CENSORSHIP AND SOCIAL ACTIVISM IN THE MIDDLE EAST AND NORTH AFRICA

May 2011

A report for the BBC

BBC

TheSecDevGroup

Table of contents

Censorship before, during and after the protests: Country snapshots

List of tables

List of figures

List of boxes

Summary: Key takeaways for the BBC

This report examines how key countries in the Middle East and North Africa (MENA) used censorship and surveillance to repress social activism before and during the recent political upheavals of the Arab Spring. Its purpose is to provide the BBC with perspective on how internet services were affected by these events.[1] Key takeaways include:

BBC news is regarded as an important information authority for most MENA audiences: Ensuring access is vital. The BBC is one of the preeminent broadcasters in the MENA region, alongside Al Jazeera and Al Arabiya. Its news website is highly valued by Arab bloggers and the wider population, as indicated by site visits: it is the fourth most popular website for Arab bloggers to link to (after YouTube, English-language Wikipedia and AlJazeera).[2] User patterns during the recent protests – including large spikes in user numbers and page views – underline the importance of BBC as a news provider and fact-checker. Views of BBC Arabic peaked towards the end of January, when the uprising in Egypt was in full swing, with nearly two million unique visitors. When Osama bin Laden was killed in Pakistan in early May 2011, visitors flocked to the website.

Local, user-generated content is vital to authentic reporting in today's cyber-enabled world. Local bloggers, front-line videos of ongoing events, and local comments on broadcaster websites offer important perspectives on what is going on during times of political turmoil, especially in states where the traditional media are state-controlled or influenced. The Arabic 'blogosphere' is large and diverse, providing political commentary alongside discussion of human rights, religion and domestic issues. And YouTube, in particular has proven to be an important vehicle for informing both local and international audiences.

Local voices can be silenced: Develop a multi-faceted strategy for ensuring access. User-generated content – which relies heavily on access to an open internet and services such as Google's Blogger or YouTube – is vulnerable to state-imposed blocking and censorship, especially during times of political turmoil. **If the BBC wants to retain access to user-generated content during times of trouble, it is important to ensure that the ways of getting content to the BBC are clearly displayed on all sites.** This could include instructions for direct emailing, using circumvention technologies etc. The package of alternative communication pathways should be part of a defined "local access" strategy.

Take care around social media. Much information in the international media comes from social media sites, such as Facebook and Twitter, and from impromptu websites – such as when Iranian activists superimposed YouTube videos on a Google Map of Tehran to show where demonstrations were taking place. But information posted to social media sites should be approached with caution. While information may be accurate for a local area, it may not be representative of what is happening in a country overall. In addition, authorities can compromise open online communication, by waging information campaigns and targeting activists. Finally, undue international attention can create misleading assumptions about the role of social media in causing protests. In reality, offline communication – text messaging and phone calls – are just as, if not more, important in organizing action, even though they remain inaccessible to external observers.

You can be blocked: Develop a multi-faceted strategy for information dissemination. Broadcasters need to be creative and nimble when their services are blocked. For instance, Al Jazeera uses bloggers to feed information back into countries when their own signals are blocked. Devising a multi-faceted counter-blocking strategy is vital.

Circumvention tools provide one obvious pillar. Others include the creation of alternative channels for information dissemination and in-country networks to maintain a presence and influence and (see next two points).

Don't rely solely on the internet, and make sure your audiences know your alternative dissemination methods. While online dissemination is a must, it should not replace alternative and traditional channels. When the internet is blocked, audiences should know what their offlineoptions for access are. The campaign needs to start now: audiences need to know the options before it becomes necessary to use them. In the case of the BBC, this includes partner-delivered content, dial-in audio, text messaging, and other services. Beyond this, it is important to remember that not everyone can access the internet or mobile phones, with women and the poor being particularly vulnerable to exclusion in many countries. Overall, satellite television, and to a lesser extent radio, remain just as important as the internet.

Create and leverage in-country networks. In several countries in the MENA region, international reporters are routinely subject to restrictions and must take extra care to ensure they avoid conflict with the authorities. Covering protests is particularly dangerous, as can be seen from the detention of reporters[3] and the reported assaults that took place in Cairo during the revolution. While this should not discourage people from doing their jobs, having a strong network of local stringers and reporters who have better local knowledge and contacts is vital to ensuring safety for all concerned.

Country strategies, based on in-depth research, are necessary. Censorship practices, as well as the demographics of online populations, differ from country to country. To be successful, access and dissemination strategies need to be tailored to each country.

Introduction

The first few months of 2011 saw remarkable upheaval in the MENA region, as country after country erupted in nationwide protests and violence.[4] Regime changes in Tunisia and Egypt – the stalwart of the Maghreb – captured the world's attention. In Libya, the steeply rising death toll prompted a UN-mandated military intervention. Meanwhile other countries grew unstable including Yemen and Syria, where the respective death toll reached into the thousands.

Behind the flurry of banners and bombs, another fight was underway to control communications in cyberspace. As this report shows, Tunisia accelerated its blocking of websites while ordinary citizens used new media to report on the violence. Egyptian authorities invoked extreme censorship measures, including a near total shutdown of Internet Service Providers (ISPs). Libya turned off the internet, while rebels mounted a new "Free Libyana" cell phone network. Syrian authorities likely mounted man-in-the-middle attacks[5] against Facebook users and used its 'internet army' to attack, spam, and deface opposition and 'hostile' websites.

The struggle for cyberspace freedom should come as no surprise. Most MENA countries have a long-standing conflicted relationship with information and communication technologies (ICTs). While internet and especially mobile phone use has been growing rapidly in all MENA countries, most state authorities fear their social and political communication potential. As a result, most states in the MENA region operate censorship and filtering practices to varying degrees (see Table 1). These strictures do not go uncontested. Research conducted in 2008 found that almost two-thirds of Arab journalists thought that ISPs should not be legally enabled (or required) to block content; 55% did not agree that filtering was in any way beneficial to society.[6]

This report provides a brief overview of how cyberspace was leveraged by people and controlled by states during the recent political upheavals. It focuses on four countries in particular – Tunisia, Egypt, Libya and Syria – providing a shapshot of cyberspace-related policies and practices before, during and after the protests. Additional briefs are provided on Yemen, Saudi Arabia, Bahrain and Jordan.

Table 1. MENA countries at risk

	Country	Population (2010)[7]	Median age (years)[8]	Internet users (% of population)[9]	Mobile phone subscribers (% of population) (2009)[10]	Index of democracy (rank) (2010)[11]	Fragile state status (2010)[12]
No filtering	**Algeria**	35.4 million	26.2	13.6%	93.8%	Authoritarian (125)	Warning
	Egypt	84.5 million	23.9	21.2%	66.7%	Authoritarian (138)	Warning
	Lebanon	4.3 million	29.2	24.2%	96.2%	Hybrid regime (86)	Alert
Selective filtering	**Jordan**	6.5 million	22.8	27.2%	36.1%	Authoritarian (117)	Warning
	Libya	6.5 million	26.2	5.5%	77.9%	Authoritarian (158)	Warning
Substantial filtering	**Bahrain**	0.9 million	31.9	88%	199.4%	Authoritarian (122)	n/a
	Saudi Arabia	26.2 million	25.3	38.1%	174.4%	Authoritarian (160=)	Warning
	Syria	22.5 million	22.5	17.7%	44.3%	Authoritarian (152=)	Warning
	Tunisia	10.4 million	29.1	34%	95%	Authoritarian (144=)	Warning
	Yemen	24.3 million	17.8	1.8%	16.3%	Authoritarian (146=)	Alert

MENA's volatility and the internet's role

The dichotomy between old and new underlies the protests in the MENA region. Ossified regimes and conservative traditions have come into conflict with large dissatisfied youth populations – many of which are well-educated, under-employed and internet savvy. Information control has always been an important pillar of power for democratically-challenged states. The advent of the internet has shaken things up, by levelling the barriers to information production and communication. Now, anyone who is connected can (usually) get his/her message out.

