# Flygtningenævnets baggrundsmateriale

| | |
|---|---|
| **Bilagsnr.:** | **437** |
| Land: | Syrien |
| Kilde: | Reporters Without Borders |
| Titel: | Syria: Online tracking is a family affair – Syrian Telecommunications Establishment (STE), Syrian Computer Society (SCS) |
| Udgivet: | 12. marts 2014 |
| Optaget på baggrundsmaterialet: | 23. april 2014 |

# Syria: online tracking is a family affair

## Syrian Telecommunications Establishment (STE), Syrian Computer Society (SCS)

**In March 2011, the government of President Bashar Al-Assad violently cracked down on peaceful demonstrations calling for democratic reforms. The authorities strengthened their control over all means of communication, including the Internet. This was relatively straightforward because of the stranglehold the authorities and the Assad family have over the telecoms infrastructure through three companies – the Syrian Telecommunications Establishment (STE), the Syrian Computer Society (SCS) and Syriatel. These companies ensured a reduction in Internet capacity in order to slow down the circulation of news and images of the demonstrations and the subsequent crackdown. With the help of units within the security services, they can deploy a whole armoury of weapons to monitor the Web and trace activists and dissidents.**

## Control over the infrastructure

In 2011 figures, nearly 4.5 million Syrians, 20 percent of the population, were connected to the Internet network, which is controlled by two bodies: the Syrian Telecommunications Establishment (STE) and the Syrian Computer Society (SCS).

The STE, more commonly known as Syrian Telecom, is headed by President Assad and comes under the ministry of communications and technology.

There are a number of Internet service providers in Syria but the STE, the government-run ISP, is key since all the others depend on it and it controls most fixed connections. It has granted other ADSL operators the use of its cables. Alternatively, users connect via landlines and 56K modems. It administers all connection points between Syria and the global Internet network.

When the government orders the blocking of a word, of a URL or of a site, the STE transmits the order to service providers.

The SCS was set up in 1989 by Bassel Al-Assad, the eldest son of Hafez Al-Assad, with the declared aim "to diffuse informatics culture by means of organizing conferences, symposia, seminars, lectures, and exhibitions, in addition to producing TV programs and issuing pamphlets concerning IT".

The STE controls the cable network and the SCS all wireless networking, since it owns the 3G network infrastructure throughout Syria. After the death of Bassel, Bashar Al-Assad took over as head of this body, which is now controlled by his wife, Asma.

Syriatel is a mobile network operator owned by Rami Makhlouf, a cousin of Bashar Al-Assad's and it has no qualms about placing its technology at the disposal of the government in order to monitor the Internet.

## The watchful eye of the security services

In addition to these bodies, each branch of the security services has a section devoted to Internet-related issues. The political security department and the state security department monitor the activities of Internet cafés. They make no bones about privatising surveillance by paying individuals to browse the Web, infiltrate Facebook groups and compile reports for the security services.

## Syria's electronic army

The Syrian Electronic Army (SEA) first appeared on Facebook in April 2011. In mid-May 2011 a site was launched by "Syrian enthusiasts" to fight those who use the Internet, and especially Facebook, to spread hatred and destabilize security in Syria. The Syrian Electronic Army is not officially linked to the government but reports indicate that the domain name of the SEA was registered on 5 May 2011 by the Syrian Telecommunications Establishment and the site is hosted by SCS-NET, the SCS Internet service provider.

The cyber army floods the pages and websites that support the protests with pro-Assad messages and tries to discredit the opposition. Twitter accounts have been created to compromise information published under the hashtag #Syria. The SEA also hacked the Twitter accounts of several news organizations in 2013, including Reuters, the Associated Press, the Guardian, the Washington Post, the Atlantic Wire, CNN, Time and Al-Jazeera.

