UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

The Citizen Lab

Middle East and North Africa CyberWatch: June 2013

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

and Internet use in the Middle East and North Africa

Table of Contents

FEATURED NEWS

IRAN: Special Election Report

The eleventh Iranian presidential elections took place on June 14, 2013 and resulted in the victory of moderate candidate Hassan Rouhani. Both leading up to and during the elections, Internet services and individual websites came under particular scrutiny.

On June 3rd, Google announced that in recent weeks a significant number of Gmail users in Iran had come under phishing attacks. Google identified the source of these attacks as emanating from Iran. Prior to the official announcement of the coalition between reformist candidate Mohammad-Reza Aref and moderate candidate Hassan

Rouhani, there were reports that the website endorsing their political coalition had been blocked in Iran. Furthermore, during this time multiple websites belonging to organizations and entities critical of the Iranian government came under attack. Among the attacked websites were Defenders of Human Rights Center, Khodnevis, Saham-News, the Communist Party of Iran, and Green Wave Voice. A number of websites were defaced with the logo of a group called 'Unknown Cyber Jihad' (Jahad-e Gomnam-e Majazi).

As previously reported, Internet users in Iran faced other difficulties during the lead up to the elections. In a recent statement, the country's Minister of Communications, Mohammad-Hassan Nami stated that reducing Internet speed during the election period was a security and intelligence related strategy, employed for maintaining calm in the country. His statement contradicts an announcement made prior to the elections by Nami's deputy, stating that any disruptions in Internet services would not be related to the elections.

CENSORSHIP AND FILTERING

IRAN: US lifts digital sanctions

On May 29, Wendy Sherman, the State Department's Undersecretary for Political Affairs, announced that the United States' has decided to lift sanctions on communication devices, software, and services to Iran. Sherman explained that "general license will allow both software and hardware to move forward to Iran and to the Iranian people so that they can have freedom to communicate with each other in ways that they don't always have." This decision came just a few weeks prior to the Iranian presidential elections.

JORDAN: Government blocks hundreds of unlicensed websites

The Jordanian government has ordered the blocking of nearly 300 websites, citing compliance with the country's Press and Publications Law. The law states that news sites must register for a license in order to operate fully in Jordan. Jordan's Press and Publications department has clarified that its decision to block unlicensed sites will not curtail press freedoms. Reporters Without Borders, however, published an open letter to Jordanian King Abdullah, in which they argued that the registration provision will create a "permanent threat" to journalistic freedom if an editorial stance goes against government views and policies.

SAUDI ARABIA: Viber and WhatsApp banned

Saudi Arabia's telecommunications regulator prohibited the use of web-based communication application Viber in the kingdom. Viber allows for free calls and instant messaging over the Internet. Saudi authorities also plan to block WhatsApp, a similar messaging application, if its distributors fail to comply with state regulations. Suggestions have been made online that the government's push to curtail use of these applications is partially meant to eliminate platforms that are difficult for the state to monitor, as well as to prevent the use of free applications that may diminish revenue flows to state-controlled telecom operators.

BLOGGER AND NETIZEN ARRESTS

MOROCCO: Arrest of blogger in Italy for terrorism related charges

Anti-terrorism police in Italy have detained a Moroccan blogger on the grounds that he plotted terrorist attacks. The blogger, named Anas El Abboubi, is facing charges of "recruitment aimed at international terrorism and inciting racial, ethnic and religious hatred" through his blog, Sharia4Italy [Italian]. Italian police also claim that the blogger used the Internet to search for instructions on "weapons and warfare techniques."

SAUDI ARABIA: Detained Saudi writer released

Novelist Turki al-Hamad, who had been detained by Saudi authorities for remarks made on Twitter, was released this month. Al-Hamad was arrested last year for tweets calling for a "renewal" of Islam and criticising religious extremism. As previously reported, activists using Twitter have been arrested for comments made on the social media platform. Saudi Arabia has also sought to limit access to Twitter to citizens who register to use the site using their personal identification papers.

CYBER ATTACKS

THE GULF: Anonymous targets Gulf energy companies

In May, Anonymous announced that it would target oil and energy companies on June 20 in an attack it called "Operation Petroleum." While its list of targets included the United States, Canada, and China, Anonymous singled out Saudi Arabia and blamed a Zionist "New World Order" for "control[ling] the population of the world like robots." According to a security analyst at Symantec only a "couple of Web pages and networks were attacked" on June 20, while another "security expert" claimed that no major damage was done to energy companies' computer networks. However, Trend Micro, a Tokyo-based security software company, reported that a number of government websites in Kuwait, Saudi Arabia, and Qatar had been taken offline. In August 2012, Saudi Aramco and RasGas, a Qatari energy firm, were both the targets of a malware attack, an act which the United States blamed on Iran.

