TECHNOLOGY & LAW COMMUNITY

Blocking Websites in Egypt
“Techniques and Laws”

https://masaar.net

TECHNOLOGY & LAW COMMUNITY

Masaar-Technology and Law Community

May 2021

Masaar.net

Blocking Websites in Egypt
"Techniques and Laws"

Background:

Previously, "Massar – Technology and Law Community" has issued several publications related to internet censorship and blocking of websites in Egypt, which can be accessed via the following links:

- **A timeline of internet censorship events in Egypt.**
- **Blocked websites in Egypt**
- **Press and Human Rights Websites Blocked in Egypt Using Sandvine Equipment**
- **Analytical Summary | The last Square? ... Systematic censorship of the Internet claiming protecting morals.**
- **Internet Censorship in Time of Social Distancing**

Introduction

This report focuses on the practice of censoring websites through blocking them in Egypt. First, the report presents the relevant legal environment, including the confirmation of the Egyptian judiciary to judicial precedents allowing websites to be blocked, and laws containing articles that allow the authorities to exercise blocking, such as Anti-Terrorism Law No. 94 of 2015, and the Law to Combat Information Technology Crimes and the Law on Regulating the Press and the Media.

The second section of the report deals with explaining website blocking tactics, such as IP blocking, Internet Protocol (TCP / IP) packet, blocking based on domain name system (DNS) blocking, and Deep packet inspection. The section also deals with the use of these tactics which are among the most common methods associated with blocking websites in Egypt, in addition to explaining how (TCP rest attack) works and the use of Deep Packet Scan to block websites via (Reset Connection).

The report also presents an account of some of the most important incidents of Internet censorship and blocking of websites in Egypt during the past years.

First: Legal developments related to blocking:

Many legislations and judicial rulings in Egypt set the rules and principles of imposing different ways to control visual, audio and readable content.

There were no legal texts regulating the process of blocking websites before 2015, so the practice of blocking websites has started by judicial jurisprudence and the use of communications laws to justify the practice, then it has evolved to passing some rules that allow the judicial authorities to impose the blocking process, according to some exceptional controls, such as blocking under the Anti-Terrorism Law, however, such exceptional rules were not enough to apply the blocking process on a large scale, so the Egyptian authorities have crossed over the crises of passing laws and started practicing the blocking process without legal cover, or the issuance of official announced decisions. By time, the blocking of websites has become the norm that users encounter on a daily basis.

Later, the authorities started the passage of a number of basic legislation and implementing regulations that regulate the blocking process.

The Egyptian judiciary approves judicial precedents allowing the blocking:

The practices of the executive authority were not the only reason for establishing the rules related to blocking, where the judicial authorities have contributed to consolidating this practice, through the wrong interpretation of the texts of the Law No. (10) of 2003 promulgating the Telecommunications Regulatory Law, and trying to find a legal justification through which a legal justification for the blocking of content could be found.

During the period between 2011 and 2015, there was no legislation that explicitly addressed the possibility of blocking or explained the authority of the administrative authorities and other law enforcement agencies to block websites.

In 2012, an Egyptian lawyer filed a lawsuit before the Administrative Court, demanding to bind the National Telecommunications Regulatory Authority and the Ministry of Communications and Information Technology to block YouTube and all links showing what was known as "the offensive movie to the Prophet" and links displaying "anti-Islam" videos.

And after the lawsuit has been deliberated, the Administrative Court issued its ruling, in 2013, by blocking YouTube for a month and blocking all links showing the offensive movie to the Prophet. The Egyptian judicial authorities adopted wrong interpretations of the provisions of Articles (64) and (67) of the Telecommunications Regulatory Law, through which it was able to find a legal justification, to compel the administrative authorities to block content, by expanding the interpretation of the concept of national security and the need to protect it.

The legal texts – from the Telecommunications Regulatory Act – that have been relied upon bind the service providers to provide the technical capabilities in terms of equipment, systems, programs and communications within the communication network to allow the armed forces and national security agencies exercising their competencies.

