirt.com/articles/20090111/1826033356.shtml

Dougherty, J. (2011, February 16). *Digital activists skirt roadblocks.* Retrieved December 5, 2013, from CNN: http://0-www.cnn.com.library.ccbcmd.edu/video/?/video/tech/2011/02/16/dougherty.digital.activism.cnn

Duffy, M. J. (2011). Networked journalism and Al-Jazeera English: How the Middle East network engages the audience to help produce news. *Journal of Middle East Media, 7*(1), 1-23.

Durac, V., & Cavatorta, F. (2009). Strengthening authoritarian rule through democracy promotion? Examining the paradox of the US and EU security strategies: the case of Bin Ali's Tunisia. *British journal of Middle Eastern studies, 36*(1), 3-19.

Dworkin, R. (1978). *Taking rights seriously* (Vol. 272). Cambridge, MA: Harvard University Press.

Dworkin, R. (1982). Law as interpretation. *Critical Inquiry, 9*(1), 179-200.

Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. *University of Chicago Legal Forum, 1996*, 207-216.

Ebbs, G., & Rheingold, H. (1997). Censorship on the information highway. *Internet Research, 7*, 59-60.

Eijkman, Q. (2012). Security, technology and accountability: reassessing the role of the state? *International Journal of Security and Terrorism, 3*(2), 29-40.

Eko, L. (2012). *New media, old regimes: case studies in comparative communication law and policy.* Lanham, MD: Lexington Books.

Eleiba, A. (2011, March 24). *Report on 'Battle of the Camel' spotlights Mubarak regime crimes.* Retrieved December 4, 2013, from Ahram Online: http://english.ahram.org.eg/NewsContent/1/64/8458/Egypt/Politics-/Report-on-Battle-of-the-Camel-spotlights-Mubarak-r.aspx

Emerson, T. I. (1963). Toward a general theory of the First Amendment. *The Yale Law Journal, 72*(5), 877-956.

Erlanger, S. (2010, January 4). *In Yemen, U.S. faces leader who puts family first.* Retrieved December 5, 2013, from The New York Times: http://www.nytimes.com/2010/01/05/world/middleeast/05saleh.html

ESCWA. (2012). *Status of the digital Arabic content industry in the Arab Region.* NYC: UN.

Ezrow, N., & Frantz, E. (2011). *Dictators and dictatorships: Understanding authoritarian regimes and their leaders.* New York, NY: Bloomsbury Academic.

Fahim, K. (2012, March 26). *Tunisia says constitution will not cite Islamic law.* Retrieved December 14, 2013, from New York Times: http://www.nytimes.com/2012/03/27/world/africa/tunisia-says-constitution-will-not-cite-islamic-law.html

Fahim, K., & Bakri, N. (2012, January 28). *Sharp rise in violence halts monitoring by league in Syria.* Retrieved December 4, 2013, from The New York Times: http://www.nytimes.com/2012/01/29/world/middleeast/arab-league-suspends-its-monitoring-in-syria.html?pagewanted=all

Fahmy, M. F. (2012, January 21). *Two Islamist parties win big in Egypt election.* Retrieved December 9, 2013, from CNN: http://edition.cnn.com/2012/01/21/world/africa/egypt-elections/

Fallows, D. (2008, March 27). *Most Chinese say they approve of government Internet control.* Retrieved December 14, 2013, from Pew Internet and American Life Project: http://www.pewinternet.org/pdfs/PIP_China_Internet_2008.pdf

Faris, R. M., Palfrey, J. G., Roberts, H. M., York, J. C., & Zuckerman, E. R. (2010). *2010 circumvention tool usage report.* Cambridge, MA: Berkman Center for Internet & Society, Harvard University.

Faris, R., & Villeneuve, N. (2008). Measuring global Internet filtering. In R. Deibert, J. Palfrey, & R. a. Rohozinski (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 5-28). Cambridge, MA: MIT Press .

Faris, R., Roberts, H., Heacock, R., Zuckerman, E., & Gasser, U. (2011). *Online Security in the Middle East and North Africa: A survey of perceptions, knowledge and practice.* Cambridge, MA: The Berkman Center for Internet & Society, Harvard University.

Feamster, N., Balazinska, M., Harfst, G., Balakrishnan, H., & Karger, D. (2002). Infranet: Circumventing web censorship and surveillance. *Proceedings of the 11th USENIX Security Symposium* (pp. 247-262). San Fransisco, CA: USENIX Foundation.

Federal Trade Commission. (2013, November 19). *Internet of things workshop tweets.* Retrieved December 12, 2013, from Federal Trade Commission: http://www.ftc.gov/sites/default/files/attachments/live-tweeting-ftc-workshops/ftc_internet_of_things_workshop_tweets_redacted_11-19-13.pdf

Fein, B. E. (1984). Access to classified information: Constitutional and statutory dimensions. *William and Mary Law Review, 26*(5), 805-844.

FIDH. (2010, January 26). *Yemen: In the name of national security... human rights violations in Yemen.* Retrieved December 2, 2013, from FIDH: http://www.fidh.org/en/north-africa-middle-east/yemen/In-the-name-of-national-security

Fielding-Smith, A. (2011, November 27). *Arab League imposes sanctions on Syria.* Retrieved December 7, 2013, from Financial Times: http://www.ft.com/intl/cms/s/0/bd22b52a-1917-11e1-92d8-00144feabdc0.html

Filali Adib, F.-Z., Driouchi, A., & Achehboune, A. (2013, July 23). *Education attainment, further female participation and feminization of labor markets in Arab countries.* Retrieved December 12, 2013, from Munich Personal RePEc Archive: http://mpra.ub.uni-muenchen.de/48516/

Filiu, J. P. (2011). *The Arab revolution: Ten lessons from the democratic uprising (comparative politics and international studies)*. New York, NY: Oxford University Press, USA.

Fleishman, J., & Parker, N. (2011, February 1). *Mubarak says he won't seek reelection but will stay in office 'for the next few months'*. Retrieved December 2, 2013, from Los Angeles Times: http://articles.latimes.com/2011/feb/01/world/la-fg-egypt-crowd-20110202

Foucault, M. (1977). *Discipline and punish: The birth of the prison* (Vol. 227). New York, NY: Vintage.

Foxman, A., & Wolf, C. (2013). *Viral hate: Containing its spread on the Internet*. Hampshire: Palgrave Macmillan.

Frantz, E. (2012). How and why do dictatorships survive? Lessons for the Middle East. *Bridgewater Review, 31*(2), 16-18.

Freedom House. (2009). *Freedom on the net: A global assessment of internet and digital media*. Washington, DC: Freedom House.

Freedom House. (2010a). *Freedom in the World 2010*. Retrieved December 9, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-world/freedom-world-2010

Freedom House. (2010b). *Freedom in the world: Tunisia*. Retrieved November 10, 2012, from Freedom House: http://www.freedomhouse.org/report/freedom-world/2010/tunisia

Freedom House. (2010c). *Syria: Freedom of the press 2010*. Retrieved December 6, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-press/2010/syria

Freedom House. (2012). *Freedom in the World 2012: Egypt*. Retrieved December 10, 2013, from Freedom House: http://www.freedomhouse.org/report/freedom-world/2012/egypt-0

Galperin, E. (2012, May). *Don't get your sources in Syria killed*. Retrieved December 5, 2013, from Committee to Protect Journalists: http://www.cpj.org/security/2012/05/dont-get-your-sources-in-syria-killed.php

GAO. (2003, February 20). *Peer-to-peer networks provide ready access to child pornography*. Retrieved December 13, 2013, from General Accounting Office: http://www.gao.gov/new.items/d03351.pdf

Garcia Marin, I. (2011). *Political participation, Democracy and Internet: Tunisian Revolution*. Munich: GRIN Verlag.

Gayathri, A. (2012, December 10). *opposing views over internet control deepen at UN conference in Dubai*. Retrieved January 12, 2013, from International Business Times: http://www.ibtimes.com/opposing-views-over-internet-control-deepen-un-conference-dubai-930875

Gazi, J. (2010). *An introduction to freedom of expression*. Retrieved December 13, 2013, from The Richmond Journal of Philosophy: http://www.richmond-philosophy.net/rjp/rjp20_gazi.php

Gellman, B., & Poitras, L. (2013, June 6). *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*. Retrieved December 15, 2013, from Washington Post: http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html

Ghannam, J. (2011). *Social media in the Arab World: Leading up to the uprisings of 2011*. Washington, DC: Center for International Media Assistance.

Ghazi, M. (2006). *The cartoons cry*. Bloomington, IN: AuthorHouse.

GIFC. (2007, September 20). *New technologies battle and defeat internet censorship*. Retrieved November 10, 2013, from Resources | Global Internet Freedom Consortium: http://internetfreedom.org/files/WhitePaper/TechnologiesBattleAndDefeatInternetCensorship70920.pdf

Giger, A. (1999). Social control and the censorship of Giuseppe Verdi's operas in Rome (1844-1859). *Cambridge Opera Journal, 11*(3), 233-266.

Goldsmith, J. L., & Wu, T. (2006). *Who controls the Internet?: illusions of a borderless world*. Oxford: Oxford University Press .

Goldstein, E. (1999). *The Internet in the Mideast and North Africa: Free expression and censorship*. Washington, DC: Human Rights Watch.

Goldstein, E. (2012). *Before the Arab Spring, the unseen thaw*. Retrieved December 5, 2013, from Human Rights Watch: http://www.hrw.org/world-report-2012/arab-spring-unseen-thaw

Goldstone, J. A. (2011). Understanding the revolutions of 2011: weakness and resilience in Middle Eastern autocracies. *Foreign Affairs, 90*(3), 8-16. Retrieved December 4, 2013, from Foreign Affairs: http://www.foreignaffairs.com/articles/67694/jack-a-goldstone/understanding-the-revolutions-of-2011

Gradstein, L. (2012, November 28). *UAE cyber-crime law 'effectively closes-off country's only remaining forum for free speech': watchdog*. Retrieved December 12, 2013, from National Post: http://news.nationalpost.com/2012/11/28/uae-cyber-crime-law-effectively-closes-off-countrys-only-remaining-forum-for-free-speech-watchdog/

Granick, J. (2005). Nixing the news: Iranian Internet censorship. *Harvard International Review, 27*(2), 11-12.

Greenawalt, K. (1989). Free speech justifications. *Columbia Law Review, 89*(1), 119-155.

Grennan, M. (2000, February 26). *Firewall and proxy server HOWTO*. Retrieved November 23, 2013, from The Linux documentation project: http://www.tldp.org/HOWTO/Firewall-HOWTO.html

Grimes, A. J. (1978). Authority, Power, influence and social control: A Theoretical Synthesis. *The Academy of Management Review, 3*(4), 724-735.

Grimmelmann, J. (2013). The illegal process: Basic problems in the making and application of censorship. *University of Chicago Law Review Dialogue, 79*, 58-70.

Gross, D. (2013, April 15). *Google boss: Entire world will be online by 2020*. Retrieved December 23, 2013, from CNN: http://edition.cnn.com/2013/04/15/tech/web/eric-schmidt-internet/

Habermas, J. (1984). *The theory of communicative action: Volume 2: Lifeworld and system: A critique of functionalist reason* (Vol. 2). Boston, MA: Beacon press.

Haigh, A. E. (2006). *The tragic drama of the Greeks*. Whitefish, MT: Kessinger Publishing.

Halaby, J. (2012, May 22). *Syria prisons are 'human slaughterhouses,' ex-detainee says*. Retrieved December 3, 2013, from The Huffington Post: http://www.huffingtonpost.com/2012/05/22/syria-prisons_n_1535107.html

Hallin, D. C., & Mancini, P. (2004). *Comparing media systems: Three models of media and politics*. Cambridge: Cambridge University Press.

Hamade, S. N. (2008). Internet filtering and censorship. *ITNG 2008. Fifth International Conference on Information Technology: New Generations* (pp. 1081-1086). Las Vegas, NV: ITNG.

Hamdy, N. (2009). Arab citizen journalism in action: Challenging mainstream media, authorities and media laws. *Westminster Papers in Communication and Culture, 6*(1), 92-112.

Hand, L., & Dilliard, I. (1952). *The spirit of liberty: Papers and addresses of Learned Hand*. New York, NY: Alfred A. Knopf.

Hartley, S. (2009, August 13). *Internet filtration in the Middle East*. Retrieved December 6, 2013, from Internet & Democracy Blog: https://blogs.law.harvard.edu/idblog/2009/08/13/oni_mena_report2009

Hatem, M., & Salam, V. (2011, February 3). *Yemenis flood capital in day of protest after president makes concessions*. Retrieved December 5, 2013, from Bloomberg: http://www.bloomberg.com/news/2011-02-02/yemenis-prepare-for-protest-as-saleh-vows-to-step-down-in-2013.html

Heins, M., Cho, C., & Feldman, A. (2006). *Internet filters* (2nd ed.). New York, NY: The Brennan Center for Justice at New York University School of Law.

Heller, P. B. (1974). The permanent Syrian constitution of March 13, 1973. *Middle East Journal, 28*(1), 53-66.

Hersberger, J. (2004). Internet censorship. In H. Bignoli (Ed.), *The Internet Encyclopedia* (Vol. 2, pp. 264-274). Hoboken, NJ: John Wiley and Sons.

Himma, K. E. (2004). Legal, social, and ethical issues. In H. Bignoli (Ed.), *The Internet Encyclopedia* (Vol. 2, pp. 464-476). Hoboken, NJ: John Wiley and Sons.

Hinnebusch, R. (2006). Authoritarian persistence, democratization theory and the Middle East: An overview and critique. *Democratization, 13*(3), 373-395.

Hoffman, D. L., Novak, T. P., & Venkatesh, A. (2004). Has the Internet become indispensable? *Communications of the ACM, 47*(7), 37-42.

Hofheinz, A. (2005). The Internet in the Arab world: Playground for political liberalization. *International Politics and Society, 3*(1), 78-96.

Holmes, O. W. (1919). *Abrams v United States* (Vol. 250). New York, NY: Vintage Books.

Houghton-Jan, S. (2008). *Internet filtering software tests: Barracuda, CyberPatrol, FilterGate and WebSense.* San Jose, CA: San Jose Public Library.

Howard, P. N., & Hussain, M. M. (2012). Egypt and Tunisia: The Role of Digital Media. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 110-123). Baltimore, MD: The Johns Hopkins University Press.

Howe, J. (2006, June 2). *Crowdsourcing: A definition.* Retrieved December 17, 2013, from Croudsourcing (web log): http://www.crowdsourcing.com/cs/2006/06/crowdsourcing_a.html

Huang, C. (2011, June 6). *Facebook and Twitter key to Arab Spring uprisings: report.* Retrieved November 20, 2013, from The National: http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report

Hubbard, B., & Jordans, F. (2013, January 2). *UN says more than 60,000 dead in Syrian civil war.* Retrieved December 4, 2013, from THE BIG STORY - AP: http://bigstory.ap.org/article/syrian-rebels-attack-air-base-north

Hussein, A.-R., & Black, I. (2012, December 7). *Egypt opposition rejects Morsi's call for talks amid thousands-strong protests.* Retrieved December 2, 2013, from The Guardian:

http://www.theguardian.com/world/2012/dec/07/egypt-opposition-morsi-talks

IFJ. (2010). *Breaking the chains: Middle East and Arab world press freedom review (May 2009-April 2010)*. Brussels: IFJ.

InteractiveME. (2009, May 21). *Alkasir BETA Launch means circumventing Website censorship*. Retrieved November 5, 2013, from InteractiveME: http://interactiveme.com/2009/05/Alkasir-beta-launch-means-circumventing-website-censorship/

Internet World Stats. (2012, June 30). *World Internet users statistics usage and world population*. Retrieved December 10, 2013, from Internet World Stats: www.internetworldstats.com/stats.htm

Internet World Stats. (2013a, September 10). *Intenet users in Africa*. Retrieved December 5, 2013, from Internet World Stats: http://www.internetworldstats.com/stats1.htm#africa

Internet World Stats. (2013b, September 10). *Arabic speaking Internet users statistics*. Retrieved December 5, 2013, from Internet World Stats: http://www.internetworldstats.com/stats19.htm#arabic

Internet World Stats. (2013c, November 20). *Internet usage in the Middle East*. Retrieved December 14, 2013, from Internet World Stats: http://www.internetworldstats.com/stats5.htm

Ismail, K. A., & Jondi, S. A. (2011). Poverty and decent work in the Arab Region: Where do we stand? *Doha Forum on Decent Work and Poverty Reduction* (pp. 1-19). Doha, Qatar: Doha International Institute for Family Studies and Development.

Israel, J. (2009). *A revolution of the mind: Radical enlightenment and the intellectual origins of modern democracy*. Princeton, NJ: Princeton University Press.

Jacinto, L. (2011, March 16). *Saudi troops in Bahrain quash hopes for reform*. Retrieved December 7, 2013, from France 24: http://www.france24.com/en/20110316-saudi-troops-bahrain-pummel-hopes-reform-sectarian-peace-shiites-sunni/

Jamjoom, M., & Almasmari, H. (2012, February 27). *Ex-President Saleh to leave Yemen after handover, officials say*. Retrieved December 5,

2013, from CNN: http://edition.cnn.com/2012/02/27/world/meast/yemen-elections/

Jefferson, T., & Hunt, J. G. (1994). *The essential Thomas Jefferson.* (J. G. Hunt, Ed.) New Jersey, NJ: Portland House.

Jiang, X., Yan, F., & Ye, K. (2012). Performance influence of live migration on multi-tier workloads in virtualization environments. *CLOUD COMPUTING 2012, The Third International Conference on Cloud Computing, GRIDs, and Virtualization* (pp. 72-81). Nice, France: IARIA.

Kalathil, S., & Boas, T. C. (2003). *Open networks, closed regimes: The impact of the Internet on authoritarian rule.* New York, NY: Carnegie Endowment for International Peace.

Karam, Z., & Kennedy, E. (2011, November 21). *Free Syrian Army transforms Syria uprising.* Retrieved December 4, 2013, from The Huffington Post (via AP): http://www.huffingtonpost.com/2011/11/21/free-syrian-army_n_1106087.html

Karlekar, K. D. (2009). *Print and broadcast media freedom: Disparities and openings.* Washington, DC: Center for International Media Assistance.

Karouny, M. (2012, July 17). *Syrian rebels start "liberate Damascus" operation.* Retrieved November 10, 2012, from Reuters: http://www.reuters.com/article/2012/07/17/us-syria-crisis-rebels-idUSBRE86G10B20120717

Kavada, A. (2012). Engagement, bonding, and identity across multiple platforms: Avaaz on Facebook, YouTube, and MySpace. *MedieKultur. Journal of media and communication research, 28*(52), 28-48.

Keen, A. (2007). *The cult of the amateur: how today's internet is killing our culture.* New York, NY: Bantam Dell Pub Group.

Khamis, S., & Vaughn, K. (2011). Cyberactivism in the Egyptian revolution: How Civic engagement and citizen journalism tilted the balance. *Arab Media and Society, 14*(Summer), 1-37.

Kienle, E. (2001). *A grand delusion: Democracy and economic reform in Egypt.* London: I. B. Tauris.

King, M. W. (2012). The troubles of free speech theory. *2012 Australian Political Studies Association Conference* (pp. 1-22). Hobart, Australia: APSA.

Kirkpatrick, D. (2012a, June 2). *New turmoil in egypt greets mixed verdict for Mubarak*. Retrieved December 13, 2013, from The New York Times: http://www.nytimes.com/2012/06/03/world/middleeast/egypt-hosni-mubarak-life-sentence-prison.html

Kirkpatrick, D. (2012b, November 28). *Panel drafting Egypt's constitution vows quick finish*. Retrieved November 25, 2013, from The New York Times: http://www.nytimes.com/2012/11/29/world/middleeast/wrangling-in-egypt-as-constitution-deadline-looms.html

Klang, M. (2006). Virtual censorship: Controlling the public sphere. *Social informatics: An Information Society for all? In remembrance of Rob Kling*, 185-194.

Klein, H. (2002). ICANN and Internet governance: Leveraging technical coordination to realize global public policy. *The Information Society, 18*(3), 193-207.

Kramer, M. (2010). *Internet censorship*. (thesis). Duluth: University of Minnosota Duluth.

Kuhlow, S. J. (2013). *The differential impact of women's pariticipation in the Arab Spring*. (Doctoral dissertation). Monterey, California: Naval Postgraduate School.

LaFranchi, H. (2011, September 2). *Ban on Syrian oil: EU tightens the noose*. Retrieved September 10, 2013, from The Christian Science Monitor: http://www.csmonitor.com/USA/Foreign-Policy/2011/0902/Ban-on-Syrian-oil-EU-tightens-the-noose

LaFraniere, S., & Barboza, D. (2011, March 21). *China tightens censorship of electronic communications*. Retrieved November 3, 2013, from The New York Times: http://www.nytimes.com/2011/03/22/world/asia/22china.html?_r=0

Landis, J., & Pace, J. (2007). The Syrian opposition. *The Washington Quarterly, 30*(1), 45-68.

Lang, J., & De Sterck, H. (2012, October 5). *The Arab Spring: A simple compartmental model for the dynamics of a revolution.* Retrieved November 25, 2013, from arXiv: http://www.math.uwaterloo.ca/~hdesterc/websiteW/Data/publications/journal/2014ArabSpring_preprint.pdf

Leberknight, C. S., Chiang, M., Poor, H. V., & Wong, F. (2010). A taxonomy of Internet censorship and anti-censorship. *Fifth International Conference on FUN WITH ALGORITHMS.* Napoli, Italy.