The roots of instability in the region are found in a number of factors: the entrenchment of governing regimes; human rights violations; government corruption; extreme gaps between the rich and poor; rising food prices; unemployment; and, (importantly) the large and growing cohorts of educated but unemployed and dissatisfied youth.

Most protests centred on demands for governance reform. Many countries in the MENA region have been under one ruler or dynasty for decades – including the now-deposed Hosni Mubarak in Egypt, the Assad family in Syria, Ali Abdullah Saleh in Yemen, and the Al-Khalifas in Bahrain. Entire generations have never known a different leader. Nominal nods towards democratic reform have tended to yield little real change. For example, Egypt's first multi-candidate elections in 2005 returned President Mubarak with an 89% landslide. Throughout this event, the official state media remained under Mubarak's control and expressed identical opinions to his own throughout the campaign. Foreign election observers were banned, and the election was widely condemned as rigged.[13]

Many protestors came from the growing ranks of disenfranchised youth, causing some commentators to speak of a "youthquake." [14] There is an enormous youth population in the MENA region. The median age in Yemen is 18. In Syria, it is 22. According to Egypt's 2006 census, roughly 40% of its population was aged between 10 and 29. And, while educational availability and levels have been improving in many countries, the prospects for employment have not. In February 2011, Egypt's youth unemployment stood at about 25%, while Tunisia's hit 30%. Many observers consider the protests to have been fueled by the tension between rising expectations and a lack of government reform. Importantly, the youth populations are also the most common group of internet users in the region.

The internet (and cyberspace more broadly) played a notable role in the protests in many countries, enabling rapid, unfettered and anonymous communication. Key features that make cyberspace the friend of those advocating for change against entrenched authorities include:

Low barriers to participation and use. New media is user-friendly and a convenient medium for social activism. Actions taken online, whether blogs, video postings, or Facebook statuses, spread fast, and can usually reach a global audience -– particularly with the advent of social media websites. The Western media's reporting of the 2009 Iranian elections would have been very different without access to Twitter and YouTube. There are low barriers to participation on the internet. Writing and posting a blog from an internet café is neither complicated nor expensive, especially when compared to broadcasting over radio or television. Moreover mobile phone penetration is very high in the MENA region (see Table 1 left), and these devices also enable internet access.

Anonymity for activists (and privacy for others). Attributing actions taken over the internet to individuals – while by no means impossible – is more difficult if precautions are taken. This characteristic allows a degree of anonymity for activists – a quality that is important in places where internet use is monitored pervasively. As one Egyptian activist tweeted during the protests: "*We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world.*"[15] The internet is a particularly important safe communication space for women, who generally face more challenges in Middle Eastern society. In December 2010, researchers at Harvard University found that in Egypt and Saudi Arabia, just under half of bloggers are female; however, they are far more likely to blog anonymously than their male counterparts. 42% of women compared to 29% of male bloggers write under no name.[16] The internet facilitates this opportunity.

Immediacy of information. Internet users can access information fast and in real time. Immediacy of information is especially important during times of political unrest and upheaval. Waiting around for broadcasts – which are often state-controlled – is not an option. By way of example, BBC Arabic recorded a large increase in visitors towards the end of January 2011, when pan-MENA protests were getting off the ground. Mobile phones are also important in this respect, because they give information on the go.

Front-line reporting and variety of views. Throughout the region, mobile phones were used to capture on-the-ground action and the resulting images uploaded to the world. Local bloggers gave front-line and eye-witness reports. These local sources of information – although also prone to bias and distortion -- offered vital counterpoints to state-run media that claimed protests were minor and crackdowns modest.

When reflecting on the socio-political significance of cyberspace in the MENA region, as well as censorship practices, it is important to consider two issues:

- **Online access and censorship practices vary substantially amongst different countries in the region.** For instance, the ONI has found no evidence of filtering in westernized and officially secular Lebanon, where there are no official restrictions on the freedom of speech. This is in direct contrast to countries such as Saudi Arabia, who monitor internet activities (including installing cameras in internet cafés) and practice heavy censorship on non-Islamic reli gious sites and those with 'immoral' social content; and,

- **The internet is but one part of a rich media environment.** Although it is indisputably a phenomenal resource and facilitates communication, the internet is not invincible. As demonstrated in Egypt, blocking the internet or ordering ISPs to cease services is possible. Rudimentary workarounds are possible, but beyond the grasp of many who have insufficient technical knowledge.[17] In comparison, radio and even print journalism are less susceptible to immediate, direct intervention. While the world looks to the internet as a symbol of advancement and modernity, it is important to remem ber that people use different media – print, radio, television, internet – in combination and interchangeably.

Censorship before, during and after the protests: Country snapshots

Tunisia

The Jasmine Revolution, sparked at the close of 2010 by the self-immolation of a street vendor, was the first uprising of the Arab Spring. After 23 years in power, President Zine El Abidine Ben Ali stepped down on 14 January in response to the demonstrations and riots throughout Tunisia. Throughout the revolution, protesters leveraged new media to get their stories out, while the government upped its control efforts.

Figure 1. Tunisia: Stats at a glance

Substantial filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	10.4 million	29.1	34%	95%	Authoritarian (144=)	Warning

- Pre-revolution: pervasive filtering of political and social content, internet tools
- Post-revolution: some filtering of social content (e.g. pornography) in line with conservative social norms

Pre-protests: Internet as threat; pervasive control. Prior to the revolution, the government exercised strict control over all media, despite constitutional guarantees for freedom of the press. Tunisia's press code banned offending the president, disturbing order, and publishing 'false news.' [18] The internet was heavily regulated and online dissidents were often punished. There was pervasive filtering of political and social content, as well as blocking of proxies. Human rights advocacy websites and video sharing websites were blocked, as were circumvention tools (see Box 1).

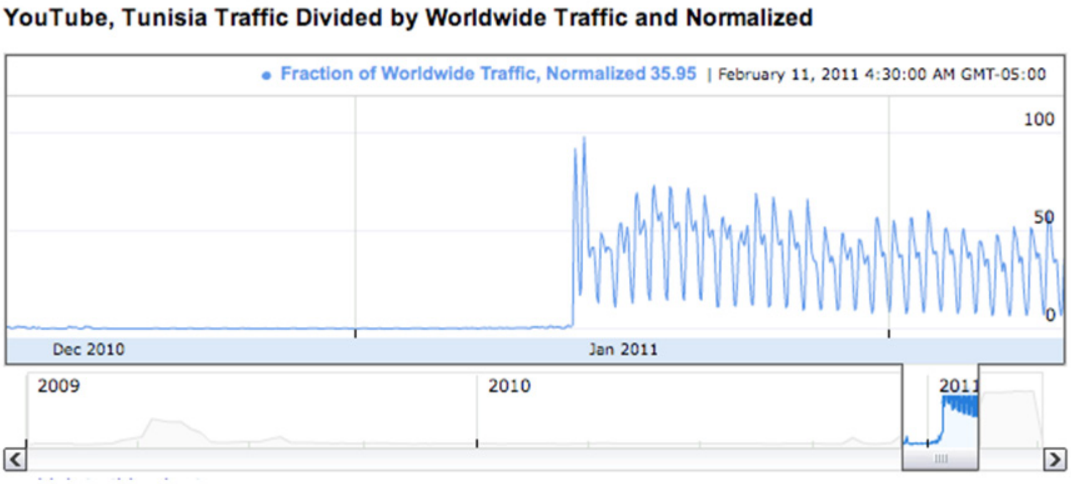
The Tunisian Internet Agency (ATI) reportedly engaged in network exploitation (hacking) of personal email accounts. In addition, all traffic flowed into the offices of the ATI prior to being routed on the internet. While the ATI themselves did not decide what should be blocked, access to their filtering technology was given to institutions mandated by the government who could decide which websites should be blocked. [19] At the same time, the government actively engaged in "freedom of information" disinformation campaigns with pro-government blogging and video-based campaigns touted Tunisia as a place of political freedom and free speech.[20]

