COGITATIO

Media and Communication (ISSN: 2183-2439)
2016, Volume 4, Issue 1, Pages 39-50
Doi: 10.17645/mac.v4i1.357

Article

Internet Censorship Circumvention Tools: Escaping the Control of the Syrian Regime

Walid Al-Saqaf

Department of Media Studies, Örebro University, 701 82 Örebro, Sweden; E-Mails: walid.al-saqaf@oru.se, walid@al-saqaf.se

Submitted: 3 June 2015 | Accepted: 3 November 2015 | Published: 18 February 2016

Abstract
Studies have shown that authoritarian regimes tend to censor the media to limit potential threats to the status quo. While such censorship practices were traditionally aimed at broadcast and print media, the emergence of the Internet and social media in particular, prompted some authoritarian regimes, such as the Assad regime in Syria, to try and exert a similar level of censorship on the Internet as well. During the Arab Spring, the Syrian regime blocked hundreds of websites that provided social networking, news, and other services. Taking Syria as a case study, this paper examines whether Internet censorship succeeded in preventing Internet users from reaching censored online content during 2010–2012. By analyzing the use of Alkasir, a censorship circumvention tool created by the author, the paper provides empirical evidence demonstrating that users were in fact able to bypass censorship and access blocked websites. The findings demonstrate that censorship circumvention tools constituted a threat to the information control systems of authoritarian regimes, highlighting the potential of such tools to promote online freedom of expression in countries where Internet censorship is prevalent.

Keywords
Alkasir; Arab Spring; conflict; democracy; freedom of expression; Internet censorship circumvention; Syria

Issue
This article is part of the issue "Peacebuilding in the Age of New Media", edited by Vladimir Bratic (Hollins University, USA).

1. Introduction

When coining the term *media studies 2.0*, media scholar William Merrin argued that the rapid growth of the Internet for media content creation and distribution by Internet users had led to a paradigm shift, which created an urgent need for the discipline to upgrade its ability to deal with digital media in order to remain relevant (Merrin, 2009, p. 9). While several social science scholars have studied censorship practices of broadcast, print and other traditional media by authoritarian Arab regimes (e.g., Al-Obaidi, 2007; Flew, 1998; Hardt, 2000; Hinnebusch, 2006; Lee, 2007; Mellor, Rinnawi, & Dajani, 2011; Rugh, 2004), only a few scholars attempted to study how censorship practices were carried out against digital media (e.g., Al-Saqaf, 2014; Deibert, 2013; Gohdes, 2014; Howard, 2010). This paper builds upon the latter group of studies but with a specific focus on Internet censorship and circumvention in Syria around the period that immediately preceded and followed the Arab Spring[1].

Syria was found to be a suitable case study given that it has a well-documented and long-standing history of traditional media censorship (Freedom House, 2010) that was followed by a wave of Internet censorship practices in 2010 and beyond (Al-Saqaf, 2014). This study empirically analyzes patterns of Internet censorship in the form of website filtering in Syria in the two year period stretching from October 2010 to October 2012 and goes one step further to assess whether such censorship was able to restrict access to those censored websites.

The subject of this paper is relevant to social scientists in general and media scholars in particular given

[1] The Arab Spring refers to the anti-government uprising that started in Tunisia in December 2010 and later expanded to other Arab countries including Egypt, Syria, Bahrain, Yemen and Libya.

the well-documented use of social media by regular citizens to become producers of media content instead of mere consumers (Gauntlett, 2007; Huang, 2011; Howard, Agarwal & Hussain, 2011; Shirky, 2011; Stepanova, 2011). By 2014, over 2.8 billion people representing about 39% of the world's population had access to the Internet (Internet World Stats, 2014). As Internet connectivity continues to become more commonly available on mobile phones, the number of global Internet users was expected to have reached over 3.4 billion by the end of 2015, bringing roughly 45% of the world's population online (Cisco, 2011). According to a prediction by Google CEO Eric Schmidt, the whole world will be connected to the Internet by 2020 (Gross, 2013). Furthermore, a growing number of countries have adopted laws considering Internet access a human right (Ayish, 2010). In 2014, Brazil for example, adopted Marco Civil—also called the "Constitution for the Internet,"—which aims to use the Internet in ways that strengthen freedom of expression, individual privacy, and respect for human rights (Kerr, 2014).

The research question this paper aims to address is: How successful were censorship practices on the Internet in Syria during 2010–2012 and what does that mean for the future of information control by the Syrian regime? To answer this question, a hypothesis is presented arguing that the structure of the Internet as a decentralized network makes it possible to circumvent censorship easily. And with the expected rise in Internet use, this threatens the systems of information control that the Syrian and other authoritarian regimes have been using for generations.

The methodology this paper uses relies on analyzing data generated from Alkasir[2], a software solution downloadable for free from the internet that the author created in 2009, which aims to help map and circumvent website censorship around the world (Al-Saqaf, 2014, p. 317). The data collected was then analyzed to measure the level of success that users in Syria had in bypassing Internet censorship and accessing websites blocked by the regime. In light of its theoretical framework and findings, the study then concludes with a forward-looking assessment as to what this means for the field of media studies in regard to the information control measures taken by authoritarian states.

2. Theoretical Framework

2.1. Controlling Information as a Trait of Authoritarianism

Censorship is a practice dating back to ancient Greece when Socrates was executed for a message deemed to threaten the moral fabric of society (Stone, 1989). Over time, censorship evolved to be the examination of books, periodicals, broadcast media, film, plays, and other media for the purpose of altering or suppressing parts found to be objectionable or offensive based on cultural, religious, political and other factors (Senat, 2011).

Authoritarian regimes have for generations adopted various forms of censorship to depoliticize the population and prevent the questioning of their legitimacy (Linz, 1964, p. 304). Such regimes hope to be viewed as worthy to rule and are even willing to be seen as a "necessary evil" needed to address societal problems (Casper, 1995, p. 43). When authoritarian regimes do call for public participation in politics through election campaigns, rallies, or referenda, they tend to control the message to the public by suppressing anti-regime rhetoric and dissuading political opponents from forming strong coalitions (Casper, 1995, p. 45). This implies that oppressive practices ranging from political persecution to media control and censorship are therefore frequent traits associated with authoritarianism and are meant to prevent the opposition from reaching a critical mass and consequently, threatening the status quo. By definition, authoritarian regimes enforce strict obedience by the media to their political authority (Ostini & Ostini, 2002). They do so by exercising restrictions on the types of content published or broadcast to ensure that the traditional media's role is confined to maintaining the existing power structures.

