



المركز العربي للأبحاث ودراسة السياسات
Arab Center for Research & Policy Studies

Strategic Analysis | 17 november 2020

The Sisi Firewall

Cyber-suppression Strategies and the Future
of Cyberspace in Egypt

Strategic Brief No. 4

Mostafa El-Sayed Hussin

The Sisi Firewall: Cyber-suppression Strategies and the Future of Cyberspace in Egypt

Series: **Strategic Analysis**

17 november 2020

Mostafa El-Sayed Hussin

Researcher at the Arab Center for Law and Society Studies (ACLSS) in Paris. He specializes in visual anthropology, cinema and sociology, and is interested in analyzing strategies of cyber oppression and power-resistance relations in postmodern societies, and the role that the development of communication

Copyright © 2020 Arab Center for Research and Policy Studies. All Rights Reserved.

The Arab Center for Research and Policy Studies is an independent research institute and think tank for the study of history and social sciences, with particular emphasis on the applied social sciences.

The Center's paramount concern is the advancement of Arab societies and states, their cooperation with one another and issues concerning the Arab nation in general. To that end, it seeks to examine and diagnose the situation in the Arab world - states and communities- to analyze social, economic and cultural policies and to provide political analysis, from an Arab perspective.

The Center publishes in both Arabic and English in order to make its work accessible to both Arab and non-Arab researchers.

The Arab Center for Research and Policy Studies

Al-Tarfa Street, Wadi Al Banat

Al-Dayaen, Qatar

PO Box 10277, Doha

+974 4035 4111

www.dohainstitute.org

Table of Contents

Introduction	1
First Strategy: Censorship	1
Second Strategy: Misinformation and Fake News	3
Third Strategy: Blockade	3
Fourth Strategy: Digitization	5
Fifth Strategy: Legal Arsenal	5
Conclusion: The Egyptian Firewall as an Expression of Power / Resistance Relations	6

Introduction

On 25 January 2011, the Mubarak regime woke up to its worst nightmare: thousands of Egyptians on the streets demonstrating in response to a Facebook invitation. The state was clearly at a loss of how to deal with demonstrators who had moved beyond the traditional forms of organization easily curbed by the regime. The government tried to partially restrict the internet before cutting it completely, along with all wireless services, three days after the start of the demonstrations.

In September 2020, nearly a decade later, calls for demonstrations against the new regime rang out on social media once again. But the response this time was very different. Although it did employ violent physical measures – such as the pre-emptive arrest of a number of activists, dispersal of demonstrations and arrest of citizens – the state’s cyber-performance was much more sophisticated than nine years previously. State agencies sought to address citizens through their various digital platforms, which millions of citizens were now following. Through the Egyptian Media Group, owned by the General Intelligence Services,⁽¹⁾ they attempted to manipulate popular opinion by making videos and sending them to opposition media platforms, and then revealing that they had been doctored after they were broadcast.

Between 2011 and 2020, the Egyptian state made enormous headway in dealing with cyberspace. This paper seeks to analyse this development by deconstructing the four main government strategies, which together form the “firewall” of the Sisi regime. From there, the article ponders the future of online political activism in Egypt.

First Strategy: Censorship

The internet and social networks were, arguably, the main intervening variables driving events during the January Revolution. The Mubarak regime did not realize that the citizens of Egypt had created a new public sphere far removed from physical spaces. Although the state occupied almost every meter of physical space in the country through a seemingly stable hierarchical structure in which power was distributed across the security services, the ruling party, and millions of beneficiaries and collaborators, it had no idea what cyberspace was, let alone the extent to which it could create political mobilisation or influence.

The revolution that began with an invitation on Facebook cut to the core of the deep state, forcing it to disable the internet for the entire country, and completely paralyzing the economy on 28 January 2011, known as the Friday of Anger or Day of Rage. It was clear to the observers that the regime and its apparatus were helpless in the face of the internet.

