# GLOBAL INFORMATION SOCIETY WATCH 2014

*Communications surveillance in the digital age*

This report was originally published as part of a larger compilation, which can be downloaded from GISWatch.org

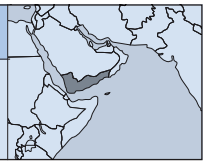
Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

ISBN: 978-92-95102-16-3

APC-201408-CIPP-R-EN-DIGITAL-207

# YEMEN

A country in transition with its share of cyber challenges



Walid Al-Saqaf
www.yemenportal.net

## Introduction

Being one of the least-developed countries in the world, it was natural to see Yemen trail all neighbouring Arab countries in utilising information and communications technologies (ICTs). With an internet penetration not exceeding 14%, it was also not surprising to see Yemen rank lowest on the Global Web Index[1] released in 2013 by the Web Foundation. Yet despite suffering from a weak telecommunication infrastructure and lack of human resources in the domain of internet services, the country recently witnessed significant growth in internet usage. Part of this may be attributed to wider use of Facebook in discussing political and social issues and in mobilising mass protests following the emergence of the Arab Spring in December 2010.

After hundreds of protestors were killed, jailed, maimed or injured during the 2011 popular revolts, a peaceful transfer of power deal was secured, ending the 33-year reign of Ali Abdullah Saleh and handing the presidency to his deputy Abd Rabbuh Mansur Hadi. Within the last several years, much has happened in the Yemeni cybersphere, particularly in the area of online freedom of expression. While Yemen's internet is relatively modest and limited in scope and impact, cases of online restrictions, privacy violations, and cyber attacks occurred, as will be described in this report.

## A brief background

Under Ali Abdullah Saleh's rule, practices of repression were committed using the 1990 Press and Publications Law and the Penal Code, which restricted free speech on multiple levels under the pretext of protecting national security, religion, foreign relations, etc. Despite the low level of internet activity compared to other countries, cases of website blocking were documented and several individuals complained about surveillance of their phone calls and hacking of their email and Facebook accounts. While there were no documented cases of digital surveillance in Yemen, some cyber activists have expressed concern that if it is not already the case, surveillance technology will soon be used by the authorities, particularly the national security agency, to spy on digital communication.

While broadcast media remain the most popular method to reach the public, internet has taken a modest share because it grants users the ability to publish, share and consume content much more easily than other forms of media. Internet usage has increased steadily since it was first introduced in 1996 by the Ministry of Telecommunication's Public Telecommunications Corporation (PTC) and Teleyemen, which was formed in 1990 as a joint company owned by PTC and the United Kingdom's Cable and Wireless plc. Today, those two companies monopolise the internet service provider (ISP) business as no private companies are allowed to operate. This has created an environment that lacks accountability and transparency and in which not many choices are provided to the public.

## An environment of fear

One of the country's most feared arms is the national security apparatus – sometimes called state intelligence – which, as is the case in many Arab countries, often keeps track of dissidents and monitors their activity. Prominent blogger and founding member of the Internet Society Yemen Chapter Fahmi Al-Baheth was one of the victims of this apparatus when he was told he would be detained or caused to "disappear" because of his online activities in support of the 2011 anti-Saleh popular revolution. Al-Baheth described how he discovered that the phone line of a fellow activist was tapped when a national security officer listed to him the people he called a day earlier. While it is known that the intelligence apparatus monitored and tracked regular dissidents and political activists, it has become clear that they have started to track and monitor cyber activists as well.

Among the more aggressive forms of attacks that targeted online journalists and activists during Saleh's rule was the blocking of websites by the government-run ISP Yemen Net, based on instructions from the national security. This practice has been verified by many websites that contained dissident

1 https://thewebindex.org/data/index

content or even news and opinion articles that contained criticism of the Saleh regime. In some cases, extensive long-term blocking of websites effectively killed their prospects and led to their permanent shutdown due to the lack of access for readers. While the government announced that blocking of news websites ceased in 2012, websites that allegedly contained socially inappropriate content (e.g. pornography and nudity) remained blocked.

A doctoral study[2] I carried out during 2010-2012 has demonstrated that forms of restrictions that targeted Yemeni websites and their operators ranged from prosecution to intimidation, and from hacking to filtering. Such violations have resulted in an environment of fear where online journalists and even regular users succumbed to self-censorship to avoid harm.