During protests: New media leveraged as government enhanced blocking tactics. The Tunisian government tried to downplay the level of violence that occurred. While dozens of people died, state media reports said only that criminals were looting. [21] By contrast, Tunisian bloggers and social network users worked to counter official disinformation, spreading news, photographs and videos online. The government's tight hold on traditional media meant that new media became a crucial source of information for those in and outside Tunisia. Activists also tried to overload government websites with distributed denial-of-service (DDOS) attacks. On the government side, there was a huge spike in blocked websites, particularly of those that mentioned Sidi Bouzid – the town where protests kicked off after Mohammed Bouazizi set himself on fire.

Post-revolution: Internet freedom improved. Following the January 2011 revolution, ONI testing found **no evidence of blocking** of any political or security-related website. It seems that in the new

Tunisia, the internet will operate more freely. For example, access to YouTube and other video-sharing services, such as Daily Motion, is now permitted. Legal changes suggest filtering will take place only with a judicial mandate: blocks are to be put only on pornographic and 'hate' sites using URL classifiers.[22] New authorities state that filtering will be retained in order to continue promoting conservative, Muslim cultural norms. The ATI also seems to be embracing more normal regulation practices.

Figure 2: YouTube traffic from Tunisia, December 2010-January 2011[23]



Box 1. Tunisia: An in-depth look at controls.

Prior to January 2011, Tunisia used four censorship processes: selective blocking by URL (where the most offensive pages are blocked), DNS filtering (banning the domain and subdomain attached to a site), IP filtering (for youtube.com, dailymotion.com and others), and keyword filtering (where access to any URL containing a specific keyword is blocked).[1] However, authorities also used some active methods to find out personal details, going so far as to harass and arrest users.

Stealing logins. The Tunisian Internet Agency (ATI) was accused of injecting JavaScript to login pages for Gmail, Yahoo and Facebook[2], which enabled them to capture usernames and passwords, and hijack accounts. The extra lines of JavaScript pull the username and password, and then encode the data. This data is then placed into the URL, and a randomly generated five-character key is added – experts suggest this is to add a sense of legitimacy to the URL. In its entirety, this is sent in the form of a GET request to a non-working URL.[3] Although configuring a filter to log the GET commands would not be difficult, this took place on a significantly large scale to warrant fears of backing by the state.

Gmail phishing. Login stealing was enabled by periodically denying access to secure con nections.[4] Those behind the operation blocked access to the secure HTTPS Gmail connection so that userswere required to sign in via a regular HTTP connection. Users were then diverted to a page with the added JavaScript, configured under EasyPHP, to steal their passwords.[5]

Arrests. Reporters Without Borders (RSF) had at least five cases of arrested bloggers and online activists in early January 2011. The individuals were purportedly arrested because of their alleged association with hacking group Anonymous (who launched 'Operation Tunisia').[6]

1. Jillian York, *A deeper look into Tunisian internet censorship*, 18 August 2010. Available online at http://jilliancyork.com/2010/08/18/a-deeper-look-into- tunisian-internet-censorship/
2. Danny O'Brien, *Internet censorship halts in Tunisia, Committee to Protect Journalists*, 19 January 2011. Available online at http://www.cpj.org/internet/2011/01/update-on-the-tunisian-internet.php
3. Steve Ragan, *Tunisian government harvesting usernames and passwords*, The Tech Herald, 4 January 2011. Available online at http://www.thetechherald.com/article.php/201101/6651/Tunisian-government-harvesting-usernames-and-passwords
4. Nate Anderson, *Tweeting tyrants out of Tunisia: global internet at its best*, Wired, 14 January 2011. Available online at http://www.wired.com/threatlevel/2011/01/tunisia/
5. Slim Amamou, *Mass Gmail phishing in Tunisia*, GlobalVoices Advocacy, 5 July 2010. Available online at http://advocacy.globalvoicesonline.org/2010/07/05/mass-gmail-phishing-in-tunisia/
6. *Wave of arrests of bloggers and activists*, Reporters Without Borders, 7 January 2011. Available online at http://en.rsf.org/tunisia-wave-of-arrests-of-bloggers-and-07-01-2011,39238.html

Egypt

Egypt's internet received worldwide attention when the services of its four major ISPs were shut down for several days at the end of January. Prior to January, there had been little to no evidence of internet filtering, despite Egypt's being under emergency law and perennial restrictions on freedom of the press. Egypt was the primary market for BBC Arabic online in 2010, through both the regular and mobile websites, with roughly 2 million page views per month.

Figure 3. Egypt: Stats at a glance

No evidence of filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	84.5 million	23.9	21.2%	66.7%	Authoritarian (138)	Warning

- Pre-revolution: active blogging community; no evidence of technical filtering, although widespread surveillance
- Post-revolution: continued control over freedom of speech, including imprisonment of blogger who criticised the army

Pre-protests: Active and politicized bloggers; heavy internet surveillance. Egypt is the most populous country in the region and has the largest number of bloggers of any Arab country. Egyptian bloggers are some of the most politically active in the region, particularly as offline political speech and organization is highly regulated in the country.[24] The Muslim Brotherhood has a particularly strong online presence, and discussions emphasize human rights. Nearly half of the bloggers are women.

Internet surveillance was high under the Mubarak regime. As of August 2008, internet café customers had to provide their names, email addresses, and phone numbers before they could access the internet. The authorities monitored online activism – for instance, on Facebook, which has proved to be a hub for social activism in Egypt, notably during the riots over food prices.[25] Additionally, during this time, Vodafone was compelled to turn over user data to the Egyptian security services, and the Skype-based phone calls of activists were heavily monitored.[26]

During protests: Mid-revolution blackout. On January 27, Egypt's four main ISPs (Link Egypt, Vodafone/Raya, Telecom Egypt and Etisalat Misr) shut down all international connections to the internet and went offline. Renesys, an internet monitoring consultancy, reports that this was not an automated process. Rather, it was a gradual sequence of events. In the day that followed, 93% of Egyptian networks were unreachable. One of the few exceptions was the Noor Group ISP, which hosts the Egyptian Stock Exchange website. The stock exchange saw a sharp fall in value, indicating the major impact that the shutdown had on the economy.[27]

The blackout was unprecedented in the region. As a Renesys blogger said, "They seem to have gone straight from plan A (block Twitter and Facebook) to plan Z (turn off the internet) without stopping at any intermediate solutions. Iran took the more subtle throttle-and-monitor approach after their dubious elections in 2009." Perhaps surprisingly, there were no significant disruptions to other countries' traffic – a potential problem given that most of internet connectivity between Europe and Asia, particularly for the Gulf states, passes through Egypt.[28] The internet returned on February 2.