These texts also allow these security agencies to make all telecommunications services and networks subject to their management, in the event of a natural or environmental disaster, or in cases where general mobilization is declared, or any other situations related to national security .

The provisions of the law have not specified the nature of those technical capabilities or the controls for their use. The law has not included a clear definition of the concept of national security either.

Therefore, the court expanded on the interpretation of that concept, which extended to include what has been called " social national security", and the need to protect it and prevent what might pose a threat to it.

[1] - Relevant provisions of the Telecommunications Regulatory Act

The court has reached a judicial precedent that obliged the administrative authorities to take blocking measures according to the Telecommunications Regulatory Law.

Therefore, the courts that deliberated the lawsuit sought to block YouTube and links to the offending movie to try to define the concept of national security, where the courts have expanded on its interpretation, to the extent that showing the offensive film harmed " social national security ". The Supreme Administrative Court has also called - during the appeal against YouTube's ruling - to the necessity of enacting legislation that prohibited and criminalized all broadcasting - whatever its means - that would harm the religious beliefs and constants of the Egyptian people, in order to preserve social peace and the unity of the national fabric .

The Anti-Terrorism Law regulates the blocking process for the first time:

In 2015, the Anti-Terrorism Act which organized the blocking of websites for the first time, was passed, where the law granted authority for the Public Prosecution or the competent investigation authority to stop or block websites , if the site was "created for the purpose of promoting ideas or beliefs, or called for terrorist acts or broadcasting", or aimed to mislead the security authorities or influence the course of justice in any terrorist crime, or took over exchanging messages and issuing assignments between terrorist groups or their affiliates, or information related to the actions or movements of terrorists or terrorist groups at home and abroad .

[2] - Court rulings mentioned above

Extending the practice of blocking without legal justification:

During the last four years, the practice of blocking websites has increased, and no official body has claimed responsibility for such practices, since there were no announced decisions through which one can read about their legality or oversee the extent of their legitimacy. That common style of practice was aimed mostly at consolidating the concepts of illegal procedures with the aim of preparing public opinion to gradually accept them, hence, facilitating the legalization of those practices by passing unconstitutional rules of law, that would impose restrictions on fundamental rights and freedoms.

As the Egyptian authorities began to use blocking systematically in May 2017, they blocked nearly 22 websites and expanded the blocking application dramatically.

[2] - Court rulings mentioned above

[3] - Article 49 of Law 94 of 2015 Anti-Terrorism Act: With regards to the crimes set forth in Articles (19) ,(15) ,(12), and (22) of this Law, the Public Prosecutor or the relevant investigating authority, according to the case, shall issue an interim order to close headquarters, premises, housing, and residencies, provided a decision is issued by at least a chief prosecutor. Luggage and furniture seized shall be considered items seized administratively as soon as they are seized until a final decision is issued in the case. After an inventory is prepared and they are recorded in a report, they shall be handed over to the guard assigned to guard the seals placed on the closed headquarters, premises, housing, and residencies. In the event they were no seizures, he shall be assigned to guard the seals in the same manner. The issuance of a verdict of acquittal shall result in the abolition of the closure order. The Public Prosecutor or the relevant investigating authority shall stop the sites provided for in the first paragraph of Article (29) of this Law, block them, or block their content to prevent any aspect of use set forth in this Article. It shall also retain the devices and equipment used in the crime.

[4] - Article 29 of Law 94 of 2015 Anti-Terrorism Act: Whoever establishes or uses a communications site, website, or other media for the purpose of promoting ideas or beliefs calling for the perpetration of terrorist acts or broadcasting material intended to mislead security authorities, influence the course of justice in any terrorist crime, exchange messages, issue assignments among terrorist groups or their members, or exchange information

Blocking Included as a basic rule in new legislation:

The authorities were able to legalise the practices that began in 2017, by including the blocking of websites in various legislations, where the blocking was stipulated in regulatory and penal legislation under different legal interpretations. Examples of such legislations were the Anti-Cyber and Information Technology Crimes Law, and the Law Regulating Media and the Press.

