EPiC Series in Computing

Volume 69, 2020, Pages 60–68

Proceedings of 35th International Conference on Computers and Their Applications

EPiC Computing

A Study of the Landscape of Internet Censorship and Anti-Censorship in Middle East

Nick Rahimi, Bidyut Gupta

Southern Illinois University, Carbondale, IL 62901, USA

shrahimi@siu.edu, bidyut@cs.siu.edu

Abstract

The power of technology is one which supersedes any other tool of communication ever formulated and implemented by human beings. The internet has been long cited by scholars and practitioners alike to be an empowerment tool that allows individuals to either seek, receive or dole out information and ideas without any basis being drawn on boundaries or geographical locations. This, therefore, means that online communication has to be protected in lieu with the international dictums and pretensions that call for the right to freedom of expression.

1 Introduction

Despite the apparent progression of the society in all facets considered, [1] opines that internet access and the use of various applications in the Middle East is viewed to be an egregious violation of the governmental laws. This is because the government views the internet as a byproduct of western civilization which is set out to disrupt their activities and destroy the morals of the society.

Various countries in the Middle East have actively banned applications and websites that they may deem to stir emotions or cause political tension. Most researchers argue that this is uncalled for as it goes past the set laws of the international convention. Proponents to the censorship back the scheme as it offers the requisite backing to their cultural values and ideologies. This essay presents the thesis that internet and application censorship in the Middle East has played a negated role in alienating the people from interacting with the outside world.

2 Censorship Reasons And Methods

Many of the censored websites or apps in the Middle East are social media platforms. These sites and apps are often censored due to the political climate of the regions in which they are censored. This can be due to political tensions and the perceived need to block content that would allow speech deemed

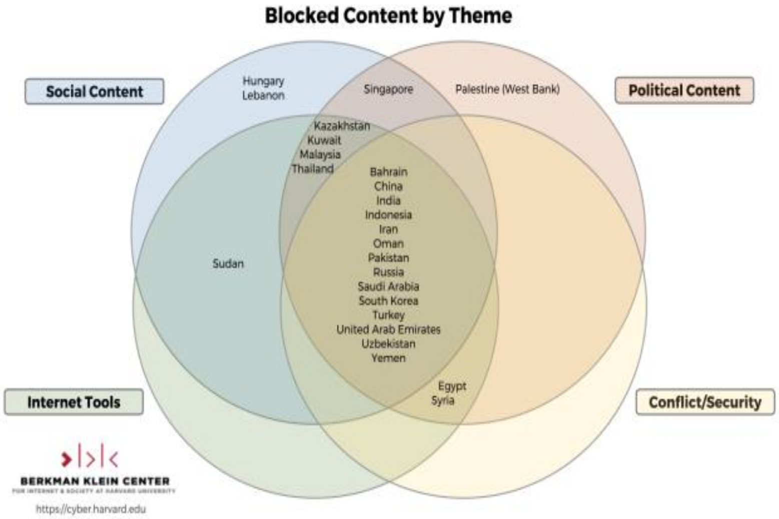

Figure 1: Blocked themes in Middle Eastern Countries [1]

offensive or committing another offense. The Middle East also has regions forming political alliances with one another. The regions in these alliances block the same content as their allies. Such content is often deemed by the censoring entity as 'fake news' or as promoting terrorism [7].

2.1 Packet Filtering

The first method that is used in censoring websites in the Middle East is packet filtering in which the government terminates the transmission of TCP packets that contain controversial and selected keywords. This inadvertently means that the results pages presented in search engines are censored. In nations like Lebanon, the government has actively taken to banning the search of politically related themes which consist of content categories like freedom of expression, religion and human rights. The Lebanese government has banned websites and applications like Grindr which are aimed at exploring one's sexuality options [1].

The filtering method also comes intact with religious filtering which focuses on straddling social and political themes. Saudi Arabia, Yemen, and the United Arab Emirates have all taken up the use of religious filtering to block religious content which is not in thrall with the religious beliefs sanctioned by the state [2]. Applications like Facebook and Whatsapp have been long cited to play a key role in the degradation of the religious morals of the state which prompted the government to ban the sites. Iran and UAE governments also banned and filtered any searches on WikiIslam, Jihad Watch and the Religion of Peace [3].

