# PLA's Information Warfare Capabilities on an Upward Trajectory

21 Apr, 2014 Brig Vinod Anand, Senior Fellow, VIF 

In end February this year, Chinese President Xi Jinping formed a new working group at the apex level on cyber security and information was seen as the political leadership's renewed efforts in underlining the threats and challenges to the national security in this arena, the has been paying particular attention to information warfare (IW) challenges since early 1990s. According to People's Liberation Army ( term information warfare encompasses cyber warfare, electronic warfare, deception warfare, psychological warfare, computer warfa beyond the military realm.

The PLA has been adapting Western concepts to suit local conditions and considers it as a 'driving force in PLA's military combat readine the construct of People's War and devised its own precepts of 'Peoples War in IW domain' where millions of Chinese, both civilians and s computers, could achieve the objectives of IW. That is what has been precisely happening since over the last one decade wh cyber/information attacks are known to have originated from China with India being one among many other countries being at the receiv years, Indian government's computers including those of National Security Council and some other important offices have been hacke pointing towards China. PLA's information warriors and hacker groups have been actively involved in virus warfare and hacking activities interest.

PLA has intensified its efforts in IW field since it officially pronounced its military doctrine of 'Local War under the conditions of inform 2004 White Paper on Defence. The objective laid down was to build an informationalised force and to win an information war anc revolution in military affairs with Chinese characteristics with 'informationalisation' at its core. Since the articulation of its current militar laid solid foundations for fighting information and cyber wars. According to PLA's precepts, before any physical operations take pla information and cyber domains that would be used to cripple the adversary's capabilities.

PLA's expanding capabilities in the use of space for military purposes provides it with the means to enhance its command and c surveillance, reconnaissance, information and cyber warfare capabilities. Space is considered as a commanding height for enab information operations. PLA's strategists have also stressed on the imperatives and necessity of 'destroying, damaging and interferin reconnaissance and communications satellite systems. No country other than China has plans of launching almost 100 satellites till China, India's plans for launching satellites are very modest; in fact in the last 37 years, India has launched 100 missions. Such end realized would add to China's counter-space and IW capabilities.

PLA has also vastly expanded its optical fiber and other terrestrial networks giving it a tremendous IW capability. At the national leve system based on fiber optic cables, satellite communications, micro-wave links and automated command and control systems. The PL and non-secured telecommunications and has an army wide data communication network and integrated field operations communicatio been strengthened in the last decade. Many joint exercises carried out by PLA show that its WAN capabilities within Chinese borders have been carrying out military exercises in Lanzhou and Chengdu Military Regions (which include the entire Sino-Indian border) where the joint and integrated operations that include 'information operations'.

According to Pentagon's Annual Report to Congress on China's Military and Security Developments of 2013, PLA's Information Operations and the top priority in peacetime is given to Computer Network Defence. As mentioned above, not only the IO/IW should be used even the campaign it would continue in all phases of war. Pre-emption also rhymes well with PLA's doctrine of active defence where counter at gain advantage even before the commencement of hostilities. Chinese military theorists also believe that if an information campaign is for military operations may not be necessary. Such a contingency may arise possibly with nations (like the U.S.) which are information de

But that is no solace for India as both military and civil arena in our country is increasingly becoming dependent on information and in and systems. Our critical infrastructure dependent on a wide variety of information systems remains vulnerable to information attacks Iranian nuclear facility did make India reflect on its vulnerabilities in the field of critical infrastructure. It has also been reported that eve of Stuxnet was Iran, Kaspersky Lab experts' data indicates that in fact it was India that was the epicenter of Stuxnet activity thus raising implications and motives of the originator. Some analysts aver that the largest power outage in Indian history (of July 2012) which affe of India was caused by the malicious ware of Stuxnet.

One also needs to take note of the theories and concepts articulated by two senior colonels of PLA in their book 'Unrestricted Warfare' wh there would be no boundaries between military and non-military areas of warfare in future.

The levels of integration between the civilian and military efforts of PRC in all the fields of information and cyber warfare have been c political and military leadership of China is thoroughly seized with the significance of acquiring information and cyber warfare capabilit Computer Network Operations (CNO) and Integrated Network Electronic Warfare is germane to their doctrine of IW. PLA's Third and Fou General Staff have been made responsible for executing CNO. While the Third Department has been tasked to collect intelligence and operations, the Fourth Department has the responsibility for network attacks and other offensive IW operations.