Lee, B., & Tamborini, R. (2006). Third-person effect and internet pornography: The influence of collectivism and internet self-efficacy. *Journal of Communication, 55*, 292-310.

Legal Information Institute. (n.d.). *First Amendment.* Retrieved December 18, 2013, from Cornell University Laws School: http://www.law.cornell.edu/constitution/first_amendment

Lessig, L. (1999). The law of the horse: What cyberlaw might teach. *Harvard law review, 113*(2), 501-549.

Lessig, L. (2002). Innovating copyright. *Cardozo Arts & Entertainment Law Journal, 20*(3), 611-623.

Lessig, L. (2008, October 11). *In defense of piracy.* Retrieved December 8, 2013, from The Wall Street Journal: http://online.wsj.com/news/articles/SB122367645363324303

Lessig, L. (2013, January 6). Innovation in Mind Conference - Lund University. (J. Kao, Moderator, Interviewer) Retreived from Lund University: http://www.innovationinmind.se/news/2013/02/lawrence-lessig-becomes-honorary-doctor-at-lund-university/

Levitsky, S., & Way, L. (2002). The rise of competitive authoritarianism. *Journal of democracy, 13*(2), 51-65.

Liang, B., & Lu, H. (2010). Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice, 26*(1), 103-120.

Linz, J. J. (1964). An authoritarian regime: The case of Spain. In E. Allardt, & A. Littunen (Eds.), *Cleavages, ideologies, and party systems:*

contributions to comparative political sociology. Helsinki, Finland: Westermack Society.

Lo, V., So, C. Y., & Zhang, G. (2010). The influence of individualism and collectivism on Internet pornography exposure, sexual attitudes, and sexual behavior among college students. *Chinese Journal of Communication, 3*, 10-27.

Lund, A. (2012). *Divided they stand: An overview of Syria's political opposition factions.* Brussels: Foundation for European Progressive Studies.

Lutterbeck, D. (2013). Arab uprisings, armed forces, and civil-military relations. *Armed Forces & Society, 39*(1), 28-52.

Lynch, C., & Fordham, A. (2012, February 4). *Russia, China veto U.N. resolution on Syria*. Retrieved December 12, 2013, from The Washington Post: http://www.washingtonpost.com/world/middle_east/russia-china-veto-un-resolution-on-syria/2012/02/04/gIQAxvVhpQ_story.html

MacFARQUHAR, N. (2013, May 25). *Yemen making strides in transition to democracy after Arab Spring*. Retrieved December 4, 2013, from The New York Times: http://www.nytimes.com/2013/05/26/world/asia/yemen-makes-strides-in-transition-to-democracy.html

MacKinnon, R. (2006). *Race to the bottom - Corporate complicity in Chinese Internet censorship*. Washington, DC: Human Rights Watch.

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice, 134*(1), 31-46.

MacKinnon, R. (2012). China's "Networked authoritarianism". In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 78-93). Baltimore, MD: The Johns Hopkins University Press.

MacKinnon, R., & Zuckerman, E. (2012). Don't feed the trolls. *Index on Censorship, 41*(4), 14-24.

Macleod, H. (2011a, April 20). *Syria sans emergency law no different*. Retrieved November 6, 2013, from Aljazeera:

http://www.aljazeera.com/indepth/features/2011/04/201142015306616501.html

Macleod, H. (2011b, April 23). *Syria: how it all began.* Retrieved December 4, 2013, from GlobalPost: http://www.globalpost.com/dispatch/news/regions/middle-east/110423/syria-assad-protests-daraa

Madison, J. (1962). *The papers of James Madison.* (W. H. Rachal, Ed.) Chicago, IL: University of Chicago Press.

Mahdavy, H. (1970). The patterns and problems of economic development in rentier states: The case of Iran. In *Studies in Economic History of the Middle East* (Vol. 1000, pp. 428-467). Oxford: Oxford University Press.

Marquis-Boire, M. &.-R. (2013, April 30). *For their eyes only: The commercialization of digital spying.* Retrieved November 4, 2013, from The Citizen Lab: https://citizenlab.org/2013/04/for-their-eyes-only-2/

Mayled, J. (1999). *People and their god.* Cheltenham: Nelson Thornes.

McCarthy, R. (2012, December 17). *On Tunisia's road to democracy, hope springs eternal.* Retrieved December 6, 2013, from The Guardian: http://www.theguardian.com/commentisfree/2012/dec/17/tunisia-democracy-hope-springs-eternal

Mcdonald-Gibson, C. (2012, February 19). *Inside the torture chamber of Assad's inquisition squads.* Retrieved December 6, 2013, from The Independent: http://www.independent.co.uk/news/world/middle-east/inside-the-torture-chamber-of-assads-inquisition-squads-7180869.html

McElroy, D. (2011, February 10). *Egypt crisis: army forced to act by threat of chaos.* Retrieved Decembe 3, 2013, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8317133/Egypt-crisis-army-forced-to-act-by-threat-of-chaos.html

McGreal, C., & Shenker, J. (2011, February 11). *Hosni Mubarak resigns – and Egypt celebrates a new dawn.* Retrieved December 9, 2013, from The Guardian: http://www.theguardian.com/world/2011/feb/11/hosni-mubarak-resigns-egypt-cairo

McLelland, M., & Yoo, S. (2007). The international Yaoi boys' love fandom and the regulation of virtual child pornography: The implications of current legislation. *Sexuality Research and Social Policy, 4*(1), 93-104.

McQuail, D. (1987). *Mass communication theory: An introduction* . Sage Publications, Inc.

Mehler, A., Gleim, R., & Dehmer, M. (2006). Towards structure-sensitive hypertext categorization. In M. S. Kruse, C. B. Nçrnberger, & W. Gaul (Eds.), *From Data and Information Analysis to Knowledge Engineering* (pp. 406-413). New York, NY: Springer.

Mehta, M. (2002). Censoring cyberspace. *Asian Journal of Social Science, 30*(2), 319-338.

Meier, P. (2012). Ushahidi as a liberation technology. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 95-109). Baltimore, MD: The Johns Hopkins University Press.

Meiklejohn, A. (1948). *Free Speech and its relation to self-government.* Clark, NJ: The Lawbook Exchange, Ltd.

Mellor, N., Rinnawi, K., & Dajani, N. (2011). *Arab media.* John Hoboken, NJ: John Wiley and Sons.

Menon, K. (2000). Controlling the Internet: Censorship online in China. *The Quill, 88*(8), 82.

Michael, M. (2011, March 21). *Egypt: Constitution changes pass in referendum.* Retrieved December 7, 2013, from The Washington Post: http://www.washingtonpost.com/wp-dyn/content/article/2011/03/20/AR2011032001465.html

Migdal, J. S. (2001). *State in society: Studying how states and societies transform and constitute one another.* Cambridge: Cambridge University Press.

Mill, J. S. (1946). *On liberty and considerations of representative government (reprint).* Oxford: Blackwell.

Milner, H. (2002). *Civic literacy: How informed citizens make democracy work.* Lebanon, NH: University Press of New England.

Milton, J. (1873). *Milton's Areopagitica: a speech for the liberty of unlicensed printing*. Harlow: Longmans, Green and Company.

Mina, N. (2007). Blogs, cyber-literature and virtual culture in Iran. *Occasional Paper Series, 15*(December 2007), 4-36.

Moiles, J. C. (2012). Unity, freedom and socialism: The Assads, the Ba'ath and the making of modern Syria. *Grand Valley Journal of History, 2*(1), 1-13.

Morozov, E. (2011). WikiLeaks and the perils of extreme glasnost. *New Perspectives Quarterly, 28*(1), 7-11.

Morozov, E. (2012). *The net delusion: The dark side of Internet freedom*. New York, NY: PublicAffairs Store.

Morsink, J. (1984). The philosophy of the Universal Declaration. *Human Rights Quarterly, 6*(3), 309-334.

Mourtada, R., & Salem, F. (2011). Civil movements: The impact of Facebook and Twitter. *Arab Social Media Report, 1*(2), 1-30.

Mourtada, R., & Salem, F. (2012). Social media in the Arab world: influencing societal and cultural change? *Arab Social Media Report, 2*(1), 1-28.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. Cambridge, MA: MIT Press.

Mullin, C., & Shahshahani, A. (2012). The legacy of US intervention and the Tunisian revolution: promises and challenges one year on. *Interface: a journal for and about social movements, 4*(1), 67-101.

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 57-72). Cambridge, MA: MIT Press.

Myers, S. L. (2011, August 18). *U.S. and allies Say Syria leader must step down*. Retrieved December 3, 2013, from The New York Times: http://www.nytimes.com/2011/08/19/world/middleeast/19diplo.html?pagewanted=all

Neagle, C. (2013, September 24). *UN report highlights massive Internet gender gap*. Retrieved December 6, 2013, from Network World:

http://www.networkworld.com/news/2013/092413-internet-gender-gap-274144.html

Negroponte, N. (1996). *Being digital.* New York, NY: Vintage Books.

Nojeim, G. T. (2010). Cybersecurity and freedom on the Internet. *Journal of National Security Law & Policy, 4*(1), 119-137.

Noman, H. (2009, August 11). *Internet filtering in the Middle East and North Africa.* Retrieved December 13, 2013, from OpenNet Initiative: https://opennet.net/sites/opennet.net/files/ONI_MENA_2009.pdf

Noman, H., & Zarwan, E. (2008). *Internet filtering in the Middle East and North Africa in 2006-2007.* Retrieved December 12, 2013, from OpenNet Initiative: https://opennet.net/studies/mena2007

Nunziato, D. C. (2010). How (not) to censor: Procedural First Amendment values and internet censorship worldwide. *Georgetown Journal of International Law, 42*(4), 1123-1160.

Nybergh, T. (2008, February 15). *Internet "child porn" censorship in Finland.* Retrieved November 10, 2012, from Thomas Nybergh: http://www.nybergh.net/notes/2008/02/15/internet-child-porn-censorship-in-finland/

Obeidat, B. Y., Shannak, R. O., Masa'deh, R., & Al-Jarrah, I. (2012). Toward better understanding for Arabian culture: Implications based on Hofstede's cultural model. *European Journal of Social Sciences, 28*(4), 512-522.

O'Donnell, G. (1973). *Modernization and bureaucratic-authoritarianism: Studies in South American politics* (Vol. 9). Berkeley, CA: University of California Press.

O'Donnell, I., & Milner, C. (2007). *Child pornography: Crime, computers and society.* London: Routledge.

ONI. (2008). Internet Filtering in Egypt. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 276-280). Cambridge, MA: MIT Press.

ONI. (2009, August 12). *Internet Filtering in Syria.* Retrieved December 4, 2012, from OpenNet Initiative: https://opennet.net/sites/opennet.net/files/ONI_Syria_2009.pdf

ONI. (2010). *Internet filtering: Tunisia.* Retrieved November 10, 2012, from OpenNet Initiative: http://opennet.net/research/profiles/tunisia

ONI. (2013, September 20). *Filtering data.* Retrieved December 10, 2013, from OpenNet Initiative: http://opennet.net/sites/opennet.net/files/ONI_data-20130920.zip

O'Reilly, T. (2009). *What is Web 2.0.* Sebastopol, CA: O'Reilly Media.

Oweis, K. Y. (2011, April 21). *Syria's Assad ends state of emergency.* Retrieved December 2, 2013, from Reuters: http://www.reuters.com/article/2011/04/21/us-syria-idUSTRE72N2MC20110421

Paireepairit, I. (2008). *Internet censorship in Thailand.* (Doctoral dissertation). Sheffield: University of Sheffield, Department of Information Studies.

Palfrey, J., Roberts, H., & Zuckerman, E. (2009). *2007 Circumvention landscape report: Methods, uses, and tools.* Cambridge, MA: Berkman Center for Internet & Society, Harvard University.

Palfrey, J., Roberts, H., & Zuckerman, E. (2011). *Circumvention tool evaluation.* Cambridge, MA: Berkman Center for Internet & Society, Harvard University.

Paquette, L. (2013). The whistleblower as underdog: what protection can human rights offer in massive secret surveillance? *The International Journal of Human Rights, 17*(7-8), 796-809.

Park, J. C., & Crandall, J. R. (2010). Empirical study of a national-scale distributed intrusion detection system: Backbone-level filtering of html responses in china. *IEEE 30th International Conference on Distributed Computing Systems 2010* (pp. 315-326). Genoa, Italy: IEEE.

PC Magazine Encyclopedia. (2012, November 10). *Amara's Law definition.* Retrieved November 10, 2012, from PC Magazine Encyclopedia: www.pcmag.com/encyclopedia_term/0,1237,t=Amaras+law&i=37701,00.asp

Pelofsky, J. (n.d.). US accuses Megaupload of copyright infringement. online],(accessed 2012-01-25),< http://www. reuters. com/article/2012/01/19/us-usa-crime-piracyidustre80i24220120119.

Peltz, R. J. (2002). Use the filter you were born with: The unconsitutionality of mandatory internet filtering for the adult patrons of public libraries. *Washington Law Review, 77*(397), 397-479.

Perrit Jr., H. H. (1995, November 9). *What is the Internet.* Retrieved November 11, 2013, from Internet Jurisdiction: http://www.kentlaw.edu/cyberlaw/resources/whatis.html

Pierson, P. (2000). Increasing returns, path dependence, and the study of politics. *American political science review, 94*(2), 251-267.

Pierson, P. (2004). *Politics in time: History, institutions, and social analysis.* Princeton, NJ: Princeton University Press.

Pipes, D. (1989). The Alawi capture of power in Syria. *Middle Eastern Studies, 25*(4), 429-450.

Postman, N. (1993). *Technopoly: The surrender of culture to technology.* New York, NY: Vintage Books.

Pratt, N. C. (2007). *Democracy and authoritarianism in the Arab world.* Boulder, CO: Lynne Rienner.

Preston, J. (2011, February 14). *Facebook officials keep quiet on its role in revolts.* Retrieved December 6, 2013, from New York Times: http://www.nytimes.com/2011/02/15/business/media/15facebook.html

Puppis, M., & d'Haenens, L. (2013). Comparing media policy and regulation. In F. Esser, & T. Hanitzsch (Eds.), *Handbook of Comparative Communication Research* (pp. 221-233). London: Routledge.

Qiang, X. (2012). The battle for the Chinese Internet. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 63-77). Baltimore, MD: The Johns Hopkins University Press.

Randall, R. S. (1968). *Censorship of the movies: The social and political control of a mass medium.* Madison, WI: University of Wisconsin Press.

Rashad, M. (2011, November 23). *Yemen's Saleh signs deal to give up power.* Retrieved December 6, 2013, from Reuters: http://www.reuters.com/article/2011/11/23/us-yemen-idUSTRE7AM0D020111123

Rashed, M. A., & El Azzazi, I. (2011). The Egyptian revolution: A participant's account from Tahrir Square, January and February 2011. *Anthropology Today, 27*(2), 22-27.

Rashwan, N. (2012, September 22). *Revolutionary website 'We Are All Khaled Said' launches constitution initiative.* Retrieved December 3, 2013, from Ahram Online: http://english.ahram.org.eg/NewsContent/1/64/53520/Egypt/Politics-/Revolutionary-website-We-Are-All-Khaled-Said-launc.aspx

Redish, M. H. (1982). The value of free speech. *University of Pennsylvania Law Review, 130*(3), 591-645.

Rininsland, Æ. (2012, April 16). *Internet censorship listed: how does each country compare?* Retrieved November 10, 2012, from The Guardian: http://www.guardian.co.uk/technology/datablog/2012/apr/16/internet-censorship-country-list

Roberts, H., Zuckerman, E., Faris, R., York, J., & Palfrey, J. (2011). *The evolving landscape of internet control: A summary of our recent research and recommendations.* Cambridge, MA: Berkman Center Research.

Rønning, H. (2009). The contemporary challenge to the concept of universal human rights and freedom of expression. In H. Rønning, & A. Kierulf (Eds.), *Freedom of speech abridged?* (pp. 9-19). Gothenburg, Sweden: NORDICOM.

Roskin, M. G., Cord, R. L., Medeiros, J. A., & Jones, W. S. (2011). *Political science: An introduction.* Harlow: Longman Publishing Group.

Ross, M. L. (2001). Does oil hinder democracy? *World politics, 53*(3), 325-361.

RSF. (2005, November 17). *The 15 enemies of the Internet and other countries to watch.* Retrieved November 11, 2013, from Reporters Without Borders: http://www.rsf.org/IMG/article_PDF/The-15-enemies-of-the-Internet-and.pdf

RSF. (2010, March 10). *Enemies of the Internet.* Retrieved December 12, 2013, from Reporters Without Borders: http://www.rsf.org/IMG/pdf/Internet_enemies.pdf

RSF. (2013). *Netizens and citizen journalists killed.* Retrieved December 5, 2013, from Reporters Without Borders: http://en.rsf.org/press-freedom-barometer-netizens-and-citizen-journalists.html

Rugh, W. A. (2004). *Arab mass media: Newspapers, radio, and television in Arab politics.* Westport, CT: Greenwood Publishing Group.

Rundle, M., & Birdling, M. (2008). Filtering and the International System: A Question of Commitment. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 73-102). Cambridge, MA: MIT Press.

Ryan, Y. (2011, January 26). *How Tunisia's revolution began.* Retrieved December 5, 2013, from Aljazeera: http://www.aljazeera.com/indepth/features/2011/01/201112612181598 5483.html

Saleh, A. (2013, December 26). Research-Related Question. (W. Al-Saqaf, Interviewer)

Saleh, H. (2006, September 24). *Yemen opposition says election was rigged.* Retrieved December 5, 2013, from Financial Times: http://www.ft.com/cms/s/0/a2b311dc-4be8-11db-90d2-0000779e2340.html#axzz2oK2WCBGc

Samaan, R. S. (2012, November 22). *Mohammed Morsi grants himself sweeping new powers in wake of Gaza.* Retrieved December 8, 2013, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/9697347/Mohammed-Morsi-grants-himself-sweeping-new-powers-in-wake-of-Gaza.html

Sanders, D. (1991). Collective rights. *Human Rights Quarterly, 13*(3), 368-386.

Scanlon, T. (1972). A theory of freedom of expression. *Philosophy & Public Affairs, 1*(2), 204-226.

Schauer, F. (2004). The boundaries of the First Amendment: A preliminary exploration of constitutional salience. *Harvard Law Review, 117*(6), 1765-1809.

Schindley, W. (1997). *The informed citizen: argument and analysis.* Belmont, CA: Harcourt Brace College Publishers.

Schmidt, S. (2006). The missed opportunity for economic reform in Syria. *Mediterranean Politics, 11*(1), 91-97.

Schonfeld, E. (2011, January 25). *Twitter is blocked in Egypt amidst rising protests*. Retrieved December 11, 2013, from Tech Chrunch: http://techcrunch.com/2011/01/25/twitter-blocked-egypt/

Scott, P. (1996). *Deep politics and the death of JFK*. Berkeley, CA: University of California Press.

Seib, P. (2007). *New media and the new Middle East*. New York, NY: Palgrave Macmillan.

Senat, J. (2011, September 19). *Defining censorship*. Retrieved November 10, 2012, from Joey Senat Home Page: http://journalism.okstate.edu/faculty/jsenat/censorship/defining.htm

Shadid, A. (2011, February 13). *Egyptian Military Dissolves Parliament*. Retrieved November 4, 2012, from The New York Times: http://www.nytimes.com/2011/02/14/world/middleeast/14egypt.html

Sharqieh, I. (2011, November 11). *Ibrahim Sharqieh on Aljazeera regarding Yemen [video file]*. Retrieved December 12, 2013, from YouTube: https://www.youtube.com/watch?v=svbgddDHlK4

Sherlock, R. (2012, December 20). *Fears Syria is turning into sectarian conflict*. Retrieved December 4, 2013, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/middleeast/syria/9759273/Fears-Syria-is-turning-into-sectarian-conflict.html

Shirazi, F., & Greenaway, K. (2009). Examining validity claims for internet filtering in Islamic Middle Eastern countries: A critical discourse analysis. *AMCIS 2009 Proceedings* (pp. 1-9). San Francisco, CA: AMCIS.

Shirky, C. (2011). The political power of social media: Technology, the public sphere sphere, and political change. *Foreign Affairs, 90*(January/February 2011), 28-41.

Shorbagy, M. (2007). The Egyptian movement for change—Kefaya: Redefining politics in Egypt. *Public Culture, 19*(1), 175-196.

Shukrallah, S. (2011, July 7). *Who are Egypt's thugs?* Retrieved December 10, 2013, from Ahram Online:

http://english.ahram.org.eg/NewsContent/1/64/15715/Egypt/Politics-/Who-are-Egypts-thugs-.aspx

Sills, S. J., & Song, C. (2002). Innovations in survey research an application of web-based surveys. *Social science computer review, 20*(1), 22-30.

Silver, V. (2012, July 25). *Cyber attacks on activists traced to FinFisher spyware of Gamma*. Retrieved November 3, 2013, from Bloomberg: http://www.bloomberg.com/news/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma.html

Simpson, B. (2008). New labor, new censorship? Politics, religion and internet filtering in Australia. *Information & Communications Technology Law, 17*(3), 167-183.

Singel, R. (2011, February 10). *Report: Egypt shut down net with big switch, not phone calls*. Retrieved December 5, 2013, from Wired: http://www.wired.com/threatlevel/2011/02/egypt-off-switch/

Smith, D., & Torres, L. (2006, February 5). *Timeline: a history of free speech*. Retrieved November 5, 2013, from The Guardian: http://www.theguardian.com/media/2006/feb/05/religion.news

Smith, L. A. (2001). Johann Gottlieb Fichte's free speech theory. *American Communication Journal, 4*(3), 1-20.

