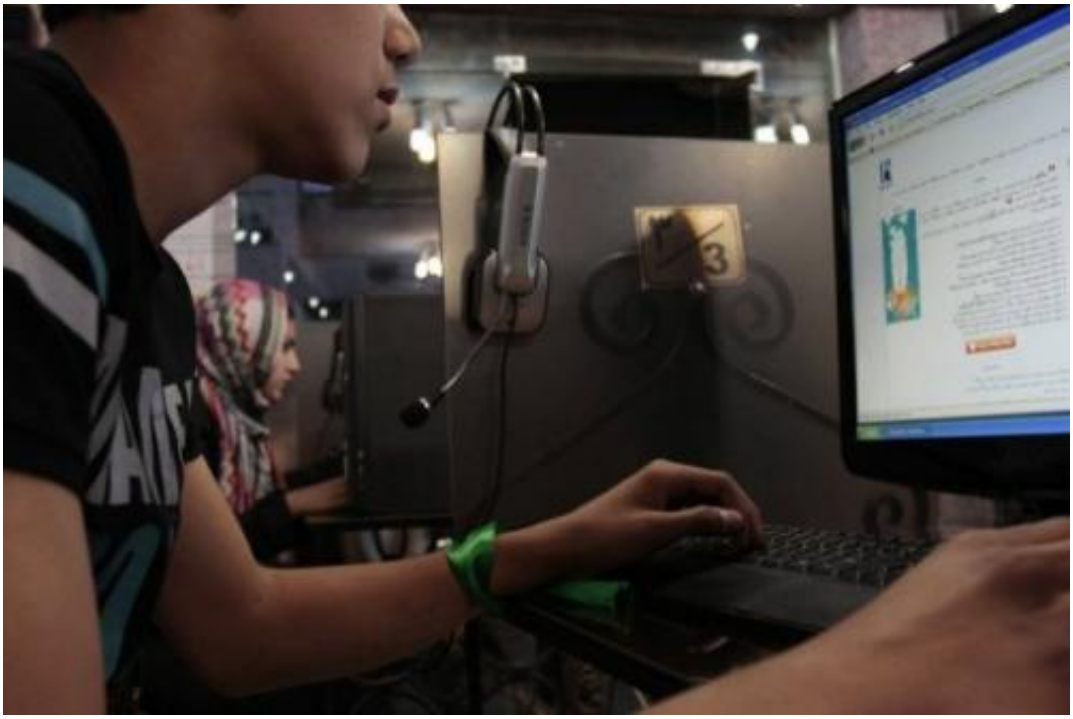
Syria, China worst for online spying, RSF reports

March 12 2013



File photo shows an Iranian youth using a computer at an internet cafe in Iran's Hamadan province. Syria, China, Iran, Bahrain and Vietnam are flagrantly spying online, media watchdog RSF said Tuesday.

Syria, China, Iran, Bahrain and Vietnam are flagrantly spying online, media watchdog RSF said Tuesday, urging controls on the export of Internet surveillance tools to regimes clamping down on dissent.

A new report entitled "Enemies of the Internet" also singled out five

companies—Gamma, Trovicor, Hacking Team, Amesys and Blue Coat—that it branded "digital era mercenaries," who were helping oppressive governments.

Syria's estimated five million Internet users are subject to rampant state spying, Reporters Sans Frontieres (RSF, Journalists without Borders) said in the report, which coincides with the World Day Against Cyber-Censorship.

Noting that 22 journalists and 18 Internet users had been jailed, it said the network was controlled by two entities including the Syrian Computer Society (SCG) founded by President Bashar al-Assad.

The SCG, it said, controlled Syria's 3G infrastructure, while the Syrian Telecommunications Establishment (STE) controlled the majority of the fixed connections.

"When the government orders the blocking of a word, of an URL, or of a site, STE transmits the order to service providers," it said, publishing a leaked 1999 bid invitation from STE to install a national Internet system in Syria.

The requirements include recording of online and offline activities, copying of all e-mail exchanges from within Syria, and the ability to detect, intercept and block any encrypted data.

Damascus beefed up its monitoring in 2011 "adding new technologies to its cyber-arsenal" including proxy Blue Coat servers, RSF said.

