Syria's cyberwars: using social media against dissent
By: Mark Clayton, The Christian Science Monitor
25 July 2012

For years, average Syrians were blocked from Facebook, YouTube and other social media by Bashar al-Assad's repressive police-state government. Early last year, however, as the Arab Spring swept through the region, something odd happened: the social media sites that were pivotal to uprisings in other Arab nations were suddenly switched back on.

Now we know why: It's easier to track people –and find out who is against you – if you can monitor computer traffic to such sites, or trick visitors into clicking on tainted links that download spyware onto their computers, rights activists and cyber experts say.

To a far greater degree than Libya, Egypt or perhaps any other nation in the Arab world, Syria's government has succeeded in flipping activists' use of digital tools and social media to the government's own advantage, cyber experts with an eye on Syria say.

A "Syrian Revolution" page showed up on Facebook in March 2011, winning 41,000 fans in just a few days, and 138,000 a few weeks later, a recent report found. By last month, it had 438,000 fans. But frequenting such pages may be potentially hazardous, as well as educational or motivational.

"Online social media, which virtually anyone can use from home, played a central role in the Syrian uprising and helped break the decades-old government media monopoly," Amjad Baiazy, a Syrian researcher living in London writes in a new study published last month by MediaPolicy.org, a London-based new media think tank. "But it helped the Syrian government crack down on activists."

As bombs fall and bullets fly, dissidents and opposition figures have had their favorite social media tools turned against them, and their cloak of anonymity pierced by veiled online hackers loyal to Syria's government.

Last fall, the government bought centralized Internet eavesdropping equipment. But dropping spyware directly onto activists' computers is Syria's newest cyber war trend.

Luring opposition sympathizers with tainted video links in e-mail, fake Skype encryption tools, tainted online documents, hackers believed allied to Syria's government have in recent months deployed an array of powerful spyware with names like DarkComet, backdoor.bruet, and Blackshades. Available on the Internet, these malware are used to infiltrate the personal computers of opposition figures, rights activists and send back information on their friends and contacts as well as passwords, cyber security experts say. Impact of this spying is hard to gauge. But even as the physical battle intensifies in around Damascas, Syria cyber watchers are worried.

The Syrian regime had long blocked access to social media sites, says Richard Zaluski, president of the Center for Strategic Cyberspace and Security Science, a London-based think tank.

"Blocking, however, prevented the tracking down of activists, so the regime ultimately responded by unblocking sites such as Facebook, YouTube, and Twitter," he writes in a recent analysis posted on the group's website. "This move enabled the regime's security apparatus to conduct its internal cyber war against its own people and aided in tracking down the identities of activists."

Alongside open electronic forums, blogs have been used by thousands of Syrians to launch a counteroffensive against the government's curbs on public expression, Mr. Baiazy's study, called "Syria's Cyber Wars," notes. These forums also provide a way for users to share information on how to bypass government website blocking. At least seven Facebook groups provide Syrians with technical means for remaining anonymous while on the Internet.

Even so, social networks and blogs in Syria have not had quite the same impact they have had in Iran and Egypt, according to Baiazy. The Internet is "still accessible by a relatively small portion of the Syrian population, and it is still limited to the elite," he writes. Just 16.4 percent of the Syrian population has Internet access, compared to 47 percent in Iran.

With Syrian activists being detained in large numbers, there are concerns that at least some portion of those are being identified by government-sponsored hackers, says Eva Galperin, with the Electronic Frontier Foundation, an Internet rights group.

Human Rights Watch has identified some 20 different torture centers in Syria. So the potential consequences for someone whose computer becomes "infected by malware written by someone in the employ of Syrian security forces are dire," Ms. Galperin says.

"It's clear that the Assad regime has learned lessons from Libya, Tunisia and Egypt and that's why they are pursuing this tactic," she says. "Using malware to infiltrate individuals' computers is a characteristic of the Syrian conflict that's not been widely seen in other Arab-spring uprisings."

To watch dissidents' activities online, the Assad government has deployed Branch 225, the secret Syrian communications security department in charge of Internet monitoring, according to both Mr. Baiazy's study and Mr. Zaluski. As part of that effort, Syria last year purchased millions of dollars of Internet filtering equipment – much of it made in the US and Europe – to track communications to Facebook and other sites.

But all that high-tech equipment has proved increasingly less effective since Facebook, Twitter, YouTube, Google and others began encrypting by default communications between their sites and users' computers, Galperin and other experts say.

As a result, Syria's government is resorting to state-supported actors who are launching attacks that take over online accounts without the user knowing it. In other cases it's meant forging fake Facebook pages to steal activists' passwords. Security forces have also used torture against captured opponents to obtain the passwords to their Facebook and email accounts, Mr. Baiazy reports.

Amid this turmoil, the Syrian Electronic Army, a hacker militia loyal to the Assad regime, has come to the fore. It is this later group that infiltrates opposition computers directly that's apparently moving hard after activists' identities by taking spyware available on the Internet –and customizing it to be invisible to anti-virus security.

"What we've seen in Syria is a campaign targeting activists with surveillance malware," says Morgan Marquis-Boire, a cyber-security researcher with Citizen Lab, a Toronto-based computer security think tank.

His research, which has involved analyzing malware captured on the hard drives of Syrian activists, has identified 16 separate types of malicious software. All of those have at their core the purpose of delivering into the computer another nasty piece of malware called a "remote access trojan" or RAT. Once activated, the RAT sends information to computers located within Syria's telecom service.

Several RATs are being used. One in particular, called DarkComet, is frequently delivered by a compromised Skype account belonging to a trusted friend, Mr. Marquis-Boire says. In that way many are infected.

Once established, DarkComet gives control of the machine to the hacker who can then order the computer to record keystrokes, capture passwords, or activate the machine's webcam or microphone. Or it can send personal information and e-mail address books back to Syrian authorities.

"We have found that Facebook and other forums that carry the comments of pro-Syria liberation groups frequently are seeded with videos of atrocities in Holms that also include malware," Mr. Marquis-Boire says. "It's dangerous to trust too much what you find online."