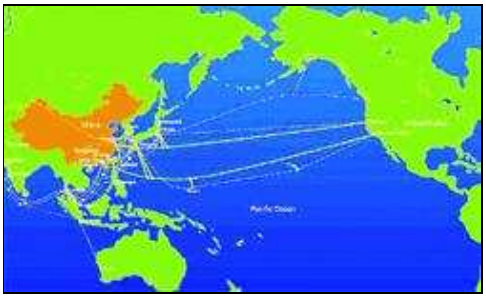
China bugs India

Environment Minister Jairam Ramesh may have survived his Chinese imprudence but the Home Ministry has reason to worry about the influx of companies from China into India's highly sensitive telecom sector. *J Gopikrishnan* delves deeper to find out why



Environment Minister Jairam Ramesh's recent remarks in Beijing — calling into question the Home Ministry's apparently "alarmist" and "overly defensive" approach towards Chinese companies that wish to operate in India — may not eventually cost the Minister his job. But his open advocacy of these firms has certainly led to legitimate questions being asked about the kind of security threats the Home Ministry anticipated for a sector as highly sensitive as telecommunication. While the Home Ministry was quick to clarify that India did not have an anti-China policy in this regard and that every proposal was decided on a case-to-case basis, the controversy has indeed pointed out to the need to explore the matter in greater detail, both in terms of its security and financial costs.

It is intriguing that despite repeated alerts from the Government's intelligence and technical units, Chinese telecom giants Huawei and Zhong Xing Telecommunication Equipment (ZTE) were allowed into the Indian telecom sector three years ago with bureaucrats and politicians alike choosing to ignore these warnings. It is still a mystery as to how, back in 2007, Huawei was entertained in India, defying common knowledge that the company is headed by officers of the People's Liberation Army (PLA) of China and that it was founded in 1987 by Brigadier Ren Zhengfei and other ex-PLA officers. In fact, much before our R&AW and other intelligence agencies raised an alarm over this company's presence here, the credentials of Huawei were questioned by junior telecom officials at the Sanchar Bhawan.

According to some telecom engineers familiar with the case, Huawei's first presentation to the Department of Telecommunication (DoT) for empanelling them as vendors, after they had crossed certain "political barriers," sowed the first seeds of doubt. They say, "Huawei engineers boasted about having the unique advantage of a Remote Access Servicing System. When asked to explain, they said that their equipment, in case of any faults, can be repaired or serviced from their headquarters in China. Our engineers, out of curiosity, asked what kind of technology this was and how could they repair equipment installed in India by sitting in China."

Clearly unconvinced, the telecom engineers decided to probe further. "When we consulted our technical counterparts in the security agencies, they also found something fishy in this technology. Back then, the entire world was researching to decode the method behind this Chinese technology. Within days we found out that the company was installing some bugging software or chip in its equipment which enables the company's Chinese headquarters to enter into our network without our knowledge," say the engineers. Despite the obvious seriousness of this alert, it was not entertained either by the DoT bureaucrats or their political masters; worse, those who raised these concerns were asked to keep quiet.

It soon became apparent that Chinese brokers had slowly but surely begun to dominate the power corridors in India, virtually kicking out existing European giants like Nokia, Ericsson, Siemens etc. It is an open secret now that most Chinese brokers in India are hawala agents operating in New Delhi, Mumbai and Chennai and whose instant and speedy delivery of strategies along side their ability to please the bureaucracy and sundry politicians outwitted the tactics employed by the European vendors.

Following Huawei, Indian authorities allowed yet another Chinese company, the ZTE, into the telecom sector in 2008. This company, founded in 1985, is a listed company in the Shanghai Stock Exchange and is a strategic partner to many Chinese defense establishments. In fact, a major stake in this company is still controlled by Chinese Government units connected with defense and aero space.

Between the two of them these telecom giants managed to corner plenty of business in the Indian telecom sector. Huawei bagged several contracts in the BSNL's southern circles, amounting to more than Rs 2000 crore. Given the stiff competition and the Chinese vendors' cheap pricing policy, private mobile operators too started getting drawn to these companies. It is a well-known fact that the Chinese Government reimburses losses, in the form of subsidy, in several ways, to their companies for bagging international contracts.

Things went largely undisturbed till Indian intelligence agencies were recently alerted by their American and British counterparts about the exact nature of the bugging software/chip hidden inside the Chinese telecom equipment. "The bugging software or chip is now widely known as the Manchurian Micro Chip. This is an advanced, spy software developed by Chinese hackers with the help of the Call-Home Technology. As soon as anyone installs a Chinese equipment, it is reported to its master server in China. That means, at any given time they can infiltrate our network and jam it as and when they wish to. The technology also helps them enter our network and access sensitive data. Still, it took months for our Government to take action and ban them," say telecom engineers.