With the advent of the Internet however, the role of traditional media started to weaken due to the ability of regular Internet users to become content producers by utilizing decentralized and distributed networks such as social media (Shirky, 2011). This feature of the Internet was quite visible during the Arab Spring when activists used social media to mobilize anti-government campaigns and organize mass rallies that helped trigger the downfall of two Arab dictators, Zine El Abidine Ben Ali of Tunisia and Hosni Mubarak of Egypt (Huang, 2011; Stepanova, 2011). This transformation has also given social media a strong complementary role to traditional media as demonstrated by Al Jazeera's use of social media content to supplement its own reporting during the Arab Spring (Duffy, 2011).

2.2. The Rise of Internet Censorship

As the Internet became more popular and widely used to mobilize protest and dissent, authoritarian regimes evolved their media control practices to include Internet censorship, which can be understood as the practice of "suppressing, limiting, or deleting objectionable or any other kind of speech" (Deibert, 2013, p. 139). Internet censorship constitutes any act or system that suppresses, limits access to, or deletes any other kind of information published or communicated on the Internet (Al-Saqaf, 2014, p. 91).

Well before the Arab Spring, some Muslim coun-

[2] The word 'Alkasir' is a transliteration from Arabic, which means 'the breaker' or 'the circumventor'.

tries had already started practicing Internet censorship by prosecuting bloggers and cyber activists and by blocking websites (Howard, 2010, p. 175). In the case of Syria, by censoring social media websites such as Facebook and Blogger, the regime had inadvertently further encouraged the use of such platforms for political dissent (Howard, 2010, p. 164). Following the Arab Spring, motives behind Internet censorship by authoritarian regimes in the Arab world appeared to stem from their desire to prevent dissenting voices from reaching the public and hence, stifling political opposition and protecting the status quo (Al-Saqaf, 2014). Those motives are aligned with those that made authoritarian regimes censor dissenting voices in traditional broadcast and print media.

Technically speaking, implementing Internet censorship often involves the use of filtering software to block access to websites in a particular network or environment (Hersberger, 2004, p. 265). Such filtering can target an individual's private computer, or can occur on a wider intranet level where the responsible network administrator or Internet service provider (ISP) sets up a digital firewall to prevent access to certain websites that include particular keywords or meet some other matching criteria. If a user tries to access any of those blocked websites, he/she would normally get an 'Access Denied' page or some other notice (Hersberger, 2004*, p. 266*). Internet censorship of a website can happen on a national level when all ISPs in the country in question block the same website. While independent filtering mechanisms for some countries are based on the terms of usage and rules that each ISP needs to enforce, e.g., blocking pornography, gambling, etc., studies have found that national Internet censorship is often devised to suppress the dissemination of dissident messages (Al-Saqaf, 2014; Bennett, Grothoff, Horozov, & Lindgren, 2003, p. 1).

The lion's share of research regarding Internet censorship has so far focused on China, where the regime maintains what is arguably the world's most sophisticated and comprehensive national Internet censorship system. Often referred to as "The Great Firewall of China", the Chinese Internet censorship system relies on a diverse set of censorship strategies ranging from website filtering (Deibert, Palfrey, Rohozinski, & Zittrain, 2008) to internal blog content monitoring and blocking (MacKinnon, 2008) and often includes legal measures that lead to the prosecution of bloggers using existing laws (Liang & Lu, 2010, pp. 116-117).

In the Arab world, website filtering is but one of several forms of censorship, which include prosecution, threats, physical intimidation, and surveillance (Zarwan, 2005). Murdoch and Anderson (2008, p. 65) detailed nine mechanisms of Internet censorship ranging from technical website filtering to domain deregistration and attacks on websites. Cyber laws can be considered a form of Internet censorship if they curtail freedom of access or use of the Internet as demonstrated by Iraq, whose proposed cyber laws were seen as a means of targeting journalists, whistleblowers, and activists (Sutton, 2012). Similarly, the UAE's decrees on cyber crime led to restrictions on the ability of citizens to criticize the state on the Internet and promoted self-censorship (Gradstein, 2012).

2.3. The Internet and Liberation Technology

The debate regarding the positive and negative uses of the Internet as a technology was invoked by Thierer (2010), who contrasted the views of "Internet optimists" with those of "Internet pessimists". Internet optimists include researchers such as Negroponte (1996), Surowiecki (2005), and Shirky (2011), who argue that the Internet contributes positively to freedom of expression, innovation, participation, anonymous communication, and empowerment. Internet pessimists such as Postman (1993), Keen (2007), and Morozov (2011) however, view the Internet as a technology that could be misused and abused. Some Internet pessimists argue that the Internet could debase culture, lead to the lack of accountability or serve as a tool used by governments to target activists or journalists. These contrasting views reflect what I see as the *neutral* and *conduit* nature of the Internet, which itself cannot be good or bad, but rather, it can be used for good causes as well as bad ones.

On the one hand, the Internet has the potential to support economic development and this aspect could be a strong incentive for its embrace by authoritarian states (Shirky, 2011, p. 37). But on the other hand, it can also be used to stifle human rights not only in authoritarian states, but also in advanced democracies as demonstrated by the mass surveillance practices carried out covertly by the National Security Agency (NSA) of the United States as revealed in 2013 by former NSA contractor Edward Snowden, who leaked around 200,000 classified documents detailing the a clandestine mass surveillance program with the government code name PRISM (Anton, 2013). This is particularly troublesome given that PRISM used private communications on Google, Facebook, and other major platforms in its surveillance practices.

Authoritarian regimes did also use the Internet against activists as highlighted by Morozov (2011), who argued that cyber activists could be targeted using various mechanisms, for example by having a social media network decide to reveal their identity to authoritarian states, or causing them to be exiled due to affiliation with US-sponsored training. This would be in addition to the exposure of Internet users to surveillance, trolling, censorship, and even prosecution for downloading some types of censorship circumvention software (Morozov, 2011).

In relation to the use of the Internet by authoritari-

an regimes against activists, a study by Gohdes (2014) found that the Syrian regime remained in control of access to some social media through censorship—including network disruptions—and surveillance. In her study, the author illustrates the use of surveillance as a means to monitor the flow of information between activists on the ground in order to track names, locations and other information for 'targeted violence' (Gohdes, 2014, p. 3). This illustrates the dangers of using social media in times of conflict, which highlights the dark side of the Internet. However, it was noticeable that Gohdes did not refer in her study to censorship circumvention tools, which could have partially contributed to addressing the censorship problem.