Sommer, J. H. (2000). Against cyberlaw. *Berkeley Technology Law Journal, 15*(3), 1145-1232.

Sonne, P., & Stecklow, S. (2011, March 28). *U.S. Products Help Block Mideast Web*. Retrieved December 14, 2013, from The Wall Street Journal: http://online.wsj.com/news/articles/SB10001424052748704438104576219190417124226

Sottilotta, C. E. (2013, January 1). Political stability in authoritarian regimes: Lessons from the Arab uprisings. *IAI Working Papers, 13*(1), pp. 1-14.

Srivastava, S., & Chawla, S. (2010). Multifaceted classification of websites for goal oriented requirement engineering. In *Contemporary Computing* (pp. 479-485). New York, NY: Springer.

Stahl, B. C. (2008). Empowerment through ICT: A critical discourse analysis of the Egyptian ICT policy. In *Social dimensions of information and communication technology policy* (pp. 161-177). New York, NY: Springer.

Stepan, A. C., & Robertson, G. B. (2003). An" Arab" more than a "Muslim" democracy gap. *Journal of Democracy, 14*(3), 30-44.

Stepanova, E. (2011). The role of information communication technologies in the 'Arab Spring'. *Ponars Eurasia, No. 159*(May 2011), 1-6.

Stevens, T. (2010, January 13). *China's cyberwar goes beyond Google.* Retrieved October 23, 2013, from The Guardian: http://www.theguardian.com/commentisfree/libertycentral/2010/jan/13/google-china-cyber-war-security

Stol, W. P., Kaspersen, H., Kerstens, J., Leukfeldt, E., & Lodder, A. (2009). Governmental filtering of websites: The Dutch case. *Computer Law & Security Review, 25*(3), 251-262.

Stone, I. F. (1989). *The trial of Socrates.* New York, NY: Random House Digital, Inc.

Subramanian, R. (2012). The growth of global Internet censorship and circumvention: A survey. *Communications of the International Information Management Association, 3*(1), 25-34.

Sultan, N. (2013). Aljazeera: Reflections on the Arab Spring. Journal of Arabian Studies, 3(2), 249-264.

Surowiecki, J. (2005). *The wisdom of crowds.* New York, NY: Knopf Doubleday Publishing Group.

Sutton, M. (2012, July 12). *Iraq cyber crime law threatens free speech says HRW.* Retrieved December 6, 2013, from ITP: http://www.itp.net/589674-iraq-cyber-crime-law-threatens-free-speech-says-hrw#.UsfsoPRDtEI

Sweis, R. (2013, January 2). *Syrian refugees strain resources in Jordan.* Retrieved December 6, 2013, from The New York Times: http://www.nytimes.com/2013/01/03/world/middleeast/syrian-refugees-strain-resources-in-jordan.html

Tait, R. (2012, December 23). *Egypt facing fresh turmoil after referendum vote*. Retrieved December 3, 2013, from The Telegraph: http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/9763937/Egypt-facing-fresh-turmoil-after-referendum-vote.html

Teleyemen. (n.d.). *Brief History*. Retrieved December 3, 2013, from Teleyemen: http://www.teleyemen.com.ye/ty_about_history_eng.aspx

The Citizen Lab. (2007, September 1). *Everyone's guide to by-passing Internet censorship*. Retrieved November 10, 2012, from Nart Villeneuve: http://www.nartv.org/mirror/circ_guide.pdf

The Global Report. (2011, March 24). *Yemen shuts Al-Jazeera offices; journalists beaten*. Retrieved December 10, 2013, from The Global Report: http://www.theglobalreport.org/articles/yemen-shuts-al-jazeera-offices-journalists-beaten

The Independent. (2011, January 21). *Tunisia: 'I have lost my son, but I am proud of what he did'*. Retrieved December 14, 2013, from The Independent: http://www.independent.co.uk/news/world/africa/tunisia-i-have-lost-my-son-but-i-am-proud-of-what-he-did-2190331.html

The World Bank. (2010). *GDP per capita (current US$)*. Retrieved December 10, 2013, from The World Bank: http://data.worldbank.org/indicator/NY.GDP.PCAP.CD

Thierer, A. (2010). The case for internet optimism, Part 1-Saving the Net from its detractors. In B. Szoka, & A. Marcus (Eds.), *The next digital decade: Essays on the future of the Internet* (pp. 57-88). Washington, DC: TechFreedom.

Thompson, A. (2007). *The media and the Rwanda genocide*. London: Pluto Press.

Travis, H. (2013). Introduction: Cyberspace as a product of public-private censorship. In H. Travis (Ed.), *Cyberspace law: Censorship and regulation of the Internet* (pp. 1-28). London: Routledge.

Tufekci, Z., & Wilson, C. (2012). Social media and the decision to participate in political protest: Observations from Tahrir Square. *Journal of Communication, 62*(2), 363-379.

UNDP. (2002). *Arab Human Development Report 2002: Creating opportunities for future generations*. New York, NY: UNDP.

UNDP. (2003). *Arab Human Development Report 2003: Building a knowledge society*. New York, NY: UNDP.

United Nations. (1948, December 10). *The Univeral Declaration of Human Rights*. Retrieved November 1, 2013, from The United Nations: http://www.un.org/en/documents/udhr/index.shtml

US Department of Treasury. (2008, February 21). *Rami Makhluf designated for benefiting from Syrian corruption*. Retrieved December 3, 2013, from US Department of the Treasury: http://www.treasury.gov/press-center/press-releases/Pages/hp834.aspx

Valentino-Devries, J., Sonne, P., & Malas, N. (2011, October 29). *U.S. firm acknowledges Syria uses its gear to block Web*. Retrieved November 10, 2012, from The Wall Street Journal: http://online.wsj.com/article/SB10001424052970203687504577001911398596328.html

Vandiver, D. M. (2000). Regulating Internet pornography. *Crime & Justice International, 16*(47), 11-14.

Varnelis, K. (2012). *Networked publics*. Cambridge, MA: The MIT Press.

Villeneuve, N. (2007). Evasion tactics. *Index on Censorship, 36*(4), 71-85.

Wacker, G. (2003). The Internet and censorship in China. In C. R. Hughes, & G. Wacker (Eds.), *China and the Internet: Politics of the digital leap forward* (pp. 58-82). London: Routledge.

Wagner, B. (2012). Push-button-autocracy in Tunisia: Analysing the role of Internet infrastructure, institutions and international markets in creating a Tunisian censorship regime. *Telecommunications Policy, 36*(6), 484-492.

Walt, V. (2012, July 23). *Is Syria's Bashar Assad going the way of Muammar Gaddafi?* Retrieved February 11, 2014, from Time Magazine: http://world.time.com/2012/07/23/is-syrias-bashar-assad-going-the-way-of-muammar-gaddafi/

Wang, S., & Hong, J. (2010). Discourse behind the forbidden realm: Internet surveillance and its implications on China's blogosphere. *Telematics and Informatics, 27*(1), 67-78.

Warburton, N. (2009). *Free speech: a very short introduction*. Oxford: Oxford University Press.

Warf, B. (2013). The Central Asian digital divide. In M. Ragnedda, & G. W. Muschert (Eds.), *The digital divide* (pp. 268-282). London: Routeledge.

Warf, B., & Vincent, P. (2007). Multiple geographies of the Arab Internet. *Area, 39*(1), 83-96.

Warschauer, M. (2001). Singapore's dilemma: Control versus autonomy in IT-led development. *The Information Society, 17*(4), 305-311.

Waterman, S. (2007, December 3). *Analysis: Egypt's new anti-terrorism law*. Retrieved November 20, 2013, from UPI: http://www.upi.com/Emerging_Threats/2007/12/03/Analysis-Egypts-new-anti-terrorism-law/UPI-86381196701541/

Watson, I. (2011, November 22). *Cyberwar explodes in Syria*. Retrieved December 5, 2012, from CNN: http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar/

Weaver, M. (2012, April 16). *Syria: first UN peace monitors arrive - Monday 16 April 2012*. Retrieved November 5, 2013, from The Guardian: http://www.theguardian.com/world/2012/apr/16/syria-un-monitors-arrive-live

Websense. (n.d.). *Master database URL categories*. Retrieved December 6, 2012, from Websense: http://www.websense.com/content/websense-url-categories.aspx

Weisman, J. (2012, January 21). *After an online firestorm, Congress shelves antipiracy bills*. Retrieved November 15, 2013, from New York Times: http://www.nytimes.com/2012/01/21/technology/senate-postpones-piracy-vote.html

Wellman, B. (2004). The three ages of internet studies: ten, five and zero years ago. *New Media & Society, 6*(1), 123-129.

Wheeler, D. L. (2007). Empowerment zones? Women, Internet cafés, and life transformations in Egypt. *Information Technologies and International Development, 4*(2), 89-104 .

White, H. (1997). *Anatomy of censorship: Why the censors have it wrong*. Lanham, MD: University Press of America.

Whittaker, Z. (2012, July 4). *'Last rites' for ACTA? Europe rejects antipiracy treaty*. Retrieved November 3, 2013, from CNET:

http://www.cnet.com/news/last-rites-for-acta-europe-rejects-antipiracy-treaty/

Wikipedia. (2011, April 22). *Alkasir*. Retrieved December 15, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Alkasir

Williams, S. D. (2002). Self-esteem and the self-censorship of creative ideas. *Personnel Review, 31*(4), 495-503.

Wilson, E. (2012). *The dual state: parapolitics, Carl Schmitt and the national security complex*. Farnham: Ashgate Publishing.

Wortley, R. K., & Smallbone, S. (2012). *Child pornography on the internet*. Westport, CT: Praeger.

Yahyanejad, M., & Gheytanchi, E. (2012). Social Media, Dissent, and Iran's Green Movement. In L. Diamond, M. F. Plattner, & L. P. Diamond (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 139-155). Baltimore, MD: The Johns Hopkins University Press.

Yanatma, S. (2011, November 29). *Turkey to impose 'step-by-step' sanctions on Syria*. Retrieved December 7, 2013, from Today's Zaman: http://www.todayszaman.com/news-264218-turkey-to-impose-step-by-step-sanctions-on-syria.html

Ybarra, M. L., & Mitchell, K. J. (2005). Exposure to Internet pornography among children and adolescents: A national survey. *CyberPsychology & Behavior, 8*(5), 473-486.

Yeranian, E. (2012, June 30). *Morsi sworn in as Egypt's new president*. Retrieved December 6, 2013, from Voice of America: http://www.voanews.com/content/egypt-morsi-constitution/1352072.html

Yoder, V., Thomas, B., & Kiran, A. (2005). Internet pornography and loneliness: An association? *Sexual addiction & compulsivity, 12*(1), 19-44.

Zahler, K. A. (2009). *The Assads' Syria*. Breckenridge, CO: Twenty-First Century Books.

Zarwan, E. (2005). *False freedom-Online censorship in the Middle East and North Africa*. Washington, DC: Human Rights Watch.

Zavis, A., & Sandels, A. (2011, December 13). *Syria holds local elections as deadly clashes reportedly continue*. Retrieved December 5, 2013,

from Los Angeles Times: http://articles.latimes.com/2011/dec/13/world/la-fg-syria-elections-20111213

Zein, D. E. (2011, September 7). *The 'new' Syrian media law is nothing new*. Retrieved December 2, 2013, from Committee to Protect Journalists: http://cpj.org/blog/2011/09/the-new-syrian-media-law-is-nothing-new.php

Zhang, Q., Xie, X., Wang, L., Yue, L., & Ma, W. Y. (2007). Computing geographical serving area based on search logs and website categorization. *Database and Expert Systems Applications: 18th International Conference, DEXA 2007* (pp. 811-822). Regensburg: Springer.

Ziadeh, R. (2009). *The Kurds in Syria: Fueling separatist movements in the region?* Washington, DC: United States Institute of Peace.

Zirulnick, A. (2011, May 26). *Yemen heads toward civil war as Saleh escalates fight with major tribal leader*. Retrieved December 4, 2013, from The Christian Science Monitor: http://www.csmonitor.com/World/terrorism-security/2011/0526/Yemen-heads-toward-civil-war-as-Saleh-escalates-fight-with-major-tribal-leader

Zittrain, J., & Edelman, B. (2003). Internet filtering in China. *IEEE Internet Computing, 7*(2), 70-77.

Zittrain, J., & Palfrey, J. (2008a). Internet filtering: The politics and mechanisms of control. In R. J. Deibert, *Access denied: The practice and policy of global Internet filtering* (pp. 29-57). Cambridge, MA: MIT Press.

Zittrain, J., & Palfrey, J. (2008b). Introduction. In *Access denied: The practice and policy of global Internet filtering* (pp. 1-4). Cambridge, MA: MIT Press.

Zuehlke, E. (2012, May). *In Arab Countries, Mobile Internet and Social Media Are Dominant, but Disparities in Access Remain*. Retrieved December 5, 2013, from Population Reference Bureau: http://www.prb.org/Publications/Articles/2012/arab-region-internet-use.aspx

Appendices

Appendix A: Comprehensive Overview of Alkasir

Introduction

As a software solution, Alkasir is at the center of this study both in terms of implementation and as a research tool used to gather data necessary to answer the research questions. It is therefore imperative for the integrity of this dissertation to open it up for review and scrutiny and to understand how it was built so it would not be seen as a mysterious black-box component.

I have dedicated this chapter to review why and how this software was developed. The challenge I faced was how to write this chapter in a language easy to understand by nontechnical readers who wish to not be confused by too technical details that would require a software analyst to fully understand. Therefore, I exerted an effort to balance between simplicity in language and the utilization of concepts commonly used in the area of software engineering. In this chapter, I give a preview of the software engineering methodology used to develop Alkasir and, in the process, explain its analysis, design, implementation, testing, evolution, and limitations. But I first start by explaining how it all started.

Problem definition

In 2009, the level of filtering of online content by ISPs had been on the rise, resulting in alarming patterns that triggered global initiatives to try to research this phenomenon (ONI, n.d.). At the time, there were some ways to get around such filtering by using software, Web-based proxies, HTTP or SOCKS, or VPNs, which were either commercial or free. However, all those solutions required significant resources to run, and this resulted in creating bottlenecks and resource depletion for those who provided them unless they were running on huge resources.

For countries in the Arab world, filtering had started reaching unprecedented levels, particularly in Tunisia, Syria, Saudi Arabia, and Yemen (Hartley, 2009). From experiences using some of them, circumvention tools that were built-in developed countries appeared to have been optimized for settings where the infrastructure is good enough to absorb the bandwidth needs required. Such solutions were also written mostly in English and sometimes in Chinese, and Arab interfaces were lacking. So to solve this problem, there was need to develop a software solution that would have a more sensible and economic approach in using resources and

with an appeal to Arab users in particular by first having an Arab identity and also an Arabic language interface to allow users to use it more effectively. That is when the idea to develop Alkasir came about so as to play that role. Before starting to describe Alkasir, it is useful to preview some of the research describing other Internet censorship circumvention tools.

Personal motive

The idea to develop Alkasir as a software circumvention solution started with two motives in mind. The first was as a reaction to the action taken by ISPs, when they censored my own website "Yemen Portal" (http://yemenportal.net), which is a search and aggregating engine for news and opinion content related to my homeland, the Republic of Yemen (Al-Saqaf, 2008, p. 164). When Yemen Portal got blocked in January 2008, I decided to take a deeper look into the subject of Internet censorship as a research subject, because I realized that it has become a serious problem for many independent and opposition websites in my country. I also came to see that there was very little attention paid to the plight of Internet users I met in Yemen as they struggled to get the other point of view when accessing online news and opinion, because that point of view was being filtered by the government-run ISP.

I consider Alkasir a project that emerged from frustrating human rights conditions in the Arab world and the need to break this cycle of online oppression, which also explains why the name stems from the Arabic word (الكاسر) meaning the circumventor.

Furthermore, I also realized that my computer engineering background could help me tremendously in assembling a software solution that would grant not only my readers in Yemen access to YemenPortal.net, but also readers across the world access to websites blocked because of critical news or opinion content. I felt the need to develop such a solution, because most of the available ones were too difficult to use and have English language interfaces only. Furthermore, I wanted to develop a solution that would make users able to visit websites blocked for political reasons while preventing them from using Alkasir to view pornography and similar content. In particular, my intention was to enhance the users ability' to view the suppressed opinions of dissidents across the world.

However, I realized that Alkasir could also be used to study the reaction of users to the possibility of accessing content that their ISPs tried to prevent them from seeing. In other words, it could be a useful tool in a scientific experiment to analyze the response of users when offered the ability

of leaving their digital enclosure and gaining more online freedom. It was not clear to me whether such a model would work and whether users would take the risk to install and run the program on their computers, knowing that the ISPs, perhaps with instructions from the government, had intentionally prevented them from accessing some content. Hence, the idea behind this dissertation came to life with the hope that analyzing user behavior after years of gathering data on the servers could contribute to a better understanding of online censorship and ways to defeat it.

Engineering Methodology

The construction of Alkasir started in the end of 2008 when I initially planned to adapt the sequential[110] software engineering methodology; I found it would be more useful to develop a working prototype as soon as possible to have the software distributed to the public, which meant that I did not have the luxury of time to wait for the four phases[111] of software engineering to be complete before it was ready for public use. Hence, I decided to use the versions methodology, which, as shown in Figure 35, allowed me to start producing working software that may have part of the requested services in the hope that the next version would have more functionality.

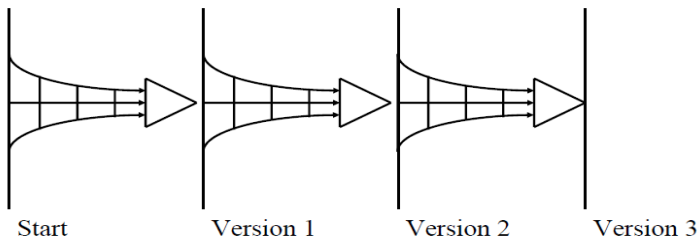

Figure 35 Versions software engineering methodology.
Source: Burback (1998)

This method allowed moving of the product from one version to another by recursively repeating the methodology steps for each version but

[110] This is also informally called the waterfall methodology, which requires that each of the four sequential phases: analysis, design, implementation, and testing must be executed in the given order before the software is ready.

[111] Analysis, design, implementation, and testing

with small added enhancements and functionalities every time (Burback, 1998, p. 50).

The development of Alkasir went through the four standard software engineering development phases of analysis, design, implementation, and testing for several versions, starting from the launch of version 1.0 and ending with the latest version 1.4.002 as of November 10, 2012.

Hereafter, I provide detailed description of the five phases of software development that were involved in developing Alkasir.

Requirement Analysis

The software requirement analysis phase of any software development is what defines the requirements of the system regardless of how they will be met. The deliverables of this phase are what the customer/user expects (Burback, 1998, p. 8).

At the analysis stage, the requirements document helps summarize what the user wants and defines the domain ontology of the software in the form of what things need to be delivered, what actions need to be taken, and what states the software needs to have. Furthermore, there will also be need for a description of the typical and atypical scenarios that the user may experience when running the software.

In the case of Alkasir, the requirements document establishes what the user expects Alkasir to do. These requirements were gathered based on my own experience and communications with several individuals who expressed interest in helping me design the circumvention solution. The main and fundamental requirement of Alkasir was represented in one formula written in mathematical logic, which utilizes formal language-based syntax or semantics to allow the creation of logic arguments using rules and axioms.

Apart from being used in social science disciplines such as philosophy and linguistics, mathematical logic is considered the most important mathematical subdiscipline of software engineering (Bjorner, 2006, p. 174).

For a particular website u, accessed in a country c, with a category t, the decision to allow it to be accessed or not would be called $P(u,c,t)$, and it would be as follows:

$$P(u, c, t) = ((u \vdash k) \vee ((\exists w \in D: w = \{u, c, s, t\}) \wedge !s \wedge (t \in \{a\_1, a\_2, \ldots, a\_n\})))$$

where

- u is the URL the user is trying to access and t is the category that u belongs to (e.g., news, multimedia, social networking, gaming, etc.)
- c is the country from which the user is connecting
- w is a set that must exist in D
- D is the database containing submitted URLs
- s is the status of accessibility of u (if it is inaccessible, then the value is false)
- k is a constant referring to the base domain (domain.com)
- $\{a\_1, a\_2, \ldots, a\_n\}$ is the set of all n categories that are approved.

What the formula means is when a user runs Alkasir, when the user opens a particular URL, the software should activate its circumvention feature to bypass the firewall restricting access if that URL was found to have been reported and exists in the database and to have had its category approved[112] or if the URL being accessed lies on Alkasir's server that must always be accessed through the proxy server in an encrypted form. It is important to note that this formula is what the program is expected to do on the basic level from the user's perspective. There are certainly other functions and features that users expect and those could be defined as the requirement goals of the software, which are not the ultimate goals behind using or developing Alkasir, but the immediate goals that the software ought to achieve for the user in terms of direct usage and application.

[112] As will be described in the algorithm section, not all content is approved for access through Alkasir (e.g., pornography is restricted) as per terms of usage of the software.

Requirement goals

The requirement goals that Alkasir must achieve from a user's standpoint should be clearly identified, as they will dictate how the software will look, how it will function, and how it will be implemented.