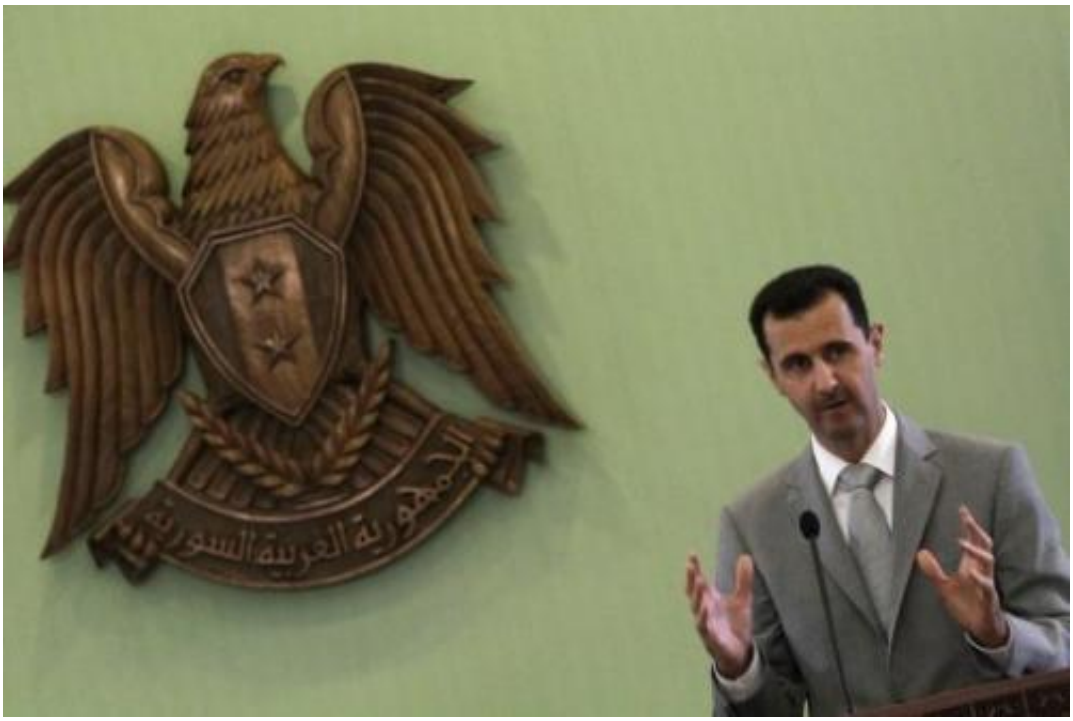


Image taken on October 11, 2010 shows Syrian President Bashar al-Assad attending a press conference at al-Shaab palace in Damascus. Media watchdog RSF said Syria's network was controlled by two entities, including the Syrian Computer Society founded by Assad.

Iran meanwhile is in the process of creating a home-grown Internet system, citing a series of cyber attacks on its nuclear installations, RSF said.

"Applications and services such as email, search engines and social networks are proposed to be developed under government control," to allow for "large-scale surveillance and the systematic elimination of dissent."

Twenty Internet users were jailed and one had been killed in the past year, it said, warning against the use of Iranian virtual private networks as it "will be like throwing yourself into the lion's jaws."

But in terms of sheer numbers, the "Chinese Communist Party runs one of the world's biggest digital empires, if not the biggest," RSF said, adding that individuals and companies have to rent their broadband access from the Chinese state or a government-controlled company.

"The tools put in place to filter and monitor the Internet are collectively known as the Great Firewall of China. Begun in 2003, it allows for access to foreign sites to be filtered," it said, and to block feeds and content deemed undesirable.

"The Chinese cyber-dissident Hu Jia and his wife Zeng Jinyang have had policemen stationed at the foot of their apartment building for months," it said.

"China jails more people involved in news and information than any other country. Today 30 journalists and 69 netizens are in prison."

Image provided by Zeng Jinyan shows her husband, Chinese dissident Hu Jia, at their home in Beijing on June 27, 2011. "The Chinese cyber-dissident Hu Jia and his wife Zeng Jinyang have had policemen stationed at the foot of their apartment building for months," an RSF report said.

Bahrain, which with an Internet penetration of 77 percent is one of the most connected states in the Middle East, has seen a dramatic increase in surveillance and news blackouts in the past three years, RSF said.

Vietnam's network is shoddy in quality but under tight state control. Thirty-one Internet users are in prison and Internet cafes are tightly monitored with users obliged to show identity documents before using them.

RSF called for a ban on the sale of surveillance hardware and software to countries that flout basic fundamental rights and crack down on any opposition.

"The private sector cannot be expected to police itself. Legislators must intervene," it said.

"The European Union and the United States have already banned the export of surveillance technology to Iran and Syria. This praiseworthy initiative should not be an isolated one."