The two sides reflect an ongoing and thorny debate that will probably continue for a long time. A more constructive approach to this debate however, could be the one taken by Diamond (2012), 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, 2012, p. 4). While Diamond argued that liberation technology has the potential to be used for the good of society, he did not rule out the possibility that it could also be abused. Advocates of liberation technology do acknowledge that like any other neutral tool, the Internet could have empowering and disempowering effects depending on context and other factors. In this paper, the focus is on the positive aspects of liberation technology while acknowledging that there are also some negative aspects.

2.4. Censorship Circumvention Tools as a Liberation Technology

In this paper, Internet censorship circumvention tools are considered to be a liberation technology because they expand political and social rights of citizens by allowing them to access websites containing dissident content that authoritarian regimes wish to hide from the public. Those tools work because they exploit one of the most fundamental characteristics of the Internet, i.e., decentralization. After all, when the Internet was born in 1969 at the US Advanced Research Projects Agency Network (ARPANET), it was built as a communication network that could survive a major attack. Because it is not centrally controlled, its solid and resilient distributed architecture allows it to operate even if large parts of the underlying networks are destroyed (Brand, 2001).

Censorship circumvention tools rely on proxies, which are analogous to intermediary agents that serve as a bridge between two communicating parties. When a recipient and a sender of information are prevented from direct communication, they can use a middleman who is not forbidden from individually interacting with either of them. In case the middleman loses access to either party due to censorship or other reasons, an alternative middleman can be used to maintain the communication. The middleman is a metaphor for a proxy server that is able to reach both the Internet user and the blocked website. For example, for a person in Beijing to access http://facebook.com, which—as of the time this article was written—is blocked in China, a circumvention tool could be used to reroute the traffic to that website via a proxy server based in the United States, for example, and send the data in an encrypted form back to the user. One common feature of circumvention tools is that they all rely on proxy servers to overcome censorship (Palfrey, Roberts, & Zuckerman, 2011, p. 5).

Theoretically, any server that is able to reach the user and target a website simultaneously could serve as a proxy. This entails that a regime with a strong enough determination to block access to a particular website would have to block access to all potential proxy servers, which is virtually impossible without blocking significant parts of the whole Internet. Such a scenario, however, is highly unlikely because the global expansion of the Internet made it indispensable for communication, business, government, transportation, and various other vital public and private uses (Hoffman, Novak, & Venkatesh, 2004; Stepanova, 2011, p. 2; Varnelis, 2012).

That being said, at least one authoritarian regime had reportedly shut down national access to the Internet as demonstrated by the case of Egypt in January 2011 (Cowie, 2011). Initially, the regime reportedly ordered ISPs to block access to Facebook and Twitter (Schonfeld, 2011). But as the availability of censorship circumvention tools and methods rendered website filtering ineffective, the regime took the radical step of shutting down access to the Internet as a whole from January 27 to February 2 (Cowie, 2011). Yet that step appears to have backfired as it led to even more protesters, some of whom wanted to be informed about developments directly given that they were no longer able to access information online (Khamis & Vaughn, 2011, pp. 15-16). It was quite evident that the decision to completely block citizens' access to the Internet did not prevent the planned protest on Friday January 28. When Egypt was brought back online on February 2, the protests had already reached unprecedented sizes, eventually leading to the resignation of Egyptian president Hosni Mubarak on February 11 (McGreal & Shenker, 2011).

The Egyptian example presents a clear dilemma for authoritarian states trying to censor the Internet. On the one hand, they cannot prevent users from using censorship circumvention tools to access blocked websites. Yet on the other, they can't afford to shut down the Internet altogether because doing so would negatively affect the economy and cripple government agencies (Howard et al., 2011, p. 217).

3. The Syrian Context

3.1. Traits of an Authoritarian Baathist Regime

When Bashar Assad inherited power from his deceased father Hafez Assad in 2000, he also took charge of the Arab Socialist Ba'ath Party, which had ruled the country with an iron fist since 1963 (Pipes, 1989). Just after the Arab Spring started however, the media reported grave human rights violations and widespread and systematic abuses across the country (Black, 2012). As is the case with authoritarian regimes, Assad's legitimacy to rule was not based on a democratic process and was often questioned by various opposition entities and dissidents, most of which had to operate in exile due to the Syrian regime's tendency to assassinate opposition figures (Zahler, 2009, p. 66).

The Syrian constitution does refer in a few clauses to citizens' right to individual freedom (Heller, 1974). However, restrictions on freedom of expression through different means including acts of censorship remained the norm and intensified since 2001, when the Press Law was enacted, giving authorities the right to deny and revoke publishing licenses of newspapers as well as enforce blatant press censorship (Freedom House, 2010). Assaults on journalists and banning of newspapers coming from certain countries or containing certain types of content were carried out on the grounds of protecting Syrian national security. The Press Law imposed a hefty fine of up to a million Syrian pounds, which was valued around USD 20,000 in 2010, and granted the judiciary the power to give jail terms that range from one to three years (Freedom House, 2010). Based on that law, any form of speech, whether written, spoken, or electronic, could be considered punishable if deemed a threat to national sovereignty or security or if it is thought to offend public morality. Among the most strictly censored messages are those that advocate autonomy or self-rule for Kurds, who are prohibited from importing Kurdish-language publications (Ziadeh, 2009).

Dissidents in Syria are usually unable to challenge the regime through traditional media because publishing houses and media outlets are either owned or influenced by the state and are mobilized in active support for the regime (Rugh, 2004, p. 56). Security agencies work with total impunity and operate under the direct oversight of the presidential office and are known for committing acts of torture to extract information and admissions from suspects or their relatives (Freedom House, 2010).

The systematic repressive practices by the Syrian regime over the years have weakened the internal opposition and resulted in a thriving exiled dissident movement, which is composed of several competing factions including moderate Sunnis, Kurds, Islamists, liberals, and others (Lund, 2012). The regime's grip on the media and the economy was further enhanced through notably strong ties with Iran and Russia, which are two powers with a strong stake in the region (Landis & Pace, 2007).

3.2. Internet Access and Censorship in Syria

The Internet was cautiously introduced to Syria in 1997 when a very limited number of state institutions were connected and operated in a highly restrictive and security-driven setting (Goldstein, 1999, pp. 55-56). When Bashar Assad became president in 2000, he expanded Internet access, which grew from 30,000 users in 2000 to over five million in 2012, representing a penetration ratio of 22.5% (Internet World Stats, 2013). The rapid growth of the Internet was used by the regime to expand its information propaganda to the masses and attack dissidents in a virtual cyberwar (Watson, 2011). Despite this growth, Syria's online environment remained highly controlled and regulated by the Ministry of Telecommunications and Technology through the Syrian Telecommunications Establishment (ONI, 2009). Investments by the regime in the telecommunication infrastructure were coupled with a monopoly of the ISP sector led by SyriaTel, a wireless 3G GSM and Internet operator owned by the first cousin of President Assad, Rami Makhlouf (US Department of Treasury, 2008). Nepotism and favoritism were practiced widely in the country, signaling a state of corruption and inefficiency (Schmidt, 2006).

