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)
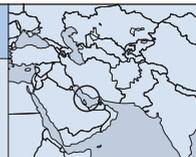AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (HIVOS)

Ali Abdulemam

Introduction

Bahrain is a tiny island in the Persian Gulf, ruled by the Al-Khalifa family since 1783. The population of Bahrain stands at 1,314,089:[1] 46% are Bahraini and the rest are foreigners, mainly workers.

The illiteracy rate stands at 1.13% of the population (2013).[2] At 87%, Bahrain has the highest internet penetration rate amongst Arab countries[3] and also has the highest Twitter usage.[4] Information and communications technologies (ICTs) are very important both to foreigners and the Bahrain economy, which is dependent on financial services and offshore banks. The internet became available in the country in 1994, making Bahrain one of the earliest Arab countries in the region to have internet.

Since the start, civil society activists have used the internet for their activities and communications – leading to the first arrest of an online activist in 1998, the censoring of sites and, recently, spying on activists through advanced surveillance technology.

Civil society organisations depend on the internet for advocacy, as the traditional media is either owned by the regime, or is controlled through publishing law.[5] Publishing stories or media releases on the internet is a way for activists to go viral in Bahrain.

Policy and political background

BahrainOnline.org[6] (BOL) was the first site to be created and funded by online activists. It was started in 1998 during the implementation of the State Security Law[7] (from 1975 to 2001), which allowed the government to arrest anyone for three years without proper investigation or trial. This was also during the Dignity Uprising in Bahrain[8] (1994-2000),

which led to dozens of deaths and thousands of political prisoners. For more than 100 years Bahrain has been known to experience uprisings every 10 years. The regime is also widely known for its human rights violations, torture, discrimination and totalitarianism.

BOL was the main source for opposition opinions and in 2001 during the National Action Charter[9] (NAC), a reform project launched by the new emir, BOL hosted an online debate to discuss it – and similar online discussions have continued since its launch. This has caused a shift from BOL just reporting on stories, to acting as a public opinion maker, often critical of the government.

Campaigns have been launched on the website, and videos and photos of protest activities or human rights violations posted online. The fact that the regime could no longer control the flow of information and news led to the arrest of activists who ran the site in February 2005.[10] The site was blocked in 2002, although massive public interest in the site remained.

Online resistance

In March 1999 the previous emir of Bahrain died suddenly and his son succeeded him to the throne. At that time the Dignity Uprising was struggling, after most of its activists on the ground had been arrested. There was also no political will to move forward with reform, the state security law and its men were controlling the island, and the economy was in difficulties.

At that time BOL started to become popular and received more attention from people trying to find news from different, credible sources.

When the new emir came to power, he promised real reform, allowing people to have their full rights, including freedom of expression, and shifting the power to the people. Basically, he promised to modernise the country. People believed him, and started to debate the NAC. Many started to share their opinions on BOL, using anonymous names which gave them some privacy and security.

1   https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html

2   www.alwasatnews.com/3654/news/read/699870/1.html

3   www.alwasatnews.com/4070/news/read/823318/1.html

4   www.alwasatnews.com/3825/news/read/742134/1.html

5   iaa.bh/ar/arpolicyRules.aspx

6   en.wikipedia.org/wiki/Bahrain_Online

7   www.legalaffairs.gov.bh/LegislationSearchDetails.aspx?id=5682#.U9EIU4BdUZE

8   en.wikipedia.org/wiki/1990s_uprising_in_Bahrain

9   en.wikipedia.org/wiki/National_Action_Charter_of_Bahrain

10 Committee to Protect Journalists. (2005, March 14). Attacks on the Press 2014: Bahrain. *Committee to Protect Journalists*. www.cpj.org/2005/03/attacks-on-the-press-2004-bahrain.php#more

BOL's credibility grew, even though it was run by an unknown group. The government started to pay attention to it in order to get a sense of how citizens felt about the reform project. However, when differences arose between the government and the opposition regarding the new constitution that had been issued by the king without reference to the opposition, BOL played a huge role in revealing the difference between a constitutional monarchy and what the king was offering with his new constitution. Articles were printed from the site and distributed. This again helped BOL to become a credible resource, especially when the opposition depended on it to post messages.

In 2002, during the first election and the opposition's call for a boycott, BOL was the only media outlet supporting the boycott. This led to the arrest of three activists who used to run the site. They were imprisoned for a period of two weeks on the charge of insulting the king, broadcasting hate speech and posting false news.

During this time BOL moved from being an online platform to playing a role "on the ground", arranging protests, visiting hospitals and even issuing media releases when important things were happening. BOL was covering the protests live, and posting pictures of events that may not have appeared in the traditional media. At times it wrote investigative stories about corruption. This led to the site being blocked in 2002.

Blocking BOL showed how loyal people in Bahrain were to the site. They shared proxies between them and members wrote a script to open the site. They used Dynamic DNS to create redirected links. When the links were censored, members shared a document on how to create your own link with readers. This kept BOL up and running, and, with 80,000 hits a day, it became the most read site in Bahrain.

This was the first hint of how people could train themselves to use new technology to avoid censorship in Bahrain. During the arrest of the administrators of BOL, the members organised several protests themselves, asking for the release of the administrators, and the dropping of charges against them. This led to widespread coverage in the media, and the release of the administrators without trial.[11]

During the arrest of the BOL administrators, the government discovered that they lagged behind in technical knowledge, and that they had failed to understand the nature of the internet. They started to use new tools to censor the opposition websites. But, again, people learned how to bypass the new censorship technology.