Circumvent URL filtering

As described earlier, one of the basic goals the user wants Alkasir to achieve is to ensure that the software has the ability to circumvent the filtering of a particular URL, which is submitted by the user, and if it meets the criteria, it would be approved by the administration of Alkasir.

As the user has supposedly read and agreed to the conditions and terms of usage before installing and running the program, he/she would understand that the policy of the program only allows the circumvention of URLs that meet the policy, which is stated clearly on the website at https://Alkasir.com/policy.[113] So the first goal is to allow the circumvention of URL filtering based on the approval policy of the software.

Speed and efficiency

Users want Alkasir to be fast for downloading and uploading data and communicating with censored websites. It should take advantage of the users' bandwidth capacity and be efficient in using the computer's resources. This goal is crucial particularly for users who live in developing countries, where infrastructures may not be as good as those in developed countries.

Simplicity and a multilingual interface

Users want to understand how to use the program's different features and functions easily. To do so, the interface of the software and its affiliated website need to be simple to use and in their own tongue. As the target is predominantly Arab users, Alkasir needs to be at least bilingual (in Arabic and English).

[113] The only criteria as of November 10, 2012 is the prohibition of submitting nudity-related URLs. This may be considered a limitation. A more detailed description of this condition/restriction and its implications is provided in the limitations chapter of the study.

Ease to upgrade
One important aspect for any software, including Alkasir, is the ease to upgrade it when it becomes out of date and when a new version is out.

Built-in Web browser
The software needs to be a standalone program that would not require the use of external Web browsers such as Internet Explorer, Mozilla Firefox, or Google Chrome. In other words, it must have its own built-in Web browser that can be run and used directly from Alkasir's interface.

Compatibility with popular browsers
In addition to having its internal Web browser, the Alkasir needs to be compatible with other external browsers, which will allow users to take advantage of the customized and private settings that they may have in the other browsers and simultaneously take advantage of Alkasir's functionality.

Security and reliability
One of Alkasir's requirements is to ensure that the program is secure in terms of not violating the user's privacy or breaching security. The traffic that it circumvents needs to encrypted to prevent digital surveillance, particularly from the ISP.

The IP addresses need not to be logged on the server. Furthermore, it has to be reliable and work in different circumstances regardless of the connection speed or other resource limitations.

Portability
Users wish to have Alkasir possible to move without having to do another installation on every new machine they use. It has to be easily portable from one system to the other, perhaps by using a memory stick or by compressing and sending it by e-mail or other data transfer methods.

Components

As a circumvention solution, users of Alkasir expect to see certain components that could carry out particular actions. Before moving to the implementation stage, it is crucial to have a clear idea of the components that Alkasir should have. In analyzing the aforementioned goals, it is possible to come up with the basic components required.

Graphical user interface
Users expect to see an interface that they could access and view with ease. Not all software developed nowadays have graphical user interfaces (GUIs), but for Alkasir to be easily accessible by novice users, having a GUI is vital.

Internal Web browser interface
As users expect to use the software directly without having to deploy an external Web browser, Alkasir's own Web browser needs to be a component with an interface that is possible to open and close directly through the software and should also have features and functions similar to those found in typical browsers. This means that within this component, all browser-related subcomponents, such as a database for bookmarks, and cache storage, should also exist.

Alkasir's website
The website of Alkasir needs to exist as a major component that keeps users informed and allows them to communicate with the developers of the program. It is also a way to download future upgrades and relevant information if required.

Authentication
Users expect to have the ability to connect to the database and fetch data relevant to their country and ISP. To do this, they expect to have authentication into Alkasir's Web server with a user login and password. Authentication should also be configurable so they could change and update their settings and profile online.

Data privacy
The ability to encrypt data from the client to the server is a major requirement and hence, as described earlier in the goals, Alkasir should protect private data from possible breaches.

Options and settings
Users expect to have a way to define particular settings that they could modify when required and options that could configure how the program and its subcomponents function.

URL submission interface
Users also expect to find a particular interface through which they could send/report URLs they suspect of being blocked by their ISP. This interface should have a form that provides detailed information about what is going on through the submission process.

Error-reporting interface
The software should give users the ability to report an issue or problem directly to the development team of Alkasir through an interface where they could find a form that they could fill out and submit regardless of the state of the software. In other words, whether Alkasir is connected or not should not prevent the user from sending a message or reporting an error to the developers. This interface is different from the form that exists online where users could also communicate with Alkasir developers.

Documentation
One of the most important components of any software is a full documentation (often called help files) that gives users a thorough idea of how to use the program and answer any possible questions they may have.

Checking for approved URLs
To stay up to date as to the status of censorship of URLs, users want Alkasir to provide a button or link that, if clicked, would provide them with an up-to-date list of all the URLs that are reported to be blocked in their country.

States
At any given moment, the user expects Alkasir to be in one of several states describing what the software is doing at any particular time.

Offline
This is the state of the software when there is no Internet connection or access is restricted to the whole network due to some authorization requirement or other restrictions, for example, at a paid Wi-Fi spot. The program should also have the ability to manipulate the state so it could be turned offline by the user.

Initializing
This is the expected state when the software is initializing the connection but is yet to be fully connected or active. For example, this is the expected state that the software goes through when the software is run after turning on the computer.

Connected and active
This is usually the desired state where the software is connected successfully, active, and ready to be used by the user.

Error
When the software fails to initialize and connect or when there is some other form of malfunction, a clear state of error should be established and visible for the user to begin troubleshooting and/or reporting the error to Alkasir developers.

Typical scenarios

Unlike a state, a scenario is not a static situation but a process that perhaps identifies a sequence of states. There are different scenarios depending on what the user is using the software for.

First-time post-installation run
When the user accesses Alkasir for the first time, it begins with an offline state and then asks the user for the interface language that should be used for the interface and the Web browser. Additionally, the user should have the ability to manually enter the country he/she is in. After doing so, the program should move to the initializing state, when it stores those settings and attempts to connect normally.

If the country provided does not match the country information obtained through the geo-location software Alkasir uses, the latter is used. After the software establishes a connection to the server successfully, it moves to the active state, which should from that moment onward allow the user to access censored URLs that were approved for access in the country where the user is.

Computer start-up or wake-up
When the computer starts up or wakes up from a state of hibernation or sleep, Alkasir should automatically refresh its connection, connect again, and fetch the latest database information to ensure that the list of accessi-

ble URLs for the particular country where the user is based becomes accessible.

Computer shutdown or program exit
Once the computer shuts down or Alkasir is manually exited, then the session's settings, including the cache and other options that were changed during the last session, should be saved before terminating the program.

Computer sleep or hibernation
The user expects Alkasir to save all settings and ensure that all browser windows and tabs are maintained and kept so they could be restored and accessed normally after the computer wakes up from sleep or hibernation modes.

Atypical scenarios

In unexpected or atypical conditions, there are some scenarios that the user expects to occur.

Loss of Internet connectivity
When the computer is no longer offline, Alkasir should automatically be turned to the offline state. However, the browser and other interfaces should not be affected and should remain open.

Sudden shutdown
If the computer was shut down suddenly, perhaps due to a power failure or computer damage, the software should be able to run normally the next time the computer is turned on successfully without having adverse effects on the internal files or settings associated with it.

Changing connection
In case the user adjusts the connection to use another ISP or moves to another location where the address of the IP changes, the software should automatically detect this and refresh itself without affecting the ongoing session on the internal Web browser. There may be a waiting period associated with this change. If this change occurs from one country to another, for example, when waking up a computer after arriving to a different country, the software should be able to adjust itself automatically to refresh the list of URLs accessible.

Removing software files
The removal of one or more files from the software's folder would require turning off (exiting) Alkasir manually to avoid corrupting it.

Copying software folder
Copying the folder of the software to a memory stick, for example, should create a complete duplicate/mirror of the same software that could thereafter be copied to and used on another computer with ease. The process of running the program thereafter would require verifying that the country is the same as the original location. When running a duplicate of the same folder, the software should not create new entries on the server but use the same entry for both copies.

Design

The second step in developing Alkasir was the design phase where a thorough plan was created with architectures and algorithms that need to be realized in the next implementation phase. The design naturally followed the analysis phase but with input from the developer perspective, because the analysis stage was merely from the user perspective, which is incomplete. The design phase for Alkasir resulted in five deliverables: architecture document, implementation plan, critical priority analysis, performance analysis, and test plan.

When it comes to architecture, Alkasir is not simply a standalone piece of software but a client/server distributed software implementation, with each side interacting dynamically with the other to ensure stability and consistency. Hence, the architecture design for Alkasir is composed of a client and server architecture. The algorithm design for the two main functions of Alkasir, that is, submitting URLs and circumvention processes, is provided to illustrate how each of the critical processes are to be carried out.

Client architecture

As with the case with every Windows application, the client application is the one that the user runs on his/her computer, and its performance would depend on the processor speed and memory of the user. For the Alkasir client architecture, the main requirements include a full understanding of how the data structure will be and how the main graphical user interface and built-in Web browser will look like and function. However, for both the main interface and Web browser, there will also be sub-windows

called by each component so that the user could view and change different fields.

Data structure

In terms of storage on the client side, a flat-file system model was utilized for the client in the form of a folder named "Alkasir-usb" by default. Upon first-time installation, the file structure can be presented by the following components:

1. Language

So far and as of version 1.4.002, only Arabic and English interfaces were available, with corresponding subfolders "ar" and "en." Each of those subfolders contains the dynamically linked resource file (Alkasir.resources.dll) along with the help document (help.chm) for the corresponding language.

2. Web browser library

This would have all files associated with the Web browser built to be an integral part of the software. An embeddable Mozilla Gecko (Firefox) library for .NET applications was to be used and its relevant libraries saved in a folder named "xulrunner."

3. Settings files

These files contain various settings for the browser, the connection, the country, city, ISP, options data, and other relevant information. They are all saved directly beneath the "data" directory.

4. List of blocked URLs

A country folder is created under the country's assigned two-letter top-level domain name (ccTLD),[114] and beneath it, separate folders are created where the lists of blocked URLs are stored in separate files based on the ISP.

[114] ccTLD is an Internet top-level domain typically reserved for countries and dependent territories to may correspond to data servers that exist in those countries. Examples are .tr for Turkey and .se for Sweden.

5. Cache folder
In case of testing if a particular URL is blocked or not, a special folder named "domains" under the particular country's folder is used to save parts of fetched and tested URLs.

6. Standby/ignored/new URLs
In special cases, there are instances when a particular URL is either new, on standby (expected to be blocked), or ignored (should not be added). Those conditions rarely apply but folders corresponding to URLs for each group are created any way in case they may be used in the future.

7. Other required dynamic library files
Those are the hotly dynamic link Microsoft Windows-compatible library files that are needed for Alkasir to function. They include alkasirB.dll for the browser, libeay32.dll, servrlib.dll and ssleay32.dll for security encryption, and proxy.dll for proxy-related functions.

8. Proxy configuration file
The file Alkasir.pac contains the JavaScript code snippet that is used to dynamically instruct browsers when to forward traffic to the proxy server for blocked URLs.[115] This file is updated dynamically every time the user connects to Alkasir servers.

9. Executables
The actual application files that run the main program are Alkasir.exe and alkasirS.exe, which are the Windows executable files.

Main GUI
The main GUI component was set to be the starting point where the program's various functions and features would be accessible. This would be the point of most recognizable part of the application to the user. The interface would require having a design that is easy to navigate and understand. With that in mind, the main GUI design was to include an Action Menu panel where there would be links that have the following functions:

- **Language:** to change the languages used on the interface on the client and website

[115] See http://technet.microsoft.com/en-us/library/dd361918.aspx for more information on how proxy automatic configuration is configured.

- **Report Blocked URLs:** to give users the ability to submit URLs for review
- **List Blocked URLs:** to list the already-approved blocked URLs
- **Adjust Options and Settings:** to view and change the program's settings/options
- **Report bugs and sending feedback:** to send encoded or plain reports of errors and feedback
- **About Alkasir:** to display a brief message explaining what Alkasir is
- **Register at Alkasir.com:** to allow the user to register as a member at Alkasir.com
- **Documentation:** the help feature, which is standard in most Windows applications

The interface also required having several control buttons:

- **Restart:** to restart the whole Alkasir application
- **Shut down:** to exit Alkasir
- **Launch internal browser:** to launch Alkasir's built-in Web browser
- **Initialize external browser:** to configure external browsers to work with Alkasir
- **Diagnose:** to find and troubleshoot problems with the connection to Alkasir server
- **Scan for changes:** to check if any of the listed blocked URL became unblocked or previously unblocked websites became reblocked again
- **Minimize:** Minimizes the interface box to the system tray

Apart from the Action Menu and the control buttons, there are also visible dynamic fields, which are useful to provide the user with information relevant to the session. Those include the number of blocked URLs approved and accessible through Alkasir, the status of the proxy service ("on" means circumvention is active, "off" means it is inactive), the status

of the Internet's connectivity, the type of the connected proxy (either public or private),[116] along with the user's ISP, city, and country information, which are possible to obtain based on the IP address using geo-location identification software.

Built-in Web browser

Like any Web browser, Alkasir's browser's design should have menus and buttons that facilitate the browsing experience. In general, there should be the following menu items (with each having its own submenu):

- **File:** contains all functions related to opening, closing, saving, printing, exiting, etc.
- **Edit:** offers usual text-editing functions such as copy, paste, cut, select, etc.
- **History:** includes a list of visited pages and allows the movement back and forth.
- **Bookmarks:** allows the modification of bookmarks and changing the home page.
- **Circumvention:** a special menu that does not exist in regular browsers. It includes a number of options and functions. It allows the disabling of circumvention, reporting of a blocked URL directly, accessing Alkasir's URL submission policy, changing proxy settings, selecting the method of circumvention, disabling dynamic circumvention,[117] plus several other functions.
- **Browser Tools:** deals with cookies, downloads, Alkasir.com login, and similar functions.

---

[116] If the public proxy is found to be inaccessible for any reason, it should be possible to test the service with a private proxy.

[117] Dynamic circumvention based on the blocked list means that any content fetched from a blocked URL will be tunneled dynamically through the encrypted proxy tunnel. In the case this is disabled, the circumvention process does not deal with the internal contents of the page, but only with the main site opened. For example, if the page http://somewebsite.com contained components from other websites that are blocked, they will only be fetched through the tunnel if http://somewebsite.com itself is blocked. In dynamic tunneling, each component on each page is fetched based on whether any of its components lie on a blocked URL or not.

- **Help:** the usual documentation menu allowing the finding of the documentation and manual information and viewing of the program's version.

Apart from the menu item, there are several buttons that serve as shortcuts. But it is possible to use all functions of the browser by exclusively using the menu items. The main body of the browser is the place where the tabs are. The way tabs are displayed is quite similar to the way of the regular browsers.

Secondary windows

Apart from the two main GUI windows representing the interface and the browser, there are other secondary windows also that allow the user to view or edit information.

The most important secondary forms are as follows:

- **Options and settings:** allows the user to decide on whether to allow automatic updates, activate a stealth (hidden) mode, receive news alerts upon start-up, change the local port number for connecting to the local dynamic proxy server that Alkasir starts,[118] the language of the interface and website, as well as the country where the user is based.
- **Initializing external browsers:** allows the user to configure the external browsers to use Alkasir's proxy to access blocked websites. It includes instructions for Internet Explorer and Mozilla Firefox.[119] The form should allow the user to configure the external browsers manually or allow Alkasir to attempt to configure them automatically.
- **Reporting/submitting URLs:** allows the user to report URLs he/she thinks are blocked in his/her country. Once submitted, the window would provide details on how the verification process is going and ultimately provide a results page on the Web browser.

[118] More on this is explained in the implementation phase

[119] There is no need to have a separate option for Google Chrome because it uses the system-wide proxy settings that can change using Internet Explorer.

Server Architecture

On the server side, there are two different servers that Alkasir utilizes. One is the data server, which hosts the databases where user activities are logged based on their connections and usage of the internal browser. That server also hosts Alkasir.com domain. The other server is simply called the proxy server, which connects the client to the blocked URLs. When referring to the server, it usually means the data server, which is the server used for storing information.

Data server

The data server has two fundamental functions. The first is to serve as the storage place for all the logged transactions of Alkasir users when they connect, access blocked URLs, and submit URLs to verify their blocking status. And the other is to host Alkasir.com website's files.

The data server is where the installation files are downloaded, the global censorship map is accessible, users register new accounts or modify old ones, newsletters and documentations are published, and, most importantly, users see the responses to their URL submissions and moderators review and decide whether to approve or reject submissions based on the submission policy. Hence, this server is fundamentally the most important central server in terms of data storage not only for the developers but also for the clients. As of November 10, 2012, the site is located in the United States, hosted on a virtual private server (VPS), and is accessed through encryption at https://Alkasir.com and plain http://alkasir.com.

Another important data server function is to connect with users for occasional surveys, such as the two that were used in this study. Having data centralized on one server facilitates backing up, updating, and accessing data seamlessly. The data server contained three databases: a statistics database (DB), the website DB, and the survey DB.

Statistics DB

In this database, there are five tables that keep log information of Alkasir usage. The first table is for installation entries called ID.

Every new installation/first run is given a particular unique ID number and saved in this table. This ID thereafter corresponds to the activity of that particular installation. The second table is called ISP, where the name of used ISPs, geo-locations, and last-update time stamp along with countries are saved. The third table is named Moderators, where the e-mails, pseudonyms, and settings of volunteer moderators responsible for moder-

ating URLs submitted by Alkasir users are. The fourth and arguably the most crucial table is called Submissions, which contains the URLs submitted, along with relevant information that is essential to utilize the mapping and circumvention function of the software. Finally, there is the Users table, which has more information about the users in terms of ISP, country, last access, history, etc., but no personal information.

Website DB

This is where the content management system (CMS) for the website Alkasir.com keeps all relevant files. It also contains scripts used for moderating and submitting URLs. The CMS used for the website is Drupal, which was chosen for its reputation of being more secure than most other similar systems. Jason Hill, cofounder of DharmaTech, said that between the two most popular open-source CMS platforms, that is, Joomla and Drupal, the latter does much better in terms of security (Dern, 2011).

Survey DB

This database is used by an open-source surveying software named LimeSurvey, which allows the creation of Web surveys that are quite complicated yet efficient directly on any Web server. It is much more secure and reliable to have the surveys on the server of Alkasir, both in terms of the security of the users and for the reliability of data. This database was required so it could include data for all surveys used for this study as well as future studies.

Proxy server

The proxy server is used to tunnel encrypted traffic between clients and blocked URLs. It also serves as the tunnel between the client and the data server that exchange encrypted data. Accessing this server is done through dozens of IP addresses that provide a way to minimize the risk of being detected by any ISP and blocked. This server exists in the United States and is hosted on a dedicated server running the 64-bit operating system CentOS 4 or 5 built on Red Hat Enterprise Linux. The server has unfettered access to the Internet, allowing it to be used by Alkasir users to access blocked URLs in their respective countries.

The proxy server runs an OpenSSH[120] daemon to accept connections from Alkasir clients and establish secure encrypted connections. The server does not log the clients' IPs or personal information and, instead, it serves as a dynamic tunneling server that saves no data on it about who uses it and for what purposes. Details of how the proxy server interacts with the data server and the client are provided in the software implementation section of this appendix.

Algorithms

In accomplishing its functions, any software must have a clear set of algorithms that serve as road maps to start the actual coding process. In general terms, an algorithm is a step-by-step process that arrives to a solution to a problem in a finite amount of time. For the case of Alkasir, two main[121] algorithm designs were needed.

The first is to know when to allow the client to use the proxy server to circumvent censorship and the other is to handle URL submissions by users.

The two algorithms were first designed using simple flowcharts, which could thereafter be translated into actual code in the implementation phase.

Circumvention algorithm

By default, Alkasir clients will connect through their ISP to reach URLs directly. The only two cases in which the circumvention encrypted tunnel will be used are as follows:

1. when the URL being requested is on Alkasir's data server and
2. when the URL being requested is found on the list of blocked URLs that every Alkasir client gets upon running the software.

The data server holds the database that contains the approved list of blocked URLs. Apart from the approved list, there is also another list

[120] OpenSSH is a software implementation that provides end-to-end encrypted replacement of applications such as telnet, rlogin, and ftp. It is an open source implementation of the secure shell (SSH) network protocol, which allows data to be exchanged using a secure channel between two networked devices.

[121] There are certainly many other smaller algorithms used in Alkasir dealing with secondary functions. But they were not be presented here due to space limitations.

containing URLs that have been submitted before but that are awaiting moderator approval (or rejection if they do not meet Alkasir's policy).

When a user runs the software, it should start initializing and thereafter become in an active state that should be clear from being turned "ON" on the system tray. While initializing, the program hooks the computer to the proxy server through a secure tunnel. The IP address of the user is used to identify the censoring ISP and country information, which are discovered through geo-location software located on Alkasir's data server. Once the country's entry on the database is accessed, the list of URLs known to be blocked in that country is downloaded from the data server to the user's computer.

- Once the list is downloaded, the user could attempt to access a particular URL and the circumvention algorithm shown in Figure 36 will be used to find how to access it as follows:
- The URL is first entered by the user and verified to be correct in syntax.
- The URL is checked against the list of URLs known to be blocked in the country where the user connected.
- If the URL is found to be on the blocked list, an entry is added to the database on the data server to increment the number of requests (visits) that the URL had from this particular ISP. If it is found to not be on the list, no entries are added, and the regular ISP connection is used to fetch the URL content.
- For the URL found to exist on the blocked list, the system attempts to use the secure proxy tunnel only if the tunnel is accessible. There could be times when the tunnel is for some reason not working, in which case the fallback would be the regular ISP. Otherwise, the content of the URL is fetched through the proxy server and data displayed on the user's browser.