A. Blocking as a procedural measure to protect national security in the Anti-Cyber and Information Technology Crimes Law

Cybercrime Law No. 175 of 2018 was issued in August of 2018 to regulate cases in which blocking can be applied as a primary measure. The law gives the investigative authorities the power to issue a decision to block websites whenever they see that the content posted on these websites constitutes a crime or threat to national security or endangers the country's security or national economy.

The law also gives the police authority in case of urgency and necessity to request blocking websites before a court ruling is issued.

The authority to block shall exist whenever there is evidence that a website inside or outside the country has posted any texts, numbers, pictures, movies, or any propaganda material, constituting a threat to national security or endangering the security of the country or its national economy .

relating to the actions or movement of terrorists or terrorist groups domestically and abroad shall be punished by imprisonment with hard labour for no less than five years. Whoever unduly or illegally accesses websites affiliated with any government agency in order to obtain, access, change, erase, destroy, or falsify the data or information contained therein in order to commit an offense referred to in the first paragraph of this Article or prepare it shall be punishable by imprisonment with hard labour for no less than ten years.

B. Blocking as an administrative penalty in the Law Regulating Media and the Press and its implementing regulations:

The Law Regulating Media and the Press No. 180 of 2018 was issued to give broad powers to the Supreme Council of Media Regulation that allow it to impose various forms of censorship on websites and personal pages .

Article 91 of the law gives the council the authority to take appropriate action in case of violation and for this purpose, it is entitled to: stop or block the website, the blog, or the account if any of them publishes or broadcasts false news, or what advocates or incites to violate the law or to violence or hatred, or that involves discrimination between citizens, or calls for racism, intolerance or includes breach of individual honour or insulting or defaming them, or insulting the religions or religious beliefs.

The executive regulations of the Law Regulating Media and the Press and the sanctions approved by the Supreme Council of Media and Press Regulation have also approved the controls related to blocking websites and private accounts on social media.

5 - If there are evidences that a website broadcast, inside or outside the State, is displaying words, numbers, images, films, any publicity materials or other, that would be an offence of those stipulated in the present Law, jeopardize the national security or economy, the concerned investigation body may order to block the website(s), subject matter of broadcasting, where applicable from the technical point of view. The investigation body shall submit the blocking order to the competent court, held at council chamber within twenty-four hours along with a memorandum of its opinion. The court shall issue its decision on the substantiated order, either by admitting or dismissing such substantiated order, in no more than seventy-two hours as of the date of submitting the substantiated order to the court. In case of summary matters due to a current risk or imminent harm, the inquiry and law enforcement bodies may notify the AUTHORITY which shall immediately notify the Service Provider of the temporary blocking of the website, content, websites, or links set out in the First Paragraph of this Article and in accordance with its provisions. Upon its receipt, the Service Provider shall implement the content of the notice. The inquiry and law enforcement body that gave the notice shall file a report establishing the procedures made in accordance with the provisions of previous Paragraph. Such report shall be submitted to the investigation bodies within forty-eight hours as from the date of notice given to AUTHORITY. Regarding this report, the procedures set out in the Second Paragraph of this Article shall be applied. In this case, the competent court shall issue its decision, either by admitting or dismissing the procedures of blocking.

If the report set out in the previous Paragraph is not timely submitted, the blocking shall be deemed null and void. During the consideration of the action or based upon the request of the investigation body, AUTHORITY or relevant parties, the trial court shall issue an order terminating or amending the scope of the blocking decision. In all circumstances, nullification of the block decision shall take place by issuing a criminal lawsuit dismissal order or a final judgement of acquittal.

Second: Techniques for blocking websites in Egypt

This section provides a technical explanation of the techniques to block the most common websites in Egypt, and we have relied on this part of the report on:

- Egypt's figures published on OONI Explore website, compiled with Probe-CLI software and the Domain List developed by Citizen Lab and OONI, which Massar – Technology and Law Community has helped develop over the previous months.
- Reports issued by Massar and local and international organizations interested in the situation of Internet freedom in Egypt locally and internationally.
- Tools that help in running TCP connection tests for websites and IP addresses blocking, such as Telnet, Curl, and NC.
- Tools that help in making the Reverse DNS lookup for DNS audit such as: nslookup, Dig, and Host.