For politically based censorship, the reasoning behind the restrictions is often due to the content having a different view on an issue or belief. The censoring power does not want the opposition to gain traction or have a recognizable support behind them. The state censors can block such content so that authority of that region can portray the information they want to be spread, and they portray it exactly how they wish. With political censorship, propaganda is a main component [4].

However, political motivations are not the only reason behind internet censorship in the Middle East. Oftentimes, the cause is morally, religiously or culturally based. Content may also be restricted due to concerns of security.

There can also be very specific reasons for a region to filter the Internet, such as for the benefit of their economic monopoly. The media is often the target of this censorship and there are restrictions placed upon online communications [5].

Social media such as Facebook, Twitter, or YouTube play a role in protests, demonstrations, or other unified clashes based on beliefs. Social media allows communication and can be a starting point for organization of citizens against their governments or other power. This form of media is harder for governing powers to manipulate and suppress.

Social media has benefited countries and regions that, prior to the widespread accessibility of these social media platforms, had restricted or directly controlled press and information sources. Censorship is their attempt to still control these platforms and restrict the facilitation of information deemed out of line with the governing powers' wishes [6].

The third component of the packet filtering technique is focused on social content filtering in which the countries highlight and block searches which go against the accepted societal norms. The content filtering method is dependent on algorithms that match the keywords and block or filter them. Countries like Thailand, South Korea, Singapore, Malaysia, Yemen, UAE, Saudi Arabia, Qatar, and Oman have all banned websites/ applications like Pornhub which produce and display pornographic content. In addition to this, Lebanon has banned poker stars client which is a gambling site/application. The government states that the gambling contents have led to youths being unable to focus on working and rather gambling their money away.

In addition to this, the governments of Qatar, Saudi Arabia, and Iran have banned the use of Telegram, FaceTime and Snapchat applications in their countries. This has been duly attained by blocking any search packets that might help one download the applications. This comes in light with regulations passed for blocking voice over internet protocol services as they not only have an economic impact on the telecom companies in the nations but also lead to heightened moral degradation.

The fourth component highlighted is based on conflict and security in which the governments of Yemen, Uzbekistan, the UAE, Turkey, Saudi Arabia, Pakistan, Kuwait, and Iran have actively blocked any websites that might contain content that might be viewed to be stated or perceived a threat to national security. The countries have substantially and pervasively filtered websites which tend to cover conflicts between the government and insurgents or even those that host content that backs insurgents. The governments also ban content that might be deemed to be extremist or terrorist.

Say, for example, the government of Iran actively blocks websites which are linked intermittently to ethnic groups like the Iranian Kurds. The kurdishproject.org has been banned in the country because it airs data and information which the Iranian government considers being a security threat. The government has also moved to block websites that air news and stories from its regional rival, Saudi Arabia. To counter this act of opposition, Saudi Arabia has also banned any websites that are associated with Iran. The figure 1 adumbrates the different themes that have been blocked in the different nations in the Middle East.

The kingdom of Saudi Arabia has taken up the use of Smart filters which blocks any access to banned websites. Tunisia, Oman and the UAE also use the software with Iran implementing a filtering proxy which displays a message that the page has been blocked on request.

2.2 Internet Service Provider Filters

Opines that the use of internet service provider (ISP) filters in blocking the searching and transmission of data is one of the least controversial ways of censoring internet access. Different nations have used this scheme in a bid to maintain sanity in their nations although oppressive regimes have been forced to strong-arm companies into blocking their internet. The oppressive regimes often find it easy to strong arm the countries when and if they own the entire internet infrastructure.

In the states of Saudi Arabia and the UAE, the government actively owns the internet infrastructure and it is of no secret that these two states have the highest rate of internet censorship. The Saudi government has resorted to the filtering of internet traffic through the implementation of software and services to mitigate the ISPs.

The filtering of the websites often applies to websites that focus on pornography, drugs and other applications which might be used in mobilizing terrorists. The state of Saudi Arabia has set up two country-level data service providers namely the Bayanat Al-Oula and the Integrated Telecom Company. Both these service providers are split between global servers and the state-owned internet infrastructure. The ISP providers have thus blocked websites like the Faith Freedom International and the WikiIslam website. MuhammadTube has been censored in Qatar by some ISPs.

