Russia deploys a massive surveillance network system

(Translated from the original Italain)

Last year I wrote about a new powerful surveillance system that Russian government committed to private business to implement a complex monitoring system, officially to prevent terrorist attacks against Russia.

The day is come, today the system has been deployed officially to prevent on-line pedophilia but it obvious that a similar system is also able to monitor internet activities of millions of citizens banning contents not approved by central government.

The project will use new complex internet-monitoring technologies to implement the "Single Register" that is able to spy on internet activities of millions of Russians.

On July Vladimir Putin signed a law that contemplates also the possibility to put under judgment non only child pornography but also online contents that express dissent against the Government.

The Register is populated with requests of censorship coming from the Agency for the Supervision of Information Technology, Communications and Mass Media (The Roskomnadzor) that applies court decisions and executes orders of three government agencies: the Interior Ministry, the Federal Antidrug Agency and the Federal Service for the Supervision of Consumer Rights and Public Welfare.

The Agency has a total control of internet, it has the power to impose to the ISP to block the indicted contents within 24 hours, to Russian ISPs is also asked to continuously monitor the Register to verify if the sites they host are present in the archive of banned contents.

But how does the Register operates?

According the article published on the Wired the Roskomnadzor system introduces DPI (deep packet inspection) on a nationwide scale despite there isn't no official mention in the signed law.

Following a passage of the declaration of the Ministry of Communications of the presence of the Deep Packet Inspection technology.

> ***"At the end of August, under the chairmanship of Communications minister Nikolai Nikiforov, a working group was held, drawing representatives of Google, SUP Media (the owner of the Livejournal social network), and of all the other big hitters. They discussed how to ensure that the [filtering] mechanism — they used the concrete example of YouTube — how to block a specific video, without blocking YouTube as a whole. And they reached the conclusion that pleased them all," Ilya Ponomarev, a member of the State Duma and an ardent supporter of the law, declared.***
>
> *Are we are talking about DPI technology? we asked.*
>
> "Yes, precisely."

DPI is most advanced and intrusive category of inspection tools, it is able to analyze every single packet of the traffic filtering particular services or contents. Let's remind that DPI systems are adopted

Russia deploys a massive surveillance network system

by various regime in the world such as the Iran but also China that adopted the technology to implement its Great Firewall project.

Eric King, head of research at Privacy International, declared:

> *"No Western democracy has yet implemented a dragnet black-box DPI surveillance system due to the crushing effect it would have on free speech and privacy,"*
>
> *"DPI allows the state to peer into everyone's internet traffic and read, copy or even modify e-mails and webpages: We now know that such techniques were deployed in pre-revolutionary Tunisia. It can also compromise critical circumvention tools, tools that help citizens evade authoritarian internet controls in countries like Iran and China."*

The accused is the SORM («System for Operative Investigative Activities») purpose of the DPI, the system could be used for internet surveillance, according a russian law passed in 1995 the FSB (state security organization) could monitor telephone and internet communications.

SORM-1 system has been established in 1996 to monitor telephone communications substituted by SORM-2 in July 1998 to monitor also internet. Internet service providers (ISPs) must install a special device on their servers to allow the FSB to track all credit card transactions, e-mail messages and web use.

Event such as the Arab Spring and the parallel growth of political activism has alerted Russian Government on the dangers of a free circulation of information on social networks and social media in general. The imperative is monitor everything to avoid surprises, to keep Western eyes far from «internal questions».

> The First Deputy Director of the FSB, Sergei Smirnov declared : *"New technologies are used by Western secret services to create and maintain a level of continual tension in society with serious intentions extending even to regime change.... Our elections, especially the presidential election and the situation in the preceding period, revealed the potential of the blogosphere." Smirnov stated that it was essential to develop ways of reacting adequately to the use of such technologies and confessed openly that "this has not yet happened."*

There is a contradiction in the Russian approach that for years has declared to be contrary to so invasive internet control raising critical on Chinese internet censorship.

According the declaration of Russian intelligence, DPI technologies has been introduced a long time ago, in 2004 the security department acquired for its internal network a Transtelecom system .

Today several companies sell DPI technology in Russia such as Canada's Sandvine, Israel's Allot, America's Cisco and Procera, and China's Huawei, by the last summer all mobile operators in Russia have deployed a DPI:

- Procera was installed in VimpelCom.
- Huawei's DPI solutions are in use in Megafon.
- MTS bought CISCO DPI technology.

