UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Middle East and North Africa CyberWatch: January 2013

A biweekly report on trends in online censorship, information operations,

and Internet use in the Middle East and North Africa

Table of Contents

CENSORSHIP AND FILTERING

Middle East and North Africa: Blue Coat used in several countries in the region

This month, the Citizen Lab released a report detailing the extent to which products created by Blue Coat Systems, an American network security company, are used in many countries across the world, including several in the Middle East and North Africa. In 2011, the Citizen Lab found evidence that Blue Coat devices capable of censorship and surveillance were actively in use in in Syria and Burma. This latest report reveals the presence of Blue Coat in Bahrain, Kuwait, Qatar, Saudi Arabia, Egypt, the United Arab Emirates, Iraq, Turkey, and Lebanon, among other countries. ProxySG and PacketShaper, the two technologies covered in the report, are capable filtering websites, blocking content according to category, and monitoring Internet traffic. While these devices may have legitimate uses, the report raises concerns that technology possessing "dual-use" functionality (i.e., both a commercial and possible military or surveillance application) may be used to undermine human rights in countries where basic freedoms are frequently curtailed by state authorities.

IRAN: New directives for monitoring text messages

With the approaching presidential election, Iranian authorities are taking measures to avoid a recurrence of the 2009 post-election unrest. The Ministry of Culture and Islamic Guidance has urged [Farsi] mobile operators to start monitoring the content of text messages. The Ministry's statement went viral on social networking websites. A few hours later, the Deputy of Iran's Communications Regulatory Authority clarified that only text messages sent by corporations as advertisement would be monitored. In addition, the Communication and Information Technology News Agency, an online news agency, has speculated [Farsi] that text message filtration in Iran happens at the key word level. For example, messages containing words like "currency" and "dollar" were filtered during the last year's currency crisis. Recently, it appears that text messages with the word "institute" have been filtered.

IRAN: Filtering of popular online computer games

Travian, the most popular online game in Iran, was filtered [Farsi] on January 1 by order of the Commission to Determine Instances of Criminal Content. Although the government lifted [Farsi] the block on January 9, this incident showed how Iranian censors have increasingly targeted online computer games. According to a report by Gerdab website [Farsi], owned and run by the Iranian Revolutionary Guard Corps Cyber Command, computer games aim to "introduce Islam as the origin of terrorism, and against the other religions in the world." Travian has been particularly criticized because the game's objective is to build a powerful and prosperous city and to control as many cities as possible. Fars News Agency also published [Farsi] a statement by a group of computer game developers, who support the filtering of non-Iranian computer games to support domestic game developers.

JORDAN: Jordanian upcoming elections highlight concerns over Internet Freedom

As Jordan heads toward parliamentary elections at the end of January, Internet freedom activists have raised concerns over the possibility that the post-election government will move forward with media censorship laws. Of particular note is a legislation that would force media sites to register with Jordan's Ministry of Press and Publication and require service providers to implement centralized filtering of pornographic websites. January 18 marked the deadline for websites to register with the Ministry. Administrators who failed to register were supposed to go offline, although the majority of sites have not done so. As previously reported, a grassroots movement in Jordan has developed in opposition to this set of legislation.

GAZA and the WEST BANK: Facebook “censors” Israeli-Arab journalist

Facebook deactivated the account of Khaled Abu Toameh, an Israeli-Arab journalist, for what it describes as “terms of use” violations. The deactivation occurred after complaints from the Palestinian Authority and Jordanian Security Services, which Abu Toameh alleged were a result of articles posted on his page criticizing the Palestinian Authority. In the past, the Palestinian Authority has arrested its citizens for posting criticism about the government on their respective Facebook pages.

SYRIA: YouTube accidentally closes accounts of human rights group

YouTube admitted to accidentally shutting down accounts belonging to the Syrian Observatory for Human Rights, a group monitoring violence relating to the ongoing civil war in Syria. The group had received messages from YouTube that those accounts were posting violent and “offensive” videos. All accounts associated with the group have subsequently been reinstated.

BLOGGER AND NETIZEN ARRESTS

ALGERIA: Hacker arrested in Thailand

Hamza Bendelladj, an Algerian hacker who allegedly stole millions of dollars from private bank accounts and financial institutions using a trojan/botnet known as Zeus, was arrested by Thai police at the airport on January 6. According to Thailand’s immigration police, the United States requested his arrest on charges of banking fraud. He will likely be extradited to the US, where he has been on the FBI’s wanted list for several years.

IRAN: Blogger arrested for insulting a governmental organization

Mohammad Reza Jahanshiri, chief of Bushehr Province’s branch of Iran’s Cyber and Information Exchange Police (FETA), reported [Farsi] that a blogger has been arrested for publishing posts deemed offensive to a Bushehri government organization. According to Jahanshiri, the arrested blogger has confessed to his “alleged offence” and is now awaiting trial.

KUWAIT: Arrests of online activists over Twitter comments

Ayyad al-Harbi, a Kuwaiti blogger, was sentenced to two years in jail for criticizing the government on his Twitter account. The government also handed out a jail sentence to opposition activist Rashed al-Enezi, who has been accused of insulting the Kuwaiti Emir on Twitter. Arresting Kuwaiti citizens for online comments is not unknown in the country; several members of the Kuwaiti royal family have been arrested for posting anti-government views through social media.