In the state of Palestine, on the other hand, the government ordered the ISPs to block at least twelve websites and Facebook application which had a relationship with the rival group Hamas. This is because the group controlled the Gaza strip. Also, the authority blocked every website that criticized the Fatah leader such as the ytnews.com and the middleeastmonitor.com

The aforementioned news agencies were cited to have been influenced by western nations and they were aimed at disintegrating the nation. This filtering and blocking scheme were significant in helping the government maintain law and order.

The state of Islamic Republic of Iran has time over time maintained strict control over its internet through the use of telecommunication structures that are owned by the government. The national agency is running and managed by the Iranian Ministry of Information which regulates the searches from every Internet Service Provider. Just like any other country in Middle East, the state of Iran has taken up the habit of prohibiting access to its citizens from any websites that are not Islamic.

The government requires each and every blog or website to acquire new licenses. The permission to post any material on the website however requires analysis conducted by the Ministry of Islamic Culture which also determines whether the content is in thrall with the Islamic teachings. The government has also utilized surveillance through deep packet inspection.

The national agency tasked with providing internet to the people creates spy tools which are installed in the networks. The authorities then use the tools in blocking internet telephony and emails as well as identifying the people using the services. Iran is undoubtedly one of the topmost nations that has invested highly in domestic spyware which has further been used in spying on foreign aids [8].

2.3 ASN blocking

The Egyptian government has been long criticized for blocking different websites and applications by blocking the autonomous system number (ASN) whenever proxies cause problems. Scholars highlight that every ISP is allocated a particular ASN with the internet provider ranging and controlling as desired. In the case that the government wants to block a website, it will revamp the internet infrastructure by providing a smaller autonomous system number which helps in the creation of a path that contains the least resistance. The allocation process also comes intact with an IP range that contains the address of the website it wants to block [1] [9].

The blocking process will direct the routers to go to the government's version of the website instead of the website itself. By changing the router and the IP address, the government can change the options of the user. Analysis of the current policies in Egypt espouses that the government has blocked every ASN to limit the transmission of any news which is affiliated to the Muslim Brother Hood. Furthermore, the Egyptian government has blocked every ASN that is related to Signal, which is a communication tool that helped the people of Egypt during the revolution. The ASN blocking tool has thus far proven to be efficient with the government bypassing the ISPs and filtering the data at the primary internet access point.

2.4 Portal Censorship and the Removal of Search Results

Key portals that might be inclusive of search engines might be forced by authorities to exclude links to web pages that they would normally include. This means that the people who search for the website will be unable to find it. This censorship is often done in a bid to satisfy the set laws and regulations of the state or even just at the discretion of the site.

The state of Turkey blocked the use of Wikipedia for a year with the authorities indicating that this was vital in the protection and enhancement of public order. The authorities also moved to ban the use of social media platforms like Whatsapp, Instagram, Facebook and Twitter which comes in light with the failed coup that took place in 2015. The government analyzes and dismisses content placated over social media with twitter accounts being withheld.

Scholars opine that Iran has not been left behind when it comes to portal censorship and the removal of search results. The study results adumbrated that over 950 Wikipedia article pages had been blocked by the Iranian government due to the fact that they contained the Persian language. The authors indicated that the censors targeted Wikipedia pages that were focused on any information that criticized the police, government officials and the state. Also, the government blocked data and information about people who had been killed or detained by the Iranian government.

Acting as a microcosm of the Iranian government, the Persian Wikipedia is a primal example of a website which contains blocked themes and filtering rules that are applied across various countries. By migrating to a HTTPs Protocol in 2015, Wikipedia left the Iranian government without a choice and it decided to not block it. The advent of Wikipedia Commons also saw slight issues as it was blocked in 2016 but the government lifted the ban later.

2.5 Network Disconnection and Connection Reset

Network disconnection is majorly focused on cutting off all the network infrastructure components to limit internet access. With connection reset, on the other hand, the government blocks the TCP connections through the use of a filter. The block is exercised over a set period with communication being routed through the blocking location.

In 2011 when the Egyptian state was engulfed in a myriad of protests and fights, the government ordered every ISP firm to shut down its services to maintain tranquility. Figure 2 adumbrates the impact of the shutdown with any remaining ISPS being tricked into going into government relayed websites.