Post-protests: Continued media control and uncertainty. Many assumed the end of President Mubarak's rule would bring about a wholesale change in media openness. However, several well-publicised incidents of continued media control suggest otherwise. An Egyptian blogger, Maikel Nabil, was jailed for three years on 11 April by a military court for criticising the army's role during the uprisings: he was found guilty of insulting the army and spreading false news.[29] The upcoming elections will provide an important testing ground to investigate the future of filtering practices in Egypt.

Figure 4. Traffic to all Google products from Egypt, mid January -mid February 2011[30]

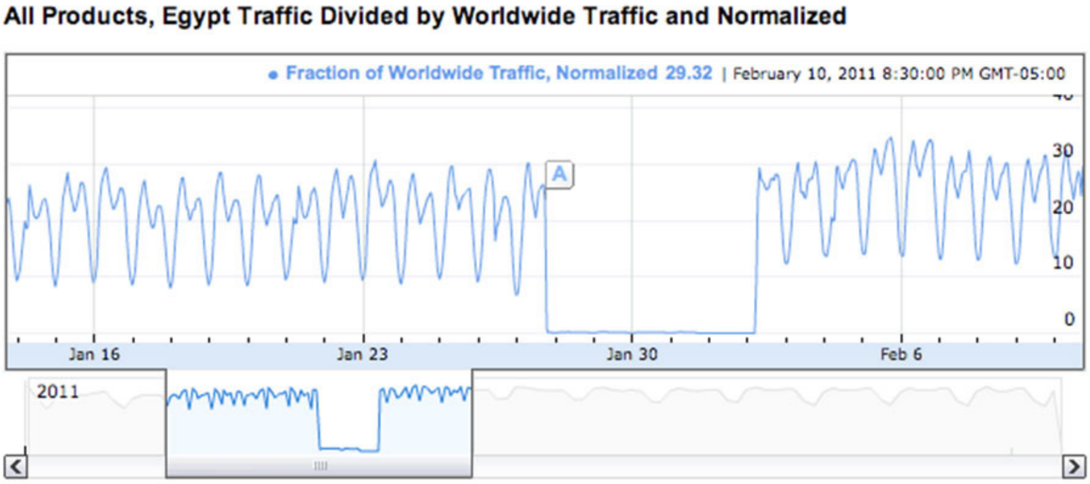
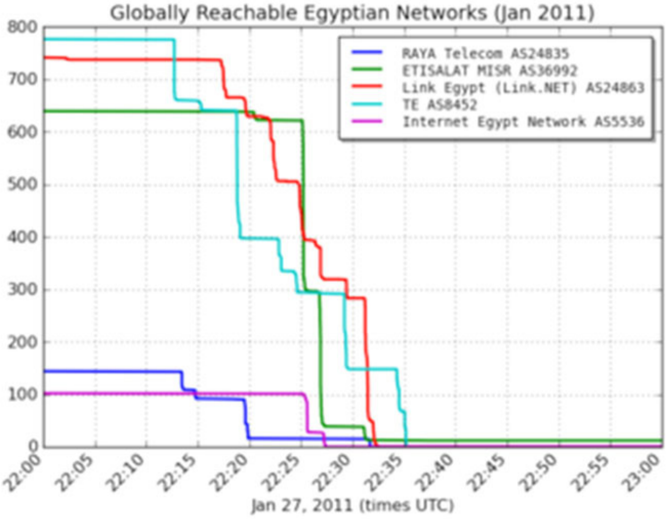


Figure 5. Globally reachable Egyptian networks, January 27 2011[31]



Libya

From February 2011 onwards, Libyans began echoing their Egyptian and Tunisian neighbours by protesting and calling for change. The level of violence has been higher than in any other country (and remains ongoing at the time of writing). And as Colonel Gaddafi held ever more repressively onto power, the UN mandated a military intervention.

Figure 6. Libya: Stats at a glance

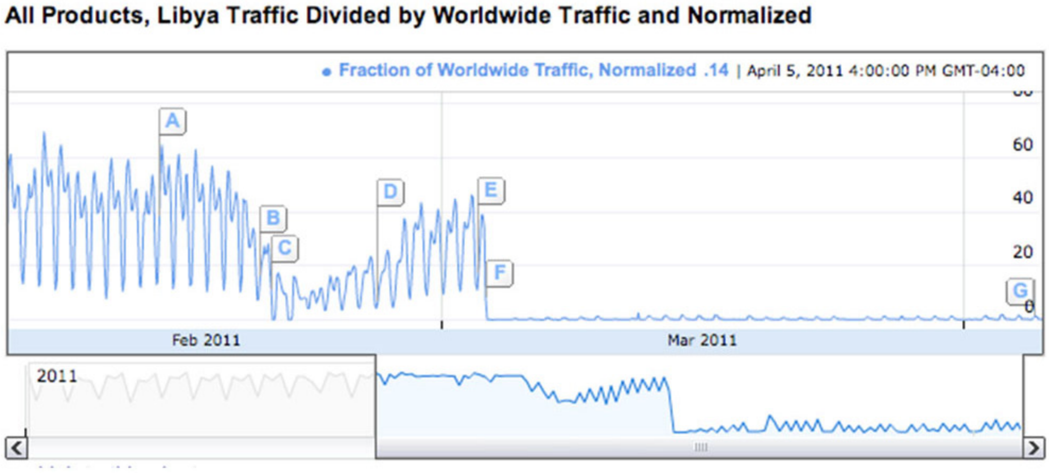
Selective filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	6.5 million	26.2	5.5%	77.9%	Authoritarian (158)	Warning

- Pre-protests: media content heavily controlled; selective filtering of political content (opposition websites); political self-censorship widespread due to fear of government retribution
- During protests (ongoing): Widespread self-censorship due to fear of government retribution

Pre-protests: Heavy state control over media, including internet. Private media is illegal in Libya. Only two public organisations have the right to publish.[32] Libyan law forbids criticism of Colonel Gaddafi, and the regime has brought defamation cases against foreign media for critical articles. The ONI found that pro-opposition websites have been blocked or even hijacked and replaced with pro-Gaddafi content. Users who try to access banned content receive time-out messages.[33] Political discourse online is rare.

During protests: Internet blackouts, rebel cell networks. Libya's internet was taken down on 19-20 February 2011 and then again in early March. Libya was able to throttle the internet because of its one centrally controlled internet service provider (Libya Telecom and Technology, LTT), which enabled authorities to prevent almost all traffic from traversing the network.[34] However, as national communication networks suffer, Libyan rebels are increasing their efforts to find workarounds.[35] They control AM and FM radio transmitters, and aim to broadcast satellite video soon. A new cell phone network ('Free Libyana') was opened on 2 April 2011, consisting of part of the Libyana network that was repurposed for the rebels. Its establishment was masterminded by Ousama Abushagar, a Libyan who lives in Abu Dhabi. Abushagar and two partners received millions in financial support from the UAE and Qatar to purchase necessary telecommunications equipment. This new equipment was then fused into the existing network in Benghazi. Etilasat provided a satellite feed through which the 'Free Libyana' calls could be routed.[36]

Figure 7. Traffic to Google products from Libya, February-March 2011[37]



Syria

Emergency laws have denied most constitutional rights to Syrian citizens since 1963, and multi-party elections do not exist. For the past forty years, the country has been ruled by the al-Assad family. Some hope that current President Bashar al-Assad will institute reform, as he indicated in an interview with the Wall Street Journal on 31 January 2011. Pro-democracy protests began towards the end of January 2011, and erupted on 18 March. Although some concessions were made, including the lifting of the emergency laws on 19 April, the ongoing crackdown on protesters has been brutal.