IRAN: Ministry of Petroleum denies cyber attacks

Ahmad Tolaei, the ICT Manager of the National Iranian Oil Company (NIOC), dismissed rumours that a cyber attack had disrupted the websites of the NIOC and Ministry of Petroleum (MOP). Tolaei stressed that the content on the websites was highly secure and attributed the disruption to an issue with the fiber-optic telecommunication lines. The MOP has been the target of a cyber attack in the past.

KUWAIT: Online swindling on the rise

Kuwait's Acting General Director for Criminal Detectives Administration recently warned that "online swindling" has increased of late and "has started affecting the economy." He suggested that individuals and businesses practice heightened vigilance and called for better information security training.

UAE: Emirati ISP launches security solution to prevent cyber attacks

Etisalat, Dubai's leading Internet service provider, now offers a security solution that it claims will guard against Distributed Denial of Services (DDoS) attacks. The "Managed DDoS Mitigation Service" will allegedly detect DDoS attacks at the backbone level to prevent them from reaching customers. Etisalat will offer the service to non-residential customers, including business and government entities. At the time of Etisalat's announcement, UAE-based companies were reportedly on guard following Anonymous' "Operation Petroleum" threat.

TECHNOLOGY

BAHRAIN: OECD considers complaint against Gamma International

The Organisation for Economic Cooperation and Development (OECD) has agreed to consider a complaint filed against Gamma International, a UK-based company responsible for developing and providing spyware like FinFisher to governments with questionable human rights records. Several human rights groups, including Privacy International, Reporters Without Borders, Bahrain Watch, the Bahrain Center for Human Rights, and the European Center for Constitutional and Human Rights, initially filed the complaint on February 1 along with an additional complaint against German firm Trovicor (formerly Nokia Siemens Networks). The groups argued that there is reason to believe that “Gamma International and Trovicor have facilitated multiple human rights abuses in Bahrain, including arbitrary detention and torture, as well as violations of the right to privacy, freedom of expression and freedom of association.” Citizen Lab researchers have been instrumental in uncovering the proliferation of Gamma International’s spyware products across the globe.

IRAN: Offering legal VPNs to individuals and organizations

Alireza Shah-Mirzaei, the Deputy at the National Center for Cyberspace announced that individuals would soon be able to register for Virtual Private Networks (VPN) on www.vpn.ir. Registration for legal VPNs began last year and, according to Shah-Mirzaie, many organizations and institutions are currently using this service. According to the National Center for Cyberspace, these legal VPNs are solely for establishing communication from inside the country to the outside, and do not include local VPNs. He added that the legal VPNs cannot be used as circumvention tools, and users need to get in touch with the Committee to Determine Instances of Criminal Content Online with regards to filtering. The reason for VPN use is among the required questions in the registration form. At the time of writing, the website www.vpn.ir was not available.

IRAN: Iran the number one victim of information surveillance

Based on a map by Boundless Informant, the National Security Agency’s (NSA) data mining tool, Iran ranks the highest on the list of countries under surveillance. Bahar Newspaper mentioned that out of the 97 billion information packages monitored by the United States, 14 billion belonged to Iran.

IRAN: Iran equipped to offer "clean Internet" to Iraq

During an official visit to Iraq by the Technical Deputy of Iran’s Ministry of ICT, both countries expressed readiness for strengthening and expanding infrastructural communication lines. Iran also announced that, given the close cultural and religious ties between the two countries, it would be prepared to offer "clean Internet" services to Iraq in order to expand the telecommunication ties between the two countries.

IRAN: Statements by the Minister of ICT

Iran's Minister of Communication has claimed that Iran ranks among the top five countries in terms of cyber defense. Mohammad-Hassan Nami, the Minister of Communications, made references to attacks such as Stuxnet and Duqu, and praised the country’s young experts in the field for dealing with such threats effectively. In a separate statement during the inauguration ceremony of a Qom data center, Nami commented that websites such as Wikipedia and Google Earth act as intelligence gathering mechanisms for Western governments. To this end, the Minister of Communications mentioned that Iran is working toward creating a website with Iranian-Islamic content which would be presented in different languages for the world.

TUNISIA: Tunisia holds summit on Internet freedom, allows glimpse at hardware

On June 17 and 18, Tunisia hosted the third annual Freedom Online Coalition summit. The conference brought together activists, policy makers, and industry representatives to discuss three key issues: “Internet freedom and security, digital development and openness and online privacy and transparency.”Ahead of the summit, the Tunisian Internet Agency (ATI) gave local Tunisian hackers access to machines used by the Ben Ali regime "to monitor Internet usage." The ATI intends to turn the space formerly dedicated to monitoring citizens’ communications into the “404 Lab,” in which they will hold workshops and host projects devoted to Tunisian Internet governance.

Read previous editions of the Middle East and North Africa CyberWatch.