## Jihadists play the same game

Unfortunately, the Syrian government is not the only agent of repression and control of information on the Internet. Jihadi groups such as Jabhat Al-Nusra and the Islamic State of Iraq and the Levant (ISIS) also monitor news and information online. These organizations do not have the resources of the Syrian government but are still able to monitor social networking sites and infiltrate Facebook groups.

Muhammad Al-Salloum, the editor of the magazine Gherbal, was forced to flee the country after he was kidnapped by ISIS in the southern outskirts of the city of Idlib in the Kafr Nabl region. The judge appointed by the group accused him of apostasy in his work as a journalist and the reports on the armed group that he posted online. The judge was particularly interested in the online activities of his fellow journalists, such as Mohammad Mallak, editor of the magazine Dawda.

## Beware the malware trap

Internet content filtering, as carried out by the STE, is aimed at censoring all criticism of the government as well as the websites of opposition parties, Kurdish and Islamic sites, some news organizations and blogs, and foreign and domestic human rights organizations. The use of tools to bypass censorship and log on to censored sites is banned.

For years records have been kept of Internet users in Syria. Internet café owners must log users' identities and usage times, as well as which computer was used. This information is then sent on to the security services. The IP addresses of machines in Internet café are registered and cannot be changed without prior agreement.

Anyone wishing to take out an Internet subscription must provide the ISP with a copy of their identity card and the telephone number of the line hat they plan to use for Internet access.

The authorities use a huge array of techniques to gain access to the Facebook accounts and email inboxes of government opponents. Phishing, "man in the middle" attacks and planting malware are frequently used in Internet attacks in Syria. Syrian authorities have taken advantage of Iran's expertise in online surveillance and has used filtering equipment supplied by the U.S. firm Blue Coat, named an "Internet enemy" by Reporters Without Borders in 2013. The case shows just how important it is to keep track of Internet surveillance and censorship equipment that is exported.

## Dissidents voices silenced

Such Internet surveillance has allowed the government to arrest many Syrian activists, media workers and dissidents since March 2011. Syrian security services have launched an all-out manhunt for news providers who assist or have contact with foreign news organizations or reporters. Dozens of Syrians involved in the news industry have been arrested and tortured after giving interviews to foreign news organizations about the repression in their country.

The experiences of those who have been released are enlightening: the intelligence agents who questioned them knew all about their activities and their contacts. Countless people have been arrested for "liking" a page supporting the uprising or for posting videos of demonstrations. Some of these cases are listed below:

Taymour Karim, a 31-year-old doctor, took part in anti-government protests. After his arrests in December 2011, he refused to divulge the names of his friends. However, his computer had already yielded its secrets to his interrogators. "They knew everything about me," he said. "The people I talked to, the plans, the dates, the stories of other people, every movement, every word I said through Skype. They even knew the password of my Skype account."

**Shaza Al-Maddad**, a contributor to several commercial news organizations such as the opposition news site *all4syria.info*, was arrested by Syrian intelligence in November 2012. She was held for 60 days by the security services then imprisoned for more than 9 months. The government seized all her belongings and froze her assets. She managed to flee to Lebanon in September last year and now lives in Europe.

**Ali Eid** was the Syria correspondent of the Saudi newspaper *Akkad* and also worked for the Syrian news agency Sana until he resigned in June 2012. He was arrested several times for reporting on mass demonstrations and on abuses carried out by army troops. In March 2012, government militiamen insulted and beat him up because of his news reports from the Deraa region.

Eid was summoned several times by the air force intelligence service. He was subjected to ill-treatment and abuse during questioning after his final summons in September 2012, when it was discovered he had contributed to foreign news organizations including Al-Jazeera.

Eid decided to leave for Egypt and then moved to another nearby country in January 2013.

This entry was posted in Enemies of the Internet and tagged Ali Eid, Shaza Al-Maddad, Syrian Computer Society (SCS), Syrian Telecommunications Establishment (STE), Taymour Karim on 11 March 2014 by moyenorient3.

← United Kingdom: World champion of surveillance