Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
92/17

RUSSIA BULDING 'BRICS' INTERNET- AN ATTEMPT TOWARDS SPLINTER-NET OR PARALLEL-NET

E.Dilipraj
Associate Fellow, CAPS

Keywords: Russian internet, BRICS, splinternet, internet governance, root servers

At a meeting on October 26, 2017, the Security Council of Russia instructed its Ministry of Communications and the Ministry of Foreign Affairs to initiate discussion among BRICS countries for the creation of a "system of duplicate root servers for domain names (DNS), independent of the control of [international organizations] ICANN, IANA and VeriSign and capable of servicing the requests of users of the listed countries in case of failures or targeted impacts ".[1] This initiative of the Russian government has caused huge outcry among the other global cyber community. The western countries are calling this act by Russia as an attempt to build its own internet. Now that the reports suggest that President Putin has set August 01, 2018, as the deadline for this project, is this really an attempt by Russia to create a splinter-net (split Internet) or to create a parallel network as backup, is a compelling question that requires attention.

The answer to this question is twofold: first, to understand how Domain Naming System (DNS) root servers of internet function and operate, and second, the political dynamics behind this very move of Russia.

The global internet is dependent on the DNS which is a distributed storage system of the World Wide Web (www) that contains all domain names and their corresponding IP addresses. In layman terms, this is the address/contact book of the global internet. This distributed storage system, as the name indicates, is primarily stored on 13 official root servers which form the backbone of the global internet and are managed by different organisations.[2]Apart from these, there are also hundreds of mirror servers which are spread across the globe that replicate the content of the 13 official root servers. It is the job of these 13 root DNS servers to provide access to information about all top-level domains –

national domains (for example, .in, .ru, .uk, .de), general-purpose domains (.com, .org) and sponsored domains (. museum, .jobs).

The problem occurs in the location and management of these 13 root servers and the agency that manages the DNS (internet address book). The 13 root servers are operated and managed by 13 different organisations, however, maximum number of these root servers are physically located inside the US and 10 out of these 13 root servers are operated either by US government organisation (such as NASA, US DoD, US Army research Lab) or organisations that are close to the US government (such as Verisign. Inc, University of Maryland, Information Science Institute, Cogent Communications, ICANN).[3]

Also the management of the DNS database system (Internet Address book) is maintained and operated by a non-governmental agency called Internet Corporation for Assigned Names and Numbers (ICANN) under its department called Internet Assigned Numbers Authority (IANA) which until October 2016 was under the contract with the US Ministry of Commerce for the job.

Therefore, this dominance of the US in the governance of the internet has always been a bone of contention for countries like Russia and China. These two countries in particular for very long have conflicted over the issue with the US and its Western allies. This conflict over the issue of internet governance reached its peak post Snowden revelations about the US cyber espionage and as a result there emerged two sides; one headed by the US followed by its western allies and the other by Russia-China with different models for governance. While the Russia-China side proposed for a multilateral model with greater role for governments under the aegis of the International Telecommunication Union (ITU) of the United Nations (UN), the US led side proposed for a multi-stakeholder approach where all stakeholders – both governments and private players (such as internet service providers, operators, etc) – would have equal role to play in the governance. Also, in favour of this multi-stakeholder model, the US also agreed to transfer the stewardship of ICANN from its Ministry of Commerce to a non-governmental international body of stakeholders. This act of the US and its tireless campaign across the globe in support for multi-stakeholder model of internet governance helped it to achieve large-scale support from countries across the world to implement the same.

The US' effort to give away the stewardship of ICANN is hailed as a smart move by many West leaning cyber experts. It is not however, wrong on the part of Russia or China to believe that the US government might still have some stakes in ICANN and its operations given the fact that the organisation is still operating inside the US. Also, due to the overwhelming dominance of the US on the root servers, Russia fears the probable meddling of the US with the Russian domains if the need arises in the future.

