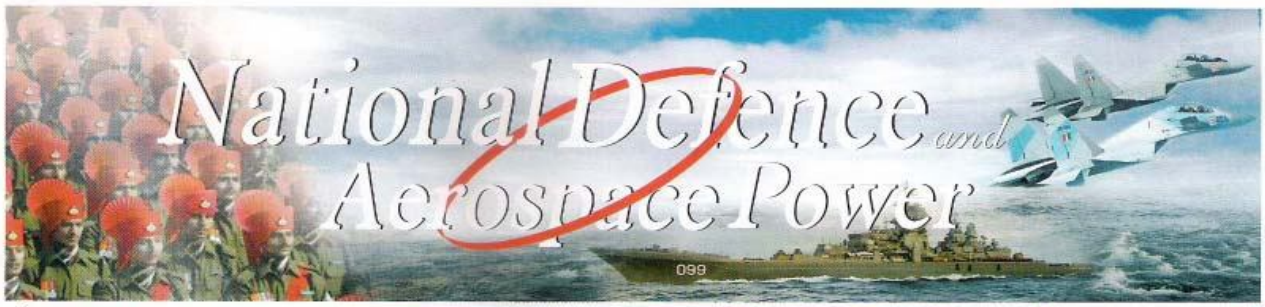

Centre for Air Power Studies ISSUE BRIEF

115 / 16 **31 AUGUST 2016**

CYBERSPACE REGULATION: THE STRATEGY TO IMPLEMENT STATE SOVEREIGNTY

E. Dilipraj

Associate Fellow, Centre for Air Power Studies

The biggest problem or complication of the cyber world is not its aspect of being a universal domain but being a domain which is still highly unregulated. For a domain which is clearly three decades old, the existing regulations are not to the desired levels. The global cyber community is more focused towards enhancing and enriching the technology. It lacks coherent measures to stabilise and secure the domain in spite of realisation of the growing threats. This is evident from the fact that new advancements and developments in cyber technology are unveiled on a daily basis in the form of new devices, software, application, etc. Simultaneously, new threats are emerging very often with varying threat potential. However, the news about new developments in the safety and security of cyber technology against the existing threats are not so often. Therefore, there is an immediate need to change this situation and seek a pragmatic solution to regulate the cyber space.

While the countries around the world have collectively started to get serious about cyber governance, every country needs to start introspecting about regulating its own cyberspace.

Cyberspace regulation is not a new concept but it is a concept which is not implemented often by countries except a few such as, China. Although, the Chinese system of regulating the cyberspace is more authoritarian in nature, it has implemented this strategy to suit its national interest. Regulation in cyber space is not a onetime activity, rather an ongoing process similar to cyber governance. Elaborating further, cyber governance per se could be seen as a more global activity and regulation in cyberspace is more domestic. While the countries around the world have collectively started to get serious about cyber governance, every country needs to start introspecting about regulating its own cyberspace.

To make it more coherent in conventional terms, it could be stated that the countries around the world have agreed to the management of air space in a collective approach, but that does not stop any country from regulating its own airspace by declaring no-fly zones, no-low flying zones, authorising airlines operators, issuing licenses, building airport infrastructures, etc. Likewise, in cyberspace too, a country could regulate and thereby establish the state's sovereignty over its own cyberspace. Unlike airspace domain, cyberspace is filled with more global players than domestic players in the form of tech giants, internet giants, etc whose activities could also be regulated along with

regulating the user activities.

There are few countries which have taken up initiatives to regulate their cyberspace from time to time. A few highlights are as follows:

• In December 2015, the Brazilian court blocked WhatsApp, a mobile based messaging application, for a period of 24 hours in Brazil after the company refused to hand over the content of communications between alleged drug dealers involved in a drug trafficking case. On March 01, 2016, Brazil's Federal Police arrested Facebook's Latin American Vice President Diego Jorge Dzudan for failing to comply with the court orders to help investigations in a drug case that involves WhatsApp, owned by Facebook.[1] Brazil is one of the countries which openly voiced for storage of a country's data in domestic servers. In this case, as the company did not comply with the Brazilian court orders the country attempted to punish the company, thereby, expecting some form of regulated service from the company in the future.