However, since Abdel Fattah al-Sisi’s rose to power, the new regime has turned a page in working with the internet, having realized the importance of modernizing its arsenal in order to be able to deal with

1 Hossam Bahgat, “Looking into the Latest Acquisition of Egyptian Media Companies by General Intelligence,” *Mada Masr*, 20/12/2017, accessed on 22/10/2020, at: <https://bit.ly/35VoO4n>



online threats. The Egyptian president has frequently expressed his annoyance at free cyberspace. During a meeting with a number of “intellectuals,” he threatened to “get two battalions to enter the net and turn it into a closed circle. The media people can get their news [...] exclusively from us.”⁽²⁾

Although it is difficult to decipher what the president actually meant, his attack on social networking sites was likely due to the variety of news and sources available, threatening that the exclusive source of news in Egypt: the ruling regime. It appears that his flat diagnosis of the problem resulted in failure over the years. By the end of 2015, Sisi had added website blocking technology to his arsenal through a UAE sponsored contract with the French company Amesys, despite French President Francois Hollande having pledged that it would not sell digital weapons to authoritarian governments.⁽³⁾

While its control over local media has been secured through private companies owned by the intelligence services, the regime has also blocked web access to various news outlets, including the London-based digital newspaper *Alaraby Aljadeed*. This policy of censorship has not been easy to implement, however. Firstly, the average internet user with basic technical skills can employ numerous methods to bypass the blocks on news sites, leaving it ineffective against a large proportion of citizens. Secondly, Egypt lacks the necessary infrastructure to provide effective digital alternatives to global services blocked by the state.

The independent news site Mada Masr provides a good example of the ineffectiveness of blocking. Journalists have used various means to continue providing their coverage to readers. They publish entire articles on Facebook, the same site that millions of Egyptians rely on to communicate and on which thousands of sellers, marketers and others rely on to make a living. Given the state’s lack of a local, controllable alternative, blocking Facebook is not only difficult but could negatively affect the country’s economy. Mada Masr also provides another version accessible to citizens inside Egypt, difficult to block because it is linked to one of Google’s search engine services.⁽⁴⁾

Of course, this is not to deny that censorship has greatly affected the volume and content of independent journalism on the Internet, but rather to say that blocks (alone at least) cannot achieve the state’s goal of preventing the internet from playing a role in public opinion formation. Technical problems aside, the philosophy behind censorship remains deficient. It fails to understand that the problem lies in the absence of the nation-state’s authority within cyberspace itself. The Internet provides citizens with a space in which they can express themselves freely and anonymously, away from the state’s ability to discipline and punish. The state ideology is unable to control the thoughts of citizens during their daily cyberspace journey, during which they are exposed to a huge amount of information and transnational ideas.

2 Mahmoud Al-Waqi, “Facebook under Attack by Sisi and Members of Parliament,” *Al-Masry Al-Youm*, 17/4/2016, accessed on 22/10/2020, at: <https://bit.ly/37v3swZ>.

3 Olivier Tesquet, “Amesys: Egyptian trials and tribulations of a French digital arms dealer,” *Télérama*, 5/7/2017, accessed on 22/10/2020, at: <https://bit.ly/3mbCoH7>.

4 Mohamed Tita, “Beating the Block: Mada Masr Launches Tor Mirror,” *Mada Masr*, 25/12/2019, accessed on 22/10/2020, at: <https://bit.ly/35CT3Np>.

Second Strategy: Misinformation and Fake News

The regime seems to understand that blocking techniques may harm cyberspace and neutralize some players, but many online actors remain effective as long as the Internet is connected to global spaces, and therefore the regime has tried instead to manipulate public opinion on the Internet. Numerous media reports refer to so-called “electronic committees,” groups affiliated with the Sisi regime that promote his views on the internet, especially social media. But I would like to focus here on the Egyptian company the activity of which was suspended by Facebook in early August 2019 called “New Waves.” According to the official Facebook statement, this company, in cooperation with one called “Newave” in the UAE, were promoting fake news to shape public opinion to suit specific political agendas in a number of Arab countries, favourable to the Sisi regime in Egypt and hostile to Qatar and Turkey.⁽⁵⁾ The Egyptian company is headed by a former army officer who ran a number of different pages on Facebook and Twitter that reached millions of Egyptians, usually providing fabricated news and shaping political opinions through a battery of memes and funny videos.⁽⁶⁾