As Internet usage grew in Syria, so did restrictions on online freedoms as manifested by the pervasive Internet filtering practiced by the state, which blocked numerous dissident websites as well as major social media platforms such as Facebook and YouTube (ONI, 2009). The international media freedom monitoring watchdog Reporters without Borders (RSF) named Syria in 2010 as one of the "enemies of the Internet" due to its repressive practices restricting freedom of expression on the Internet (RSF, 2010). Since the uprisings started in the beginning of 2011, at least ten citizen journalists and online activists were reportedly killed by the end of the year, after which the number spiked fivefold to 49 deaths in 2012 (RSF, 2013). The Syrian regime started in 2011 to ban traditional journalists from going into the country for reporting. This resulted in a high number of casualties among citizen journalists, who became a major source of news (Arnold, 2012). Furthermore, the lack of sufficient experience in safe communication, encryption techniques and other digital protections made online journalists vulnerable to being identified, tracked, and targeted (Galperin, 2012).

3.3. From a Potential Revolution to an All-Out Civil War

Inspired by the uprisings in Tunisia and Egypt, Syrians in the city of Dara'a took to the streets in big numbers in March 2011 demanding more rights and to protest the arrest of schoolboys for writing political graffiti call-

ing for an end to the Assad regime (Macleod, 2011). The protests were faced with a violent security crackdown, which resulted in more and bigger protests to a degree that prompted the regime to cut taxes and raise state salaries. Soon after, Assad attempted to deal with public anger by ending the state of emergency that was in place since 1963 and issued a decree to dissolve the long-feared state security court and to regulate the right to peaceful protest (Oweis, 2011). Despite these measures, violence intensified and opposition groups turned from peaceful protests to armed rebellion, supported by defections of military and government personnel and followed by mounting international pressure (Myers, 2011). When the opposition Free Syrian Army was formed in July 2011, it helped transform the popular peaceful uprisings to a militant opposition that led to an all-out civil war (Karam & Kennedy, 2011).

By 2013, the UN reported a death toll exceeding 60,000 with over half a million internally displaced (Hubbard & Jordans, 2013). Additionally, hundreds of thousands of Syrian refugees fled across the borders to Turkey, Jordan, and Lebanon, resulting in over one million refugees (Sweis, 2013). The types and magnitude of the crimes committed by the Assad regime since 2011 made it a candidate for an international tribunal for committing war crimes and crimes against humanity, which discouraged the regime from handing over power to a transitional government (Walt, 2012).

4. Discussion

4.1. Methodology

This study uses data collected through Alkasir website censorship mapping and circumvention tool to quantify website censorship in Syria during October 2010–October 2012. I originally created the software in 2009 as a means to circumvent censorship of my own news aggregator website yemenportal.net, which was blocked in 2008 by the Yemeni authorities citing concerns that it may have posed "national security" risks because it allowed dissident content to be viewed on it (Al-Saqaf, 2014, p. 326). Alkasir started out as a Microsoft Windows application that enabled Internet users to report blocked websites and access them freely afterwards using a secure and encrypted tunnel to a proxy server located in the United States. By October 2012 however, Alkasir had been installed over 72,000 times and was downloaded in more than a hundred countries around the world.

The sample used for this paper is confined to the data generated by users inside Syria. Alkasir's proxy is a US-based server, which fetches data from blocked websites requested by the users and sends those websites' content to the users in an encrypted format that the ISP cannot read. This renders the censor role of the ISP useless because all it sees is garbled encrypted traffic exchanged with a destination that is not meant to be censored, i.e., Alkasir's proxy server[3].

The software was used to identify blocked websites in Syria by allowing users to report them first before being able to access them through a special proxy server. Every user running Alkasir had a graphical user interface with clearly marked buttons that were used to report one or more websites. There were over twenty thousand instances of Alkasir being voluntarily installed and used by users using different ISPs inside Syria during October 2010−October 2012. This allowed the detection of national website censorship to a highly reliable degree. The technical data was stored securely in a MySQL database on a US-based server that also hosted Alkasir's official website (https://alkasir.com). Raw MySQL database content was later manually converted to datasets and imported to a computer running IBM SPSS[4].

For the study to identify which websites were filtered nationally, it was necessary to have multiple reports coming from users in different parts of the country using different ISPs. Otherwise, a website filtered by a single ISP may be mistakenly interpreted as being censored nationally. A public library or cyber cafe, for example, could block facebook.com due to the terms of service. If a student attempts to access facebook.com they can still report the website and access it through Alkasir, which adds the ISP to a database containing information about censored websites in Syria. If someone else using another ISP in another part of the country also reports the website blocked, that ISP is added to the database as well. The more ISPs found to block a particular website, the more likely that it is blocked nationally. This study considers that websites reported to be blocked by a threshold of more than 15 ISPs to be blocked nation-wide.

One of the limitations of Alkasir is its inability to know precisely when a website was unblocked. This is because it relies on the users' active updates by reporting websites regularly. It is rarely the case that users report a particular website regularly to keep its status up-to-date. This meant that in order for a website to be removed from the list of nationally censored websites, manual intervention was needed to directly remove the website from the database containing the list of blocked websites in a specific country. This procedure was not used in the case of Syria given the high probability that a website that was blocked before would be blocked again in the future.

Alkasir has an internal web browser, which allows it to collect metadata on the frequency of access to various blocked websites. Every attempt to access a blocked website via the browser increments the total

[3] A more thorough description of how Alkasir works can be found in an earlier study (Al-Saqaf, 2014)

[4] IBM SPSS is software that many social science researchers use for statistical analysis.

number of page views of the website. The study was able to identify the total number of views of blocked content without having to identify who accessed them because no personal information that could be used to identify users was saved on the server due to privacy considerations. The quantitative data collected over the period of the study includes data about the reported websites, the countries and ISPs that blocked them, the number of times Alkasir was accessed, and the number of page views of each website. The data was then analyzed using SPSS to identify patterns that answered the study's research questions.