China's defence budget (as also the internal security budget) has witnessed a double digit growth (in percentage terms) every year According to one study, the Chinese government actively funds IW related research in commercial IT companies and civil and milita number of universities conducting such research is put around 50 which indicates the importance and priority given to security information technologies. Further, China's commercial IT companies involved in R & D actively seek collaboration with foreign firms to technologies which have dual use and therefore, in the end, benefit the PLA also. In certain cases, the civil use is only nominal and routir development through the civil entities is undertaken as a matter of expediency. Such a subterfuge also helps in lowering the costs for known, China's official defence budget is said to be much less than the actual one.

In fact, in January this year, Chinese telecom equipment companies Huwaei was accused of hacking into Bharat Sanchar Nigam Limite and sabotaging its expansion plans in Rajahmundry in coastal Andhra Pradesh. A five-member team comprising senior officials from th Council Secretariat, Intelligence Bureau, Ministry of Home Affairs and BSNL was formed to investigate the issue. Even a US Congressior the security threat posed by the Chinese companies like Huwaei and ZTE.

In conclusion, security threats and challenges to India in information warfare domain that includes cyberspace cannot be overemphasized forces have promulgated a joint Information warfare doctrine and a tri-service Cyber Command is in the process of being established. S government have also been made in the shape of establishing a Computer Emergency Response Team and formulation of a National Cy 2013. However, what is needed of integrating the efforts of a number of ministries and stakeholders in this field. Allotment of additional f supporting such activities in educational institutions and universities is an imperative. Creating of space assets that support the info warfare efforts is also an imperative.

Information deterrence is equally important as a conventional military deterrence or even nuclear deterrence (which in turn is depen information capability). If critical infrastructure of a nation like banking, power industry, and railway or air communication networks are may be no need for a war. The nation would stand defeated as depicted by the Chinese military writers

---

Published Date: 21st April 2014, Image source: http://img.over-blog-kiwi.com

## Post new comment

**Your name:** *

Anonymous

**E-mail:** *

The content of this field is kept private and will not be shown publicly.

**Comment:** *

Message*

Input format

I'm not a robot

reCAPTCHA
Privacy - Terms

Save Preview

# Related Articles

**China's Maritime Challenges in the Indo-Pacific**

**दक्षिण चीन सागर में पी ?**

पीपुल्स लिबरेशन आर्मी (प?

**पंचम भारत-चीन रणनीतिक ?**

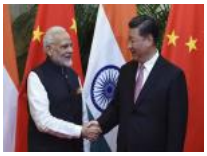
भारत चीन के बीच घटते व्या

**Overview** With the status quo under challenge

**Narendra Modi and Xi Jinping signal reset at Wuhan, but BRI**

**Commentary: Modi Xi-Summit: All About 'Feel Good'!**

The informal meeting between the Indian Prime Minister Narendra M



**Commentary: M Summit: Strivin**

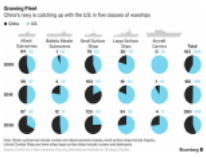
The inforr between Mo taken place

**पाकिस्तान में बढ़ती चीन**

**चीन का जिवानी कार्यक्**

**Commentary: PLA Navy's Major Exercise in the South China S**

The massive People's Liberation Army (PLA) Navy exercises condu



**हिन्द महासागर में**

हिन्द महासागर

## About Us

The Vivekananda International Foundation (VIF) is a New Delhi-based think tank set up with the collaborative efforts of India's leading security experts, diplomats, industrialists and philanthropists under the aegis of the Vivekananda Kendra. The VIF's objective is to become a centre of excellence to kick start innovative ideas and thoughts that can lead ...

Read More

## Contact Us

Name*

Email Id*

Phone Number*

Message*

I'm not a robot

reCAPTCHA
Privacy - Terms

Submit

## Tweet With Us

**VIF India**
@vifindia

'The organs are the horses, the rein, the intellect is the charioteer the rider, and the body is the ch master of the household, the Ki of man, is sitting in this chariot.' #SwamiVivekananda