Although the company tried to revive its activities, Facebook shut it down again in March 2020. Based on my analysis of data that Facebook made exclusively available to researchers and political decision-makers, I have been able to identify three out of five people working in the company, including the army officer and the former director of the company. They have quickly moved to work as social media managers for other state agencies, such as the National Council for Women. But the Sisi regime has enjoyed little success in its plan to shape public opinion through fake news, which has been dealt successive blows by Facebook and Twitter.

Third Strategy: Blockade

Successive waves of outrage have begun on social media before making the transition to reality, and attempts to stop this transition have failed repeatedly. Perhaps the most important of these failures are the events that followed the issue of the cession of the Tiran and Sanafir Islands to Saudi Arabia, in addition to the September 2019 protests triggered by contractor and dissident politician Muhammad Ali who testified about his relationship with the Egyptian regime through videos he published on Facebook. The Sisi regime used one of the intelligence-owned channels to delete the video from the Internet, claiming that the intellectual property rights belonged to this channel. This reaction in turn sparked citizens’ interest in the video and led them to follow Ali, who then filmed a second and third video, and simply carried on.

5 Nathaniel Gleicher, “Removing Coordinated Inauthentic Behavior in UAE, Egypt and Saudi Arabia,” *Facebook*, 1/8/2019, accessed on 22/10/2020, at: <https://bit.ly/3jke1oQ>

6 Mostafa Elsayed Hussin, “The Story of the Egyptian Company whose Pages Were Shut Down by Facebook,” *Sasa Post*, 5/8/2019, accessed on 22/10/2020, at: <https://bit.ly/3koRwAG>.



On 21 November, the Egyptian Attorney General's Decree 2376 of 2019 formed a bureau to create accounts on social media and act as a "control tower for cyberspace." Michel Foucault's writings speak about the power of the nation-state to use discipline and punishment to control the thoughts of citizens. For Foucault, prisons are not only an isolated place inhabited by criminals, but they reside as an idea in the minds of citizens, which gives the state sufficient power to normalize certain behaviours in society. This is exactly what the government seeks from its latest strategy to neutralize cyberspace in the public domain. During the past year, this bureau, along with the National Council for Women and other (theoretically) independent, state institutions have intensified their interaction through social media, during which these bodies engaged with and, in some cases, directly shaped public opinion.

The bureau became infamous following the case of the TikTok girls, as they were known in the media. The Attorney-General's Office ordered the arrest of several young women on charges of "violating the values and principles of the Egyptian family and society." In April 2020 the office's webpage published a statement drawing upon the features of the new strategy of the Egyptian state to impose its authority over control and punishment through cyberspace.

According to the statement, this case has created a fourth (cyber) border for the Egyptian nation-state alongside the traditional air, sea and land frontiers. The Attorney-General believes that these borders "inevitably lead us to radical changes in the policy of legislation and administrative and judicial controls, as we are facing new cyber borders whose scope is online. This requires deterrence and precautions to guard it, like other borders."⁽⁷⁾ The new bureau was to serve as this border guard.

The bureau subsequently instigated several cases that targeted content creators on social media. The exact nature of the cases brought against these influencers differed – whether based on their anti-regime political views, or because they violated what the prosecution considers the principles and values of the Egyptian family. It also engaged with a number of issues that occupied public opinion on these sites, such as rape and sexual harassment cases, about which testimonies were published anonymously on the Internet. The National Council for Women accounts also engaged with these issues.⁽⁸⁾

Regardless of how we assess the positive solutions to these issues provided for by the authorities, what we are interested in here is the strategy that these parties have pursued through these issues to create collective awareness of extending the state authority over control and punishment beyond tangible boundaries to include cyberspace as well. The state is trying, through this strategy, to normalize a behavioural model that makes citizens think twice before sharing publicly online.