From Figure 2, one needs to understand that the government forced the ISPs to shut down at least 3599 BGP routes for a set period. The government implemented the full block without affecting the fiber opting links which connected the people to the international community. The Libyan government also implemented a full block of the ISPS and the routers with the Syrian authorities following suit [1].

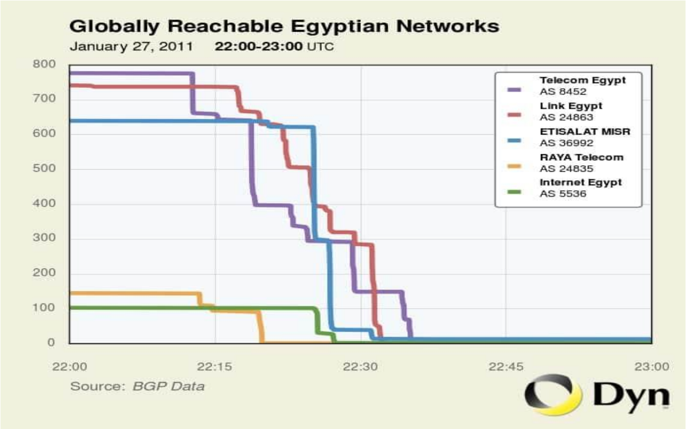

Figure 2: Internet Disruption by the Egyptian Government. [2]

The Bahrain government most recently reset the connections in areas that are densely populated by the Shiites. This is because the Shiites actively used the internet in mobilizing and protesting the government. The Iraq and Algerian authorities also disrupted the internet in a bid to mitigate the leaking of exams as well as hampering communication between students. Iran has also been cited to be at the forefront of cracking down protests by slowing down or shutting down the internet. During the 2009 protests, the internet was riddled by a myriad of videos which showed the government attacking protestors. For the purpose of quelling international scrutiny and fostering peace and tranquility, the government decided to slow down the transmission rates of the data. This made it hard for the people to communicate with others through the use of social media.

The UAE manages and determines the type of data and communication which passes through its communications company, Etisalat. The company is the only ISP provider in the country. In addition, the UAE government has filtered internet content on all cyber cafes. Summations show however that homes and businesses can be exempt from the blocks and the filters.

In the state of Oman, on the other hand, the government has full control over the main ISP provider which is Oman Tel. The company monitors every communication coming from and into the country when using its fixed and mobile phone services. The Oman government has ordered every cybercafé to remove every barrier that exists between their personal computers in order to analyze what the users are doing. The state of Yemen has also passed a similar policy with Websense being used to censor the internet.

3 Anti-Censorship Tools & Techniques

As a growing challenge to online freedom of expression in different countries around the world, private and public entities have taken up circumvention and anti-censorship tools which are designed

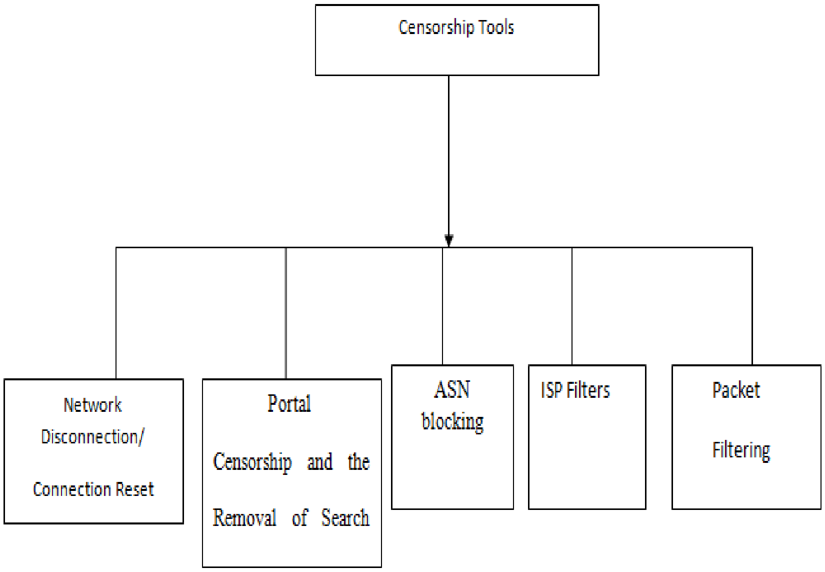
Censorship Tools
Network Disconnection/ Connection Reset
Portal Censorship and the Removal of Search
ASN blocking
ISP Filters
Packet Filtering