Figure 8. Syria: Stats at a glance

Substantial filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	22.5 million	22.5	17.7%	44.3%	Authoritarian (152=)	Warning

- Pre-protests: Syrian bloggers are highly politicized, but repercussions are harsh; freedom of the press arbitrarily restricted; internet penetration low; pervasive filtering of online political content and tools; heavy surveillance; self-censorship common due to imprisonment of bloggers and journalists.
- During protests: Previously blocked sites (YouTube, Facebook, Wikipedia) unblocked (appeasement strategy?), man-in-the-middle attacks on Facebook users and hacking of opposition websites.

Pre-protests: Politicised bloggers (**although most others self-censor); poor internet penetration rates; control of the press; pervasive online filtering; heavy surveillance and punishment of dissidents.** Syria has carefully controlled access to the internet for several years. Internet infrastructure is underdeveloped compared to its neighbours, and penetration is generally low. According to the ITU, only 18% of the population used the internet as of 2009. Steps have been taken to improve matters: as of January 2011, all Syrians could sign up for high speed internet. Media is monitored and journalists face arrest for ambiguous reasons. (Although press freedom is protected in the constitution, the ongoing state of emergency restricts these guarantees) The security services are numerous and well integrated.

With respect to the internet, sites are heavily filtered and users surveilled. Facebook was blocked in November 2007 (officially due to the potential for Israeli influence on Syrian youth) and services such as YouTube and Skype were made inaccessible, resulting in many internet cafés installing proxy servers on computers. According to the ONI, even Amazon.com has been blocked. Internet cafés were mandated in March 2008 to provide the identities and times of use of their customers to the authorities. Still, Syrian bloggers are fond of writing about politics, and *"among the least likely…to express support for domestic political leaders."*[38] Online dissidents face harsh repercussions ranging from harassment to imprisonment for a few years. At least 10 bloggers are currently in prison.[39]

During protests: Surprise unblocking, regrouped efforts at control and surveillance. Just as protests got underway in Syria, the heavy censorship appeared to dissipate. According to the Google Transparency Project, YouTube was made accessible on 8 February. Access to Facebook, Amazon and Wikipedia was made unhindered. Local media reported that the block had been lifted due to demands from youth. The government might have been trying to appease the masses. Alternatively, the enhanced freedom of access may have been to enable greater surveillance of activists (see discussion of man-in-the-middle attacks on Facebook below).

Al Arabiya reported via Twitter on 28 January that all internet services were suspended;[40] however, this was quickly denied by the Syrian authorities.[41] Despite the protests, there were no substantial 'official' restrictions until the majority of

Syrian networks became unreachable on 3 June 2011. The routes returned the next day, and as yet it is not clear how or why the networks were offline.[42]

Nevertheless, several Syrian Facebook users have reported an inability to log in to their accounts. It was reported by the Electronic Frontier Foundation on 5 May 2011[43] **that the Syrian Telecom Ministry has launched a man-in-the-middle attack on the HTTPS version of Facebook,** providing a fake certificate warning which lets them access and control users' accounts who continue to login to the page. Although there is no proof that this is occurring from the Syrian Telecom Ministry itself, in such an unstable situation these type of attacks are of concern to those using Facebook to mobilise and organise protests.

In addition, **the government-controlled Syrian Electronic has been attacking, spamming, and defacing opposition and 'hostile' websites, both political and commercial.**[45] In May 2011, the Syrian Electronic Army hacked a British town council website), leaving a message imploring the British government to not interfere in Syria (see Figure 10). This type of attack indicates that Syria may be moving to third generation controls.

Figure 9. YouTube traffic from Syria, January-February 2011[46]

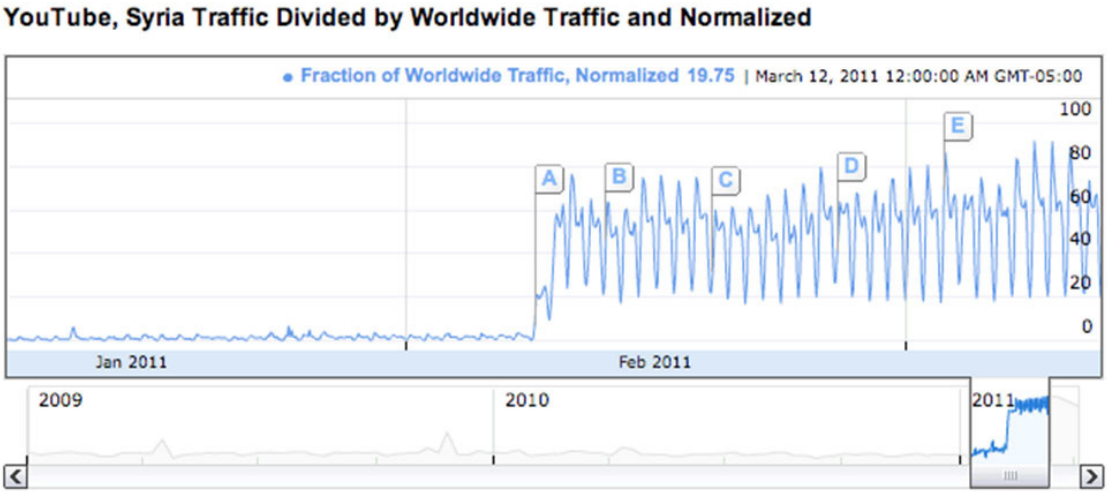
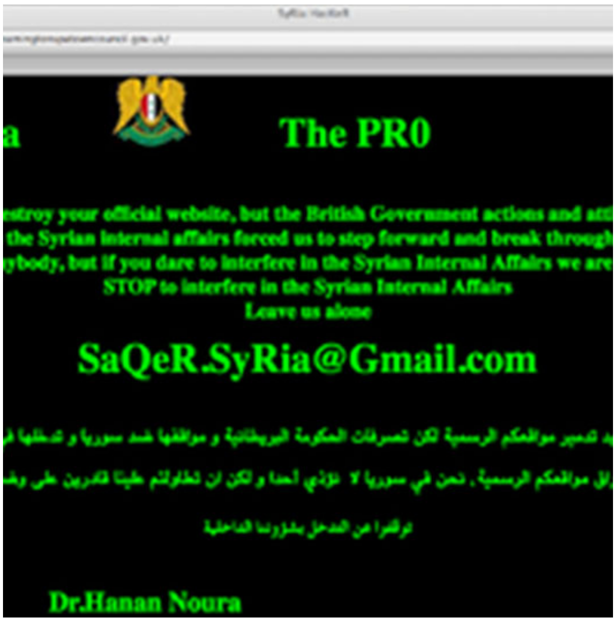


Figure 10. Screenshot of www.leamingtonspatowncouncil.gov.uk, 16 May 2011


a
The PR0

estroy your official website, but the British Government actions and att
the Syrian internal affairs forced us to step forward and break through
ybody, but if you dare to interfere in the Syrian Internal Affairs we are
STOP to interfere in the Syrian Internal Affairs
Leave us alone

SaQeR.SyRia@Gmail.com

يد تدمير مواقعكم الرسمية لكن تصرفات الحكومة البريطانية و مواقفها ضد سوريا و تدخلها في

زال مواقعكم الرسمية . نحن في سوريا لا نؤذي أحدا و لكن ان تطاولتم علينا قادرين على وضـ

توقفوا عن التدخل بشؤوننا الداخلية

Dr.Hanan Noura

Other at-risk countries

Yemen

Figure 11. Yemen: Stats at a glance

Substantial filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	24.3 million	17.8	1.8%	16.3%	Authoritarian (156=)	Alert

Despite Yemen's relatively large size, internet infrastructure is underdeveloped. Only 2% of the population uses the internet.[47] There is only one originating autonomous system:[48] Yemen Net, a state-owned Yemeni ISP, is run under the auspices of Yemen's Public Telecommunication Company. ONI has found that Yemen Net typically filters some websites. In particular, political sites that have content relating to religious conversion, commentary and criticism, and free expression are blocked. Websites with pornographic or sexual content are also filtered, as are social networking sites, circumvention tools and other internet tools.