• Iran is another country which has strict regulations in cyberspace. In fact, Iran's cyber monitoring and censorship technologies are mostly bought from China. In May 2016, Iran's Supreme Council of Cyberspace made a new regulation by asking all the foreign messaging companies active in the country to transfer all data and activity linked to Iranian citizens into the country in order to ensure their continued activity.[2] This move by the Iranian government has not been welcomed by the tech companies and the users in Iran, the country is still following its regulation to suit its national interest.

• Being the cradle of cyber technology, the US companies enjoy a sort of monopoly in many aspects of the cyberspace including operating systems. This pattern has continued in the age of mobile phones too, where the three most popular mobile OS used around the world are Google's Android, Apple's iOS and Microsoft's Windows mobile OS. However, the US is exploiting the monopoly of its companies to conduct its covert cyber operations on other countries by manipulating the operating systems. In order to avoid being a victim of such covert cyber operations and to challenge the US monopoly, Russia is developing its own mobile operating system. For this reason, the Russian company - Open Mobile Platform, has been chosen to create a Russian Mobile OS. The project is reportedly on the line. The new operating system being developed by Russia is a Linux-based OS developed on top of the Sailfish OS, an open source platform.[3]

• While Russia is working on its version of mobile operating system, China on its part has already executed a similar strategy by developing its own version of operating system for personal computers known as *Kylin* operating system. The operating system was developed (since 2001) indigenously by the National University of Defence Technology and there are nearly four versions for public use. This is again a strategy of China to regulate the operating systems market in the country and to avoid exploitation of foreign developed OS by China's rivals through covert cyber operations.

• The Infocomm Development Authority, a government agency under the government of Singapore announced that from May 2017 public servants in the country will be blocked from accessing the internet on work computers. The agency stated that this change was necessary to ensure more secure working environment and to stop any potential leaks from work e-mails and shared documents amid heightened security threats.[4] In the age where sensitive information has become the target, Singapore government's regulation could be seen as an effort to contain data leak from its government offices.

• In June 2016, the Cyberspace Administration of China imposed new regulations on distribution of mobile apps. The list of criteria that the app stores and app developers must meet when operating in China are:

- App providers must verify users' identities by requiring their mobile numbers or other information.
- Providers should protect their users' information and cannot use the information without their consent.
- Providers should improve censorship and punish anyone releasing illegal information through warnings, shutting down accounts or suspension of service.

- Providers are forbidden from collecting user's location data and reading their contacts stealthily.

- Providers are also banned from pirating their rivals' products.

- Providers must record user logs and keep the information for at least 60 days.

These regulations by China on app distributors are only seen as a new move by the Chinese government to tighten its control over the internet (especially the mobile apps). However, similar regulations barring the negative ones on censorships could provide many other countries (like India) a regulated distribution of apps, where the situation now is chaotic.

• Post Snowden revelations, it is clear that government agencies of different countries around the world are desperate to put secret backdoors in other countries networks; devices and software. In order to avoid such instances, Bulgaria has passed legislative amendments to its Electronic Governance Act that requires all software written for the country's government to be fully open-sourced and developed in the public Github repository.[5] This means that whatever computer software, code, databases and programming interfaces the government procures will be freely available for others to read, modify and use, thereby, enabling public sourcing for fixing bugs in the government software.

India and Cyberspace Regulation

The above mentioned experiences of different countries in regulating their respective cyberspace at different levels are examples of what is happening around the world. However, with some exceptions like China, the efforts of other countries are limited to few aspects of cyberspace which dilutes the purpose of regulation to a large extent. India's own experience in regulating its cyberspace from exploitation by the cyber giants in recent times can be cited in the instance when India denied Google's proposal to implement their 'street view' project throughout the country citing security reasons.[6] The effort to make 'Geospatial Information Regulation Bill, 2016' a reality can also be seen as an attempt towards regulation. Also, the Indian government from time to time restricts public access to few websites which are deemed offensive and against national interest. Therefore, it could be stated that the aspect of cyberspace regulation is not a usual phenomenon in the country but there is cetainly huge potential to bring order in a tumultuous space. India could take a cue from efforts undertaken by various countries in regulating their respective cyberspace and formulate its own strategy in order to stabilise the country's cyberspace and also to ensure better safety and security.