## Breaches of privacy

As Yemen has no laws or regulations protecting the privacy of citizens, cases where private information was published online have emerged. The monopoly over the ISP sector maintained by the government resulted in a lack of transparency and accountability when it comes to the data transferred through or stored on the local servers. According to a source who requested to stay anonymous, the national security has backdoor direct access to the servers of Yemen Net, which exposes sensitive and personal data of millions of Yemeni users to potential abuse. The United States Department of State's 2012 human rights report[3] has also given credibility to reports that the Yemeni authorities monitored email and internet chat rooms.

An app entitled Yemen Phone was produced, allowing anyone to access millions of Yemeni citizens' names and phone numbers and even physical addresses. Such an app, according to several privacy advocates, is a violation of privacy and should have been investigated by the authorities.

The Yemeni government was accused of breaching the privacy of citizens as early as 2009, when subscribers to the Yemen Mobile GSM service, which is run by the PTC, were assigned a special ring tone[4] in the form of a national song without their consent, causing outrage among some subscribers.

The lack of sensitivity to citizens' privacy was demonstrated again in 2013 when the Supreme Commission for Elections and Referendum made public the databases of citizens who applied to work in voter registration positions. Initially, all the applicants' information was made public, including their name, data and place of birth, academic qualifications, place of work, addresses, telephone numbers, email addresses, and even their national identity card numbers. To many privacy advocates such as Fahmi Al-Baheth, this was a major privacy breach that was only partially remedied by removing telephone numbers and email addresses while keeping all the other information public and accessible on the Commission's official website.[5]

## Victims of hacking

The fact that Yemen is a relatively inexperienced nation when it comes to technical internet-related operations has contributed to creating a fertile environment for hacking websites, emails and social media accounts. The lack of awareness of how the technology works and how to take proper precautions to prevent attacks was exploited during the peak of the popular revolution during 2011-2012. According to an anonymous source working for Yemen Net, the national security apparatus hired a large team of hackers in 2011 to target many websites, personal social media accounts and email accounts.

Hamza Alshargabi, who was active on Facebook in supporting the 2011 anti-Saleh uprising, indicated that his Facebook account and those of many of his friends were hacked during that period, probably due to their activities in support of the revolution. He discovered that his account was hacked when he realised that notifications were marked as "read" during the time he was logged off. He further indicated that an anonymous source working for Yemen Net verified the existence of advanced spying tools utilised by the national security.

Among the highest profile individuals attacked during that time was Nobel Laureate Tawakkol Karman, whose Facebook account was hacked multiple times. Due to her vocal opposition to the Saleh regime, she was subject to both physical and cyber attacks over the course of the revolution. In a recent correspondence, she described how Facebook decided to close her account due to the apparent changing of the telephone number used for verification. She remained unable to get her account back despite applying the instructions provided to her by Facebook. She also indicated that her email account was attacked several times, but not hacked due to the added security measures she has taken.

2 The full text of the study can be found at: oru.diva-portal.org/smash/record.jsf?pid=diva2:710477

3 www.state.gov/j/drl/rls/hrrpt/2013/nea/220385.htm

4 A news story in Arabic can be accessed at: marebpress.net/news_details.php?sid=16695&lng=arabic

5 web.scer.gov.ye/ar-page.aspx?show=47

But it is not only oppositional websites that got hacked. In 2011, a major governmental website was hacked for political reasons by elements in exile calling for the secession of south Yemen from the north. The attack on the website was possible after hacking the email account of its manager, who requested to stay anonymous. Thereafter, the hacker took over the whole domain by changing the name server settings on the GoDaddy domain registrar. While it was possible to fix the domain configuration after reclaiming the email address, the incident highlights the level of sophistication and extent of the cyber warfare that went on during that turbulent period of Yemen's recent history.

While it would be expected that such incidents would subside after the transfer of power in 2012, in reality, such cases not only continued, but also increased in depth and breadth. One of the most severe attacks[6] targeting several websites happened in April 2014 when at least six news websites were hacked all at once in what appeared to be a planned systematic attack. While it was not evident who was behind it, website owners accused the Yemeni authorities.