In February 2009, a member of BOL using the nickname "äÇÒß ÇáãáÇ̧ÆßÉ"[12] posted the full list of the names of the employees of the National Security Apparatus (NSA). Two months later,[13] on 14 May, Hasan Salman was arrested and charged with "publishing secret information over the internet".[14] In September 2009 Hasan was sentenced to three years by the High Criminal Court.[15] He was recently released.

After this incident, and the same year, the Telecommunications Regulatory Authority (TRA) issued new regulations for internet service providers (ISPs)[16] saying that all ISPs should retain their communications logs for three years, as well as providing technical access for the NSA to monitor or block online communications in Bahrain. This regulation was greeted with huge opposition from the media, NGOs and members of parliament. However, it seems it will be implemented soon.[17]

In 2010, when the government arrested human rights activists, public figures and bloggers (including a BOL administrator for the second time), the NSA confronted them with printouts of SMS text messages and emails, even though their devices had not been confiscated by the authorities.[18]

The only explanation for this is that the government had bought new surveillance technology, and installed it at all the ISPs. This includes the Bahrain Internet Exchange (BIE), as stated by Mai Al Khalifa[19] in her first resolution in 2009 as minister of culture and media. This forced all ISPs to provide access to the government to block websites by installing the necessary equipment. This resolution was received negatively by NGOs and online activists.

When the Arab Spring started, the youth tried to organise themselves in a movement to push forward with reform. BOL was the platform used to talk about the idea,[20] plan it,[21] organise it, and cover it, second by second. They called this push the Day of Rage and issued media releases stating their demands.[22] Because people started to learn online

11   https://www.youtube.com/watch?v=-GrIfNi74hw

12   bahrainonline.org/showthread.php?t=229316

13   freehasan.wordpress.com/2009/05/15/arrest

14   freehasan.wordpress.com/calendar

15   freehasan.com/?p=310

16   www.tra.org.bh/media/document/
     PublishedLawfulAccessRegulation-1.pdf

17   www.alwasatnews.com/2393/news/read/44106/1.html

18   Silver, V., & Elgin, B. (2011, August 22). Torture in Bahrain becomes routine with help from Nokia Siemens. *Bloomberg*. www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

19   www.alwasatnews.com/2323/news/read/33266/1.html

20   bahrainonline.org/showthread.php?t=258985

21   bahrainonline.org/showthread.php?t=259468

22   bahrainonline.org/showthread.php?t=259370

security tactics the government could not recognise or arrest the people behind the uprising.

When the crackdown started in Bahrain, the international media turned its back on what was going on in the country. Only the internet and the youth who believed they could bring about change kept the uprising alive, and now after three and a half years the movement in Bahrain is still alive because of them.

In 2012, Alaa Alshehabi,[23] among other activists, received suspicious emails from someone claiming to be from Al Jazeera. The attachment was infected with the FinFisher virus, sold by a UK-based company. An investigation by BahrainWatch.org led to the discovery of others infected by the same spy tool and raised awareness in Bahrain about the new technology that the government was using to attack activists.

BahrainWatch.org found that after the release of their IP Spy[24] report, no new activists were targeted. The investigation also found that the awareness of online security by activists is high, and that even non-activists have started to download encryption tools and more secure instant messaging.

Conclusions

In February 2014, the king ratified a law that severely punished those who insulted him, with from three to seven years imprisonment and a fine of up to USD 1,000. The problem is not with insulting the king as much as with the way the government is using the laws to take revenge on the opposition. Recently more than 15 people are either in prison or awaiting trial for using the internet. Some of them are accused of insulting religious symbols or figures, and some of them for insulting the king or the prime minister.

We also came across stories that people had been fired from their work because they had "liked" an article on Facebook, while others had their telephones stolen because pictures or a chat had been found on them.

Freedom of expression is defined as a universal human right which is needed by all human beings, and it should be protected by governments. Bahrain has ratified laws which should protect freedom of expression, but in reality the opposite happens: those laws are used as "political revenge", as the UN spokesperson said at the Human Rights Council in Geneva. Bahrain failed to obey 176 recommendations by the Human Rights Council in May 2012.

Internationally respected NGOs are keeping pressure on the Bahraini government to free bloggers, photographers, and human rights and political prisoners, as well as to stop human rights violations, but nothing is changing. Bahraini activists are simultaneously receiving international awards even though they are still in jail under fake charges, like Ahmed Humaidan, who has been imprisoned for 10 years.

If the international community cannot put pressure on the regime to start reform to meet the demands of the people in Bahrain, at least we should put pressure on companies to stop selling surveillance technology to Bahrain that is used to violate human rights. When spy tools are sold to the government, human rights defenders will have to work harder, they will not be able to move freely, they will not be able to communicate and document stories, and they will always feel as if their ICT devices are a weapon being used against them.

We should not accept the argument that companies are not responsible for the way their products are used; they know that some countries have a bad human rights record and a long history of attacking activists. This technology will definitely be used to violate human rights.

Action steps

The state of Bahrain is using laws to repress remaining freedoms as a method of "political revenge". Selling it technology that allows it to do this is not making the world a better place. With more than 20 online activists and photographers in jail right now, and more than 15 journalists and bloggers living in exile, we should launch a global campaign against selling surveillance technology to Bahrain. We should also argue that the companies that sell this technology to governments should uninstall it remotely. By sharing information with the public on the kind of technology used, and through offering training, citizens can learn how to protect themselves online.

Over the past 16 years the people of Bahrain have managed to teach themselves how to avoid censorship or use secure routes for their online activities. But we should not rely on them continuing to understand the new surveillance technology entering the market, and being able to fight it.

23 Doward, J. (2013, May 12). UK company's spyware 'used against Bahrain activist', court papers claim. *The Guardian*.

24 https://bahrainwatch.org/ipspy