4.2. Findings

When studying patterns of Alkasir usage in Syria, it was found that the number of successful connections to the proxy server increased from 13,826 in October 2010 to 958,548 in October 2012, which is a seventy-fold rise. In order to understand whether this increase was triggered by any developments on the ground in Syria, a deeper analysis was carried out. The analysis revealed a noticeable sharp rise at the peak of the Tunisian and Egyptian uprisings in January 2011 in terms of the number of censored websites reported as shown in Figure 1. After a relative period of calm, a renewed wave of reports was witnessed in July 2011, which is when a heavy wave of defections from the Syrian army took place, later leading to the creation of the Free Syrian Army (AFP, 2011). After another period of limited website censorship reporting activity, a spike emerged in mid-2012. The highest number of websites reported censored was in July 2012 when 677 unique Websites were reported 3,207 times in total. By October 2012, the number of page views of blocked websites in Syria through the internal browser reached over 4.4 million while the number of installations reached 22,415.

By more closely examining the month of July 2012, one can see that there were two spikes on July 15 and 26 as shown in Figure 2. The first spike on Sunday July 15 coincided with the Free Syrian Army's announcement to launch the operations Damascus Volcano and Syrian Earthquake aimed at liberating the capital Damascus (Karouny, 2012). The other spike occurred on Thursday July 26 when strong signs of an imminent battle in Aleppo emerged a day after the Free Syrian Army took control of some of its districts (Weaver & Whitaker, 2012).

The empirical data shows that as a censorship circumvention tool, Alkasir was indeed used effectively to bypass government-imposed censorship at a very delicate and important period in the history of Syria. This indicates that the Syrian regime strived to control the flow of information online using filtering software. However, the decentralized and open design of the Internet allowed users to overcome the challenge of censorship to remain informed.

When looking into the specific censored online content that was accessed using Alkasir, the results revealed that online resources such as social media and media sharing websites received the highest attention. As the pie chart in Figure 3 shows, social media constituted around 92% of all visits to blocked websites during the period represented in this paper. Within the social media group, the dominant website was Facebook with around 98% of the visits followed by other less known social media websites. The Syrian regime's censoring of Facebook could be attributable to its perceived threat as a means to mobilize rallies and protests through social media, leading to the overthrow of the Tunisian and Egyptian presidents.

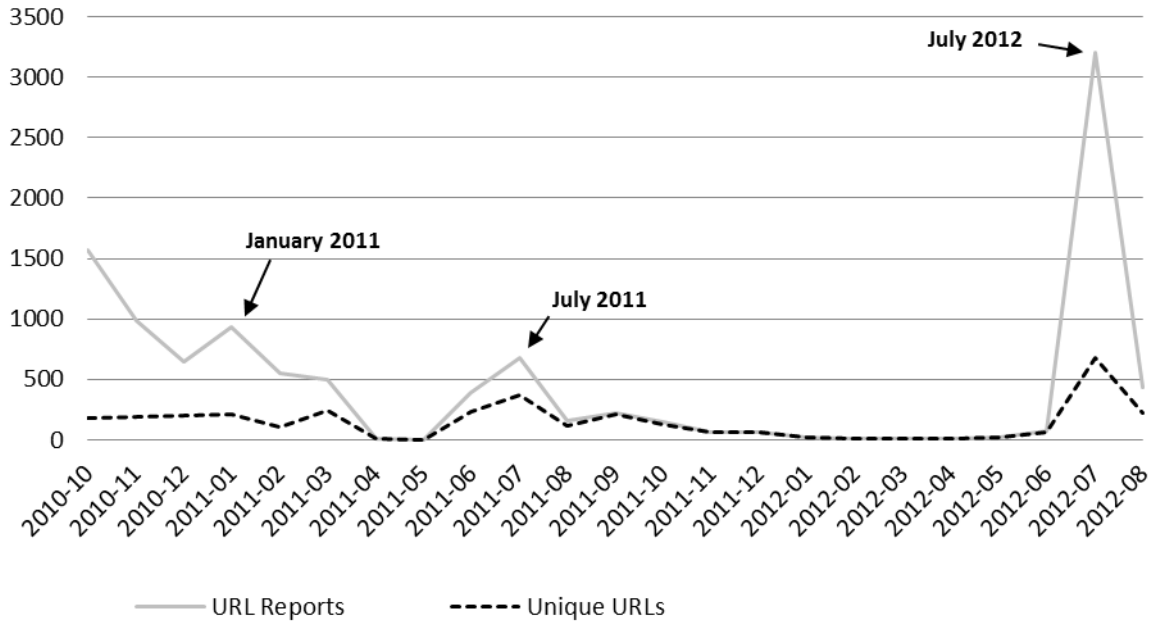

Figure 1. Level of user activity in reporting censorship through Alkasir in Syria.

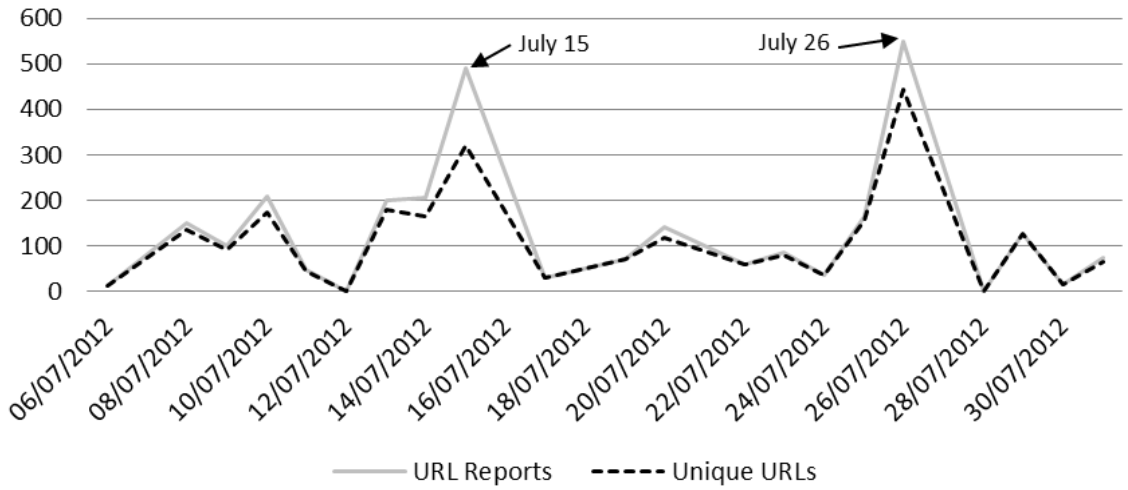

Figure 2. Level of user activity in reporting censorship through Alkasir in Syria during July 2012.