1- How To Perform IP and TCP / IP Blocking:

Each device – connected to any network – carries the Internet Protocol (IP) address, which acts as a digital identifier for the device.

This device can be a computer, a printer, a mobile or any other device connected to the Internet or any network using the TCP / IP protocol.

There are two types of (TCP / IP) protocols; the first is the fourth version, which is the most popular one, and it consists of 32 bits and is written in the form of numbers separating each point number (.), while the second is the sixth version which consists of 128 bits and is written in the form of groups separated by the symbol (.).

The Transport Control Protocol (TCP) is one of the fundamental protocols in the Internet protocol stack, since it is responsible for transferring data between two or more devices connected to the Internet. Major Internet applications (such as e-mails, websites, and file transfer services) depend on such protocol.

Every website online domain carries an IP address, referring to the server on which the website is hosted, for example the domain (Masaar.net) carries an Internet protocol address (104.21.78.86), and when the user uses the Internet browser to browse the website (Masaar.net), the Internet browser searches for the IP address corresponding to the domain the user wants to browse.

Such process is performed through the Domain Name System (DNS), which is the system responsible for storing information related to domain names, in a database that contains the data needed to associate protocol addresses with different domain names.

Entities responsible for managing and operating communications and Internet service providers can block websites by blocking the IP address and IP packet, so that the flow of data to and from a specific IP address or port is prevented.

A port is a number attached to the Internet Protocol is used to distinguish the different services on the same server so that this server can provide more than one service.

In the case of blocking a website by blocking the IP address and IP packet, when the user requests browsing a specific website; The Internet service provider prevents the users from accessing that specific IP address, and the Internet service provider may prevent the use of a specific port in order to prevent a specific service, such as virtual network services (VPN), for example.

Blocking based on IP and TCP/IP blocking is relatively weak, as websites and services that are blocked through such method can easily change the IP address, and the spread of content delivery network services. Also, the widespread of content delivery network services defeats this type of blocking.

Content delivery networks are a group of servers distributed in different geographical locations containing copies of websites, so that when a user in a specific geographical area requests browsing a website that uses this feature, the content delivery network sends it to the nearest server so that the browsing becomes fast.

2- DNS Blocking:

As previously mentioned, the domain name system (DNS) is a database that stores information related to domain names so that the Internet Protocol address and the domain name can be linked.

This database is stored on central servers called (Root name servers) that contain the complete database of domain names and addresses, and their internet protocol. Internet service providers also use Recursive DNS Servers for the DNS that contains a copy of the DNS database, to improve the efficacy and speed of the domain name search process.

When the user requests the Internet browser to access the domain name of a specific website (masaar.net for ex.), the browser asks – on behalf of the user – the server (Resolver) to send inquiries regarding the information in the domain name system and send it to the user machine. Such inquiries result in the translation of domain names into an IP address.

When the Internet service provider uses a blocking technique based on DNS blocking, the Resolver server will investigate if the website requested by the user is blocked, and when the user requests to enter a blocked website, the Resolver server delivers incorrect information and thus the user cannot complete the process of accessing the website.

3- Blocking based on (Deep packet inspection)

Deep packet inspection is an advanced technology that can be used by Internet service providers to inspect the content of data packets and manage their network traffic.

When Internet service providers (ISPs) use blocking based on deep packet inspection, the service providers will have the ability to see the data traffic between the user and the Internet servers through computers prepared for this, to prevent the user from accessing a website or specific services such as VoIP services. This blocking technique is not effective if the connection is completely blind.

HTTPS

There are many protocols on which the Internet relies for data transmission, such as (HTTP, FTP, VoIP). At the beginning, the Internet relied on the Hypertext Transfer Protocol (HTTP) to transfer website pages. HTTP works through a set of actions that an Internet browser performs by sending the user request to the server, which in turn responds to the browser request with the required content, and then the user receives the required content.

