

## **India looking the wrong side<sup>1</sup>**

China has the unpleasant habit to peep into everybody's computers.

In India, it is not a major issue as the nation was too busy trying to guess (if not bet on) the next move of the BCCI president.

But it bothers others; quoting a new US report prepared by the Defense Science Board, Reuters recently mentioned Washington's worries: "Chinese hackers have gained access to designs of more than two dozen major US weapons systems".

(In Australia, the Chinese 'dark visitors' would have done better: they are said to have stolen the blueprints of the country's new intelligence headquarters).

Quoting the US report, The Washington Post affirmed that the 'hacked' designs included advanced Patriot missile system, the Navy's Aegis ballistic missile defense systems, the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the F-35 strike fighter.

Many rightly ask: has China the ability to bring down the communication networks and corrupt vital information in the case of a conflict? Nobody can answer this question with certainty.

Though a Chinese Defense Ministry spokesman stated that the US report was 'erroneous', the Chinese latest hacking prowess will certainly speed up the Middle Kingdom's R&D programs in the defense field.

Spokesman Geng Yansheng asserted that China already has the ability to build the weapons needed for national security, why should Beijing steal

---

<sup>1</sup> Published in ***Niti Central*** on **June 4, 2013 (URL not available)**

designs. He says that the US report both underestimates the Pentagon's security capabilities and the Chinese people's intelligence.

But what is disturbing for Washington, (I wish India would also be disturbed) is the recurrence of the fact.

Last month, the Pentagon said that China was using espionage to modernize its military and that the US government had been the target of hacking 'attributable directly to the Chinese government and military'.

In February already, the US computer security firm Mandiant affirmed that a PLA unit was behind a series of hacking attacks targeting the US and that the data from some 100 US companies had been stolen.

It is clear: China is getting prepared.

On May 28, 2013, Xinhua reported that the PLA's Academy of Military Science (AMS) released a report titled 'The Strategic Assessment 2012'. Chinese experts and scholars from several different disciplines analyzed the international strategic situation and 'sensitive issues'; they also suggested some counter strategies.

Chen Zhou, chief editor of the AMS 2012 report said that "the annual assessment report is to let the world learn about our viewpoint and to hear our voice."

The Voice of China says that the Asia-Pacific region has become "the new global geopolitical, economic and military center" because "the US has accelerated its eastward shift of its strategic focus." The report warns of 'security risks to China's environment' and possible clashes with Japan over the Diaoyu Islands.

For Beijing, think-tanks' discussions on the purported threats are not enough; *the nation needs to be ready*.

*The People's Daily* reported that the PLA would soon conduct its first joint drills involving cyberwarfare, special troops, army aviation and electronic countermeasures units "to test the integration and co-ordination of its land and air forces".

Xinhua announced that the joint exercises are scheduled for June at China's largest military training center, on the Zhurihe base in Inner Mongolia: "Eight military academies will also join the exercises. ...The high-profile drills were aimed at showing the world China had successfully narrowed the gap with Western countries in terms of modern warfare strategies."

Clearly, the PLA is keen to test its IT skills as the drill will simulate 'non-contact assaults' alongside conventional operations.

Xu Guangyu , a former general now associated with China Arms Control and Disarmament Association in Beijing told *The South China Morning Post*: "Non-contact assaults means digital operations, including cyberwarfare, electronic warfare and intelligence warfare systems, as well as others. ...Assault operations' doesn't mean the PLA will stage a 'pre-emptive strike' drill, but it is based on the existing 'active defence strategy' to simulate how to fight back if our country is invaded."

According to Xinhua, the PLA will test new types of combat forces including units using digital technology in order to prepare for an informationalized war.

Another interesting piece of news, the Chinese Defence laboratories have been extensively using 3-D printing technology for its aviation industry, thereby saving money, materials and time.

One can imagine that once plans are 'borrowed' from the top US laboratories, China is able to create aircraft components from 3-D printers. It bypasses the traditional manufacturing processes such as casting, forging and assembling.

3-D printing, or laser rapid forming, is the manufacturing technology of tomorrow. Blueprints made on computers (or stolen from third parties' computers) can be turned into actual objects by a special printer which adds layer after layer of different materials until the designed shape is materialized.

Stratasys, the world's leading manufacturer of 3-D printers affirms that its printers are able to combine more than 100 different materials to form a 3-D product; it includes wood, plastics or metals.

Apparently, this technology would have been used for preparing parts and components of the C-919, China's first commercial airliner, the J-15 jet fighter; the J-15 and J-16 multi-role fighters as well as the 2 stealth planes, the J-20 and the J-31.

Obviously, the prototype has not come out of a 3-D printer, but it has greatly speeded up the production process.

Remember former US defence secretary Dr Robert Gates had announced that China would not have a "fifth-generation aircraft by 2020", but the day Gates landed in Beijing in January 2011, the J-20's had a successful maiden test flight in Chengdu, Sichuan.

I have the feeling that China took India for a ride in the desolate plateau of Depsang Plain. While the planners in South Block will now ploddingly strengthen the defenses of Ladakh, China happily prepares for the next generation 'informationalized' war.