Aug 27 2016 : The Economic Times (Delhi)

SCORPÈNE SUBMARINE LEAK - Don't Let it Go Off the Radar

Subimal Bhattacharjee

The writer is former country head of a major defence multinational

Earlier this week, The Australian published the story of 22,400 pages of leaked secret documents marked `Restricted Scorpène India'. These revealed threadbare details of the Scorpène-class submarine project in India consisting of technical literature, manuals and other operational details.

India's Scorpène submarines are being built at the Mazagon Dock in Mumbai, a defence public sector undertaking (DPSU), by the French company DCNS. The first of the six submarines is set to be commissioned and named INS Kalvari next month.

The Indian government was quick to respond to the situation and the defence minister termed the incident as a case of "hacking". The ministry of defence (MoD) press release had initially mentioned that the source of the leak was `overseas' and not from India. The next day it claimed that the documents were examined and do not pose any security compromise as the vital parameters have been blacked out.

It's needless to say that such detailed leaks or even `hacks' with serious national security connotations have many angles that have to be studied before any conclusions can be arrived at. At the same time, the issue is a wake-up call to check how secure processes are and how stringent checks and balances have been in place since sensitive and national security data have been put under cyber security.

The notorious `Naval War Room' leak case of 2006, in which 7,000 pages were stolen via drives, was already a red flag for the overall national security

apparatus. While much analysis has happened on the impact of that leaked content, what is a real matter of concern is India's readiness to deal with such situations in a Digital Age. Defence assets and data are very much a part of the national security-related critical information infrastructure. Dealing with them needs well defined standard operating procedures.

Clearly, the leak of these `restricted' data could have happened physically or by `hacking'. So the whole paraphernalia would entail the data storage and transmission protocol agreed between the vendor and the government, the defined and approved list of access points at both ends, the redundancy and backup measures if something went wrong, and the available capacity to deal and arrest any further spread of such leaked data.

Further, one needs to check if the application of legal arrangements application of legal arrangements adequately covers current cyber capabilities. The contract, one must remember, for the submarines was signed way back in 2004. Likewise, one must examine the capacity of cyber forensics to investigate such cases and identify the actual source of the leak even if it happened in 2011. As all the players in this context are responsible and legally bound, the `leak' or `hack' has to be identified to bring the perpetrator to justice and maintain the integrity of India's defence cyber security system.

This case can be well addressed by the provisions of the Information Technology Act, 2008. Section 66F (B) clearly makes this case one of cyber terrorism. Whatever be the geography of the act and motive, the legal umbrella is there. The perpetrator can face life imprisonment. Likewise, Section 120B (criminal conspiracy) of the Indian Penal Code (IPC) read along with Section 3 (penalties for spying) and Section 5 (wrongful communication, etc, of information) and Section 9 (attempts, incitements, etc, of commission of offence) of the Official Secrets Act also apply .

But the larger point is to realise how much cyber security today is important for the country's national security, and how proactive steps have been taken to

bolster such measures across critical information infrastructures (CIIs). The National Cyber Security Policy, 2003, needs a bigger push for implementation with adequate budgets. Also, our defence forces need to go many steps forward to have their assets and data protection measures in overdrive.

The doctrine of warfare has been changing globally. Cyber espionage forms a major strategy of many countries that employ means to gather sensitive data and also hack into critical networks. For years, our adversaries have been regularly targeting strategic assets. Cyberspace allows much more to sneak, probe and launch attacks.

It is crucial for the government to consider the impact of cyber attacks as an act of war in many cases. There is no global binding agreement on cyber security, and neither will there be one in place very soon.

So, while the Scorpène data would have spread far and wide through the social media and dark networks with or without portions being `blacked out', it is time to devise a more proactive strategy to deal with such exigencies.