The mobile operators motived the acquisitions of DPI to control the use of bandwidth saturated by improper adoption of peer to peer protocols, the introduction of DPI in this case allow to suppress any undesired services such as torrents.

Not only mobile operators have installed DPIs technologies, every Russian ISP has installed a DPI as required by law at his own expense, minor operators

Russia deploys a massive surveillance network system

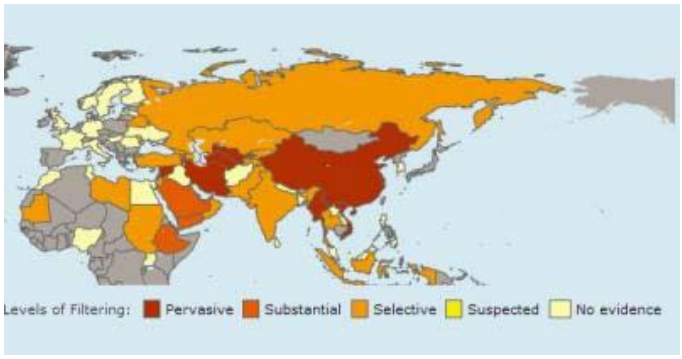
have so searched for cheap solutions found in the used market of CISCO DPIs.

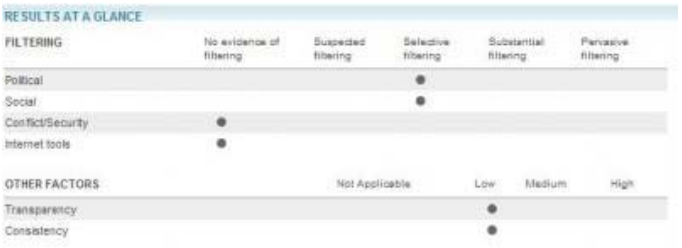
The situation is really worrying in my opinion, it's true that every government to protect homeland security control communications of the country, but not all has policy such as the Russian one. The Russian government has demonstrated to have zero tolerance against any kind of opposition, in Russia express any idea against Putin's Governments is really dangerous.

Let's me also add that censorship is not the only action adopted by central government against dissidents that use internet to divulgate information outside, it is known that Putin is very alert on cyberspace, foreign intelligence is sure that he controls one of the most dangerous group of hackers that is able to track back dissidents spreading malware and to deface web site of opponents.

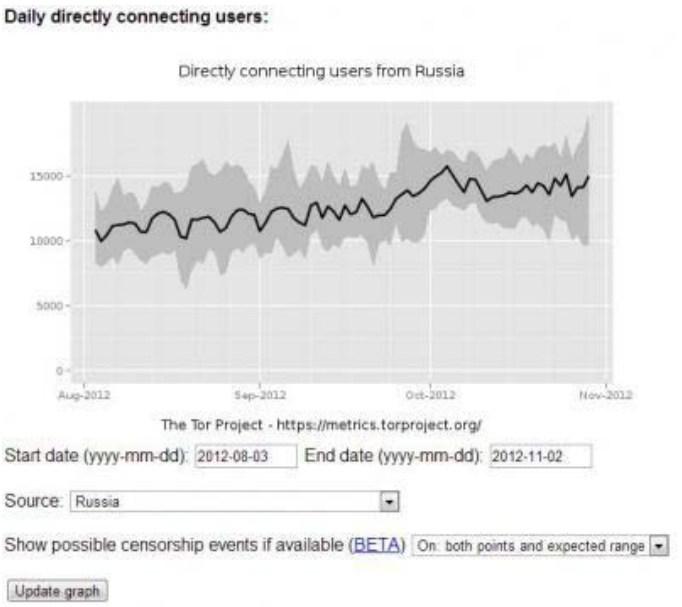
Another factor that must be considered when we face with internet filtering is the level of corruption related the country. Censorship in many cases has led to serious consequences in many cases was the main cause of persecutions.

Let's propose some information public available on the Russian situation, according the OpenNet Project that collects data on world wide internet filtering, in Russia is implemented a selective filtering mainly for political and social issues.





Another interesting information could be derived analyzing the number of users connected to anonymizing Tor network. The graph shows an increasing usage of Tor network, Russia with a mean daily of 12696 users represents the 2,61% of total Tor users and it is the ninth country for number of accesses. Russian know that someone is spying on them!



What will happen in the coming months? ... time will provide the answer, but the situation is very worrying!

Pierluigi Paganini

References

Russia deploys a massive surveillance network system

http://securityaffairs.co/wordpress/9956/intelligence/russia-deploys-a-massive-surveillance-network-system.html