Figure 3: Censorship tools used

to bypass the blocks and internet filtering schemes. The first type of anti-censorship software that can be used by Middle Easterners is CGI (Common Gateway Interface) proxies which implement the use

of scripts that run through servers to perform circumvention functions. The proxies tend to send a request URL which contains the data portion of the requested HTTP to the server [10].

The server then pulls the required information on the destination from the information accorded in the request and sends out its request to the destination after which the client receives the result. The security levels of the CGI proxy are top notch as long as the proxy server operator has set up the required trust metrics. The proxy tools also do not require any manual configuration of the browsers as it comes with all the required tools for circumventing the internet filters and blocks.

The second type of anti-censorship software is HTTP proxies which are used in the transmission of HTTP requests to the server [8-10]. The proxies are connected to a client who sends the same request to the server after which the request is parsed by the HTTP proxy. The parsing process also involves the request being sent to the ultimate destination servers and the response is transmitted back to the client. The tool requires configuration protocols to ensure that the user can use their browser interfaces without any hassles whatsoever.

The third type of anti-censorship systems is the rerouting tool which helps the users in shielding their requests from blocks and filters by sending responses and requests through a myriad of proxying servers. The data is often encrypted at every proxy in order to ensure that the proxy is unaware of the destination or origin of the data. This plays a key role in circumventing the blocks [10-12].

Onion routing can also be implemented when trying to circumvent through blocks and filters. The scheme is built through the wrapping of a message by divergent layers of encryption which can only be decrypted once the data reaches the destination. The message is often encrypted as it is transferred between the nodes with the origin and final destinations being anonymous [13].

For the purpose of creating and transmitting the onion, the users need to create a directory node from a list provided. The nodes are then compounded into chains through which the messages are transmitted. For the identity of the sender to remain anonymous, no node in the circuit will be able to identify the sender data. The originator will use a public key that is encrypted by the use of asymmetric key cryptography. The link will be sent between the various nodes until it gets to the destination. The nodes ensure that the link and the chain remain the same for the transmission of data between the receiver and the sender.

A key technique that can be used by the middle easterners in evading filters and blocked content is through the use of copies, mirrors, and pages that have been cached. Take for example the use of an RSS (Really Simple Syndication) aggregator which receives and passes every RSS feed that has been blocked prior. The users can also access copies of the sites through the use of archive sites like the Wayback Machine which stores a copy of every website and mirrors it. Cached pages are also important when accessing blocked sites as they are hosted by search engines. The cached pages are often indexed by the engines and may not be viable to filters.

Proxying is another technique that can aid in evading filters and blocks. The first type of proxy is Tor which is used in routing encrypted traffic by utilizing divergent servers. The tool plays a vital role in making the destination and the source of the traffic to become less traceable and it evades every filter and blocks implemented.

A virtual private network (VPN) is another tool which helps in the creation of a viable connection between the user and the server without having to worry about being detected. The VPN services are often paid or offered for free with at least 400 million people using the services in a bid to increase the privacy or circumvent blocks. The 8th tool that can be used is domain fronting whereby the user hides the initial request by passing the tokens through a popular website.

Psiphon [14] is another primal example of an internet circumvention tool which was formulated by Wickr Inc. the tool combines the use of HTTP proxy technology, SSH and VPN when providing the users with uncensored access to the internet. In addition to this, the technology uses the SSH as its central strategic initiative. This is due to the fact that it prevents ISPs from deep packet inspection in a bid to identify the origin and destination of a message.

The Psiphon tool comes intact with a layer that is not only obfuscated but also open by nature. The layer is vital in the development of a random stream by transforming the handshake. The process of development is significant in allowing the handshake to get a random padding. When the client starts using the protocol, they are enabled to connect to up to ten divergent servers in a simultaneous manner. This helps in the minimization of the wait time incurred when the servers try to block various protocols.