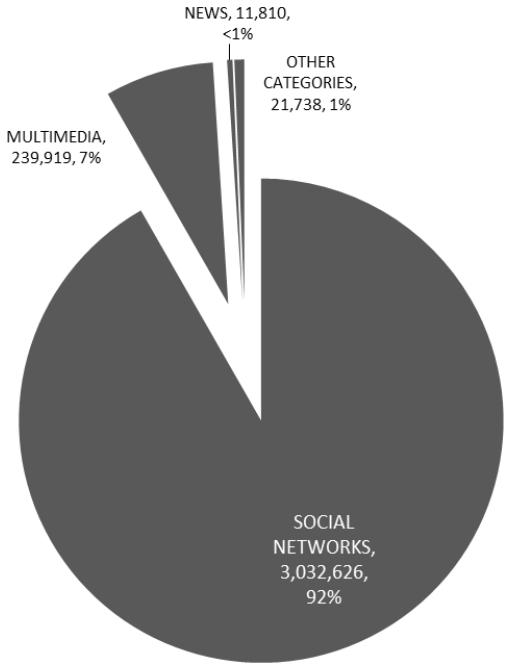

Figure 3. Visits of censored websites using Alkasir in Syria.

Table 1. The top ten censored websites.

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

The second group of blocked websites included those that allow the sharing of multimedia content, such as YouTube, which was also used to expose footage portraying the destruction of homes and properties by Assad forces. YouTube videos were also shared on Facebook showing images of injured and killed civilians by the shelling of villages and cities where opposition forces were based. It is therefore evident that bypassing censorship of such platforms by utilizing Alkasir helped broaden the perspective of Internet users and allowed them to access information from sources that are not controlled by the regime.

Table 1 shows the top list of blocked websites in terms of number of visits using Alkasir in Syria during the period covered by this paper. The top website, Facebook, was by far the most dominant with over 92% of all visits. Four of the ten websites were categorized as social media, which demonstrates the high value Alkasir users gave to the ability to interact and share information online. Alkasir did have the potential to allow users to access hundreds of other blocked websites as well but they received a much smaller number of visits.

While these findings point to a strong interest by users in accessing social media websites, it is important to note that one cannot conclude with certainty that the users of Alkasir used it merely to access and share anti-government content or used the software purely for mobilizing protests or dissident activities. However, it is possible to conclude that the attempt by the Syrian regime to prevent the public from accessing Facebook after the downfall of the presidents of Egypt and Tunisia illustrates a perceived threat by the social networking website to its authority. The study's findings point to the determination of users in Syria to access Facebook in large numbers despite the ban, allowing Alkasir to emerge as a liberation technology with the potential to limit information control by the government and al-

low users to engage in political mobilization through the web.

Additionally, the fact that censorship increased with developments on the ground and that among the top blocked websites was all4syria.info, a news website that included stories that promoted the Free Syrian Army, lends support to the hypothesis that Alkasir was also used to disseminate and access dissident material. In a time of conflict, such a contribution is arguably positive because it supports the free flow of information by limiting the regime's ability to manipulate online content.

While no particular qualitative research was carried out in this study, it is worthy noting that the use of Alkasir to prevent information blackouts during the Syrian conflict was in some way life saving as well. This was found by interviewing one of the Syrian activists who used Alkasir for an extended period of time. In a personal communication by email in 2013, he gave a couple of examples demonstrating how the use of Alkasir may have helped save lives. The activist, who requested to remain anonymous for his safety, said that he used Alkasir to publish footage and videos on Facebook and YouTube from areas affected by the fighting. He indicated that he was also able to use Alkasir to communicate a warning message through Skype, a voice chatting platform blocked in Syria at the time. The warning he sent had arrived just in time to the intended recipients, who were also using Alkasir, giving them the chance to evacuate an area before it was raided by the regime's security.

The activist gave a second example of a case when he used Alkasir to access blocked online resources, which he then used to communicate to international humanitarian missions to provide urgently needed humanitarian aid. The anonymous Syrian activist said: "When inspection operations began seeking leaders and organizers of the revolution, the software allowed us to send warnings on Skype or Facebook that security vehicles were approaching a particular neighborhood or street." (Syrian Activist, personal communication, 24 July, 2013)

These two examples illustrate that in certain situations during a conflict, having a tool to break free from censorship could be a matter of life or death. By empowering even a single individual in times of war, Alkasir demonstrates that technology can be used for the good of society.

It is important to note that while Alkasir was mainly used to access censored social media, the above examples illustrate that in order to assess the impact of a particular technology, one should not only take the number of visitors of blocked websites into account but should consider the significance of the type of content being circulated via those blocked websites. It might well be that a few users were able to access a censored website to upload timely and critical reports to the web. But the content they uploaded may have a substantial impact nationally and even globally. War news and footage published on Facebook using Alkasir for example, could then reach remote parts of the world and be shared and be picked even by transnational broadcast media. Such an impact is very difficult to assess, but should not to be ignored.

5. Conclusion

For a long time, media studies remained well behind the times by failing to adequately study how the Internet is used for political mobilization and dissent. The Arab Spring was a point in history when media scholars tried to catch up by studying the use of social media to promote freedom for people living under the rule of authoritarian regimes. However, many of those scholars fell in love with positive aspects of social media studies and very few made an effort to highlight the reaction of authoritarian regimes in the form of Internet censorship and the use of censorship circumvention tools as a form of liberation technology in response to the growth of censorship on the web.

This study is among the few that stand out in this area with a special focus on Syria. The study tried to understand how the Syrian regime censored the Internet during the initial period of the Arab Spring. By highlighting how Internet users in Syria fought back using censorship circumvention tools and eventually defeated website blocking, the study opens new doors to further explore this new and relatively unexplored area of research.

Being the seemingly indestructible, decentralized and global network that it is, the Internet will continue to garner more interest in the media studies field particularly as repressive practices by authoritarian regimes are expected to continue and evolve over time. The strong and unwavering resistance to repression as demonstrated by the Syrians that used censorship circumvention technology is a sign that the subject of Internet censorship will continue to be important and attract more research.

It is necessary however to critically reflect on the role of Internet censorship circumvention tools given that their ability to unblock websites is insufficient to address Internet censorship, which includes many other forms of practices that range from prosecuting bloggers to practicing mass surveillance on activists. While this study helps shed light on the important role those tools have, it merely scratches the surface when it comes to addressing the many forms of Internet censorship.

Furthermore, by serving as an intermediate agent between a user and a blocked website, any circumvention tool becomes vulnerable in its own right. With increased sophistication in online monitoring and tracking techniques, authoritarian regime are improving their capacity to identify the methods and operators of

those circumvention tools and take some steps to render them ineffective. Financial incentives to companies to stop hosting proxy servers could also be a move that some larger governments may take. While not invincible, censorship circumvention tools should be supported and encouraged to improve and spread to limit the ability of authoritarian regimes to target them.