India could take a cue from efforts undertaken by various countries in regulating their respective cyberspace and formulate its own strategy in order to stabilise the country's cyberspace and also to ensure better safety and security.

India could look into publicising it's indigenously built operating system "Bharat Operating System Services (BOSS)"[7] by recommending the government agencies to operate their systems with duel OS by installing BOSS as a standby to the existing operating system. This might enable wider public reach and publicity for the OS in the future and the government might also look at the possibility of switching all government computers to BOSS at multiple faces. Such an effort, if successfully implemented, would not only enrich indigenous technological development but at the same time reduce the country's dependence on foreign developed operating systems for everyday computing in the government sector.

The country might also consider encouraging Indian App developers to develop new messaging apps like WhatsApp, Viber, etc. for domestic consumption with localised servers. It could also encourage the public to use the same which would enable data of Indian users to stay within the country and it would also be easy for Indian government agencies to acquire data whenever required for any legal procedures.

More efforts like enhanced internet monitoring mechanisms are required in the future to secure and safeguard the country from the variety of sophisticated threats evolving in this highly technical domain.

More efforts like enhanced internet monitoring

mechanisms are required in the future to secure and safeguard the country from the variety of sophisticated threats evolving in this highly technical domain. Therefore, it is time for the country to devise and implement a strategy for regulating cyberspace at a national level. Cyberspace might be a universal domain without borders; however, it requires virtual borders for smooth operations which can be achieved only through implementing state sovereignty over their respective cyberspace. Despite clash of interests at various levels between countries during the implementation of regulations, such an effort would bring in order, and more importantly, it would bring stability in the longer run to a space which is critically important, is here to stay and may shape the future evolution of humanity.

Notes

[1] "PF cumpre mandado de prisã o em desfavor do representante do Facebook no BR", *Notices,* Federal Police of Brazil, March 01, 2016, http://www.pf.gov.br/agencia/noticias/2016/03/pf-cumpre-mandado-de-prisao-em-desfavor-do-representante-do-facebook-no-br, accessed on June 20, 2016.

[2] "Iran orders social media sites to store data inside country", *The Reuters*, May 29, 2016, http://www. reuters. com/article/internet-iran- idusl8n18q0in, accessed on June 24, 2016.

[3] Mohit Kumar, "Russia to get rid of Android and iOS by launching its own Mobile Operating System", *The Hacker News*, June 06, 2016, http://thehackernews.com/2016/06/russian-mobile-os.html, accessed on June 24, 2016.

[4] "No Internet for Singapore Public Servants", *BBC*, June 08, 2016, http://www.bbc.com/news/world-asia-36476422, accessed on June 24, 2016.

[5] Chris Merriman , "Bulgaria passes law requiring all government-developed software to be open source", July 07, 2016, http://www.computing.co.uk/ctg/news/2464089/bulgaria-passes-law-requiring-all-government-developed-software-to-be-open-source, accessed on July 10, 2016.

[6] "India denies Google's Street View, cites security risk", *The Economic Times*, June 09, 2016, http://economictimes.indiatimes.com/news/politics-and-nation/india-denies-googles-street-view-cites-security-risk/articleshow/52673967.cms, accessed on August 08, 2016.

[7] BOSS (Bharat Operating System Solutions) is a GNU/Linux distribution developed by C-DAC, Chennai in order to benefit the usage of Free/Open Source Software in India. BOSS GNU/Linux is a key deliverable of NRCFOSS. It has enhanced Desktop Environment integrated with Indian language support and other software. The software has also been endorsed by the Government of India for adoption and implementation on a national scale. The operating system is currently in its sixth version and has been tested positively to stand strong against different kinds of cyber attacks.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Marshal Vinod Patney, SYSM PVSM AVSM VrC (Retd).

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com