HTTP does not provide encryption during the transfer of data between the user and the server, so a Secure Socket Layer-SSL protocol was developed that worked in coloration with the (HTTP) so that it secures the data during movement between different parties on the Internet, where it encrypts all communication without user intervention while using any SSL Internet service.

Later, the Transport Layer Security-TLS protocol was introduced to succeed the Secure Socket Layer-SSL protocol as a standard encryption protocol used and installed on already existing data transfer protocols such as (HTTP, FTP).

The most common use - and most important in the context of this report - is the use of the (TLS / SSL) protocol with (HTTP) to access Internet pages to provide a more secure and encrypted version, which is known as the (Hypertext Transfer Protocol Secure-HTTPS). A user can detect if a website depends on such protocol by checking the website address, so if it starts with (HTTPS) then it uses the protocol and if it starts with (HTTP) then it does not.

How Does HTTPS Work?

To encrypt the communication between the server and the user, the SSL/TLS protocol uses an algorithm that relies on generating two pairs of keys; one public key and a private key, and they are generated so that each key is unique and cannot be duplicated.

Any party can send data that is encrypted using the public key and this data can only be decrypted using the private key associated with the public key. To perform both the encryption and decryption processes; The SSL/TLS protocol uses an authentication certificate (Public key Certificate) to bind a pair of encryption keys to the identities of websites, so that a process called (Digital Signature) can be performed through which the identity of websites is authenticated to prevent any server impersonating another server identity in order to deceive the user. Certificates contain the public key, an electronic signature, and information about both the identity associated with the certificate and its issuer (Certificate Authority).

There are many entities that issue digital certificates (Certificate Authorities). Such entities issue digital certificates for use by third parties (such as owners of websites), so that the certificate issuing authority guarantees that its public key is owned by a specific institution or website.

If a certificate presented by a website using HTTPS protocol was signed by a trusted Certificate Authority to issue digital certificates, users can be sure of the identity of the site since it has been verified by a trusted and verified third party.

How to use Deep Packet Check to block websites in Egypt

In general, this technique depends on deep packet inspection technology to intercept the largest amount of (unencrypted) data traffic across the network, analyze it, then extract information from it such as the protocol used, the connection destination, and refer to the name of the server (Server Name Indication-SNI) containing a value indicating the name of the domain that the client (user) is trying to access.

Detection Of Website To Be Blocked

At the beginning of establishing the connection between the server and the client (internet browser), a process called handshake is performed, which is responsible for setting the rules that will be relied upon for communication between the server and the client before the start of the connection, so that some metadata is sent in an unencrypted form (Plain/text), including referring to the (Server Name Indication-SNI), which carries the name of the domain to be accessed.

The importance of indicating the (Server Name Indication-SNI) is to ensure that the server sends the certificate for the domain name, especially in case of hosting other sites and domains on the same server.

For various considerations, most important of which is the nature of the infrastructure supporting the applications and services on the Internet, for example, cloud computing services such as Google Cloud Platform and AWS, the reference to (Server Name Indication-SNI) a key factor on which a successful HTTPS connection depends to determine the encryption keys needed for a successful connection.

Server Name Indication-SNI is a major goal for censorship and blocking operations based on Deep packet inspection, as it is used to identify the communication between a specific server and the client(s) and in turn the communication between them is interrupted by the use of TCP reset injection.

How Is TCP Reset Injection Used To Break Communication?

We have previously discussed Transport Control Protocol (TCP); the protocol that controls and organizes traffic throughout the network in the form of packets and metadata between the server and the client.

TCP also ensures that data packets arrive through the connection properly and re-send any lost or corrupted data.

Each data packet includes a set of headers/flags, that are used to organize the traffic between the communication parties in different scenarios. The flags in each data packet include a (RST flag). Under normal circumstances, RST flag is used to inform one party of the communication that there is a problem with the other so that it stops to send/receive data.

In most Web Traffic, RST flag is assigned a value of 0 and has no effect. If it is set to 1, then the TCP communication should immediately stop.