Yemen is in dire straits: economic disparity, unemployment and corruption are rife. Activists inspired by the events in Tunisia and Egypt have taken to the streets with the aim of ousting Ali Abdullah Saleh, who has led Yemen for 33 years. His traditional pillars of support have waned, to the point where the Gulf Cooperation Council called for Saleh to form a unity government and then step done within 30 days. Until some changes take place, there is the potential for civil war in the country, and the military has reportedly launched violent attacks against protestors. However, no further internet restrictions have been reported.

Bahrain

Figure 12. Bahrain: Stats at a glance

Substantial filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	0.8 million	28.1	88%	199.4%	Authoritarian (122)	n/a

Bahrain is well-connected, with an online connectivity score of 210.4% per person – far greater than the Gulf average of 135.4%.[49] Freedom of expression and of the press is not guaranteed and censorship of online and print media is rife. As of January 2009, the Bahraini Ministry of Information has the legal right to order the immediate blocking of any website. Political websites, pornographic sites, those referring to internet tools (such as proxies) are all blocked in Bahrain; however, filtering focuses on sites that are critical of the government and royal family. Several such sites were shut down, and two bloggers (Abduljalil Alsingace, and Ali Abdulemam) were arrested, prior to the elections in October 2010.[50] Facebook, Twitter and YouTube are not blocked in their entirety, but individual pages occasionally are: content is limited to an extent.[51]

Youth groups in Bahrain are strong advocates for democracy and political reform. The most popular site for the discussion of Bahraini news is Bahrainonline.org, which has over 50,000 members – however, the site is banned. Activists commonly use Twitter, Facebook and other online forums to spread their message; at least two groups, the Youth of the 14 February Revolution and the Bahrain 14 February Peaceful Movement have issued official online communiqués in February and March 2011 calling for change.[52] However, violence has been steadily increasing.

In mid-March 2011, several protesters were killed in the capital, Manama, when tanks entered a square where they were camped. Saudi troops were called in by the Bahraini authorities in order to help maintain control over the protesters.[53]

Saudi Arabia

Figure 13. Saudi Arabia: Stats at a glance

Substantial filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	26.2 million	25.3	38.1%	174.4%	Authoritarian (160=)	Warning

Saudi Arabia is one of the largest audiences for BBC Arabic online (after Egypt and the USA), with over 1 million page requests per month during the second quarter of 2010. Saudi Arabia is well connected internationally and has a steadily growing telecoms sector, with the Saudi Telecom Company aiming to provide high-speed internet in the country; there are over twenty licensed ISPs that connect users to the national network.[54] The internet is particularly important for Saudi women, giving them a safe space in a country where many rights are restricted.

Censorship is implemented by the government's Internet Services Unit (ISU). In keeping with the centrality of Islam to Saudi Arabia, the ISU extensively filters social content. Several religious sites are blocked, and some sites related to human rights are also inaccessible. Sewar Technologies, a Saudi company, has developed a filtering solution called WireFilter that enforces Google and Yahoo SafeSearch policies to provide censored search results.

Most global media sites are currently accessible, as are YouTube, Facebook, Twitter and most international blog-hosting sites. YouTube was used by Saudis during the major floods that occurred in Jeddah in 2009 to demand action from the authorities – the response to which was the immediate establishment of a commission by King Abdullah to investigate the disaster. Facebook was also used to organize and mobilize rescuers.[55]

A major online campaign began in early 2011, advocating political and economic change. In response to in-country protests, King Abdullah offered benefits to Saudi Arabian citizens valued at almost $11 billion. These included loans for housing and an increase in wages for state employees. However, no political reforms were announced. The reaction to the protests has been strong and brutal: a fatwa was announced on 6 March opposing demonstrations, and on 11 March, one of the administrators of the Facebook group calling for a 'Day of Rage' was allegedly killed by security forces.[56]

Jordan

Figure 14. Jordan: Stats at a glance

Selective filtering	Population	Median age	Internet penetration	Mobile phone subscribers	Index of democracy (rank) (2010)	Fragile state status
	6.5 million	22.8	27.2%	36.1%	Authoritarian (117)	Warning

Known as one of the more liberal and Westernised countries in the MENA region, largely due to its influx of tourists and comparatively peaceful relationship with Israel, Jordanians tend to enjoy unproblematic access to the internet. Facebook, Twitter and YouTube are particularly popular in Jordan (and are not blocked), with Facebook reportedly having 1.4 million Jordanian members in April 2011.[57]

However, this peaceful relationship is changing. In a paper published 18 April 2011, Freedom House marked Jordan as an at-risk country, particularly due to the ambiguous wording of a new cybercrimes law introduced in August 2010 which "prohibits the posting of any previously nonpublic information relevant to foreign affairs, national security, the national economy, or public safety." [58]

There are some restrictions on internet cafés: measures introduced in March 2008, and increased in 2010, require café owners to install censorship programs filtering pornographic, drug-related and anti-religious content,[59] and to install surveillance cameras and record relevant customer details. Few sites are actually filtered except for the occasional one that is critical of leadership, such as arabtimes.com. However, self-censorship is common, and traditionalist readers have been known to flood comments on websites with threatening messages.[60]

Tensions have run high in recent months, with several weeks of protests in January 2011. In response, King Abdullah made several concessions, including replacing most of the cabinet (the new cabinet was sworn in on 9 February) and promising reform. However, protests on 25 February attracted some 6000 protesters. No changes to internet restrictions (or lack thereof) have been observed. The general perspective is that the Jordanian government is attempting to appease protesters instead of tighten their control over them.

Fallout and future trends

The situation in the MENA region is fluid. At the time of writing, Egypt and Tunisia's regimes have been overturned, military action is taking place in Libya, and escalating violence is spreading throughout Syrian and Yemen.

When Mubarak stepped down, the world wondered whether the dominos were about to fall across the Middle East. However, no governments have fallen since and it is an open question as to whether any more will.

The international community has reacted strongly to the Middle East protests, with the United States ending up in the perhaps surprising position of encouraging rebellions against pro-American governments. Of particular relevance to this report was Hillary Clinton's speech at George Washington University in February 2011, which culminated in the State Department laying out financial support for companies developing circumvention technologies. Some commentators put this down as hypocritical in light of the Patriot Act, whose provisions entitle federal agencies to request the disclosure of electronic communications and ISP records. At the opposite end of the spectrum are those countries who, to put it bluntly, do not care about the possibility of social activism spilling over. China and Iran, with justifiably little concern for the stability of their repressive regimes, have stepped up efforts towards greater state control over national cyberspace.