It is unlikely that the Syrian regime will give up the fight against censorship circumvention tools. In fact, it is likely that it will try other ways to limit the ability of citizens to challenge its authority. Surveillance strategies as demonstrated by Gohdes (2014) could perhaps be a preference over censorship in the long run if those circumvention tools continue to be successful. Such a scenario could be devastating to activists if they are not diligent and careful when publishing personal information on social media.

The door is open to carry out more research in this exciting and growing field. What is needed more than ever is to engage media scholars with questions about liberation technology because the conversation surrounding freedom of expression and censorship on the Internet will likely continue unabated.

Acknowledgements

I wish to thank Professor Stig-Arne Nohrstedt for his support and supervision of the doctoral dissertation that permitted the collection of the data that was used to produce this study. This article was carried out with funding from Örebro University's Department of Media Studies.

Conflict of Interests

The author is the creator and administrator of Alkasir, on which he relied to extract the data needed for the study. However, Alkasir is free and is used mainly for educational purposes and activism. It is not a commercial product.

References

AFP. (2011). Syrian colonel claims big defection. *News24*. Retrieved from http://www.news24.com/World/News/Syrian-colonel-claims-big- defection-20110730

Al-Obaidi, J. (2007). *Media censorship in the Middle East*. New York: Edwin Mellen Press.

Al-Saqaf, W. (2014). *Breaking digital firewalls. Analyzing internet censorship and circumvention in the Arab World* (Doctoral dissertation). Retrieved from DiVA.

Anton, D. K. (2013). The dark days of NSA indiscriminate data surveillance. Retrieved from http://www.canberratimes.com.au/comment/dark-days-of-data-collection-20130613-2o6yl.html

Arnold, D. (2012). Syria: A war reported by citizen-journalists, social media. *Middle East Voices: VOA News*. Retrieved from http://middleeastvoices.voanews.com/2012/06/syria-a-war- reported-by-citizen-journalists-social-media-41863

Ayish, M. (2010). Universal Internet access is the new human rights issue. Retrieved from http://www.thenational.ae/news/universal-internet-access-is-the-new-human-rightsissue

Bennett, K., Grothoff, C., Horozov, T., & Lindgren, J. (2003). *An encoding for censorship-resistant sharing*. Munich: GNUnet.

Black, I. (2012). Syrian regime engages in systematic torture, says report. *The Guardian*. Retrieved from: http://www.theguardian.com/world/2012/jul/03/syria-torture-human- rights-watch

Brand, S. (2001). Founding father. *Wired*. Retrieved from http://www.wired.com/wired/archive/9.03/baran.html

Casper, G. (1995). *Fragile democracies: The legacies of authoritarian rule.* Pittsburgh, PA: University of Pittsburgh Press.

Cisco. (2011). Global internet traffic projected to quadruple by 2015. *Cisco's Technology News Site*. Retrieved from http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=324003

Cowie, J. (2011). Egypt leaves the Internet. *Renesys*. Retrieved from http://www.renesys.com/2011/01/egypt-leaves-the-internet

Deibert, R. J. (2013). Black Code Redux: Censorship, surveillance, and the militarization of cyberspace. In B. Megan (Ed.), *Digital media and democracy: Tactics in hard times* (pp. 137-163). Cambridge: 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.

Diamond, L. (2012). Liberation technology. In L. Diamond & M. F. Plattner (Ed.), *Liberation technology: Social media and the struggle for democracy* (pp. 3-17). Baltimore: The Johns Hopkins University Press.

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.

Flew, T. (1998). From censorship to policy: Rethinking media content regulation and classification. *Media International Australia, Incorporating Culture & Policy*, *88*(August), 89-98.

Freedom House. (2010). Syria: Freedom of the press 2010. *Freedom House*. Retrieved from http://www.freedomhouse.org/report/freedom-press/2010/syria

Galperin, E. (2012). Don't get your sources in Syria killed. *Committee to Protect Journalists*. Retrieved from http://www.cpj.org/security/2012/05/dont-get-your-sources-in-syria-killed.php

Gauntlett, D. (2007). Wide angle: Is it time for Media Studies 2.0. *Media Education Association Newsletter, 5*(2007), 3-5.

Gohdes, A. (2014). *Repression in the digital age: Communication technology and the politics of state violence* (Doctoral dissertation). Retrieved from Universitätsbibliothek Mannheim.

Goldstein, E. (1999). *The Internet in the Mideast and North Africa: Free expression and censorship.* Washington, DC: Human Rights Watch.

Gradstein, L. (2012). UAE cyber-crime law 'effectively closes-off country's only remaining forum for free speech': watchdog. *National Post*. Retrieved from http://news.nationalpost.com/2012/11/28/uae-cyber-crime-law-effectively-closes-off-countrys-only-remaining-forum-for-free-speech- watchdog

Gross, D. (2013). Google boss: Entire world will be online by 2020. *CNN*. Retrieved from http://edition.cnn.com/2013/04/15/tech/web/eric-schmidt-internet

Hardt, H. (2000). Communication is freedom: Karl Marx on press freedom and censorship. *Javnost-Ljubljana, 7*(4), 85-100.

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: 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.

Howard, P. N. (2010). *The digital origins of dictatorship and democracy: Information technology and political Islam*. Oxford: Oxford University Press.

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When do states disconnect their digital networks? Regime responses to the political uses of social media. *The Communication Review*, *14*(3), 216-232.

Huang, C. (2011). Facebook and Twitter key to Arab Spring uprisings: Report. *The National*. Retrieved from http://www.thenational.ae/news/uae-news/facebook-and-twitter-key-to-arab-spring-uprisings-report

Hubbard, B., & Jordans, F. (2013). UN says more than 60,000 dead in Syrian civil war. *The Big Story.* Retrieved from http://bigstory.ap.org/article/syrian-rebels-attack-air- base-north

Internet World Stats. (2013). Internet usage in the Middle East. *Internet World Stats*. Retrieved from http://www.internetworldstats.com/stats5.htm

Internet World Stats. (2014). World internet users statistics usage and world population. *Internet World Stats*. Retrieved from http://www.internetworldstats.com/stats.htm

Karam, Z., & Kennedy, E. (2011). Free Syrian Army transforms Syria uprising. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/2011/11/21/free-syrian-army_n_1106087.html

Karouny, M. (2012). Syrian rebels start "liberate Damascus" operation. *Reuters*. Retrieved from http://www.reuters.com/article/2012/07/17/us-syria-crisis-rebels-idUSBRE86G10B20120717

Keen, A. (2007). *The cult of the amateur: How today's Internet is killing our culture.* New York, NY: Bantam Dell Pub Group.

