Centre for Air Power Studies

ENHANCING INDIA's CYBER HUMAN RESOURCE

Dilipraj. E
Research Associate, CAPS

India made unprecedented progress in the cyber domain in the year 2013 and took a big leap forward in promoting cyber security in the country. This was enunciated with the release of the country's first 'National Cyber Security Policy' (NCSP) followed by the release of a set of 'Guidelines for the protection of National Critical Information Infrastructure' (NCII) framed by National Technical Research Organization (NTRO) and also by gaining the status of 'Authorising Nation' for the IT products under the Common Criteria Recognition Arrangements (CCRA). In the policy paper for national cyber security, it was identified that the country needs to build a force of 5 lakh 'cyber security experts' in the next 5 years. The paper did not, however, propose the strategy to acquire this desired number.[1] In another document, where guidelines for the protection of National Critical Information Infrastructure was outlined, a hierarchical structure was proposed highlighting the role of Chief Information Security Officer and his team who would act as the backbone for safeguarding the security of the NCIIs. However, India is yet to find the people who would take charge of these grave responsibilities.

While India's Information Technology sector is a significant contributor to the economy of the country, it is also one of the leading sectors in the world. The country has enough young IT professionals who, unfortunately, remain scattered across India's huge landmass. In fact, most

of these talented young minds are in contact with one another through various platforms on internet. They operate in cyber space with strange pseudonyms and with different agendas. Although a few wander off as black hat hackers, there are many more prospective young vibrant brains which, when harnessed, could prove as potential assets to the country. The Government of India needs to tap these young talented individuals to overcome its shortage of a highly skilled workforce of cyber security experts. While this seems to be an easy enough strategy, the question remains as to how this talent can be identified from amongst India's huge population. The answer, in my opinion, is by conducting a nation-wide talent hunt through 'Cyber competitions'.

The Path Weavers

This is not a new technique as it is being followed by many leading countries of the world, like USA and China. On 08 May 2009, the White House came up with a proposal for conducting a nation-wide cyber challenge with the aim of finding and developing 10,000 cyber security specialists to help the United States regain the lead in cyberspace.[2] In the same proposal, the following statement by *Jim Gosler*, NSA Visiting Scientist and the founding Director of the CIA's Clandestine Information Technology Office, was highlighted: "*There are about 1,000 security people in the US who have the specialized security skills to operate effectively in cyberspace. We need 10,000 to 30,000".*[3] It was also mentioned in the proposal that such competitions would act as a diversion to young talented people from going astray. This competition was conducted by the government of USA in association with SANS Institute - a leading institution in Information Security Training and Security Certification in the world.

In fact, the Americans borrowed this idea of conducting nationwide Cyber challenge from the Asian giant and India's neighbour, China. The practice of conducting such Cyber competitions in China is prevalent for more than a decade and they have a more structured approach to it. China's approach can be seen in two stages: one at the regional level and as a next

step at the national level. The People's Liberation Army (PLA) conducts these competitions on behalf of the Chinese government. As a first step, the PLA invites young talented people to participate in the regional level cyber competitions which are conducted in all the military regions of the country. As the second stage, the top few contenders of every region are formed as a team and made to represent the region in the nation-wide competition.[4]

The victorious talented lot is then tapped by the PLA to work for them either as private operatives or recruited into their cyber armies, i.e. Unit 61398. The most popular case of one such identified talent of China is *Tan Dailin* who operates with the pseudonym "*Wicked Rose*" and who, at the young age of 20, was the leader of a private hacking unit from China called Network Crack Program Hacker (NCPH). '*Wicked Rose*' was the champion of the national cyber challenge of China in the year 2005. After his victory, he started operating with few other cyber experts as a team known as NCPH. He was sponsored by the PLA for his missions and the group was an expert in exploiting "Zero-day vulnerabilities" in Microsoft Office software and they were also experts in building Trojans. Using this technique they were able to make number of successful attacks on their targets, including the critical infrastrucutres of the US and were able to extract thousands of documents for their commanders in the PLA.[5]

ARTICLES BY SAME AUTHOR

"ACCESSING THE INACCESSIBLE" PART I: NSA's DIGITAL TOOLS OF ESPIONAGE

PART II: KEYBOARDs, USBs & VGAs

PART III: NSA'S TOOLS OF ESPIONAGE ON COMPUTERS

PART IV: NSA'S TOOLS OF ESPIONAGE IN W-LAN AND ROUTER

PART V: NSA'S TOOLS OF ESPIONAGE IN FIREWALLS AND SERVERS

More Articles

The Way Ahead

Although India does not support or encourage such covert cyber operations by any individual/ groups, yet the above can be taken as an example to understand the ability of young minds in this highly technical and complex domain. Though a few educational institutions and Universities in India are conducting few cyber related competitions now and then, their reach and level of testing is far below the desired standards. However, if the same is conducted on a larger scale by the government, it might have a nation-wide reach and participation from all parts of the country that would enable the Indian government to identify the hidden talent. There are a number of pro-Indian hacker groups in the country who have been involved in hacking wars with their counterparts from Pakistan, China and other countries. The talents of such hackers would be a potential supplement for the country if harnessed properly, or else they could end up being an embarrassment for India.

Mere identification of talents will not be enough for the country to acquire the desired results. The government needs to take steps to form a framework which would enable the identified talented youth to be groomed to put their skills to work in the national interest, which in turn would serve the purpose of defending the cyber front of the country. The existing cyber defence agency, National Technical Research Organisation (NTRO) in the Department of Electronics and Information Technology under the Ministry of Communications and Information Technology can be made as the nodal agency to undertake this onerous task of enhancing India's cyber security by identifying, grooming and producing highly skilled cyber warriors for the country. The proposed technical university by the state-run telecom service company, BSNL, can also be involved in the process to provide technical training and grooming the identified talented youth.[6]

Another strategy to hunt for talented youth for enhancing cyber security of the country is to announce rewards to experts who can help solve complex cyber problems. This would be akin to a 'Capture the flag' style program which will not only help the government to reach out to the right talents but will also act as an awareness program to the common public regarding the cyber domain.

At a later stage, after achieving a considerable level of workforce and technical capabilities, the country can also focus on rehabilitation of the black hat hackers in order to reduce cyber crime in the country. Such rehabilitated talented youth can be carefully picked to be included in the cyber defence of the country. As the saying goes in the Indian Armed forces "C*atch them young*", the same approach can also be followed in the cyber domain – which has been acknowledged as the fifth domain of warfare - to have an effective offensive and defensive cyber capability in the future.

(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] "National Cyber Security Policy 2013", *Department of Electronic and Information Technology*, File No. 2(35)/2011-CERT-IN, Ministry of Communication and Information Technology, Government of India, July 2, 2013.

[2] "The United States Cyber Challenge", *The White House Files*, May 08, 2009.

[3] Ibid.

[4] Ken Dunham & Jim Melnick, "Wicked Rose and the NCPH Hacking Group", *An iDefence Research Report,* 2007.

[5] Ibid

[6] "BSNL to open technical university, offer cyber security training", *Times of India*, April 13, 2014.