When using (TCP reset attack) with the aim of blocking websites, the ISP launches an attack by shooting fake metadata containing an RST flag with value 1, causing the connection to terminate from one of its parties and to be considered a failed connection.

Third: The Egyptian authorities continue to block them

This section of the report deals with some incidents of Internet censorship and blocking of websites, which were confirmed during the previous period.

Discovering Middle Boxes In Some Cases

In September 2019, demonstrations broke out in Egypt, and the Egyptian authorities arrested a large number of demonstrators in addition to multiple random arrests, and as a result, the Egyptian authorities blocked websites and instant messaging applications.

Blocking AlHurra and BBC

A report issued by OONI indicated that the Egyptian authorities in September 2019, blocked both websites of AlHurra and BBC.

The report monitored that many measurements collected from Egypt on the BBC website showed TLS errors on the Egyptian Telecom Company network (AS8452), Orange Egypt Network (AS37069), and other measurements collected from Vodafone Egypt (AS36935) also showed a timeout error when trying to obtain website content.

The measurements have strongly indicated a form of deep packet inspection (DPI) technology dealing with TLS and is likely the signature of the SNI field of the TLS handshake.

Also, measurements collected by Massar from Egypt indicated that AlHurra website has been blocked in Egypt, as these cases were observed on two tested networks; Vodafone Egypt (AS36935) and Telecom Egypt (AS8452).

Measurements collected during September 2019 from Egypt indicated that Egyptian internet service providers were resetting the connection through the use of DPI equipment.

Blocking Instant Messaging Applications

Measurements collected in September 2019 showed that the Egyptian authorities tried to block the websites of popular instant messaging apps, especially those that offer an encryption feature, where 14 websites of popular instant messaging applications have been blocked as follows;

On Vodafone network: wickr.com, signal.org and wire.com

On We network: wechat.com, line.me, surespot.me, pryvatenow.com, skype.com, icq.com, groupme.com, kik.com, voxer.com, zello.com, trillian.im

By checking related measurements to the website of Wire application and the domains that the application uses to run its services, it was found that the application uses the following domains:
https://prod-nginz-https.wire.com
https://prod-nginz-ssl.wire.com
https://prod-assets.wire.com
https://wire-app.wire.com
https://clientblacklist.wire.com

The measurements gathered from Vodafone network showed that the aforementioned domains were blocked, and that another set of Wire.com subdomains have been also blocked:
https://pwa.wire.com
https://wire-docs.wire.com
https://services.wire.com
https://teams.wire.com
https://support.wire.com

Blocking access to Twitter

In September 2019, many Egyptian users reported that they were unable to use the Twitter application on mobiles through mobile Internet (4g/3g), and it is likely that the Egyptian authorities had tried to block Twitter on Vodafone network or at least attempted to throttle access to Twitter (throttling).
Testing the Twitter app on Android, it was found that it uses the following IP addresses:
104.244.42.1
104.244.42.2
104.244.42.3
104.244.42.65

The IP address (104.244.42.65) refers to the domain twitter.com, and it was found that this domain is blocked, and measurements collected by UniProp showed the presence of DNS Tampering. The IP address (104.244.42.65) refers to 6 domains, all of them were Blocked;

jhpath.com

twitter.com

twitter.eus

twitter.hk

twitter.jp

twitter.org

It was also found that the IP address (104.244.42.1) is blocked (DNS Tampering), which is an address that refers to 5 domains, all of them blocked:

equity-app.com

milchreis.xyz

twitter.com

twittertrademarks.com

Twopensource.com

Attempts to block Facebook Messenger

In September 2019, many users reported that they were unable to use Facebook Messenger application on some mobile Internet networks, as users got a "Waiting for network" message on the Messenger application on Android and "Messenger is currently unavailable" on computer web browsers.

It is likely that the Egyptian authorities tried to block Facebook Messenger (messenger.com) on Vodafone (ASN: AS36935) and We (ASN: AS8452) for several hours on September 23rd, 2019, before it worked again.