The above steps are all that are needed for the user to bypass filtering of websites dynamically with Alkasir. However, this process is incomplete without the ability to create the list of blocked URLs that meet Alkasir's policy so as to effectively utilize the circumvention method devised in the algorithm. To do this, an algorithm to report censorship was devised.

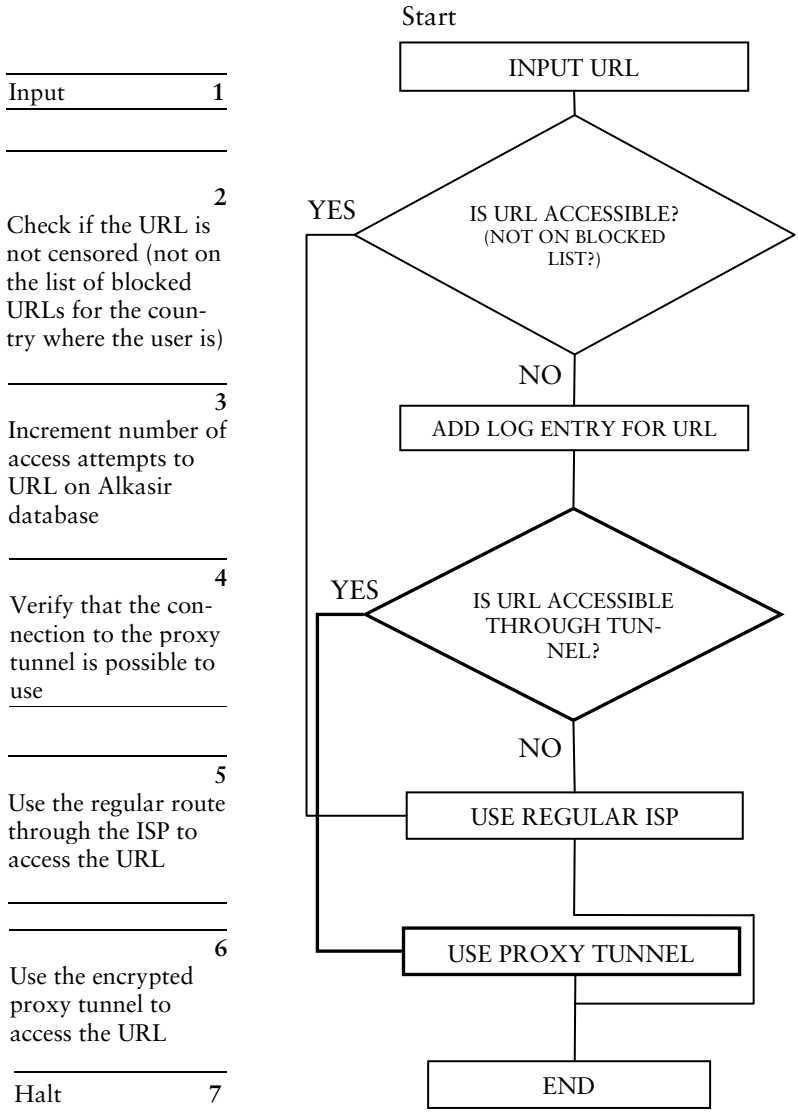

Figure 36: Algorithm flowchart for circumvention

Reporting censorship algorithm

Alkasir users should be able to report what URLs they believe may be filtered and thereafter let Alkasir verify this information dynamically and with the help of moderators when required. If many users do this, it results in the process known as crowdsourcing, which is defined by Howe (2006) as "the act of a company or institution taking a function once performed by employees and outsourcing to an undefined (and generally large) network of people in the form of an open call" (Howe, 2006, p. 5).

With the public call for using Alkasir and reporting about blocked websites, Alkasir is utilizing crowdsourcing in an attempt to map censorship patterns around the world. This is helpful in the long run because it improves the reliability of data when it comes to national censorship in each country. It helps rule out individual cases where computer and software-related problems may have been the cause of inaccessibility to certain URLs.

For each individual user, the algorithm of reporting a URL is as follows and as shown in the flowchart in Figure 37:

- The user finds that a particular URL that used to be accessible in the past is no longer opening. So he/she clicks a button on Alkasir's interface where the blocked website's address could be fed and reported as *blocked*.
- Once the URL, which is validated for syntax before being accepted, is reported to the server, the content of the URL is fetched locally and sent to Alkasir's server to compare with the one fetched through the uncensored external server. A comparison mechanism takes place on the server to verify if the website is blocked or not. If there is a mismatch, this raises a red flag and points to a potential case of censorship. If there is no mismatch, the URL is probably not blocked. If it was found to be inaccessible at both ends (client and server), it may be that the server where the URL is located is having a problem that has nothing to do with the firewall.
- Once a website is verified to be potentially blocked, the database on the server is checked to see if it has been reported before or not. If the URL was reported for the first time and was found to have indeed been filtered, it is added to the database on the server for review by a moderator.

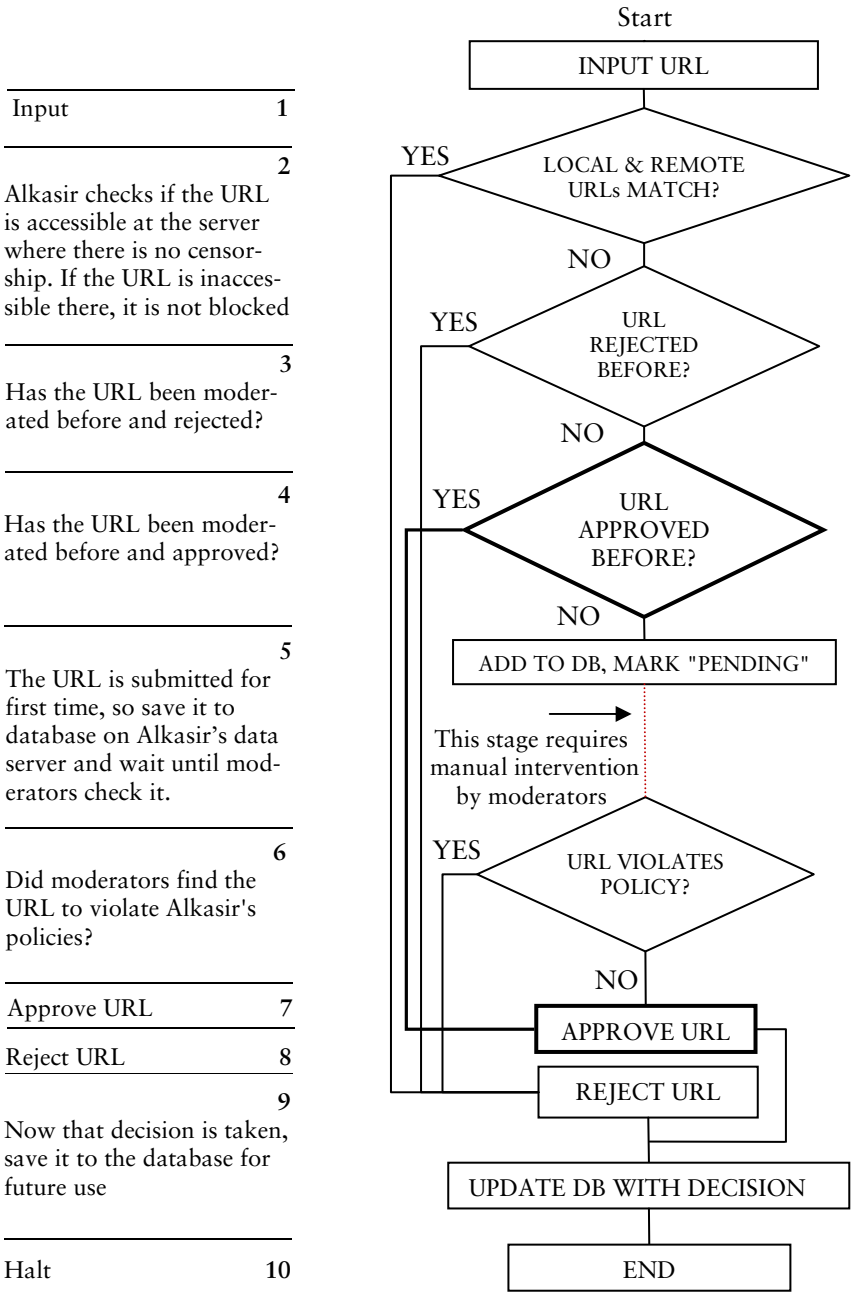

Figure 37: Algorithm flowchart for reporting censorship

- Once a moderator approves the website and finds it in agreement with Alkasir's policy, the URL is marked as approved on the database and is added to the list that the user downloads every time Alkasir starts. Once it is added, it joins other URLs that become accessible through the tunnel as described in step (4) of the circumvention process to the Alkasir user who reported it along with all Alkasir users in the same country.
- To apply crowdsourcing more effectively, the URL is reported on behalf of other users using different ISPs in the same country where it was originally found to be blocked. Based on the results from different users in the same country, maps can be created to identify which URLs appear to be censored on a national level and which are censored on an ISP level.[122]

As explained above, the two main functions of Alkasir, that is, allowing users to circumvent censorship and to report about blocked websites, complement each other. Every time a new URL is reported by a single user and approved by a moderator, that website becomes accessible by all Alkasir users in that specific country. The more users use Alkasir, the more likely blocked websites will be reported and approved and hence the more likely that users will be able to bypass censorship.

The process of reporting a website, however, does not guarantee that the website will be approved, because it should meet two basic conditions. The first is that it should be verified to be blocked and the second is that it should satisfy the policy of Alkasir. Oftentimes, a reported website is not approved because it is either found to be already approved or not blocked at all. This explains why only a portion of reported websites is approved.

It is important to understand that Alkasir necessitates that users take the initiative in reporting about blocked websites. Otherwise, the crowdsourcing potential of Alkasir would not be used. This explains why using Alkasir is not productive in countries with no censorship or in countries where censorship happens only to URLs that violate Alkasir policy, for example, pornography. Meanwhile, Alkasir would be most effective in countries where political/security content is pervasively filtered (e.g., Middle East, China).

[122] This map is then put on the website so it could be publicly accessible at https://Alkasir.com/map

Implementation Plan

The devised implementation plan for the development of the software constituted of a schedule that required completing all the three architectural components: client application, data server, and proxy server. At this stage, it was time to plan for the implementation phase in terms of defining the programming languages, the platforms, the programming environment, and resources, as is the standard for software engineering tasks (Burback, 1998, p. 14).

At the client's end, the plan was to build a Windows application built on the Microsoft .NET Framework, which is a component available for Windows users. It was an integral part of Alkasir as it provided with a number of dynamic libraries that add the functionality required to run the program smoothly. However, because the Framework is only available on Windows operating systems, it meant that Alkasir was confined to Windows users. The decision was made to have Alkasir start as a Windows-based program due to the complex functionality that the software required, which required Microsoft .NET Framework. Furthermore, the overwhelming majority of PC users in the world have Windows as their operating system (W3 Schools, 2012).

The programming languages used to develop Alkasir were C/C++, C#, and JavaScript. As a development environment, Microsoft Visual Studio 2008 was chosen because it is an integrated development environment used by many researchers and software developers to create Windows-based software solutions. The environment for the data and proxy servers was planned to be a virtual or dedicated server running the 64-bit operating system CentOS 4 or 5 built on Red Hat Enterprise Linux. Both servers must have back-end administration interfaces with WebHost Management and cPanel interfaces installed for easier administration.

As the implementation of this software development project was based on the versions methodology, it was important to come up with a first working version (Alkasir version 1.0) as quickly as possible. So the implementation plan was to have the first working prototype developed and built and launched in its beta version by mid-May 2009. When the first version of the software was launched, the storage used on the server for logging purposes was of a flat text file structure. The release of version 1.2.0 was when the software moved to use a more efficient MySQL database structure, which has since been used in all following versions. The plan was to have a major version release every 6 months on average, with every newly launched version having fewer bugs and new features. At the

time of planning, only limited resources to start the first phase were available. So they were used sparingly to purchase a modest server and Web hosting package. As the software gained popularity, the plan was to apply for future funding to expand and horizontally increase the capacity and speed of the software to absorb more users, although it was not clear how many users there would be. That is why the versioning methodology was useful, as it allowed revisiting the plan for every new version.

Critical priority analysis

The critical priority analysis is a crucial phase needed to identify the critical tasks that software should achieve. For the first version of Alkasir to be published, the first critical task was to build a complete working application connected to a data server that was not exclusive to Alkasir, but could be used for other purposes.

The plan was to use the server of Yemen Portal (http://yemenportal.net) at the beginning to first understand if the software worked. Thereafter, the second critical task was to measure the speed of the proxy server and see if it is possible to deploy it for multiple users without affecting the performance of the Yemen Portal server.

The possibility of reviewing the critical priority list for every version made it possible to add new functionality and components for every new major version release. For the case of Alkasir version 1.0, many of the functions that exist in the latest version 1.4.002 were not of priority, including bilingual support and the built-in browser. Those features were added down the line, as will be described in the evolution section toward the end of this part of the dissertation.

Performance analysis

It was important to have in mind the performance expectations of the software as that would reflect on its functionality, particularly if hundreds of users end up using it. In analyzing the performance requirements, it was important to devise a method that would minimize bandwidth usage, so more users could use the same server efficiently. To achieve this, a mechanism based on a popular concept in network communication called split tunneling was adapted.

Minimizing bandwidth use through split tunneling

In a typical software circumvention solution, a client runs the software on his/her computer, and, thereafter, all the traffic to and from the Internet

would go through the proxy server, creating a tremendous burden on it in terms of bandwidth consumption. If thousands of users use the service simultaneously, this would end up lowering the share of bandwidth that each connected client would use.

In order for Alkasir proxy server to avoid this, split tunneling, illustrated in Figure 38, was devised so as to ensure that the proxy server is only used for URLs that cannot be reached directly due to filtering. This meant that if for example only website W1 is censored in country A, and another website W2 is censored in country B, the proxy server would only be used when W1 in A or W2 in B is accessed. But if W2 was accessed in A, Alkasir will not use the proxy server, nor will it use the proxy when W1 is accessed in country B. Similarly, all other websites (e.g., W3, W6, W8), which are not blocked in either country, would all go through the regular ISP without using proxy resources. In this way, the proxy server could serve many more clients compared to typical circumvention software that tunnel all traffic.

However, to be able to map censored content, Alkasir was required to have a complex system of identifying which URLs are blocked in which country. And that is the role of the URL submission strategy, which also needed to have some performance objectives.

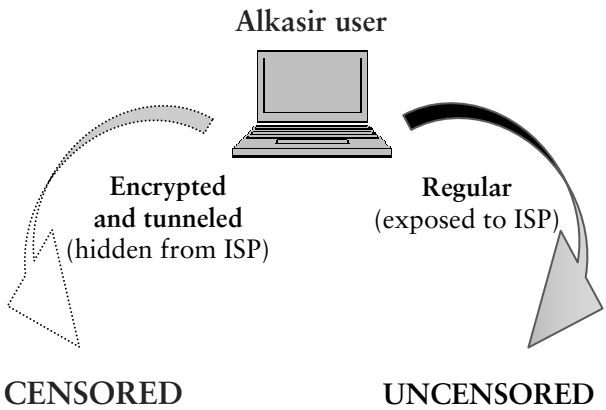

Figure 38: How Alkasir split tunneling works

Submitting URLs

It would be quite demanding if the user had to view a website and see if is blocked or not and then report this manually through the program, so to save time and bandwidth, Alkasir devised a more efficient solution by grabbing only the HTTP header[123] fields, along with the first one kilobyte that followed. In this way, it would be possible to check tens of URLs without having to download them in full. If there is a mismatch between the headers retrieved at the client's computer and the headers of the same URL retrieved at Alkasir's server, the only possibilities are as follows:

1. The URL is blocked intentionally and hence it is censored.
2. The client's computer is not able to view the URL for some specific issue to do with that particular computer and not necessarily with others in the same country.
3. The URL being requested has different versions of the same address based on where the request is coming from (e.g., if google.com is accessed in Sweden, the connection may be redirected to google.se).
4. There are other technical bottlenecks that are preventing access, but they are not intentional.

In each of those scenarios, the result is a report of potential censorship of that particular URL. The number of URLs mistakenly identified as censored should be negatively correlated to the number of users using Alkasir in that country. Hence, to ensure that only those who need the service get it, the software should do the following:

1. Apply crowdsourcing so that Alkasir users from the same country access the same URL and verify its status. If multiple clients get the same result, then the URL may be inaccessible nationwide.
2. Routinely check to see if the URLs reported earlier remain blocked or not by having scheduled scans to remove those URLs found no longer to be censored.

By applying the above steps, the level of performance of the architecture improves, allowing more users to use the same server more efficiently, while allowing the system to have more reliable information on the pat-

[123] HTTP header fields define the operating parameters of any request for an HTTP link. They are the first lines of data that are sent when a particular web page is requested.

terns of censorship in any particular country at any given time provided that there are enough users in that country running the software.

Apart from the use of crowdsourcing to reduce the burden on every user, another important performance improvement was having the server learn about URLs that have been rejected or approved before. Hence, if one website was submitted once and approved by moderators, it would be automatically approved if a user anywhere in the world submits the same URL for review. The same applies for rejected URLs. This also reduces the burden on manual moderation. Those two features are added to maximize efficiency and reduce overhead for the staff and the users themselves.

Test Plan

A devised test plan was defined in three stages; the first is the internal stage where I, as the developer, would do the testing rigorously with multiple computers using multiple ISPs. This would last for at least one week for every version. The next stage is to invite a closed circle of volunteers who are familiar with the work and live in different countries. They would provide feedback on the quality, design, speed, and other features that may be less frequently used. Bug reports are then compiled into a to-do list for the next test. Once the final test by the core group is complete, the version is officially launched for the general public to use and report bugs whenever possible.

This testing methodology was devised for each specific version. When doing tests, there should be an ability to report internal information saved from within the system and encrypted before it is sent to the developers for decryption and analysis. Thereafter, notes are to be taken, and, based on that, bugs get fixed for the next launch.

Implementation

In software engineering, the implementation phase is when the actual coding process starts and the different components are built and assembled together. For the case of Alkasir, coding was done on the client side using the Microsoft Visual Studio environment with C#, C, and JavaScript and on the server side using PHP, HTML, and JavaScript. Some components used open-source libraries while others were written from scratch. All the components were combined together to work seamlessly as one distributed client-server solution.

Local SOCKS proxy implementation

The coding of the most important part of the project was the implementation of the local SOCKS proxy, which is an Internet protocol that routes data between a particular client and the Internet through a proxy server. It can be used for different protocols such as HTTP for browsing, e-mail, FTP, and other applications that support SOCKS.

Because circumvention requires that the SOCKS proxy be set up on the client's computer, it requires a connection to a remote proxy server. Hence, Alkasir's proxy server was set up to accept connections through SSH. On the client side, a modified version of PuTTY,[124] which is an open-source emulator application used for Telnet, rlogin, and SSH connections, was used to create a dynamic local port that could serve as an encrypted tunnel and with a SOCKS proxy interface.

The PuTTY implementation was written in C and was recompiled and integrated into Alkasir with the executable alkasirS.exe, which is the application that runs the SOCKS proxy in the background and accepts connections that are forwarded to the proxy server. The GUI of Alkasir included options that would allow modifying the local port number to be used to connect to the SOCKS proxy on the client's computer. This would prove helpful in case of any conflict with ports used by other programs.

On the server side, the OpenSSH server daemon was used to receive and forward traffic between the client and the Internet. The proxy tunnel would be used by default only when confronted with a blocked website as per the circumvention algorithm described earlier. The implementation for the first working version took over two weeks to complete, but remained infested with bugs and weaknesses. Follow-up fixes and improvements

[124] PuTTY was created by Simon Tatham and remains under constant development. See the official website: http://www.chiark.greenend.org.uk/~sgtatham/putty/

continued ever since, and the software in its latest version 1.4.002 remains under development.

Once the proxy is running successfully and connected to the Internet, the main GUI indicates that the proxy is "ON" and the icon is lit red. This is clearly shown in a snapshot of the main Alkasir GUI in Figure 39.

Figure 39: A snapshot of Alkasir's main GUI for a user located in Sweden

Built-in Web browser

Similarly, another open-source library was utilized to build Alkasir's built-in Web browser, which to some degree emulates common browsers such as Mozilla Firefox and Internet Explorer. However, as indicated in the design subsection, it had some additional circumvention-related features

implemented. The library used was GeckoFX, which is a Gecko Mozilla Firefox .NET Framework implementation built on C#. It was possible to be integrated into Alkasir with many modifications and changes, so it could be seamlessly part of the whole solution. The dynamic library files needed to run the browser were added to the software folder, and an additional file was compiled and named alkasirB.DLL, which is stored with the main executable Alkasir.exe and the SOCKS proxy-initiating application alkasirS.exe. Figure 40 shows a snapshot of the browser interface with several tabs open.

The status at the bottom of the browser window indicates whether the active open tab is running on the proxy connection or through the local ISP. For the case when a URL on Alkasir.com is open, it is essential, as indicated earlier, that it uses the proxy to maximize security in communicating with the data server. This mode is activated for the data server regardless of Alkasir.com being blocked or not in the country where the user is located.