With respect to the future openness of cyberspace in the MENA region, it is difficult to make sweeping generalizations. As this report has detailed, different regimes reacted very differently during their respective crises: Egypt cut off the internet entirely; Libya throttled it; Tunisia blocked additional sites, but has now freed up access; and, Syria lightened up its internet controls, but then appears to have exploited the new freedoms (the presumed man-in-the-middle Facebook attacks) while encouraging cyber attacks by its Syrian Electronic Army. In general, after the international reaction to the Egyptian blackout, leaders seem to have proceeded more cautiously with their overt controls.

Even if political freedoms increase in some countries, it is likely that censorship practices will continue -- especially with respect to social and cultural content that lies outside the region's conservative norms. And, for those countries that remain democratically-challenged, state efforts to surveil and control cyberspace are likely to continue and grow more sophisticated. Overall, this review of censorship and activism during the recent protests has yielded a number of important takeaways for international broadcasters and the BBC in particular. These are found at the beginning of this report.

Endnotes

[1] Research sources used include the OpenNet Initiative, the Berkman Center at Harvard Law School, the International Crisis Group, as well as the Google Transparency Report, Al Jazeera and other media. Note also that this report does not address the nature of the events themselves or the military action that occurred.

[2] Etling et al., *Mapping the Arabic blogosphere: politics and dissent online*, New Media & Society, 16 December 2010, p1237. The researchers indicated that BBC News is particularly popular among bloggers in the Levant.

[3] Gregg Carlstrom, *Hazards of reporting from Egypt*, Al Jazeera, 8 February 2011.

[4] For a concise overview see http://en.wikipedia.org/wiki/Arab_Spring

[5] A man-in-the-middle attack is a form of "active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker" (Wikipedia, http://en.wikipedia.org/wiki/Man-in-the-middle_attack)

[6] Research conducted by Helmi Noman, presented 26 June 2008 at the Global Voices Summit in Budapest. The survey had 108 responses.

[7] http://populationpyramid.net/

[8] Population Division of the Department of Economic and Social Affairs of the United Nations Secretariat, *World population prospects: The 2008 revision*, http://esa.un.org/unpp

[9] Internet World Stats

[10] International Telecommunications Union

[11] *Index of democracy*, Economist Intelligence Unit, 2010. Available online at http://graphics.eiu.com/PDF/Democracy_Index_2010_web.pdf Countries are ranked based on their democratic status, with 1 being a full democracy, and the highest numbers authoritarian regimes. Norway is ranked 1, while North Korea is the lowest ranked at 167.

[12] *Failed state index scores 2010*, The Fund for Peace, 2010. Available online at http://www.fundforpeace.org/web/index.php?option=com_content&task=view&id=452&Itemid=900

[13] T*he best man always wins*, The Economist, 15 July 2010.

[14] Reverchon, Adrien; de Tricornot (13 April 2011). "*La rente pétrolière ne garantit plus la paix sociale*" as cited on Wikipedia http://en.wikipedia.org/wiki/Arab_Spring

[15] "*The Arab Uprising's cascading effects*". Millermccune.com. 23 February 2011, as cited on Wikipedia http://en.wikipedia.org/wiki/Arab_Spring

[16] Etling et al., *Mapping the Arabic blogosphere: politics and dissent online*, New Media & Society, 16 December 2010, p1236.

[17] *Signalling dissent*, The Economist, 17 March 2011.

[18] Committee to protect journalists, Tunisia report: *The smiling oppressor*, September 2008. Available online at http://cpj.org/reports/2008/09/tunisia-oppression.php, as cited in ONI country profile: Tunisia.

[19] Mike Elkin, *Tunisia internet chief gives inside look at cyber uprising,* Wired, 28 January 2011. Available online at http://www.wired.com/dangerroom/2011/01/as-egypt-tightens-its-internet-grip-tunisia-seeks-to-open-up/

[20] *Freedom on the net 2011: a global assessment of internet and digital media*, Freedom House, April 2011, p325. Available online at http://www.freedomhouse.org/uploads/fotn/2011/FOTN2011.pdf

[21] Mike Elkin, *Tunisia internet chief gives inside look at cyber uprising*, Wired, 28 January 2011. Available online at http://www.wired.com/dangerroom/2011/01/as-egypt-tightens-its-internet-grip-tunisia-seeks-to-open-up/

[22] Ibid.

[23] Screenshot from Google Transparency Project

24. Etling et al., *Mapping the Arabic blogosphere: politics and dissent online*, New Media & Society, 16 December 2010, p1232.

25. This was exemplified in April 2008 when a general strike protesting against rising food prices and the government gained much support through the social networking site. See Noam Cohen, *In Egypt, a thirst for technology and progress*, The New York Times, 21 July 2008. Available online at http://www.nytimes.com/2008/07/21/business/media/21link.html.

26. *Mideast uses western tools to battle Skype rebellion*, available on http://online.wsj.com/article/SB10001424052702304520804576345970862420038.html?mod=googlenews_wsj

27. Internet Society Monthly Newsletter, 29th January 2011

28. Jamie Cowie, *Egypt leaves the internet*, Renesys (blog), 27 January 2011. Available online at http://www.renesys.com/blog/2011/01/egypt-leaves-the-internet.shtml

29. See: *Egypt blogger Maikel Nabil jailed by military court*, BBC News, 11 April 2011. Available online at http://www.bbc.co.uk/news/world-middle-east-13038937; and Egyptian blogger jailed for three years, Al Jazeera, 11 April 2011. Available online at http://english.aljazeera.net/news/middleeast/2011/04/2011411135325204241.html

30. Screenshot from Google Transparency Project

31. Screenshot from Renesys

32. Programme on Governance in the Arab Region, Civil Society: Libya, United Nations Development Programme,. Available online at http://www.pogar.org/countries/theme.aspx?cid=10&t=2#sub5.

33 OpenNet Initiative, country profile: Libya

34. Jamie Cowie, *What Libya learned from Egypt*, Renesys (blog), March 5 2011

35. Graeme Smith, *Libyan rebels focus on boosting communication networks*, The Globe and Mail, 10 April 2011. Available online at http://www.theglobeandmail.com/news/world/africa-mideast/libyan-rebels-focus-on-boosting-communication-networks/article1979339/

36. Margaret Coker and Charles Levinson, *Rebels hijack Gadhafi's phone network*, The Wall Street Journal, 13 April 2011. Available online at http://online.wsj.com/article/SB10001424052748703841904576256512991215284.html

37. Screenshot from Google Transparency Project

38. Etling et al., *Mapping the Arabic blogosphere: politics and dissent online*, New Media & Society, 16 December 2010, p1233.

39. Jillian York, *Arabs blogging in defiance*, Al Jazeera, 22 March 2011.

40. http://twitter.com/AlArabiya_Eng/status/31002490816167936#

41. http://twitter.com/AlArabiya_Eng/status/31006701473767426#

42. James Cowie, *Tracking the Syrian blackout*, 10 June 2011. Available online at http://www.renesys.com/blog/2011/06/tracing-the-syrian-blackout.shtml

43. Eckersley, *A Syrian man-in-the-middle attack against Facebook*, Electronic Frontier Foundation, 5 May 2011.

44. Qtiesh, *Did Syria replace Facebook's security certificate with a forged one?,* Global Voices Advocacy, 5 May 2011. Available online at http://advocacy.globalvoicesonline.org/2011/05/05/did-syria-replace-facebooks-security-certificate-with-a-forged-one/print/

45. Helmi Noman, *The emergence of open and organized pro-government cyber attacks in the Middle East: the case of the syrian electronic army,* The Information Warfare Monitor.