The first official international alarm against Chinese telecom operators was sounded in September 2009 by the Australian intelligence agency, Australian Security Intelligence Organisation (ASIO) that officially started investigations into Chinese telecom equipment installed in their country. Following investigations, Huawei was promptly asked to replace all Chinese engineers in Australia and the ASIO ordered the insulation of their network by de-bugging the devilish Manchurian Micro Chip. Predictably, amid allegations pouring thick and fast against this bugging software, Chinese diplomats chose to term the entire matter, "American pulp fiction". Playing the aggrieved party, they said investigations on Chinese cyber infiltrations worldwide amounted to denial of a level playing field.

Back in India, the Telecom Ministry's plan to grant a Rs 36,000 crore GSM line tender to Huawei recently was cancelled by the Prime Minister's Office after security agencies confirmed the presence of bugging software in their equipment. In a shocking move, however, the Telecom Ministry, advocating Huawei's cause, said that while border areas can be avoided, the company must be allowed access to the rest of the country. Fortunately, on the intervention of the Central Vigilance Commission and the Advisor to Prime Minister on Public Information Infrastructure and Innovations, Sam Pitroda, cancellation of the entire tendering procedure was ordered. Following this, the DoT was compelled by the Home Ministry to remove Chinese companies from the empanelled list of vendors. In fact, the Home Ministry had to put up a strong front against private Indian operators who lobbied heavily for the purchase of Chinese equipment.

Clearly caught on the wrong foot, Huawei and ZTE are now trying to lure the Indian authorities with tall claims about "huge investments" they plan in India. Only hours ahead of Chinese Ambassador Zhang Yan's meeting with Home Secretary GK Pillai on Thursday, the two companies came out with a press release about their plans — of setting up plants across India that would offer limitless employment opportunities to the Indian youth, of developing areas where proposed plants would be located, and even of setting up technical campuses all over. Whether our political system has the requisite will to resist this Chinese temptation remains to be tested.

Now to return to the more specific issue related to Jairam Ramesh and whether his love for the dragon is really a new-found one. Here, it would help to rewind to UPA I (2006-2009, to be specific) when Ramesh was a junior Minister in the Commerce Ministry, then headed by Kamal Nath. It was this Ministry which facilitated the entry of cheap Chinese mobile handsets in early 2006. These mobiles, with internet connectivity and little known funny brand names, were sold at anything between Rs 3,000 and Rs 6,000 when established companies like Nokia, Sony-Ericsson, and Motorola were selling handsets between Rs 15,000 and Rs 25,000. Why the Chinese were allowed to sell handsets at such throw-away prices, remains an abiding mystery of the telecom industry.

Nonetheless, the unimaginably cheap prices lured the common man adequately, business flourished and, according to industry estimates, around five crore Chinese mobile sets were pumped into India in the space of three years. But clearly, the Chinese should not have been trusted. Three years later Indian authorities found out that these phones were illegal because they were violating basic security norms.

Here is why. Seven years ago, in order to track mobile phones, the International Telecom Union (ITU), had insisted that all manufacturers provide a unique number for each mobile set called the International Mobile Equipment Identity (IMEI) number. Every mobile user can get this 15-17 digit IMEI number by pressing *#06# on his or her handset. According to the ITU, service providers must not provide connection to a mobile phone without this IMEI number because this number helps security agencies track a subscriber.

The question is: Why did the Commerce Ministry under Kamal Nath and his deputy Jairam Ramesh, back in 2006, allow illegal Chinese mobile phones, that clearly violated international standards, into the Indian market? Woken up with a rude shock, Indian intelligence agencies, in a rather delayed intervention, alerted the DoT which then ordered service providers to disconnect all service to Chinese mobile phones operating without the IMEI number. The damage, however, had been done with five crore unaccounted for Chinese handsets already out in the market.

More was to follow. Even as disconnection was ordered, China's Indian brokers worked out another game plan. Close to six times, the last date for disconnecting services to illegal Chinese mobiles was pushed back, keeping the general public in dark about the developments even as Indian markets remained awash with cheap Chinese mobiles. Intriguingly, the Government did not issue an advertisement or notification in the media about the illegality of the Chinese mobiles. In fact, the ban on providing connection to Chinese mobiles was fully imposed only six months ago. The five crore handsets sold in India are now mere paper-weights, the common man's hard-earned money, Rs 20,000 crore to be exact, having long found its way to China. Apart from the obvious security compromises made vis-à-vis Chinese telecom companies, this issue too begs attention.