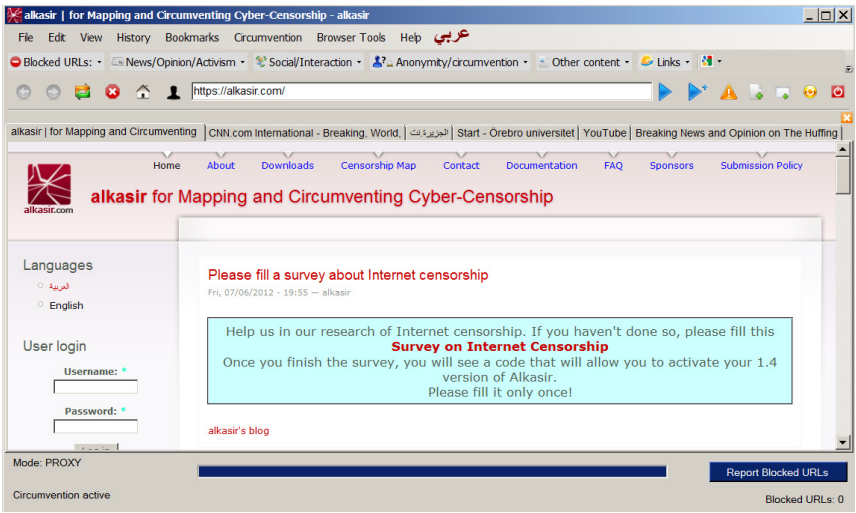

Figure 40: A snapshot of Alkasir's built-in Web browser

Data server implementation

On the data server side of the solution, several different components were built. Those are mainly PHP-based script files that have different functions and can be summarized in the following:

Submitting URLs

When a user submits a URL, the client first fetches the header and mines the file for other URLs that are present within it. Each of those URLs is then added to the list that will be checked for filtering. Then for each URL found, the script will attempt to get the header and first one kilobyte of data from them locally and sends this information to the server, where another script analyzes the content received from the client and compares it to the header and content received on the server where there is no censorship. If there is discrepancy indicating that there may be some censorship, results are then displayed to the user with information on whether the URL may be censored or not. If it is censored and was found to have been approved or rejected before, this information is shown to the user on the same page. If the URL is submitted for the first time, the user is then informed that moderators will review the site and send their decision to his/her e-mail if an e-mail address was provided or just update the database with the decision as shown in the algorithm design.

Figure 41 shows a snapshot of the response page shown to a user who tried submitting a URL that had already been submitted by him or some other user in Syria and was already approved by Alkasir's administration because it met the submission policy. As the software uses crowdsourcing to verify the status of a particular URL, the script adds information confirming that the person who submitted the URL is correct in assessing the status of the URL, which was also found to be blocked by other ISPs.

The script also automatically sends a brief notification by e-mail to all active moderators when a URL is submitted. Furthermore, as the solution is bilingual, every script can automatically detect the language used at the client's end and present the information in the desired language to ensure that the user understands the response.

Figure 41: An example of a server response to a URL submission

Moderating URL submissions

One of the basic functions of the Alkasir server is to call for the moderators to review a list of pending requests for review. The moderator would get an idea of what URL was reported and decide on its category as well as on whether to approve or reject it based on Alkasir's URL submission policy. In relation to the example shown in Figure 41 concerning URL submission, a moderator has in fact approved the website before and what he/she got by e-mail is demonstrated in Figure 42, which presents the form that the moderator needs to fill out.

This form includes the title of the URL in English and its native language (usually Arabic), category, and other options. If a category does not exist among the available categories to select, the moderator can in fact add a new one, which would thereafter be used in future moderating sessions.

It is also possible for a moderator to call this script after a decision is made to change it at a later stage. This would be useful in cases when a particular URL, for example, changed its content or category, or went offline. In such situations, the moderator can override earlier decisions, and this would reflect on the database, which in turn would affect all the users in the particular country where the URL was reported as blocked.

The moderator also has an ability to consult other moderators in the loop to know which category the URL fits best. Once the database is updated with the latest change, a new e-mail is sent to the other moderators informing them about this update, so they would be aware that someone had actually completed the process, and if they disagree with the decision,

they could ask to revisit it and have another round of consultations. There are also daily and weekly reminders that are sent by e-mail to moderators in case there were pending submissions.

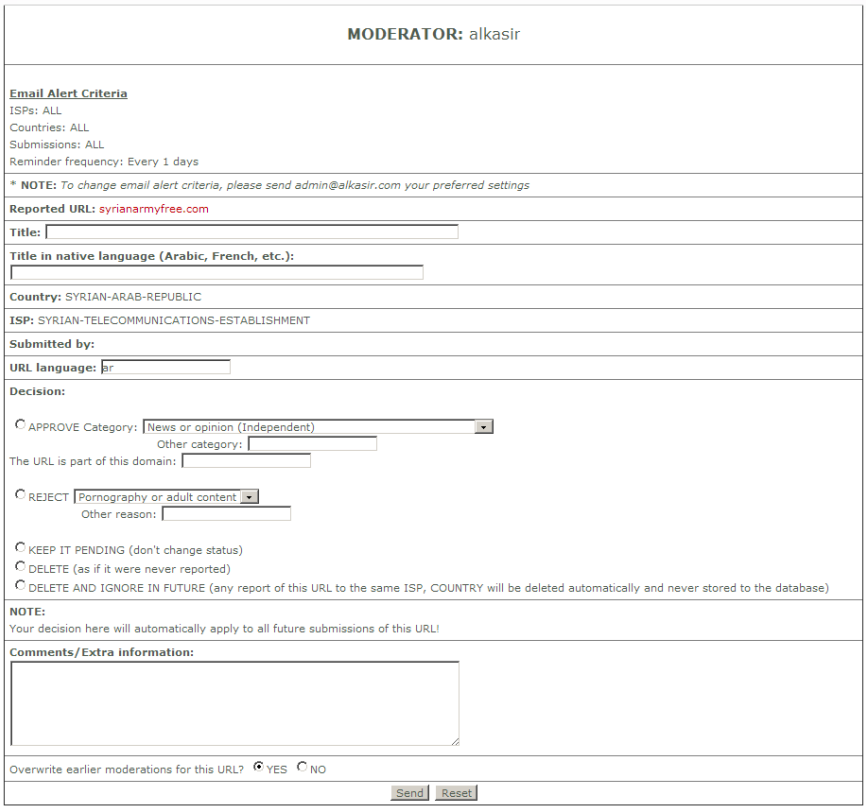

Figure 42: An example of a message sent to moderate a new URL

Other functions

Among many others, the data server handles the following main functions:

- **Geo-location:** When the server gets a request to find the ISP and country of a particular user, this is required so as to send back the appropriate URL list.

- **Forwarding country-based URL lists:** Every time a client initiates a connection, a freshly retrieved list of blocked URLs in the user's country is sent, and there is a particular script on the data server that handles this.
- **Mapping:** There is a routinely updated Google Maps map that identifies the number of ISPs per country blocking a particular URL and in a particular category. This map[125] is publically accessible and serves as a resource for those wishing to learn about censorship patterns around the world. A map retrieved on November 5, 2012, is shown in Figure 43.

Figure 43: A snapshot of the map generated dynamically on alkasir.com (using Google Maps) on November 5, 2012

[125] See https://Alkasir.com/map (English) and https://Alkasir.com/ar/map (Arabic)

Testing and Evolution

It is standard practice to have a testing phase for software projects that have been completed. For Alkasir, the moment the first version, 1.0, was completed, the testing phase started as planned, with internal testing by me on different computers running Windows operating systems ninety-eight and Vista and using different ISPs. Thereafter, a small number of volunteers contributed in identifying issues, bugs, and loopholes. After I got reasonably satisfying results, I launched it to the public domain via the website, so it could be tested by those who would try out a product that they do not know much about. Thankfully, several people and friends including technology experts and even other software developers were able to point some serious flaws in the software at the beginning, security issues, and bugs. As time progressed, the software evolved and became less prone to errors. Yet, as with the case with all software, Alkasir remains under development.

Hereby, I present a quick overview of the evolution of Alkasir through the versions methodology to highlight some of the bugs and issues discovered and fixed along the way while stressing that even the latest version is subject to continuous testing by users, who get to know about new updates automatically through the program itself and also by e-mail for those who subscribed to the software's newsletter at Alkasir.com. Subscription at Alkasir.com does not require personal information but just an e-mail address that is verified to prevent spam. Not every user of Alkasir needs to be a subscriber to be able to use the software. As of November 10, 2012, Alkasir had 13,836 newsletter subscribers on its website.

Alkasir 1.0

Work on the first version of Alkasir started at the end of 2008 and the official release of Alkasir 1.0 was on May 16, 2009. The first public announcement was made in a presentation at the American University in Cairo. The software was funded with seed money from MidEast Youth, which is a nonprofit organization based in Bahrain. The organization then released a post on its websites explaining the intentions of Alkasir and why it is different (Esra'a, 2009).

The first version was rather simple and had basic functionality that allowed circumvention to a limited number of websites as the number of reported URLs was limited due to the limited number of users. It was albeit a rather buggy version with many issues to fix and improve. Nonethe-

less, the fact that it functioned as a circumvention tool was quite encouraging.

Alkasir 1.01

In June 2009, Alkasir 1.01 was released after users used the software, because as new bugs were reported, fixes were made. Among the problems that were fixed was a bug that prevented normal operation of Alkasir in Windows Vista when record of blocked websites gets updated. Administrative rights for Windows Vista were also added to allow writing into the program's directory. The new version also added more debugging information to help with testing and fixing future versions.

Alkasir 1.2.0

It was estimated that Alkasir 1.01 was installed over a thousand times by mid-2010. It was an impressive leap given that the software had virtually no marketing or social networking presence. Word of mouth may have been what made some users try to use the software. Although minor reversions were produced during that time, the biggest paradigm shift for Alkasir was in June 2010, when 1.2.0 was released. This version included many radical new features and additions. The new version had the following changes:

- Introduced a multilingual capacity and added Arabic as the second interface language.
- Removed the internal browser of Alkasir in favor of the system's default browser (based on popular request).
- Introduced a private proxy setting through which certain computers could be linked through a privately allocated proxy server. This feature is intended for testing and censorship verification purposes.
- Added the ability to report blocked URLs and not only domains.
- Eliminated the need for manual updating of active list of blocked URLs by introducing a built-in timer to ping the server for changes.
- Eliminated all non-secure transfers within the file.
- Moved from flat-file storage of raw log data to MySQL.
- Fixed the bundling issue to allow automatic launch of Net Framework Setup 2.0 when needed.

- Added a button that could diagnose if the connection to the proxy server is working or not.
- Added a special function to enable the user to send encrypted debugging information to the developer by e-mail or through the interface.
- Added a stealth mode in the preferences, which allows users to prevent the program's icon from appearing on the system bar.
- Fixed some missing links on the interface.
- Enabled the user to restart the browsers with a button click (exiting normally so as to save sessions when possible).
- Ensured that the proxy tunnel is working before Alkasir is lit on the system tray.
- Added a more robust method to retrieve the ISP and Geo-location information (ISP, city, region, and country).
- Added an e-mail notification to submissions (once approved or rejected).
- There were also several additions/changes on Alkasir.com's side of the solution in terms of approval of submissions and other features.

Alkasir 1.3.0

Two years after releasing the last major version, Alkasir 1.3.0 was released in January 2012. It was two years of growth for Alkasir, which may have become more popular and useful due to the Arab Spring and because of the rise in censorship in Tunisia in 2010 and the uprising that led to the short-lived censorship of Twitter and Facebook in Egypt in the beginning of 2011. The total number of successful installations since the launch of version 1.3.0 of Alkasir soared in early 2012 to reach unprecedented numbers exceeding 50,000 for the first time, which prompted optimization steps in this version to improve user experience. Many users were reporting URLs actively and indicating their success in circumventing censorship in their countries. Version 1.3.0 of Alkasir had the following changes:

- Optimized procedures to extract data from main servers, so it has become faster to launch.
- Eliminated the possibility to modify local and remote ports to minimize conflicts and abuse.

- Eliminated the process of downloading and classifying blocked URLs to speed up opening of the browser.
- Disabled the automatic scan function to reduce load on connections.
- Applied a more complicated procedure to updating the Proxy Automatic Configuration (PAC) file for proxy configurations, which is more reliable for the internal browser but requires more work with external browsers.
- Fixed a number of other minor bugs.

Alkasir 1.4.0

The last biggest change to the program was in June 2012, when version 1.4.0 introduced further changes that altered the way the software functioned and added more sophistication to the data traffic transfer to minimize the risk of surveillance and inspection. A few months after releasing this version, the number of successful installations reached over 70,000. It is important to note that this does not necessarily indicate the number of users, because some users may opt to have multiple copies of the program and some multiple users may be using the same installation. But it is a measurement that indicated that growth continued during this time. However, the level of growth was not as rapid as that in 2010–2012 for reasons to be explained in the finding chapter of this study, as they relate to the context and developments in the area of Internet censorship. This version is the most stable with fewer reported bugs or crashes. It had the following new features and changes:

- Reduces the number of protocols used to connect to just one, reducing the use of resources and ports for connections.
- Adds an additional level of obfuscation to help reduce the possibility of detection.
- Re-enabled the ability to adjust the local port (based on popular demand).
- Re-enabled the default PAC file name (based on popular demand).
- Enhanced the scanning capability for suspected blocked websites.
- Fixed a number of other minor bugs.

Limitations, Challenges, and Potentials

There are certainly several limitations and weaknesses that Alkasir suffers from. It is useful to highlight those and be aware of them in an effort to improve transparency and understand how they may adversely impact this study. Furthermore, challenges and potentials in growth and improvement are also mentioned here to give a heads-up of what to expect in the future development of the project.

Incompatibility with non-Windows platforms

Because Alkasir is only a Windows-based application, it cannot be utilized by users who have other operating systems such as Apple Macintosh and Ubuntu. Furthermore, the software lacks a mobile app that could be used on iPhones and Android-based hand-held devices. Although this restriction did not prevent the software from reaching to a large sector of potential users given that Windows-based PCs are dominant for the time being, this reality may not last long given the tremendous growth in tablets, particularly those based on Android systems, while PCs have seen their market sales stall in recent years (Dobby, 2012).

In order to overcome this weakness, Alkasir needs to be cross-platform by having multiple versions that could be used on different operating systems as well as apps that are possible to install on tablets and mobile devices. The prospects of proceeding in that direction are challenged by the fact that Alkasir was built largely on libraries and platforms that are heavily dependent on Windows-based infrastructure such as the .NET Framework. Hence, producing a set of versions compatible with different platforms would require redesigning some parts of the software from bottom-up to the conditions of the target systems. Apart from the engineering complexity of this challenge, the manpower and financial resources required for such a task are not yet at hand.

However, as the project's use expands, particularly the area of researching Internet censorship, it is hoped that funding would be available through international research projects or through grants provided by civil society organizations with the aim of promoting freedom of expression on the Web.

Not censorship-resistant

One thing that has affected the performance of Alkasir in some countries is the persistent attempts of ISPs to censor Alkasir itself. As of October 2012, the domain Alkasir.com was found to have been filtered by some

ISPs in Iran, China, the United Arab Emirates, Syria, Yemen, Nigeria, and Colombia. This would usually not prevent those who already have Alkasir from accessing censored content, but it hinders the ability of users in those countries to access the website and download the software. To supply the software to potential users in those countries, Alkasir offers the ability to have the software sent directly by an auto responder e-mail simply by sending an e-mail to get@alkasir.com.

The situation gets more difficult in cases when ISPs target the physical IP addresses of all servers or service providers affiliated to Alkasir's proxies or use special sophisticated mechanisms that prevent Alkasir from working. So far, only Saudi Arabia has succeeded in using a powerful digital firewall to filter all available IP addresses and effectively rendered Alkasir useless (as of version 1.4.0), which is a grim reminder of the vulnerabilities of censorship circumvention solutions when confronting governments with resources. To overcome this form of censorship, Alkasir needs to invest more resources, which are not available in the time being, and find more creative ways to hop from one domain to the other and camouflage itself to not be detected by firewalls. This challenge is not unique to Alkasir, as many other circumvention tools have suffered a similar fate.

Gatekeeper role

As described earlier, Alkasir utilizes split tunneling, which requires having a previous list of URLs that were found to be blocked in a particular country and approved if and only if they met the policy of Alkasir. This meant that reported URLs that contain nudity or pornographic content, for example, will be rejected. This may be viewed by some as an attempt to restrict access by serving as a gatekeeper instead of liberation technology. Other relevant questions would be who is to decide if a particular website contains nudity or not? What if a website contained one nude image while the rest of the website had nothing of the sort? What about websites containing sexual education, anatomy, or breast-feeding advice? Those questions are quite relevant and pose a serious limitation to the claim that Alkasir is a tool to enhance freedom of expression and access to online content.

My counterargument is of three aspects. The first is that bandwidth usage in nudity/pornography is extremely high, and inviting users to use it to unblock such websites would certainly result in excessive consumption of server resource, which would then end up slowing the service for all other

users seeking news, opinion, social networking, and other informational websites. So that is a pragmatic reason to block such websites.

The second argument has to deal with social norms in the countries that are predominantly targeted by Alkasir: Arab states. In those countries, watching nudity is considered unacceptable and violates the conservative traditions and beliefs in those countries. Hence, the fact that Alkasir is a homegrown solution serving Arab users makes it offensive to allow accessing content that violates those norms. It is worth noting that Alkasir is not alone in adopting a policy that prevents the publishing of nudity. Almost all social networks either totally forbid nudity (e.g., Facebook) or allow it with the condition of registering to prevent children from accessing it (e.g., YouTube).

The third argument is the most serious, and that is the legal aspect. Although Alkasir remains a conduit and should not be held accountable for how it is used and does not retain personal information on its servers, the risk of being sued for violating certain norms or laws is there, regardless of the lawsuit being justified or not. It has happened in the past in the case of the social networking site Tagged.com, which was sued for allegedly having child pornography on its pages (Singel, 2010). Megaupload.com was also sued and even shut down for violating certain laws regarding intellectual property rights (Anderson, 2012). Hence, the risks in allowing such content are much higher than the reward.

Finally, users wishing to circumvent censorship of pornography- or nudity-containing websites can still freely access websites that allow the downloading of circumvention tools that allow such content (e.g., Tor, Hotspot Shield, and Ultrasurf). As those programs are also conduits that should not be held liable for how their users utilize them, Alkasir allowed circumventing censorship of their websites so that they could be accessible, after which they can access all websites they want easily.

Closed-source

As Alkasir is a closed-source (proprietary) software solution, its source files are not open to public scrutiny. The reason for that lies in several aspects of the code, which includes sensitive information that could be exploited—if discovered—by parties that would work hard to render the software useless in an effort to thwart its circumvention capabilities. Furthermore, if revealed, the code may be recompiled using a different name and then could be potentially used to harm users or hack the servers used by Alkasir. Opening up the code without paying special attention to po-

tential loopholes that exist in the software may also lead some to intentionally exploit those security loopholes, affecting Alkasir users' experience.

Becoming open-source has some advantages such as helping develop the software by crowdsourcing programmers and analysts to elevate its performance and reliability and hence reducing the burden on the original developer as well as pinpoint and help fix security holes and bugs. Moving to open-source may help promote transparency and build trust among users and observers alike.

Yet, although some researchers studying the advantages of open-source over closed-source software concluded that open-source software fosters creativity and indicates and fixes bugs faster, they also found that closed-source solutions were less complex and less prone to coupling errors (Paulson, Succi, & Eberlein, 2004). So there are advantages and disadvantages in closed-source solutions. One of the less technical challenges of conversion to an open-source project also means that commercial aspects of the project may be diminished, resulting in dependency on outside funding such as donations and donor support to keep it running. Converting Alkasir to an open-source solution entails substantial work to minimize the potential negative consequences from exposing the code publicly. The transition to open-source could be accomplished through incremental steps in revealing small parts and pieces of the software in a gradual process until the whole project is open-source. Human and financial resources would be required for such a process, which may actually require the redesigning of some of the core algorithms and concepts currently in use.

Insufficient localization

Although Alkasir added localization into Arabic in version 1.2.0, there has been demand to add Persian, Chinese, Vietnamese, and other languages to expand its use beyond the Arab world. Language would be quite helpful to users in countries where neither English nor Arabic is widely spoken. In such cases, users may not fully understand how to effectively utilize Alkasir's options and settings. The challenge for Alkasir lies in the lack of sufficient resources to translate interfaces, Web content, and newsletters and to moderate websites in languages that are neither Arabic nor English.

One proposed mechanism was to introduce machine translation, which has improved over the last few years but which remains quite far from perfect and could be confusing. Coming back to the earlier section, one of the potential benefits from transforming the project to open-source is the

possibility to allow volunteer developers to contribute their own translations, as is the case with several known open-software projects such as Joomla, Drupal, and LimeSurvey. Without utilizing crowdsourcing, the cost of localization could be quite high. Yet localization remains an important area for expansion. That may explain why Microsoft spends around $300 million per year to localize its products to forty-seven languages with an estimate of $300,000 for the localization of a particular product into one additional language (Collins, 2002).

Legal and personal risks

The area of censorship circumvention of Internet censorship is a form of cyber activism and entails possible risk to the developer and perhaps to the users. The legal risk varies from country to country based on the laws that may prohibit the use of encryption, for example, or that consider developing and using tools that thwart censorship illegal. Although there were no reported consequences to the users of Alkasir, there were cases where the main domain of Alkasir was blocked from access, triggering a red flag that could mean that the developer may not be welcome at least in the countries that censor the software's website itself. However, the more noticeable risk is to the functionality of the software. Iran had for a particular period deployed deep-packet inspection in an attempt to detect and thwart the usage of circumvention tools such as Alkasir, to make it difficult for users to access blocked content. Only after version 1.4.0 was released was it possible for users to use the program even under such conditions.