DNS based filters are also used in circumventing the blocks and the filters. The systems are vital in converting the inherent internet provider address to a standard universal resources locator. The filters, when implemented on a specific site, will help in blocking and bypassing censorship protocols. They tend to change the DNS server or the website providers. The filters also work towards ensuring that the second server remains open in order for the user to circumvent censorship.

Sneakernets [15] are used in the transfer of computer files between different computers especially when the network is being scrutinized. The nets physically carry data through the use of storage media, and they might not exactly depend on the government infrastructures for the transmission of data. The sneakernet can work in tandem with the anonymous P2P communication systems in maintaining communication [16-18].

4 Conclusion

The preceding analysis represents the manner through which different Middle Eastern nations view the internet. The investigation suggests that it is high time for the denizens to practice their right instead of bowing to political exigencies in the name of patriotism. Several circumvention tools have been presented which will help the citizens in accessing the internet and gaining access to data and information.

References

[1] Lavanya Rathnam. (2017, November) Internet Censorship: Five Countries That Block The Web. [Online]. https://www.cloudwards.net/internet-censorship/

[2] Radom, R. (2007). Internet Filtering Companies with Religious Affiliations in the Context of Indiana Public Libraries. LIBRES: Library & Information Science Research Electronic Journal, 17(2).

[3] Justin Clark, "The Shifting Landscape of Global Internet Censorship," 2017.

[4] Noman, H. (2019). Internet Censorship and the Intraregional Geopolitical Conflicts in the Middle East and North Africa. *SSRN Electronic Journal*. doi:10.2139/ssrn.3315708

[5] Shishkina, A., &Issaev, L. (2018). Internet Censorship in Arab Countries: Religious and Moral Aspects. *Religions, 9*(11), 358. doi:10.3390/rel9110358

[6] Smidi, A., & Shahin, S. (2017). Social Media and Social Mobilization in the Middle East: A Survey of Research on the Arab Spring. *India Quarterly: A Journal of International Affairs*,*73*(2), 196-209. doi:10.1177/0974928417700798

[7] Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The Shifting Landscape of Global Internet Censorship. *SSRN Electronic Journal*. doi:10.2139/ssrn.2993485

[8] Aryan, S., Aryan, H., & Halderman, J. A. (2013). Internet censorship in Iran: A first look. In Presented as part of the 3rd {USENIX} Workshop on Free and Open Communications on the Internet.

[9] Mitchell, J. (2013). Autonomous system (AS) reservation for private use (No. RFC 6996).

[10] Leberknight, C. S., Chiang, M., Poor, H. V., & Wong, F. (2010). A taxonomy of Internet censorship and anti-censorship. Erişim adresi: https://www. princeton. edu/~ chiangm/anticensorship. Pdf.

[11] Rahimi, N., Nolen, J. and Gupta, B. (2019) Android Security and Its Rooting—A Possible Improvement of Its Security Architecture. Journal of Information Security, 10, 91-102.

[12] Rahimi, Nick, Jacob J. Reed, and Bidyut Gupta. "On the Significance of Cryptography as a Service." Journal of Information Security 9.04 (2018): 242.

[13] Goldschlag, D., Reed, M., & Syverson, P. (1999). Onion routing for anonymous and private internet connections. Naval research lab Washington DC center for high assurance computing systems (CHACS).

[14] Jia, J., & Smith, P. (2004). Psiphon: Analysis and estimation.

[15] Gray, J., Chong, W., Barclay, T., Szalay, A., & Vandenberg, J. (2002). TeraScale SneakerNet: Using inexpensive disks for backup, archiving, and data exchange. arXiv preprint cs/0208011.

[16] Rahimi, N., Sinha, K., Gupta, B., Rahimi, S., & Debnath, N. C. (2016, July). LDEPTH: A low diameter hierarchical p2p network architecture. In 2016 IEEE 14th International Conference on Industrial Informatics (INDIN) (pp. 832-837). IEEE.

[17] Rahimi, N., Gupta, B., & Rahimi, S. Secured Data Lookup in LDE Based Low Diameter Structured P2P Network.

[18] Rahimi, S. (2017). A Novel Linear Diophantine Equation-Based Low Diameter Structured Peer-To-Peer Network.