7 "Facebook Contradictory Acts and Human Trafficking ... a New Verdict against Egyptian Haneen Hossam," *Al-Hurra*, 9/5/2020, accessed on 22/10/2020, at: <https://arbne.ws/31wrsfc>.

8 See, for example: "The Fairmont Crime ... the National Council for Women Calls on Survivors to Communicate with It," *Egypt time*, Alaraby TV, accessed on 22/10/2020, at: <https://bit.ly/2HrCbRf>.

Using the analogy of the famous Panopticon prison model, it can be said that the Attorney General's office operates as a central watchtower.⁽⁹⁾ In theory, social media websites cannot be blocked nor can everything posted on them be monitored, but as with the Panopticon, where inmates do not know when they are specifically monitored, the randomness of targeting in these cases is also an important factor in creating this feeling among citizens.

Fourth Strategy: Digitization

The Egyptian state is also trying to impose digitization through its various agencies, as well as developing internet and communications infrastructure; many online services are now available to citizens. In May of this year, the government launched a program of government payments with banknotes, coinciding with the launch of prepaid cards for government services (Miza). This rapid digitization will give the Egyptian state an advantage, better equipping it to monitor citizens in cyberspace and to provide alternative services as censorship becomes more effective. The Egyptian state has already started building its own platforms and applications outside the realm of government services, such as the Watch.it app for movies and programs.

This is not to criticize digitization but rather to analyse the political power that the Egyptian state possesses. Power is not necessarily evil and analysing it does not necessarily mean destroying it either, as Foucault tells us.⁽¹⁰⁾ However, analysis does allow us to view the digitization process from another angle, reminiscent of the colonial reforms undertaken by the British occupation in Egypt during the nineteenth century, such as the establishment of the railways, the construction of roads and so forth.

Fifth Strategy: Legal Arsenal

Finally, the Egyptian state has recourse to an arsenal of laws passed by the 2015 parliament that aim to censor cyberspace. Perhaps because the Sisi regime typically treats parliament as a cosmetic rubber stamp for whatever laws it wants to pass, this facet of its strategy is often overlooked. Although the state started blocking websites without any statutory sanction, it has since been given a range of new internet powers in legislation.⁽¹¹⁾

The most important of the new statutes is the Media and Press Regulation Law, which has created critical obstacles to establishing a website, as well as designating the operator of any account that

⁹ Imaginary prison, proposed by the English philosopher and social theorist Jeremy Bentham, which is a circular prison with a tower in the center. The guards in the tower can watch all the prisoners but they cannot watch them all at the same time, but the prisoners behave well all the time because they do not know whether the guards are watching them or not at a given moment.

¹⁰ Nickolas James, "Law and Power: Ten Lessons from Foucault," *Bond Law Review*, vol. 30, no. 1 (2018), p. 31.

¹¹ Hassan Elazhary & Mohamed El Taher, "Occasionally by Decree... Update on the Block of Websites in Egypt," *Freedom of Thought and Expression Law Firm*, 18/5/2018, accessed on 22/10/2020, at: <https://bit.ly/3jlli6X>.



has more than five thousand followers as a part of the media. Also important is the Cybercrime Law, which was ratified in 2018 and legalizes blocking websites for national security considerations, a loose concept left to the interpretation of investigation authorities.

Conclusion: The Egyptian Firewall as an Expression of Power / Resistance Relations

China has built up its “Great Firewall”; an arsenal of legislation and technology that allow the ruling Communist Party to monitor and control the internet in China. We can thus refer to these five strategies of the Egyptian state as the Egyptian Firewall, which may well expand further in the near future.

Historically analysing this firewall while it is still in the process of construction provides an opportunity to understand that it is not an expression of a totalitarian regime’s monopoly over discipline and punishment in cyberspace, but rather an expression of the continuous relationships of power/resistance between internet users and this regime. The failure of the regime to achieve its goal of web control through one strategy has created a power structure distributed across the hierarchical system of various state agencies, including the media, the judiciary, and the intelligence services. It also elicits a reconsideration of the importance of free and anonymous cyberspaces.