When it comes to risk to users, the software presents a statement that clearly indicates the terms of usage that users must agree. This makes the developer not liable for how the software is used. This was a necessary measure to protect the developer from any harm that could be caused. Although personal information—such as IP number—is not retained in the logs of Alkasir servers, assessing the risk in using the software remains very crucial for the safety of users. There are, as with the case of any Web browser or Internet tool, risks associated with browsing the Internet and hence using the internal Web browser to access a site that may contain malicious code that could in turn cause harm to the user's computer, which is also a risk to be considered and weighted against the advantage of using the software. There are other technical and nontechnical risks that could be assessed, but they require further exploration and research to assess properly.

Theoretically, the terms of use agreement should protect the developer from possible lawsuits filed against him by companies claiming that one of the users using it breached intellectual property laws by downloading copyrighted material from the Web or through BitTorrent file-sharing software. There were no such lawsuits yet, but the risk of having one filed against the software remains. On the one hand, such tools may empower people to overcome repression and promote democracy, but on the other, they could be used by cybercriminals for hacking and other cybercrimes. In an ideal world, such tools are considered neutral conduits and ought not to be responsible for how people use them, but Wolfgang's words ring true today and that is what one needs to consider moving forward.

Inaccuracies in filtering detection

The way Alkasir works in detecting if a particular URL is blocked is through the use of HTTP status response headers and by comparing the first kilobyte of text at the client's end with those at the server's end. However, occasionally, some websites intentionally block their website for various reasons (e.g., customization, localization, marketing, data gathering, and legal issues). So if Alkasir reports a particular website as filtered, it may actually be an inaccuracy.

Furthermore, dealing with sub-domains of websites constitutes yet another challenge. If a particular website's main domain is blocked, Alkasir assumes that all sub-domains would be blocked as well. This assumption may occasionally be mistaken, as some ISPs may block http://domain.com, but allow, for example, access to http://news.domain.com. To deal with such issues, it may be useful to put exceptions, learn by experience, and even contact website owners.

Resources for further Development

As Alkasir became more widely used globally, reports on bugs, issues, and problems along with feature requests and suggestions started to pour in. Many of the reported bugs were fixed while others, especially minor ones, were delayed due to the limited human and financial resources available to the project.

The software is certainly far from perfect and there is tremendous room for improvement in many aspects, such as in the area of censorship detection algorithms. This limitation restricted the developer's ability to cope with those requirements and develop the software at a faster and more desirable level. Furthermore, the resource requirements needed for the

software in terms of server capacity, bandwidth, and customer service have risen since 2010 with the increase in the level of Internet censorship, particularly in the Arab world. Hence, in order to speed up code optimization, bug fixing, the introduction of new features, and implementation of long-term strategies to broaden the global user base, investments would be needed in terms of human capital by recruiting staff and in providing more hardware resources to enhance the reliability and quality of service. Securing those resources through either fund-raising, commercial ventures, or direct investment are being considered for the long-term success of the project.

Since 2010, Alkasir has come to be among the relatively well-known circumvention tools available for all to use freely[126] but requires much more time and effort to improve further.

[126] Alkasir has earned its own Wikipedia entry accessible through this link: http://en.wikipedia.org/wiki/Alkasir and it served me will in winning me several awards, fellowships and opportunities to speak, participate and appear at several international conferences, of which some are academic institutions of strong reputation including Stanford and Harvard.

Bibliography

Al-Saqaf, W. (2008). U*nstoppable trends: the impact, role, and ideology of Yemeni news websites.* (Master's thesis). Orebro: Orebro University. Retrieved November 10, 2012, from Örebro University: http://oru.se/Extern/English/Schools/HumUS/GJC/MAGJ-student-works/Walid%20Al%20Saqaf.pdf

Anderson, N. (2012). Why the feds smashed Megaupload. *Ars Technica, Jan , 19*.

Bjorner, D. (2006). *Software Engineering 1: Abstraction and Modelling* (Vol. 1). New York, NY: Springer.

Burback, R. (1998). *Software engineering methodology: the Watersluice.* (Doctoral Dissertation). Retrieved November 16, 2013, from Stanford University: http://infolab.stanford.edu/~burback/water_sluice/sluice6.25.97/ws/watersluice.html

Collins, R. W. (2002). Software localization for Internet software, issues and methods. *Software, IEEE , 19*, 74-80.

Dern, D. P. (2011, April 19). *Joomla or Drupal: Which CMS handles security best?* Retrieved December 1, 2013, from IT World: http://www.itworld.com/security/157395/joomla-or-drupal-which-cms-handles-security-best

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The second-generation onion router. *Proceedings of the 13th USENIX Security Symposium* (pp. 303-320). San Diego, CA: USENIX Association.

Dobby, C. (2012, November 6). *As tablet market set to boom, PC and hard drive sales stalling.* Retrieved November 10, 2013, from Financial Post: http://business.financialpost.com/2012/11/06/as-tablet-market-set-to-boom-pc-hard-drive-sales-stalling-jpmorgan/

Esra'a. (2009, May 25). *The intention of Alkasir, and why it is different.* Retrieved November 5, 2013, from Mideast Youth: http://www.mideastyouth.com/2009/05/25/the-intention-of-alkasir-and-why-it-is-different/

Hartley, S. (2009, August 13). *Internet filtration in the Middle East.* Retrieved December 6, 2013, from Internet & Democracy Blog: https://blogs.law.harvard.edu/idblog/2009/08/13/oni_mena_report2009

Howe, J. (2006, June 2). *Crowdsourcing: A definition.* Retrieved December 17, 2013, from Croudsourcing (Web log): http://www.crowdsourcing.com/cs/2006/06/crowdsourcing_a.html

Murdoch, S. J., & Anderson, R. (2008). Tools and technology of Internet filtering. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access denied: The practice and policy of global Internet filtering* (pp. 57-72). Cambridge, MA: MIT Press.

ONI. (n.d.). *About filtering.* Retrieved December 20, 2013, from OpenNet Initiative: http://opennet.net/about-filtering

Paulson, J. W., Succi, G., & Eberlein, A. (2004). An empirical study of open-source and closed-source software products. *Software Engineering, IEEE Transactions on, 30*(4), 246-256.

Singel, R. (2010, October 6). *New York AG suing social network Tagged.com for child porn.* Retrieved December 10, 2013, from Wired: http://www.wired.com/threatlevel/2010/06/tagged-child-porn-ag/

W3 Schools. (2012, October 31). *OS statistics.* Retrieved October 31, 2012, from W3Schools.com: http://www.w3schools.com/browsers/browsers_os.asp

Links for Reference

- The Guardian article: http://www.guardian.co.uk/technology/2010/nov/28/internet-radicals-world-wide-web
- WIRED: http://www.wired.co.uk/news/ted/2010-09/03/ted-fellows-walid-al-saqaf
- Voice of America: http://www.voanews.com/content/opening-the-middle-east-internet-97310199/172116.html
- Untangling the Web Blog: http://untanglingtheweb.tumblr.com/post/1657710833/interview-walid-al-saqaf
- CNN report mentioning Alkasir as a tool used in the Egyptian revolution: http://edition.cnn.com/video/#/video/tech/2011/02/16/dougherty.digital.activism.cnn
- Huffington Post: http://www.huffingtonpost.com/magda-abufadil/yemeni-develops-program-t_b_209321.html
- The Guardian: http://www.guardian.co.uk/public-leaders-network/2012/apr/18/open-government-yemen-censorship
- TED: http://blog.ted.com/2011/08/05/fellows-friday-with-walid-al-saqaf/
- Gant Daily: http://gantdaily.com/2010/05/30/the-circumventor-awarded-for-arab-anti-censorship-software/
- Fast Company News Website: http://www.fastcompany.com/1731691/yemen-hero-access-blocked-sites-facebook-twitter-egypt-revolution-protests
- Alkasir's main page: https://alkasir.com , documentation: https://alkasir.com/help
- Alkasir Wikipedia entry: http://en.wikipedia.org/wiki/Alkasir
- Cship Wiki Entry: http://en.cship.org/wiki/Alkasir
- TED 2010 talk: http://www.youtube.com/watch?v=8jfAbRHANIw
- TEDxStockholmSalon 2012 talk: http://www.youtube.com/watch?v=ZlR_iO1eWgI

Appendix B: Survey on Internet Censorship of Political and Security Content

Welcome Message

Welcome to this survey and thank you for your time. Please note that this survey is expected to contribute greatly to a PhD study on Internet censorship of dissident content. Your time is highly appreciated. Kindly ensure that you answer all questions.

Your anonymity will be secured and the number of personal questions will be limited. The results of this survey will be purely used for academic purposes and not for any commercial or any other interests. This survey contains dynamic questions so the number of questions are not set in advance and may change based on your answers. But on average, it could take **20 to 30 minutes** to finish this survey.

You can any time save the survey to be filled in later by pressing the button **'Resume Later'** button found below any of the survey questions.[127]

Introductory questions

1 [Q1] What is your country of residence?

<A list of 325 countries> or Other:_____

2 [Q2] Do you run a blog or website? If not, just skip this question and move to the next. Otherwise, please indicate what website(s) you manage.

Please choose **all** that apply:

- ☐ I manage a blog
- ☐ I manage an opposition/dissident website
- ☐ I manage an independent news website
- ☐ I manage a human rights or activism website
- ☐ I manage a discussion forum with some political content
- ☐ I manage an aggregator website collecting content from other websites
- ☐ I manage a website with a different kind of content

3 [Q2.1] You said you manage a website of another type. Could you explain (e.g., entertainment website, sports website, etc.)?[128]

[127] A note about the number of question was added as there were 33 questions in the first survey and 37 questions in the second.

[128] Shown depending on the answer to Q2

4 [Q3.1] In the last 12 months, how often did you publish political* or security content?**[129]

- ○ Daily
- ○ At least once a week
- ○ At least once a month
- ○ Less than once a month
- ○ Never
- ○ No answer

** Examples of political content: News or views on the regime or government, human rights, freedom of expression, corruption, elections, minority rights, religious movements, etc.*
*** Examples of security content: Content related to war reports, inner conflicts, rebel movements, separatists, militants, resistance movements, etc.*

Questions on nontechnical censorship

5 [Q3.1.1] In the last 12 months, have you been exposed to any of the following?[130]

	Yes, it happened more than once	Yes, it happened just once	No, but I feel threatened	No, & I don't feel threatened	Don't know / Don't remember	No answer
Legal prosecution	○	○	○	○	○	○
Kidnapping or illegal detention (without court orders)	○	○	○	○	○	○
Harassment, threats, hostility, or intimidation	○	○	○	○	○	○
Torture, physical violence	○	○	○	○	○	○
Surveillance (wiretapping or other types of surveillance)	○	○	○	○	○	○
Other forms of pressure	○	○	○	○	○	○

6 [Q3.1.1.other] You said you were exposed to some other type of pressure. Could you kindly explain?[131]

[129] Question is only shown if Q2.1 was answered positively

[130] Question is only shown if the answer to Q3.1 was not 'Never' and not 'No answer'

[131] Question is only shown if Q3.1.1 was answered positively

7 [Q.3.1.1.1.why] Do you believe you were exposed to such pressure because of the political or security content you published on your website?[132]

- ○ Yes, definitely
- ○ Yes, most probably
- ○ Maybe
- ○ No, probably not
- ○ No, definitely not
- ○ I don't know
- ○ No answer

8 [Q3.1.1.1] What effects did exposure to such pressure have?[133] **Please choose** all **that apply**

- ☐ No effect
- ☐ Created an environment of fear and increased self-censorship
- ☐ Reduced the volume of political/security content
- ☐ Reduced the strength of political security content targeting the government
- ☐ Reduced the number of website visitors, contributors, or commentators
- ☐ Resulted in closing the website or suspension of activity
- ☐ Don't know / Can't assess
- ☐ No answer
- ☐ Other: _____

9 [Q3.1.1.2]Since you started feeling the threat of being exposed to such pressure, what effects did that have? [134] (Please choose **all** that apply)

- ☐ No effect
- ☐ Created an environment of fear and increased self-censorship
- ☐ Reduced the volume of dissident content
- ☐ Reduced the strength of dissident content
- ☐ Reduced the number of website visitors, contributors, or commentators
- ☐ Resulted in closing the website or suspension of activity
- ☐ Don't know / Can't assess
- ☐ No answer
- ☐ Other: _____

[132] Question is only shown depending on answers to Q3.1.1

[133] Question is only shown depending on answers to Q3.1.1

[134] Question is only shown depending on answers to Q3.1.1

Questions on technical censorship

10 [Q3.1.2] In the last 12 months, has your website or e-mail been exposed to any of the following? [135]

	Yes, it happened more than once	Yes, it happened just once	No, but I feel threatened	No, & I don't feel threatened	Don't know / Don't remember	No answer
Blocked (filtered) from access inside <country>	○	○	○	○	○	○
Exposed to an attack (e.g., DDoS, SQL injection)* making it unresponsive	○	○	○	○	○	○
Had viruses or trojans planted in it	○	○	○	○	○	○
Had its login credentials or e-mail compromised	○	○	○	○	○	○
Had its domain taken over	○	○	○	○	○	○
Other forms of technical pressure	○	○	○	○	○	○

** Those are two of the most popular attacks that either destabilize the website's response and traffic by excessive requests (DDoS) or by injecting code that could destroy databases or execute harmful code (SQL injection).*

11 [Q3.1.2.other] You said your website or e-mail was exposed to some other type of technical pressure. Kindly explain[136]

12 [Q.3.1.2.1.why] Do you believe your website was exposed to such pressure because of the political or security content published on it? [137]

- ○ Yes, definitely
- ○ Yes, most probably
- ○ Maybe
- ○ No, probably not
- ○ No, definitely not
- ○ I don't know
- ○ No answer

[135] Question is only shown depending on the answer to Q3.1

[136] Question is only shown depending on the answer to Q3.1.2

[137] Question is only shown depending on the answer to Q3.1.2

13 [Q3.1.2.1] What effects did exposure to such pressure have? [138] Please choose all that apply

- ☐ No effect
- ☐ Created an environment of fear and increased self-censorship
- ☐ Caused technical problems for the website
- ☐ Reduced the data transfer rate to/from the server
- ☐ Reduced the number of website visitors, contributors, or commentators
- ☐ Resulted in closing the website or suspension of activity
- ☐ Don't know / Can't assess
- ☐ No answer
- ☐ Other: _____

14 [Q3.1.2.2] Since you started feeling the threat of being exposed to such pressure, what effects did that have? [139] Please choose all that apply

- ☐ No effect
- ☐ Created an environment of fear and increased self-censorship
- ☐ Reduced the volume of dissident content
- ☐ Reduced the strength of dissident content
- ☐ Reduced the number of website visitors, contributors, or commentators
- ☐ Resulted in closing the website or suspension of activity
- ☐ Don't know / Can't assess
- ☐ No answer
- ☐ Other: _____

[138] Question is only shown depending on the answer to Q3.1.2

[139] Question is only shown depending on the answer to Q3.1.2

15 [Q4] Do you think that it is ever appropriate to block the following from access by users in <country>?

	Always appropriate	Mostly appropriate	Sometimes appropriate	Mostly inappropriate	Never appropriate	Don't know	No answer
Political content critical of regime (e.g. corruption, power abuse)	○	○	○	○	○	○	○
Security content targeting regime (e.g. separatism, rebellions)	○	○	○	○	○	○	○
Content offensive to religion (including prophets, etc.)	○	○	○	○	○	○	○
Content containing nudity or porn	○	○	○	○	○	○	○
Websites linked to or promoting terrorism	○	○	○	○	○	○	○
Websites offering censorship circumvention (e.g., proxies)	○	○	○	○	○	○	○
Websites offering gambling	○	○	○	○	○	○	○
Websites promoting illegal drug dealing	○	○	○	○	○	○	○
Websites promoting hate/racist speech, or ethnic conflict	○	○	○	○	○	○	○
Websites allowing illegal access to copyrighted media (e.g, music, movies, applications)	○	○	○	○	○	○	○
Websites that offer advice/instructions for hacking	○	○	○	○	○	○	○

16 [Q5] Do you know of any websites that were blocked from access to users by the government of <country>? If you do, how many of them include political or security content?

- ○ No, I am not aware of any websites blocked in <country>?
- ○ Yes, and all of them include dissident content
- ○ Yes, and most of them include dissident content
- ○ Yes, and some of them include dissident content
- ○ Yes, but only a few of them include dissident content
- ○ Yes, but none of them include dissident content
- ○ No answer

17 [Q5.1] How did the blocking in <country> of the websites that contained political or security content affect your Internet use for the following purposes/activities? [140]

	Mostly negative	Somewhat negative	Had no effect	Somewhat positive	Mostly positive	No answer
Democratic practice of expressing opinions and distributing content	○	○	○	○	○	○
Communication and social networking	○	○	○	○	○	○
Accessing information from diverse sources	○	○	○	○	○	○
Accessing educational content	○	○	○	○	○	○
Accessing entertainment content	○	○	○	○	○	○
Other miscellaneous uses	○	○	○	○	○	○

Questions about Circumvention

18 [Q5.2] Is it appropriate in your opinion for Internet users in <country> to use circumvention solutions (proxy servers or software) to bypass Internet filtering? [141]

- ○ Yes
- ○ No
- ○ I don't know
- ○ No answer

[140] Question is only shown depending on the answer to Q5

[141] Question is only shown depending on the answer to Q5

19 [Q.5.2.0] In the last 12 months, how often have you used circumvention solutions to bypass filtering in <country>? [142]

- ○ Daily
- ○ A few times a week
- ○ Less than once a week
- ○ Less than once a month
- ○ Never
- ○ No answer
- ○ Other: _____

20 [Q5.2.1] In the last 12 months, which of the following circumvention methods have you SUCCESSFULLY used to circumvent filtering in <country>?[143] **Please choose** all **that apply**

- ☐ One or more Web-based proxy (proxify.com, guardster.com, etc.)
- ☐ Ultrasurf
- ☐ Hotspot Shield
- ☐ Tor (The Onion Router)
- ☐ DynaWeb
- ☐ GPass and FirePhoenix
- ☐ JonDo
- ☐ Your-Freedom
- ☐ A VPN service (free or paid)
- ☐ I don't remember
- ☐ No answer
- ☐ Other: _____

21 [Q5.2.1.0] You indicated that you used proxy websites or servers to access blocked content. How did you learn about them? [144] **Please choose** all **that apply**

- ☐ I found them through the use of a search engine (Google, Yahoo, etc.)
- ☐ I read about them on a blog or discussion forum
- ☐ I was told by another person
- ☐ I saw them on an advertisement or e-mail
- ☐ I learned about them through traditional media (newspaper, TV, etc.)
- ☐ I found them on a specialized circumvention website (e.g., xroxy.com, proxy4free.com)
- ☐ I don't remember
- ☐ No answer
- ☐ Other: _____

[142] Question is only shown depending on the answer to Q5

[143] Question is only shown depending on the answer to Q5.2.0

[144] Question is only shown depending on the answer to Q5.2.1

22 [Q5.2.1.1] You indicated that you used at least one circumvention solution. How did you obtain the program? [145] **Please choose** all **that apply**

- ☐ I downloaded it from its official website
- ☐ I downloaded it from another website
- ☐ I got it from another person
- ☐ I received it by e-mail
- ☐ I got it through external storage (CD, USB, etc.)
- ☐ I got it through a P2P connection (e.g., through utorrent)
- ☐ Don't remember
- ☐ No answer
- ☐ Other: _____

23 [Q5.2.2] Why haven't you used any circumvention solution?[146] **Please choose** all **that apply**

- ☐ I believe it is inappropriate to access blocked content
- ☐ I don't need or want to access blocked content
- ☐ I don't trust circumvention solutions and/or their producers
- ☐ I don't believe they work reliably
- ☐ I fear consequences from the government
- ☐ I fear consequences from society, work, or family
- ☐ I don't know how to get such solutions or use them
- ☐ No answer
- ☐ Other: _____

[145] Question is only shown depending on the answer to Q5.2.1

[146] Question is only shown if Q5.2.1 had no checked options

24 [Q5.2.3] How do you assess the importance of the following factors for you to use a specific circumvention solution confidently and regularly? [147]

	Vital	Very important	Somewhat important	Of little importance	Not important	Don't know	No answer
Fast and stable connection	○	○	○	○	○	○	○
User-friendliness (e.g., does not need installation or other programs)	○	○	○	○	○	○	○
Accessibility (possible to download or get from many locations)	○	○	○	○	○	○	○
Anonymity, i.e., must always keep my identity (IP) hidden	○	○	○	○	○	○	○
Free (should not cost money to use)	○	○	○	○	○	○	○
File size (the smaller the better)	○	○	○	○	○	○	○
Capable of opening all content types (video, flash, JavaScript, etc.)	○	○	○	○	○	○	○
Cross-platform (must be usable on Mac, Windows, Unix, etc.)	○	○	○	○	○	○	○
Must not log or keep my information	○	○	○	○	○	○	○
Changes servers and other acts to be immune from being blocked	○	○	○	○	○	○	○

[147] Question is only shown depending on answers to Q5.2.1 and Q5.2.2

25 [Q5.2.4] Given that you were able to use circumvention solutions successfully, what is the best method to disseminate information about circumvention solutions and software in <country>? [148]

	Vital	Very useful	Somewhat useful	Of little use	Useless	Don't know	No answer
Internet advertising	○	○	○	○	○	○	○
CD and flash disk dissemination	○	○	○	○	○	○	○
Advertisements on traditional media (newspapers, TV, etc.)	○	○	○	○	○	○	○
Workshops, seminars	○	○	○	○	○	○	○
Discrete distribution among small & closed networks	○	○	○	○	○	○	○
Users like myself should educate others about such circumvention solutions and methods	○	○	○	○	○	○	○
Other approaches	○	○	○	○	○	○	○

26 [Q5.2.4.1] You selected 'other approaches' in the last question. Kindly explain what approaches you meant[149]

[148] Question is only shown depending on answers to Q5.2.1

[149] Question is only shown depending on answers to Q5.2.4

International and foreign actors

27 [Q6.0] Do you think it is appropriate for the international or foreign actors to take the following steps to limit/prevent Internet censorship in <censorship>?