OMAN: Jail terms upheld for bloggers

An Omani court has upheld jail terms between one year and 18 months for eight bloggers and writers accused of defaming the monarchy. As previously reported, lèse majesté arrests in Oman were common in 2012. State prosecution of "online crimes" has been made significantly easier through Oman’s Cyber Crime Law enacted in 2011.

Tunisia: Blogger stands trial for accusing foreign minister

The public prosecutor's office in Tunisia is investigating Olfa Riahi, a blogger and independent journalist, for alleging that Foreign Minister Rafik Abdessalem misused public funds to pay for personal accommodations at the Sheraton Hotel. The Tunisian press has named the incident "Sheraton Gate." Riahi also posted leaked communication implicating Abdessalem in the acceptance of "a one million dollar gift from the state of China" without proper budgetary oversight. The minister's legal team has accused Riahi of "violating article 86 of the telecommunications code, articles 89 and 90 of Law 63-2004 on the protection of privacy, articles 126, 148 and 253 of the criminal code, and finally article 54 of [the new press law]." Reporters Without Borders condemned the use of criminal, telecommunications, and privacy laws to punish press freedom.

CYBER ATTACKS

SAUDI ARABIA: Majority of Saudi companies at risk of cyberattack

According to a report published in Saudi newspaper Al-Eqtisadiah, Symantec, a global computer security company, has found that 69 percent of Saudi companies are unprepared for potential cyber attacks. A Symantec representative stated that Saudi companies' "lack of data backup operations on a daily basis" is their biggest vulnerability to data loss or theft. Last August, Saudi Aramco, the country's national oil company, was hit by a widely publicized virus called "Shamoon," an attack that United States and Israeli officials blamed on Iran. Symantec also alleged in its annual Norton Cybercrime Report that cybercrime cost Saudi Arabian consumers some SR 2.6 billion in 2012, launched primarily via social network and mobile phone exploits.

SYRIA: Syrian Electronic Army leaks government documents

On January 21, Al-Akhbar, a Lebanese newspaper, reported that the Syrian Electronic Army (SEA) would soon release "secret documents from Turkey, Qatar, and Saudi Arabia" through its English language website. The collection of e-mail exchanges, contracts, and official papers purportedly clarify the role that foreign governments have played in the Syrian conflict. The first set of documents, taken from the Qatari Ministry of Foreign Affairs and dubbed "Qatar Leaks," was released two days later on Al-Akhbar and the SEA's website. The files include a transcript of a meeting between the Qatari Prime Minister Hamad bin Jassim and Egyptian President Muhammad Morsi in which the two intimate support for the Syrian opposition.

UAE: Activists hit with targeted malware

Bahrain Watch reports that an activist in the United Arab Emirates (UAE) was recently the target of a malware attack via a suspect e-mail. The e-mail text linked to a video containing an embedded Java applet. Days earlier, international news media reported a massively exploited Java vulnerability, causing the United States' Department of Homeland Security to warn users to disable Java on their computers. In the UAE activist's case, the exploit's payload appeared to be a spyware program that would grant the attacker keylogging, password stealing, and screen viewing capabilities on the victim's computer. Based on similar incidents that have occurred over the past several months, Bahrain Watch believes that the Emirati government is ultimately responsible for the targeted malware attacks.

IRAN: Unconfirmed cyber attacks against a petrochemical plant

Asr-e Ertebat [Farsi], a weekly online magazine, and Fars News Agency [Farsi] reported that 1,072 cyber attacks have been directed against a petrochemical plant. Based on government speculation, the news agencies believe that the attacks originated from Israel. Iran's National Computer Emergency Response Team (MAHER) has not confirmed the news and the story has received little coverage in the international media.

TECHNOLOGY

IRAN: Smart software to control social networking websites

Iran's chief of police, Esmail Ahmadi Moghadam, announced [Farsi] that Iran plans to develop software for controlling social-networking sites. Ahmadi Moghadam believes that "smart control" of social-networking sites is more useful than filtering because the "harm of social networking websites would be avoided, and at the same time, people could benefit from their useful features." However, Nima Rashedan, an Iranian tech expert based in Switzerland, expressed doubt that Iran has the adequate infrastructure and knowledge to produce such software. Rashedan believes that the announcement was made without "knowing the exact technical difficulties of the project."

IRAN: Recent updates on the status of National Information Network

Iran's Deputy of Communications and Technology at the Ministry of Information and Communications Technology stated [Farsi] that more governmental organizations are gradually being connected to the National Information Network (NIN). Deputy Communications Minister Ali Hakim Javadi also added that at this time the NIN is completing the data sharing system between organizations and making the single-window system for services operational. Javadi announced recently [Farsi] that the International Exchange Center will soon be launched. This centre would act as a "switch," which connects governmental organizations to one another and enables them to share and transfer information.

IRAN: Planning the National Network of Cyber Defence

Alireza Rahai, chancellor of Amirkabir University of Technology, announced [Farsi] that, in collaboration with the Ministry of Information and Communications Technology, a national network of cyber defence will be launched. Rahai added that it is crucial to prepare for an increasing number of cyber attacks that could potentially target Iranian infrastructure. Rahai said that the recently formed Information Security group at Amirkabir University will engage in research and software development in the areas of cyber defence and information security.

Read previous editions of the Middle East and North Africa Cyber Watch.