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

IS "GREAT FIREWALL" AN INHIBITOR OR AN ACCELERATOR FOR INDIGENOUS INNOVATION AND GLOBAL EXPANSION OF CHINESE INTERNET COMPANIES?

Gp Capt Ashish Gupta
Research Fellow, CAPS

The Communist Party of China, while being weary of implications of unrestricted online access to information to its legitimacy, has enthusiastically promoted the use of Internet as an inalienable part of its quest for global hegemony, economic growth and orchestration of its technical prowess. With an estimated 640 million people using Internet, China holds the distinction of having world's largest number of Internet users outnumbering the entire U.S. population two to one.[1] China views Internet as a fertile ecosystem that germinates, fosters, nurtures, and engenders political dissent, detrimental social activities and societal unrests. To counter this, China has an aggressive and multi-faceted online censorship system, commonly known as the Great Firewall. After viewing the contents on the Internet through **the prism of its** own contentious policies and cultural interests, the censorship apparatus filters or blocks access to online material deemed dangerous to the state.

Chinese leadership since long has had an ambivalent relationship with the Internet. During Arab Spring in early 2011, China bolstered its censorship bureaucracy, reportedly creating a new office under State Council Information Office to "regulate every corner of the nation's vast Internet Community,"[2] However, confinement within the precinct of Great Firewall has given impetus to an evolving and thriving Chinese online ecosystem **driven, sustained and** perpetuated by **indigenous innovation**, enterprise and

entrepreneurship. Beijing's efforts to alienate its citizens from the global net has paved the way for homegrown companies to cater to online requirements and needs of 1.3 billion people in their societal interactions, financial transactions, knowledge exploration, online resource exploitation and a myriad of other services. The Internet's ubiquitous and totemic icons - Google, Wikipedia, Twitter, YouTube, Facebook, Instagram — are under the censorship of ruling Communist Party's due to fears of fanning the flames of anti-government sentiments. In absence of a competitive environment, Chinese home grown companies are thriving and have garnered market **capitalization,** even exceeding that of their foreign counterparts whom they emulate.

At the helm of Chinese online oppression against free speech and **tyrannical censorship is** China's new Internet czar Lu Wei who took over the State Internet Information Office in 2013 and became the director of a powerful Internet committee headed by President Xi Jinping in 2014.[3] While unrepentantly defending the China's need for stronger Internet content control, he issued new regulations restricting sharing on social media sites and increasing censorship of popular online video sites. In response to such controls, Lu Wei said that "The internet is like a car. If it has no brakes, it doesn't matter how fast the car is capable of traveling, once it gets on the highway you can imagine what the end result will be." [4]

The homegrown Chinese firms have ensured that for most of the Chinese, incarcerated behind the Great Firewall are not deprived of online experiences and services unless they want to voice their political dissent online. Adherence to Chinese government regulations and sticking to Chinese sites is rewarded with sufficiently high speeds and reasonable access charges. In first quarter 2015, the total transaction value of China e-commerce market exceeded USD$ 567.49 billion, an increase of 10.1% on a **year-over-year** basis.[5] As of 31 December 2014, top five listed Chinese internet companies by market value were Alibaba (US$253.41 billion), Tencent (US$135.50 billion), Baidu (US$80.32

billion), Jingdong (US$31.52 billion) and Netease (US$13.01 billion). In September last year, e-commerce king Alibaba scored the largest IPO in Wall Street history. Tencent, the designer of messaging company WeChat has a market capital more than that of IBMs. As a hybrid of Twitter and Facebook, Sina Weibo has emerged as most popular Chinese microblogging website with a market penetration comparable to that of Twitter.