Kerr, D. (2014). Brazil lays down the law with Internet 'Bill of Rights'. Retrieved from http://www.cnet.com/news/brazil-lays-down-thelaw-with-internet-bill-of-rights

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.

Landis, J., & Pace, J. (2007). The Syrian opposition. *The Washington Quarterly, 30*(1), 45-68.

Lee, F. L. (2007). Hong Kong citizens' beliefs in media neutrality and perceptions of press freedom: Objectivity as self-censorship? *Asian Survey,* 47(3), 434-454.

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 & Y. Littunen (Eds.), *Cleavages, ideologies and party systems (*pp. 291-342). Helsinki: Transactions of the Westernack Society.

Lund, A. (2012). *Divided they stand: An overview of Syria's political opposition factions.* Brussels: Foundation for European Progressive Studies.

MacKinnon, R. (2008). Flatter world and thicker walls? Blogs, censorship and civic discourse in China. *Public Choice,* 134(1), 31-46.

Macleod, H. (2011). Syria: how it all began. *GlobalPost*. Retrieved from http://www.globalpost.com/dispatch/news/regions/middle-east/110423/syria-assad-protests-daraa

McGreal, C., & Shenker, J. (2011). Hosni Mubarak resigns—And Egypt celebrates a new dawn. *The Guardian*. Retrieved from http://www.theguardian.com/world/2011/feb/11/hosni-mubarak-resigns-egypt-cairo

Mellor, N., Rinnawi, K., & Dajani, N. (2011). *Arab media.* Hoboken: John Wiley and Sons.

Merrin, W. (2009). Media Studies 2.0: Upgrading and open-sourcing the discipline. *Interactions: Studies in Communication & Culture, 1*(1), 17-34.

Morozov, E. (2011). *The net delusion: how not to liberate the world.* London: Allen Lane.

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: MIT Press.

Myers, S. L. (2011). U.S. and allies say Syria leader must step down. *The New York Times*. Retrieved from

http://www.nytimes.com/2011/08/19/world/middleeast/19diplo.html?p agewanted=all
Negroponte, N. (1996). *Being digital.* New York, NY: Vintage Books.
ONI. (2009). Internet filtering in Syria*. OpenNet Initiative*. Retrieved from https://opennet.net/sites/opennet.net/files/ONI_Syria_2009.pdf
Ostini, J., & Ostini, A. Y. (2002). Beyond the four theories of the press: A new model of national media systems. *Mass Communication and Society*, *5*(1), 41-56.
Oweis, K. Y. (2011). Syria's Assad ends state of emergency*. Reuters*. Retrieved from http://www.reuters.com/article/2011/04/21/us-syria-idUSTRE72N2MC20110421
Palfrey, J., Roberts, H., & Zuckerman, E. (2011). *Circumvention tool evaluation.* Cambridge: Berkman Center for Internet & Society, Harvard University.
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: Vintage Books.
RSF. (2010). Enemies of the Internet*. Reporters without Borders*. Retrieved from http://www.rsf.org/IMG/pdf/Internet_enemies.pdf
RSF. (2013). Netizens and citizen journalists killed. *Reporters Without Borders*. Retrieved from: 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.
Schmidt, S. (2006). The missed opportunity for economic reform in Syria. *Mediterranean Politics, 11*(1), 91-97.
Schonfeld, E. (2011). Twitter is blocked in Egypt amidst rising protests. *Tech Crunch*. Retrieved from http://techcrunch.com/2011/01/25/twitter-blocked-egypt
Senat, J. (2011). Defining censorship*. Joey Senat Home Page*. Retrieved from http://journalism.okstate.edu/faculty/jsenat/censorship/defining.htm
Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign Affairs, 90*(January/February), 28-41.
Stepanova, E. (2011). The role of information communication technologies in the 'Arab Spring'. *Ponars Eurasia, 159*(May), 1-6.
Stone, I. F. (1989). *The trial of Socrates.* New York: Random House Digital.
Surowiecki, J. (2005). *The wisdom of crowds.* New York: Knopf Doubleday Publishing Group.
Sutton, M. (2012). Iraq cyber crime law threatens free speech says HRW. *ITP*. Retrieved from http://www.itp.net/589674-iraq-cyber-crime-law-threatens-free-speech- says-hrw
Sweis, R. (2013). Syrian refugees strain resources in Jordan*. The New York Times*. Retrieved from http://www.nytimes.com/2013/01/03/world/middleeast/syrian-refugees- strain-resources-in-jordan.html
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.
US Department of Treasury. (2008). Rami Makhluf designated for benefiting from Syrian corruption*. US Department of the Treasury.* Retrieved from http://www.treasury.gov/press-center/press-releases/Pages/hp834.aspx
Varnelis, K. (2012). *Networked publics.* Cambridge: The MIT Press.
Walt, V. (2012). Is Syria's Bashar Assad going the way of Muammar Gaddafi? *Time Magazine*. Retrieved from http://world.time.com/2012/07/23/is-syrias-bashar-assad- going-the-way-of-muammar-gaddafi
Watson, I. (2011). Cyberwar explodes in Syria. *CNN.* Retrieved from http://edition.cnn.com/2011/11/22/world/meast/syria-cyberwar
Weaver, M., & Whitaker, B. (2012). Syria crisis: US fears Aleppo 'massacre'. *The Guardian*. Retrieved from http://www.theguardian.com/world/middle-east-live/2012/jul/27/syria-us-fears-aleppo-massacre-live
Zahler, K. A. (2009). *The Assads' Syria.* Breckenridge: Twenty-First Century Books.
Zarwan, E. (2005). *False freedom: Online censorship in the Middle East and North Africa.* Washington, DC: Human Rights Watch.
Ziadeh, R. (2009). *The Kurds in Syria: Fueling separatist movements in the region?* Washington, DC: United States Institute of Peace.

About the Author

Dr. Walid Al-Saqaf
Walid Al-Saqaf is a Yemeni scholar based in Sweden with a multidisciplinary academic background in computer engineering and media studies. He is among a few Arab scholars studying social aspects of digital media as well as actively developing sophisticated software for enhancing democracy and studying the use of social media and analyzing trends. In 2015, Al-Saqaf was elected to the board of trustees of the Internet Society, the international organization concerned with the active development of a resilient, stable and open Internet that is accessible to all citizens of the world.