AMP blocking

The "AMP (Accelerated Mobile Pages) Project" service is a technology to improve the performance of websites pages on mobiles to provide a convenient experience for smart phone users, as the project provides an open-source tool that enables Internet publishers to increase the speed of downloading and browsing through smart phones. The technology also provides the websites an interface suitable for smartphones regardless of the different screen sizes of mobiles and tablets. These features can also useful for traditional computer-oriented versions of websites.

In February 2018, many of the blocked press websites in Egypt were using the AMP service in an attempt to find easy mechanisms to reach their audience, such as relying on alternative platforms to publish the content of the blocked websites, since (AMP) service shows alternative links to the original links in the search results on Google search engine referring them to other links from Google domain, hence in the event that a blocked site appears in Google search results and it uses mobile phone pages, (AMP) will direct the user to an unblocked page.

This is the method adopted by some blocked websites in Egypt, where the links produced by AMP and published on social media networks to reach the audience without having technical experience would enable them to bypass the blocking And after the spread of this mechanism to counter blocking, the Egyptian government resorted to blocking the service on February 3rd, 2018, which affected smart phone users coming from Google search engine for any website using AMP, as users were unable to access these websites, including websites that the Egyptian government has not blocked, hence blocking billions of pages using AMP technology, and accordingly, Google has announced the suspension of the service in Egypt.

Random blocking ... Blocking of websites based on IP and TCP/IP blocking: In April 2019, Egyptian authorities blocked the websites of the "Void Campaign"; a campaign launched by activists in conjunction with the constitutional amendments called for by the President of the Republic.

The campaign used the domain (voiceonline.net) for its website, which called for collecting signatures from citizens against the constitutional amendments.

The next day (April 9th), the campaign website was blocked after announcing the collection of 60,000 signatures rejecting the amendment of the constitution.

The website was blocked only 13 hours after its launch, which prompted the campaigners to change the domain name to avoid blocking and reach the public, just as all other alternative domains – up to 10 – launched by the campaign were blocked.

As mentioned in two reports issued by Netblocks Foundation and the Association for Freedom of Thought and Expression, there were thousands of websites that have been blocked due to the Egyptian authorities use of the technique of blocking websites based on blocking IP and (TCP/IP), because blocking one website (blocking protocol address) means blocking any other domain shared with it on the same server and with the same IP address.

The report issued by the Association for Freedom of Thought and Expression mentioned that the Egyptian authorities used the tactic of blocking websites by blocking IP and Internet protocol package for many websites such as Stock Exchange, Daily News Egypt, Fikr Tani, Egypt Daily News, New Arab and Arab Media Freedom Monitor, in addition to the Void Campaign website, which caused the blocking of thousands of other websites that share the same IP address.

Blocking Telegram

On October 22nd, 2020, "Massar" monitored the Egyptian authorities blocking of both Telegram website and application, on the three networks; We, Vodafone, and Orange. That was after many Internet users on the three networks had announced that they could not access Telegram.

Telegram is one of the most popular and widespread encrypted applications in the world.

Massar confirmed that users of the three networks – We (AS8452), Orange (AS24863) and Vodafone (AS36935) – could not access Telegram application on smartphones, as the Egyptian authorities blocked access to IP addresses.

The authorities also blocked the "Telegram" website itself (telegram.org), and the desktop (web.telegram.org).

The blocking also included internet networks connected to landlines (ADSL) and mobile internet (4G/3G).

Sandvine in Egypt

Massar conducted a series of tests on a sample of blocked websites in Egypt, to detect the use of "Sandvine" equipment to block such websites, and found out that 15 of the 20 websites (test sample) have been blocked by Sandvine equipment.

Massar conducted those tests on the Internet service provided by We network (AS8452), formerly known as TE Data, which is operated by Telecom Egypt, and the Egyptian government owns %80 of its shares.

(Citizen Lab) has published a documentary report about the existence of PacketLogic devices, and the report indicated that the (IPID) filed always carried the fingerprint "0) 13330x3412)", which matched the same fingerprint that the researchers found with "Citizen Lab" for one of the PacketLogic devices they purchased.