In fact, Alexei Platanov, Director General of the Russian organization – Internet Technical Centre (TIC) – stated during an interview that the country's Ministry of Communications had conducted an exercise in 2014 focusing specifically on addressing violations. Under the terms of the possibly simulated exercise, the Russian leg of DNS network worked inadequately when the information about the .RU domains was removed from ICANN database. The exercise also included deploying of a backup root server as a copy of one of the 13 root servers serving the upper layer of addressing in Russia by Moscow Internet Exchange (MSK-IX). As a result of this it was found that the system continued to work even when .RU domain information was removed from the 13 root servers as Russian internet was simulated to function close to the backup server.[4] Therefore, it can be opined that Russia wants to implement this simulated process in order to secure its internet domains thereby assuring itself an uninterrupted internet service.

Moreover, from a technical point of view, the current proposal by the Security Council of Russia to create a system of duplicate root servers and to initiate discussion among BRICS countries can be seen as Russia's attempt to grab the US dominance over the internet root servers and to share the power among its peers.

Now the political dynamics behind Russia's action is least technical but more interesting. Post Trump's victory in the US presidential elections in late 2016, to the surprise of many Americans, leave alone the rest of the world, the country's security agencies have alleged that Russia had tampered with the elections through cyber means. Serious investigations are underway in the US to find links between Russia's alleged role in Trump's victory. This allegation from one perspective seems that the self proclaimed 'world's oldest democracy' – the US – has failed in its democratic process. Nevertheless, the US claims that Russians have advanced cyber offensive capabilities and have mastered cyber disinformation campaigns through internet. The European allies of the US have also echoed similar sentiments in accusing Russia of meddling with few European countries' elections.[5]Russia fears that such accusations, at a later stage, might turn into actions in terms of removing .RU domains from the internet root servers by the US and its allies to counter it in the cyber domain.

Moreover, many cyber experts, mainly from western countries, opine that Russia's attempt to create the system of duplicate root servers is to enhance Russian cyber offensive capabilities. While that may be a reason, as a sovereign country, Russia too has its right to pursue its own national interests. Besides, while the US now accuses Russia of attempting to disturb the internet architecture, one should not forget how the US had exploited its dominance over internet in the past through its covert surveillance and espionage programmes, such as PRISM, to gather intelligence about internet users around the world.

Also, since the US led multi-stakeholder model of internet governance had garnered popular support across the world, Russia and China feel defeated and want to gain more stakes in the process. This could also be the reason why Russia has proposed for a discussion with BRICS countries for its new proposal as an effort towards reaching out to its peers. However, the question whether the other BRICS members, namely China, India, Brazil and South Africa will join this effort, remains ambiguous. Given China's close cooperation with Russia in the recent past and also considering China's interest in dominating the internet, it would be in the interest of China to join Russia. However, Brazil and India have pledged themselves to the multi-stakeholder model of internet governance and hence, it is doubtful whether they would participate in this effort by Russia.

Clearly, the vigor with which Russia is re-emerging as a global power in recent years through its enhanced military diplomacy in Syria and its close cooperation with China in many other global affairs, it could be stated that Russia would leave no stone unturned in order to acquire itself a greater role in internet governance. Fireworks are on the way!

(Disclaimer: The views and opinions expressed in this article are those of the author and do not necessarily reflect the position of the Centre for Air Power Studies [CAPS])

Notes

[1] "Совбез России поручил создать «независимый интернет» для стран БРИКС", *RBK group*, December 28, 2017, available at https://www.rbc.ru/technology_and_media/28/11/2017/5a1c1db99a794783ba546aca, accessed on December 01, 2017.

[2] Available at root-servers.org, accessed on December 01, 2017.

[3] Ibid

[4] "Интернет "ляжет" на сутки? Я этого вообще не понимаю", *Kommersant*, March 17, 2016, available at https://www.kommersant.ru/doc/2939964, accessed on December 02, 2017.

[5] Oren Dorell, "Alleged Russian political meddling documented in 27 countries since 2004", USA Today, September 7, 2017, available at https://www.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/, accessed on December 02, 2017.