In its infancy, Internet shook the very foundation of sovereignty as propagated by the dominant 'Westphalian conceptions'. The belief that Internet's **transcendence** of physical boundaries would render it immune to **oppressive regulatory regimes** has given way to acceptance of the fact that a determined state with technical underpinnings can regulate and control the Internet. The Chinese Internet strategy, aimed at containing the simmering political dissent has a much more sinister dimension to it. Chinese state-backed hackers have been accused of cyberespionage. In a recent report made public by Fireeye Labs, a company that provides cyber security solutions, examination of malware aimed predominantly at entities in Southeast Asia and India revealed a decade-long operation focused on targets—government and commercial—who hold key political, economic and military information about the region. The planned development efforts aimed at regional targets and mission made the lab to believe that this activity was state sponsored—most likely by the Chinese government.[6]

China is also determined to extend its oppressive regime beyond its borders. In cyber lexicon repository, the "Great Cannon" has been added alongside "Great firewall" christening a new tool for censorship developed by China. When used offensively, that ability can turn a normal internet user into a vector of attack. In one such case, the Great Cannon intercepted traffic sent to Baidu infrastructure servers and returned a malicious script, unwittingly enlisting the web surfer in the hacking campaign against foreign websites that have helped the circumventing of Chinese censorship. [7]

In recent decades, a creative adoption of western technology **catalysed by government** encouragement, Chinese tech firms are aggrandizing themselves by making inroads in global markets. In spite of being stymied by U**.S. government** 'national security' concerns and thwarted by ban on selling networking equipment in the U.S., the Chinese Telecom giant Huawei earned more than 65% of its revenue from overseas by tapping markets in Europe and developing countries. WeChat, the brainchild of Tencent is making inroads into East Asia and Africa. Tencent claims that more than 100 million people outside China use its messaging service despite concerns of close monitoring by the Chinese government. Chinese firms in telecom field enjoy what Joseph Schumpter terms as 'latecomer advantage': the ability to learn from and improve on work of one's immediate predecessors.

Some critiques believe that many Chinese Internet firms owe their stupendous success and massive domestic market share to a policy environment in which these firms do not have to compete with foreign challengers. President XI's cherished goal of building an "innovation society," with very strong global presence of Chinese tech firms capable of competing internationally will require a level playing field for foreign companies with their Chinese competitors. However, the innovative, intellectual and imitative capacity of Chinese firms spurred up by spirit of entrepreneurship can transform them into brands with enviable global presence and commitment to innovation.

(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])

End Notes

[1] Euan McKirdy, "China's online users more than double entire U.S. population," CNN, February 4, 2015, at http://edition.cnn.com/2015/02/03/world/china-internet-growth-2014/, accessed 21 July 2015.

[2] Scott J. Shackelford, *Managing Cyber Attacks in International Law, Business, and Relations: In Serach of Cyber Peace,* (Canbridge University Press, New York, 2014).

[3] Paul Mozur and Jane Perlez, "Gregarious and Direct: China's Web Doorkeeper," *New York Times*, Dec 02, 2014, at http://www.nytimes.com/2014/12/02/world/asia /gregarious-and-direct- chinas-web-doorkeeper. html?_r=0, accessed July 21, 2015.

[4] David Bandurski "Lu Wei: the internet must have brakes," *China Media Project*, November 11, 2014, at http://cmp.hku.hk/2014/09/11/36011/ Lu Wei: the internet must have brakes, accessed July 21, 2015.

[5] Cecilia, "China E-commerce Market in Q1 2015," *China Internet Watch*, July 16, 2015, at http://www.chinainternetwatch.com/13430/e-commerce-marketq1-2015/, accessed July 21, 2015.

[6] Fireeye Labs. "APT30 and the mechanics **of a long-running cyber espionage operation :**How a Cyber Threat Group Exploited Governments and Commercial Entities across Southeast Asia and India for over a Decade." April 2015

[7] Alex Hern, "Great Cannon of China' turns internet users into weapon of cyberwar," *The Guardian*, April 13, 2015 at http://www.theguardian.com/technology/2015/apr/13/great-cannon-china- internet-users-weapon-cyberwar, accessed July 21, 2015.