Sandvine PacketLogic is one of the equipment manufactured by Sandvine. Governments and telecommunications and Internet service providers use PacketLogic devices to perform Deep Packet Inspection-DPI, enabling them to monitor the Internet, block websites, tamper with user communication, monitor network traffic in real time, and filter network traffic, including websites, apps, and protocols (like P2P).

In March 2018, Citizen Lab published a report titled “Traffic Crisis” revealing the use of “Sandvine Pocket Logic” devices in Egypt, which were used to redirect users of many Internet service providers to ads and scripts for cryptocurrency mining.

On September 21st, 2020, Qurium Media Foundation published a report on the use of “Sandvine” to block AlManassa; an independent press website in Egypt.

While undergoing network data packet analysis tests for a sample of blocked websites on We network (AS8452) by (Tcpdump) program, we found out that 15 of the 20 websites (test sample) showed the same PacketLogic fingerprint “0) 13330x3412)” referred to in the report.

The following table shows 14 of the 20 websites (test sample) that we found to be blocked by (Sandvine PacketLogic):

Website	Domain	Category	IP Address
Nord VPN	Nordvpn.com	Identity Conceal tools	104.17.49.74
Tor Project	Torproject.org	Identity Conceal tools	95.216.136.36
ANHRI	Anhri.net	Identity Conceal tools	213.108.104.110
AlManassa	Almanassa.com	Media Outlets	83.68.31.235
AlAraby TV	Alaraby.tv	Media Outlets	152.195.32.173
Hibr	7iber.com	Media Outlets	104.26.10.93
Darb	Daaarb.com	Media Outlets	213.108.104.107
Raseef 22	Raseef22.net	Media Outlets	104.18.60.54
Arabi 21	Arabi21.com	Media Outlets	172.67.96.169
Moheet	Moheet.com	Media Outlets	35.231.141.67
Mada Masr	Madamasr.com	Media Outlets	104.26.15.160
Medium	Medium.com	Blogging&Hosting Platform	104.16.124.127
Masr Alarabia	Masralarabia.net	Media Outlets	138.201.47.90
Human Rights Watch	Hrw.org	Human Rights Issues	72.251.236.179

Conclusion

Over the past ten years, the Egyptian authorities have developed legal and technical mechanisms to block websites for reasons related to blocking political opposition, preventing the public from accessing certain information and opinions, or imposing censorship on some content for religious or moral reasons.

During such period, the authorities have developed their legal strategies; from arbitrary interpretation of laws regulating communications, to conservative judicial interpretations of legal concepts such as national security, to imposing censorship through exceptional legislation such as the Anti-Terrorism Law, ending with the legalization of permanently blocking websites in regular laws, either as part of the investigation procedures in cases related to what has become known as cybercrime, or as an administrative penalty against journalistic websites, through the Supreme Council for Media Regulation.

The development of the legislative environment to legalize the blocking of websites has coincided with the development of blocking techniques; from relying on IP address blocking and IP packet blocking, or blocking based on deep packet inspection, to the use of sophisticated techniques such as Sandvine equipment.

The authorities interest in imposing censorship on the Internet comes as the cyberspace constitutes a new dimension of what is known as the public sphere.

While the authorities succeeding to siege all outlets of opinion expression from newspapers, to political parties, to civil society organizations, to peaceful protest in its various forms; the cyberspace remained resistant to suppression for a not-short-time.

At the same, Internet was a source of concern for the authorities due to its decentralized nature and the difficulty of controlling the content published through it.

Activists were able to use cyberspace as an alternative to all other spaces that the authorities had confiscated for political, religious or moral reasons. Despite the continued effectiveness of Internet in Egyptian society, the monitoring efforts practiced by the state in particular since 2017 have prevented users from accessing at least hundreds of press, political and cultural websites, which has doubled the volume of violations against individuals in recent years in the areas of freedom of accessing information, freedom of opinion and expression, freedom of the press, as well as freedom to use the Internet.

TECHNOLOGY & LAW COMMUNITY

https://masaar.net