Much of the talk about who is behind the hacking and malicious attacks remains speculation due to the lack of technical documentation and research. Given that hacking tools and know-how are accessible globally by anyone willing to invest time and energy to find them, it is likely that different political rivals were involved in attacks and counter-attacks for various motives. Prior to the Arab Spring, however, it was evident that the government was more pervasive in attacking activists and online journalists. When the power transfer deal went into force in 2012, it was hoped that those attacks would subside. However, it was later found that attacks resumed, but this time, they seem to have come from different players.

In June 2014, a Yemeni media report[7] identified signs that surveillance and wiretapping will resume but now under the guidance of the new president, and will target dozens of journalists, activists and military leaders. According to the report, the feared national security apparatus will be used by Jalal Hadi, who is the son of the new president, to track and monitor phone calls and activities of those who could be a "threat to the transitional period."

## Conclusion

While Yemen remains one of the countries with the lowest internet penetration levels, it has had its share of troubles when it comes to surveillance, privacy, security and human rights on the internet. The few incidents described above present examples of violations that ranged from threats to bloggers and cyber activists to website filtering and hacking attacks. They constitute a major concern to human rights advocates who argue that free speech on the internet needs to be defended vehemently, particularly during this critical period for Yemen: a country undergoing massive political and social transformations.

One of the major challenges noted was the lack of sufficient skills on the part of users of the technology to keep their transactions safer and their websites and accounts protected. The need to address this challenge is pressing given the growth in internet usage the country is expected to witness. It is also important given that the political transition will require the free flow of information and ideas to contribute to the various new developments, from elections to new forms of cyber dissent.

The lack of legal frameworks to protect freedom of expression and privacy is another major concern because the status quo gives authorities a free hand to practice online restrictions on free speech. The revolution that emerged in 2011 and led to the downfall of Saleh's presidency had the promotion of free speech and access to information among its main goals. As a result, any deterioration in that respect would carry with it a great deal of disappointment, particularly after so many lives were sacrificed to achieve the desired political change.

Unfortunately, however, Yemen faces numerous challenges ranging from poverty to security and from water shortages to power outages. Those challenges have used up most of the energy of the government, private sector and even civil society, who have given human rights on the internet a back seat in favour of other more pressing issues. Nonetheless, there remains hope in bringing the violations against online journalists and activists to the forefront, particularly with the rise in social media use and after the launch of the Internet Society Yemen Chapter, whose goals include protecting security, privacy and freedom of expression on the internet. The chapter's role could be significantly important given that improving human rights and freedom of expression helps stability, and stability in this part of the world is crucial for the fight

6 Read an Arabic story about those attacks at: www.sanaapress.net/news9376.html

7 Read the Arabic story at: marebpress.net/mobile/news_details.php?sid=100613

against terrorism and for protecting the Bab Al-Mandab Strait, through which most of the world's oil passes.

These challenges facing Yemen were also mentioned in the Arab Internet Governance Forums (IGF) in 2012 and 2013 in Kuwait and Algiers respectively, and these were useful to compare experiences with other countries in the region and learn as the country moves forward.

The threats that Yemeni internet users are facing are but a reflection of the risks that are associated with using the internet at large. Discussions at the IGF and efforts undertaken by international bodies such as ICANN and global software platforms to provide more secure services, better regulatory models and more human rights-conscious policies, will all have a positive impact on Yemen as well.

## Action steps

For Yemen to confront the challenges described earlier, it is important to address the issues based on the particular subjects in question.

Firstly, the low internet penetration level in Yemen is a hindrance because it deprives the population of taking advantage of the enormous benefits that the internet has to offer. It also limits the number of people with enough skills and know-how to provide training and develop solutions that could tackle issues that are of a technical nature, such as securing accounts, tracking attacks, etc. To address this, the government's monopoly over the ISP business should end, and the private sector needs to be able to provide adequate, secure and competitive services to reduce the cost and increase accessibility, particularly in remote areas.

When it comes to acts of surveillance, civil society needs to do more systematic research to identify how surveillance is being carried out. As of mid-2014, reports of digital surveillance remain speculative and lack empirical evidence to back any claims. Researchers in Yemen, perhaps in collaboration with international donors and institutes, could work together in tracking and identifying cases of digital surveillance and suggest solutions.

Finally, there will be a need for advocacy groups to coordinate their actions, hold discussions with different stakeholders, and suggest policies to limit abuse of power, whether by the government or any other party. For this to be done, it will be necessary to engage more with international and regional actors in this area and pull resources to launch systematic and long-term campaigns and projects that could put the issue of human rights on the internet at the forefront.