

Syria activists using U.S. tech to beat curbs
By Mohammed Abbas, Reuters
21 June 2012

(Reuters) - U.S. technologies that may include a mobile phone "panic button" and an "internet suitcase" are being used by activists in Syria and other authoritarian countries to override government communications controls, a U.S. official said on Thursday.

Alec Ross, U.S. Secretary of State Hillary Clinton's senior adviser for innovation, said the United States was working on between 10 and 20 classified technologies that could be used by protesters and others facing communications curbs.

He also described how Facebook and other social networks could be used to challenge propaganda spread online by what he called the "Syrian Electronic Army".

"They're (some of the new technologies) being used in Syria. A number of the organisations that have benefited from our training include Syrian citizens," Ross told reporters in London, declining to specify which of the technologies were being used.

Ross outlined one U.S. innovation that he said was inspired by the detention of protesters in Iran and the mining of their phones for information on activist networks.

The so-called "panic button" is a pin code that when entered into a mobile phone will immediately wipe its address book and messages.

Another is the "internet suitcase", which he said could be used to set up a communications network even when the state-controlled telecommunications provider has shut off connectivity or is using it to monitor and punish dissent.

Ross said there was "clear evidence" that Syria's main mobile phone operator Syriatel, which is currently under U.S. sanctions, was being used to identify and punish dissent.

More than 10,000 people have been killed in Syria since an uprising began against President Bashar al-Assad last year, inspired by a wave demonstrations across the Middle East that toppled autocratic leaders in Egypt, Libya, Tunisia and Yemen.

SYRIAN ELECTRONIC ARMY

Social networks played a key role in rallying activists during the Arab Spring, and authorities responded by shutting down networks to make it harder for protesters to coordinate.

In Syria, Ross gave an example of how Facebook could be used to undermine state propaganda, and described how the U.S. envoy to Damascus had taken to posting messages on the social networking site to avoid being misinterpreted.

The ambassador's posts were then flooded by anti-U.S. and pro-Assad responses, Ross said, implying that they were a coordinated onslaught.

"What happened is real Syrian citizens began to out members of the Syrian Electronic Army, and so while the army might have put 500 comments, normal Syrians put another 500 up saying 'Ignore all these comments that are pro-Bashar'," Ross said.

"At the end of the day the Syrian Electronic Army came out with egg on its face," he added.

Ross said Washington communicated with Google and Facebook to share information on their operations in "oppressive environments", giving an example of talks prompted by cyber attacks by the government of ousted Tunisian leader Zine al-Abidine Ben Ali to stifle protests against his rule.

"We have open communications and discussions with companies like Google and Facebook in oppressive environments so we can share information," Ross said.

"The Ben Ali government cyber-attacked 1.4 million of its own citizens to try to identify the 'movement leaders' and Facebook actually told us about the cyber attack. We then shared information over the weeks that followed over the respective responses."

© Thomson Reuters 2012 All rights reserved