46. Screenshot from Google Transparency Project

47. International Telecommunications Union

48. Presentation by Jamie Cowie, Middle Eastern internet trends, Renesys, 22 October 2010.

49. Arab Advisors Group reveals Bahrain's communications connectivity leading the region, AMEinfo, August 5, 2008. Available online at http://www.ameinfo.com/165459.html, as cited in the OpenNet Initiative country profile. This 2009 score measures both internet access and fixed and mobile telephone lines.

50. New web crackdown blocks dozens of websites and electronic forums in Bahrain, Bahrain Center for Human Rights, 4 September 2010.

Appendix 1. An overview of censorship techniques

Timeline of the Arab Spring

December 2010

17 -- Fruit seller Mohamed Bouazizi sets fire to himself in Tunisia

January 2011

14 -- Tunisian President Zine El Abidine Ali steps down

25 -- Protests erupt in Cairo, Egypt

27 -- Four major Egyptian ISPs shut their services down

February 2011

2 -- Internet connectivity returns to Egypt

8 -- After lengthy blocking, Google reports YouTube accessible in Syria

9 -- New Jordanian cabinet sworn in

11 -- Hosni Mubarak steps down as President of Egypt

19 - 20 -- Internet traffic in Libya is throttled for two nights

20 -- Unrest reaches Tripoli, Libya

25 -- ‘Day of rage’ across the Middle East, with thousands of protesters gathering in city squares

March 2011

3 -- Internet blacked out in Libya

6 -- Public protests are banned in Saudi Arabia

11 -- An administrator of the Saudi Facebook group calling for a ‘Day of Rage’ is reportedly killed by security forces

16 -- Protesters camping in Pearl Square in the Bahraini capital, Manama, were killed by troops (including those from Saudi Arabia)

18 -- Pro-democracy protests erupt in Syria

-- UN Security Council backs no-fly zone in Libya

-- King Abdullah of Saudi Arabia announces reforms

19 -- NATO military strikes begin in Libya

29 -- Syrian cabinet resigns

April 2011

2 -- New rebel-run ‘Free Libyana’ cell phone network opened

11 -- Maikel Nabil, an Egyptian blogger, is jailed for three years by a military court

-- Yemeni President Saleh promises to step down in 2013

19 -- Emergency Law lifted in Syria

27 -- Civil disobedience campaign calling for President Saleh to quit closes schools, shops, and government offices in Yemen

May 2011

5 -- Electronic Frontier Foundation reports that the Syrian Telecom Ministry has launched a man-in-the-middle attack against the HTTPS version of Facebook

17 -- The Syrian Electronic Army claims to have attacked over 50 websites

27 -- Yemeni government forces are reported to be carrying out air strikes against tribal forces

29 -- Tanks surround two towns north of Damascus, cutting off water and electricity to residents

June 2011

3 -- The majority of Syrian networks are taken offline for the night

Appendix 2. An overview of censorship techniques

Censorship of print journalism and radio has been common in the MENA region for several years, often effected through the careful control of infrastructure. Censorship of the internet is slightly different as there is not the same potential for control through the ownership of infrastructure. Rather, as documented by the OpenNet Initiative (ONI) internet censorship follows four main patterns:

- technical blocking, which includes IP and URL blocking as well as DNS tampering;
- search result removal, where search services cooperate with government requests to omit certain results;
- takedown, where regulators can demand the removal of websites or deregister web sites; and,
- encouragement of self-censorship, through the threat of legal action, promotion of social norms, or informal methods of intimidation.

These censorship methods fall into three 'generations' of internet control techniques (as defined by the ONI) :

- First generation controls: *"Lists of IP addresses, keywords and/or domains are programmed into routers or software packages that are situated at key internet choke points, typically at international gateways or among major ISPs;"*

- Second generation controls: "*…create a legal and normative environment and technical capabilities that enable actors to deny access to information resources as and when needed, while reducing the possibility of blowback or discovery.*"

- Third generation controls: "*… focus less on denying access than on successfully competing with potential threats through effective counter-information campaigns that overwhelm, discredit, or demoralize opponents. [These controls] also focus on the active use of surveillance and data mining"*

All of these approaches to censorship are common throughout the MENA region. Technical blocking is used in many countries (with exceptions including democratic Lebanon). And, as evidenced by Google Transparency Report's Government Requests, governments around the world request search result removal and Google usually complies. Many MENA countries employ some form of surveillance (i.e. third generation controls) on internet users, and this, combined with a general conservatism in both secular and religious societies, means self-censorship is prevalent.

However, these control techniques are used to varying degrees of impact and sophistication (see Table 2). Some countries, such as Jordan, employ technical filtering of only a few websites that are notably critical of the government. Others, such as Saudi Arabia, block websites of human rights organizations, the Voice of Saudi Women (which focuses on the place of women in Saudi society), various media as well as those advocating political reform.

Table 2: Generations of filtering breakdown (ONI research, 2009)

	First generation		Second generation			Third generation			
	Internet filtering	Policing cybercafés	Legal environment for information control	Internet shutdowns and disruptions	Computer network attack	Warrantless surveillance	National cyber-zones	State-sponsored information campaigns	Direct action
Algeria	■	■	■	■		■			
Bahrain	■		■	■	■	■			■
Egypt	■	■	■	■		■			■
Jordan	■	■	■						
Lebanon									
Libya	■	■	■	■		■		■	
Saudi Arabia	■	■	■		■	■			
Syria	■	■	■			■			
Tunisia	■	■	■	■	■	■			
Yemen	■	■	■	■		■			

When considering state-led censorship and surveillance in the region, it is important to note the role played by Western companies. Despite claims to openness, Western technology companies participate both directly and indirectly in censorship in the MENA region. For example, testing in January 2010 revealed that Microsoft's Bing search engine, which tailors its services to different regions, uses keyword filtering in order to block certain results (especially those that have some form of sexual content, or discuss homosexuality).

Other companies actively provide filtering technologies to governments in the MENA region. ONI researchers found that ISPs in Yemen, UAE, Qatar, Oman, Saudi Arabia, Kuwait, Bahrain, Sudan, and Tunisia use Western technology to block content. The first three employ Netsweeper, a Canadian product (although not exclusively). The latter use SmartFilter products – a company now owned by Intel. Black lists are maintained by the companies themselves, as opposed to ISPs.   Previously, Western-facilitated filtering services were relatively undisguised. More recently, companies seem more concerned to disassociate themselves from such practices by omitting reference to their products from blocked pages.

About The SecDev Group

The SecDev Group works at the cross-roads of global security and development. We provide intelligence, toolsets and investigations that inform policy and address risk in the information age. Our focus is countries at risk from violence, insecurity and underdevelopment. Our methods combine in-field research -- consulting people on the front line of events -- with advanced data-mining and visualization techniques. Our goal is to bridge the gaps between research, policy and practice.

We represent a global consortium of practitioners, scholars, and former policy-makers with expertise in development, conflict and recovery, armed non-state actors, security, intelligence and the cross-cutting impacts of cyberspace.

The SecDev Group
World Exchange Plaza,
45 O'Connor Street, Suite 1150
Ottawa, Ontario K1P1A4, Canada
T 1-(613)-755-4007
info@secdev.ca

www.secdev.ca

BBC

TheSecDevGroup