	Always appropriate	Mostly appropriate	Sometimes appropriate	Mostly inappropriate	Never appropriate	Don't know	No answer
Pressurize governments to end censorship	○	○	○	○	○	○	○
Support activist efforts financially & morally	○	○	○	○	○	○	○
Support circumvention software developers financially & morally	○	○	○	○	○	○	○
Help victims of censorship take legal action against the government	○	○	○	○	○	○	○
Encourage reforms of laws dealing with Internet usage	○	○	○	○	○	○	○
Other methods	○	○	○	○	○	○	○

28 [Q6.1] You mentioned 'other methods' in the last question. Kindly explain what methods you meant[150]

[150] Question is only shown depending on the answers to Q6.0

Questions related to motives behind Internet censorship & impact of circumvention[151]

29 [ArabSpring1] How important are the following factors behind the decision a government to censor websites that contained political or security-related information (such as news websites, social networking websites such as Facebook, etc.)?

	Vital and primary	Important	Somewhat important	Of little importance	Not important	I don't know	No answer
Raising public awareness of corruption and malpractices of the regime	○	○	○	○	○	○	○
Helping organize rallies, protests, and sit-ins	○	○	○	○	○	○	○
Causing dissent within the army or prominent officials	○	○	○	○	○	○	○
Providing content to other traditional media (e.g., uploading directly to aljazeera.net)	○	○	○	○	○	○	○
Encouraging strikes in government circles and the economic sector (shops, etc.)	○	○	○	○	○	○	○
Other factors	○	○	○	○	○	○	○

30 [ArabSpring1_1] You said that there are other factors. Kindly indicate what they are and how important they were: [152]

[151] Questions 29-33 were only part of the second survey

[152] Question is only shown depending on answers to question ArabSpring1

31 [ArabSpring2] Do you think that Internet censorship has succeeded to limit the impact of the different factors mentioned earlier? To what degree?

	Completely rendered it useless	Substantial but not devastating	Moderate	Had little effect	Had no effect	I don't know	No answer
Raising public awareness of corruption and malpractices of the regime	○	○	○	○	○	○	○
Helping organize rallies, protests, and sit-ins	○	○	○	○	○	○	○
Causing dissent within the army or prominent officials	○	○	○	○	○	○	○
Providing content to other traditional media (e.g., uploading directly to aljazeera.net)	○	○	○	○	○	○	○
Encouraging strikes in government circles and the economic sector (shops, etc.)	○	○	○	○	○	○	○
Other factors	○	○	○	○	○	○	○

(Example: if censorship succeeded in stopping the use of websites in organizing rallies, then you should check on 'completely rendered it useless' for the first factor). However, if censorship had no effect, then you should select 'Had no effect'.

32 [ArabSpring3] How important are Internet censorship circumvention tools in confronting Internet censorship and limiting its consequences?

- ○ Vital and primary
- ○ Important
- ○ Somewhat important
- ○ Of little importance
- ○ Not important
- ○ I don't know
- ○ No answer **Make a comment on your choice here:**

33 [ArabSpring4] Do you think that circumvention tools remain important even for countries that have ended Internet censorship or never had it and why?

- ☐ Yes, because censorship could happen any time and it is important to be prepared
- ☐ Yes, because such tools are useful for anonymity and protection of privacy
- ☐ Yes, but for other reasons [use box to indicate what they are]
- ☐ No. If there is no Internet censorship, such tools are not needed
- ☐ I don't know
- ☐ No answer

General questions

34 [Q7] What is your age?

[ ]

35 [Q8] What is your gender?

- ○ Female
- ○ Male

36 [Q9] Where do you use the Internet most frequently?

- ○ Home
- ○ Work
- ○ School/Institute
- ○ Cybercafé or public venue
- ○ Mobile phone (3G, WAP,..)
- ○ Laptop with wireless access (different locations)
- ○ No answer
- ○ Other

37 [Q10] How many hours on average do you spend online each week?
Each answer must be between 0 and 168

[ ]

Completion Message

Thank you for filling the survey.
If you are not yet a member of alkasir.com, I kindly encourage you to join by signing up here. Your effort has been tremendously helpful.
If you are going to download and install alkasir, please use the below unique activation key. Ensure that you keep it safe so you could use it in the future.
It can be used to activate alkasir only once. Once activated, the key will be invalid.

Alkasir activation key:
<code>

Appendix C: Reported Websites in Arab Countries (FCL>=25%)

Algeria

1. facebook.com

Bahrain

1. alduraz.net
2. alialasghar.net
3. alsingace.katib.org
4. althaqlain.com
5. alwefaq.org
6. anhri.net
7. annaqed.com
8. answering-islam.org
9. arabchurch.com
10. arabseed.com
11. attackcensorship.com
12. awaal.net
13. bahrainblogs.org
14. bahrainonline.org
15. bahrainrights.org
16. bintjbeil.org
17. cdn2.ustream.tv
18. d.ustream.tv
19. ero-advertising.com
20. eskanaali.net
21. fadak.tv
22. faithfreedom.org
23. freecopts.net
24. haaq.org
25. jannousan.org
26. karranah.org
27. kurdtimes.com
28. ladeeni.net
29. ladeenyon.net
30. montadayat.org
31. proxyserverfreetrial.com
32. rezgar.com
33. shaheedbh.com
34. static-cdn1.ustream.tv
35. thequran.com
36. torproject.org
37. twitter.com/freebahrain
38. ultrasurf.com

39. ustream.tv
40. vob.com
41. vob.org
42. wattani.net
43. wattaninet.net
44. wattaninet.org
45. xroxy.com

Egypt

1. facebook.com
2. twitter.com

Jordan

1. arabtimes.com

Kuwait

1. skype.com
2. zwjate.com

Libya

1. akhbar-libyaonline.com
2. alarabiya.net
3. aljazeera.net
4. almanaralink.com
5. blog-video.tv
6. doubleclick.net
7. facebook.com
8. gdata.youtube.com
9. libya-alyoum.com
10. libya-watanona.com
11. libyanfsl.com
12. youtube.com

Oman

1. arabtimes.com
2. mig33.com
3. oovoo.com
4. skype.com
1. Palestine
1. iba.org.il
2. panet.co.il

Qatar

1. anchorfree.com
2. hotspotshield.com
3. proxy.org
4. torrentresource.com
5. ultrareach.com
6. yahosein.org

Saudi Arabia

1. 20w.com
2. abubaseer.bizland.com
3. acpra6.org
4. adenpress.com
5. ads.premiumaccounts.com
6. ahl-alquran.com
7. al-hora.net
8. al-majalis.com
9. al-oglaa.com
10. al-tahreer.net
11. al-yemen.org
12. alalam.ir
13. alboraq.info
14. albrrak.net
15. aldhfer.com
16. alfaloja.net
17. alhejazi.net
18. aljazeeratalk.net
19. almajalis.org
20. almedad.com
21. almenpar.com
22. almenpar.info
23. almenpar.net
24. almenpar.org
25. alqimmah.net
26. alquds.co.uk
27. alsa7a.com
28. alsaha.com
29. alsahaat.net
30. alzakera.eu
31. anhri.net
32. animenfo.com
33. animesuki.com
34. annaqed.com
35. anon.inf.tu-dresden.de
36. apps.facebook.com/texas_holdem
37. aqaed.com

38. arabic.outcampaign.org
39. arabmatchmaking.com
40. arabtimes.com
41. as-ansar.com
42. as-ansar.net
43. atahadi.com
44. avaxhome.ws/video/elearning/lynda_com_perl_5_essential_training.html
45. awamia.com
46. badawifahim.com
47. barakooda.net
48. benaa.com
49. benkerishan.blogspot.com
50. bigmir.net
51. bittorrent.am
52. blinkx.com
53. btjunkie.org
54. burathanews.com
55. ccell.mobi
56. celebfanforum.com
57. datinggold.com
58. depositphotos.com
59. dr-alahmad.com
60. ejaz.ws
61. el7ad.com
62. el7akeem.com
63. ero-advertising.com
64. fenopy.com
65. fooooo.com
66. forgottenl.hopto.org
67. freeanonymouswebproxy.com
68. fulldls.com
69. general-search.com
70. hanein.info
71. harfnews.org
72. hegabs-nekabs.blogspot.com
73. hezbullah.org
74. hi5.com
75. hotgirls4u-renat4u.blogspot.com
76. hotspot-shield.en.softonic.com
77. hotspotshield.com
78. humanf.org
79. islah.info
80. islam-qa.com
81. islam.ws
82. islamlight.net
83. islammedia.tv
84. islamqa.com
85. islamway.com

86. kickasstorrents.com
87. ladeenyon.net
88. lahdah.com
89. m3-f.com
90. m3ark.com
91. magaupload.com
92. mageupload.com
93. magicandastronomy.com
94. majahden.com
95. media.picfor.me
96. megaupload.com
97. moltaqaa.com
98. monova.org
99. montditna.com
100. myarabia04.info
101. myftp.org
102. myvnc.com
103. no-ip.com
104. no-ip.info
105. no-ip.org
106. ramadan.ws
107. rasid.com
108. rawndy.net
109. sada-najdhejaz.info
110. sadahonline.org
111. salafimujahed1.blogspot.com
112. sendspace.com
113. shamikh1.net
114. snipurl.com
115. startimes2.com
116. static.btjunkie.org
117. tagged.com
118. tawhed.ws
119. texasproxy.info
120. tf1.fr
121. thelandofsands.com
122. tinyurl.com
123. tomaar.net
124. torrenthound.com
125. torrentreactor.net
126. travian.ae
127. twhed.net
128. veoh.com
129. watan.com
130. xclicks.net
131. yahosein.org
132. ye1.org
133. youtube.com

Sudan

1. adobeflash.com
2. dailymotion.com
3. isohunt.com
4. video.google.com
5. video.search.yahoo.com

Syria

1. 12avdar.com
2. 14march.org
3. 1montreal.ca
4. 20thingsilearned.com
5. 2shared.com
6. 38.121.76.242
7. a2.twimg.com
8. aaram.net
9. aawsat.com
10. adobe.com
11. ahewar.net
12. ahewar.org
13. akhbaar.org
14. al-akhbar.com
15. alalamonline.net
16. albaladonline.com
17. alenfetah.com
18. alesbuyia.com
19. alhourriah.org
20. aljabha.org
21. aljayyash.net
22. all2chat.com
23. all4syria.info
24. almarfaa.net
25. almokhtsar.com
26. alnoor.se
27. alquds.co.uk
28. alraimedia.com
29. alsafahat.net
30. amazon.com
31. amude.com
32. amude.net
33. annahar.com
34. annidaa.org
35. anonymouse.org
36. aohrs.org
37. apps.facebook.com
38. ar.wikipedia.org
39. arabrenewal.com

40. arabrenewal.net/index.php
41. arabrenewal.org
42. arabtimes.com
43. arraee.net
44. arrouwad.com
45. arrwa.org
46. asharqalarabi.org.uk
47. badoo.com
48. baladnasms.com
49. bbc.co.uk/arabic/middleeast/2010/09/100901_israel_settlements_talks.shtml
50. bits.wikimedia.org
51. blogspot.com
52. c-we.org
53. cartoonstock.com
54. chat-host.com
55. checkedproxylists.com
56. cihrs.org
57. cool-proxy.net
58. couchsurfing.com
59. dailymotion.com
60. daliluk.com
61. damascusbureau.org
62. delicious.com
63. dl.google.com/update2/installers/chromesetup.exe
64. dostor.org
65. ebuddy.com
66. efrin.net
67. el7ad.com
68. elaph.com
69. elmahdy.org
70. facebook.com
71. facebook.oodle.com
72. fatehforums.com
73. feedproxy.com
74. feedproxy.google.com
75. forsyria.org
76. fpdownload.macromedia.com
77. free-syria.com
78. freeproxylists.com
79. fring.com
80. g-ecx.images-amazon.com
81. gdata.youtube.com
82. gemyakurda.net
83. gistcapital.com
84. godaddy.com
85. hadatha4syria.org
86. haithammalehfoundation.org
87. hdhod.com

88. hidemyass.com
89. http-tunnel.com
90. ifex.org
91. ihc.ae
92. ikhwan.net
93. ikhwanonline.com
94. ikhwansyria.com
95. iraqoftomorrow.org
96. islammemo.cc
97. islammessage.com
98. islamonline.net
99. islamtoday.net
100. islamway.com
101. israeligirl.typepad.com
102. israelweather.co.il
103. jawlan.org
104. jidar.net
105. kafasamtan.org
106. khayma.com
107. knntv.net
108. lahdah.com
109. levantnews.com
110. lightc.com
111. m.youtube.com
112. maktoobblog.com
113. menassat.com
114. meta.wikimedia.org
115. metacafe.com
116. metransparent.com
117. middleeasttransparent.com
118. mig33.com
119. mobily3araby.com
120. moheet.com
121. mokarabat.com
122. myguitarsolo.com
123. naharnet.com
124. ndshb.com
125. netlog.com
126. news.maktoob.com
127. nidaasyria.org
128. nimbuzz.com
129. nowlebanon.com
130. nvidia.com
131. ogurano.com
132. palringo.com
133. panet.co.il
134. peyamner.com
135. playerdex.com

136. pokemonworldonline.net
137. proxy-list.org
138. proxy.org
139. proxz.com
140. psfreedom.com
141. psgroove.com
142. pubsubhubbub.appspot.com
143. radiosawa.com
144. rasid.com
145. rojava.net
146. rosaonline.net
147. sandroses.com
148. saowt.com
149. secure.tagged.com
150. securepaynet.net
151. shaffaf.net
152. shrc.org
153. shril-sy.info
154. skeyesmedia.org
155. skype.com
156. sohbanet.com
157. sooryoon.net
158. soparo.com
159. sotaliraq.com
160. sourceforge.net/t7.php
161. souria.com
162. static.nimbuzz.com
163. store.ovi.com
164. syria-event.sy
165. syriahr.com
166. tagged.com
167. teachparentstech.org
168. teedoz.com
169. thisissyria.net
170. tp-link.com
171. transparentsham.com
172. ultrasurf.en.softonic.com
173. ummah.com
174. unitedna.net
175. upload.wikimedia.org
176. upsyr.com
177. wikimapia.org
178. wikimedia.org
179. xroxy.com
180. yamli.com
181. youtube.com
182. yui.yahooapis.com

Tunisia

1. advoca-cy.globalvoicesonline.org
2. albadil.org
3. alhiwar.net
4. aljazeera.net
5. anchorfree.com
6. anon.inf.tu-dresden.de
7. anonymitychecker.com
8. aqlamonline.com
9. archet.net
10. bakchich.info
11. crldht.org
12. dailymotion.com
13. debatunisie.canalblog.com
14. debatunisie2.canalblog.com
15. free-race.blogspot.com
16. fsurf.com
17. geocities.com
18. guardster.com
19. hacktivismo.com
20. hrinfo.org
21. http-tunnel.com
22. ifex.org
23. kalima-tunisie.info
24. kitab.nl
25. lesoir.be
26. metacafe.com
27. multiproxy.org
28. nawaat.org
29. netdisaster.com
30. omarkhayyam.blogsome.com
31. paldf.net/forum
32. pdpinfo.org
33. perspectivestunisiennes.net
34. proxytools.sourceforge.net
35. psiphon.ca
36. rrdb.org
37. rsf.fr
38. samibenabdallah.rsfblog.org
39. stupidcensorship.com
40. thepiratebay.org
41. tunezine.com
42. tunisalwasat.com
43. tunisie.over-blog.org
44. tunisnews.net
45. ultrareach.com
46. wat.tv

47. youtube.com
48. zensur.freerk.com

UAE

1. 1000zoom.com/free-download-skybe/index.html
2. accesssure3.com
3. actionvoip.com
4. ads.whaleads.com
5. anchorfree.net
6. anonymous-proxies.org
7. arabtimes.com
8. arbcinema.com
9. arenabg.com
10. bestproxysites.com
11. bodycontact.com
12. btjunkie.org
13. clicktorrent.info
14. cyberghostvpn.com
15. daveproxy.co.uk
16. el7ad.com
17. extratorrent.com
18. facebook.com/pages/-/198806935606
19. ficall.com
20. freecopts.net
21. freetubetv.net
22. globe7.com
23. hassan2007.nireblog.com
24. hotspotshield.com
25. megauploadsearch.net
26. nimbuzz.com
27. oovoo.com
28. orkut.com
29. poivy.com
30. pop6.com
31. powertracker.org
32. proxy-heaven.blogspot.com
33. proxy-list.org
34. proxy4free.com
35. proxychatroom.com
36. proxylist.net
37. rpt.anchorfree.net
38. samair.ru
39. skype.com
40. smslisto.com
41. static.nimbuzz.com
42. static1.orkut.com
43. sumotorrent.com

44. surfbouncer.com
45. topfreeproxy.com
46. uaeprison.com
47. xroxy.com
48. yourfilehost.com

Yemen

1. 7be.com
2. abyanboard.com
3. aden-na.com
4. aden-tv.net
5. adengulf.net
6. adennews.net
7. adenpress.com
8. adenpress.net
9. adentimes.net
10. al-ayyam.info
11. al-majalis.com
12. al-masdar.com
13. al-tahreer.net
14. al-teef.com
15. al-teef.net
16. al-yemen.org
17. alamalbank.com
18. albadell.net
19. algnoubal-hur.com
20. alhadath-yemen.net
21. alkasir.com
22. almasdaronline.com
23. almenpar.com
24. almenpar.info
25. amaan-fi-amran.info
26. armiesofliberation.com
27. banners.getiton.com
28. cdns.xtube.com
29. dhal3.com
30. dns4me.com
31. forum.sh3bwah.maktoob.com
32. gnoub.net
33. gulfofaden.net
34. hdrmut.net
35. hnto.org
36. marebpress.net
37. muharrer.net
38. nashwannews.com
39. newomma.net
40. oovoo.com

41. pagewash.com
42. pfingo.com
43. proxize.me
44. sadaaden.com
45. sadaaden.net
46. sadahonline.com
47. sadahonline.org
48. sattonet.com
49. shabwahpress.maktoobblog.com
50. shabwahpress.net
51. shamsannews.com
52. siyasapress.net
53. soutalgnoub.com
54. tajaden.org
55. traidnt.net
56. ultrareach.com
57. watan.com
58. wikimapia.org
59. xtendmedia.com
60. yaatc.net
61. ye1.org
62. ye22.com
63. yemen-results.com
64. yemenat.net
65. yemenhurr.net
66. yemenn.com
67. yemenna.com
68. yemenportal.net
69. yemenportal.org
70. your-freedom.net
71. z5x.net

Publications *in the series*
Örebro Studies in Media and Communication

1. Eriksson, Göran. *Den televiserade politiken – Studier av debatt- och nyhetsjournalistik*. 2002
2. Eriksson, Mats. *Från ingenjörskonst till informatörskonst. Studier av PR och riskkommunikation*. 2003
3. Olausson, Ulrika. *Medborgarskap och globalisering. Den diskursiva konstruktionen av politisk identitet*. 2005
4. Berglez, Peter. *The Materiality of Media Discourse. On Capitalism and Journalistic Modes of Writing*. 2006
5. Platen von, Sara. *Intern kommunikation och meningsskapande vid strategisk organisationsförändring. En studie av Sveriges Television*. 2006
6. Buskqvist, Ulf. *Medborgarnas röster. Studier av Internet som politisk offentlighet*. 2008
7. Norén, Mikael. *Designing for Democracy. End-user Participation in the Construction of Political ICTs*. 2008
8. Östman, Johan. *Journalism at the Borders. The Constitution of Nationalist Closure in News Decoding*. 2009
9. Fogde, Marinette. *The Work of Job Seeking. Studies on career advice for white-collar workers*. 2009
10. Rasmussen, Joel. *Safety in the Making. Studies on the Discursive Construction of Risk and Safety in the Chemical Industry*. 2010
11. Nilsson, Johan. *Hollywood Subversion. American Film Satire in the 1990s*. 2011
12. El Gody, Ahmed. *Journalism in a Network. The Role of ICTs in Egyptian Newsrooms*. 2012
13. Jakobsson, Peter. *Öppenhetsindustrin*. 2012
14. Kaun, Anne. *Civic Experiences and Public Connection. Media and Young People in Estonia*. 2012
15. Andersson, Linus. *Alternativ television. Former av kritik i konstnärlig TV-produktion*. 2012

16. Stiernstedt, Fredrik. *Från radiofabrik till mediehus. Medieproduktion och medieförändring på MTG-radio.* 2013

17. Al-Saqaf, Walid. *Breaking Digital Firewalls. Analyzing Internet Censorship and Circumvention in the Arab World.* 2014