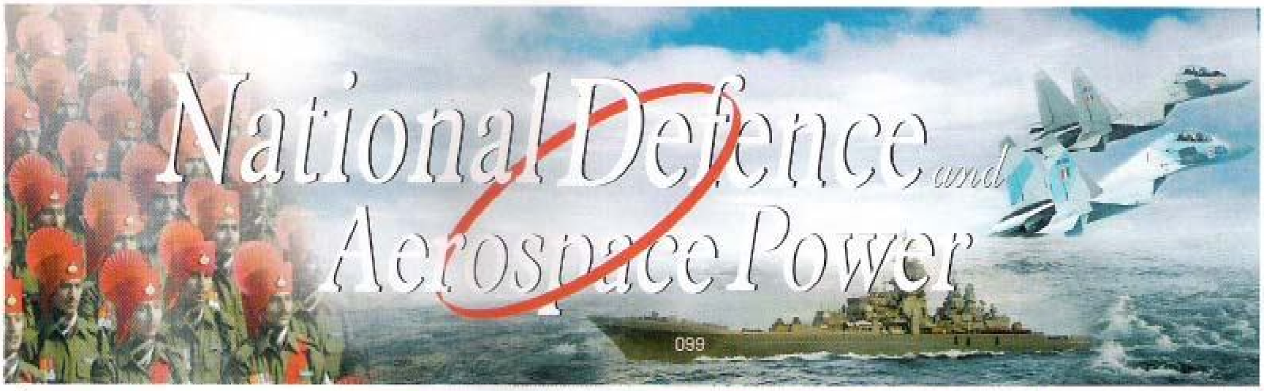


Centre for Air Power Studies ISSUE BRIEF

97 / 14 27 January 2014

INDIA'S CYBER SECURITY 2013: A REVIEW

E. Dilipraj

Research Associate, Centre for Air Power Studies, New Delhi

The year 2013 was truly an eventful year in the field of Cyber Security for India. Starting from 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), India took a big leap forward in bringing the country's cyber security on track. On the other hand, India also faced one of its biggest embarrassments in the cyber world when the US Cyber Espionage Program (PRISM program) came to lime light when whistleblower Edward Snowden exposed it to the world audience, in which India was identified as the fifth most snooped country. Apart from this, as a usual affair, the year 2013 also saw various Indian networks and websites both government and private alike coming under cyber attacks from various sources around the world. Therefore, having all these ups and downs faced by India in its cyber security platform in mind, this brief tries to give a short relook into the various highlighting events that happened in relation to India's cyber security in the year 2013 and the various challenges involved in enhancing India's cyber security in the years to come.

> **India took a big leap forward in bringing the country's cyber security on track. On the other hand, India also faced one of its biggest embarrassments in the cyber world when the US Cyber Espionage Program (PRISM program) came to lime light when whistleblower Edward Snowden exposed it to the world audience, in which India was identified as the fifth most snooped country.**

Advancements

Firstly, the 'National Cyber Security Policy' (NCSP) – 2013 which was released on July 2nd 2013, was initiated with a vision to build a secure and resilient cyber space for citizens, businesses and government activities and also to integrate the various events happening in the highly dynamic cyber arena of the country. The policy is an overview of the government's approach and strategy for protection of cyber space in the country. The policy also includes broad strategies for

- Creating a secure Cyber Ecosystem,
- Creating an assurance framework,
- Strengthening the Regulatory framework,

- Creating mechanisms for early warning and response to Cyber Security threats,
- Security for E- Governance services,
- Protection and resilience of National Critical Information Infrastructure,
- Promotion of Research and Development in Cyber Security,
- Reducing supply chain risks,
- Human Resource Development,
- Developing effective Public-Private Partnership, and
- Most importantly the implementation of the policy itself.[1]

This document, which is the first of its kind in the country, gives a holistic perspective in which, each and every field identified has to be studied separately in order to effectively implement the policy. Moreover, the process of implementation has to be made quickly so that the policy does not become obsolete in the highly dynamic cyber environment. However, there are a few questions that arise regarding the policy document:

In September 2013, India crossed one more milestone in the field of cyber security by becoming an 'Authorising Nation' for IT products from its previous status of a mere 'Consuming nation'.

- The first question is regarding the swiftness in which this policy would be implemented.
- The policy outlines the need to build 500,000 cyber security workforces in the next 5 years but it does not propose from where this desired numbers will come from.
- There is no clarification on whom or which agency will be responsible for conducting the audits and other regular checks that are outlined in this policy document.

Inspite of many unanswerable questions, the whole agenda of bringing a policy for the National Cyber Security by India is a commendable job and this brought in hope that there would be more developments in the future in this particular field.

Secondly, on July 19, 2013,[2] National Technical Research Organisation (NTRO) which is the technical intelligence agency under Prime Minister's Office of India, released the guidelines for securing the National Critical Information Infrastructures (NCII) of the country. Having identified 14 critical information infrastructures like Energy, Transportation, Banking/ Finance, Telecommunication, Defence, Space, etc, the NTRO guidelines created a framework for securing these infrastructures all over the country. The document was distinct as it was elaborative in nature, studying each and every aspect of cyber security related to the critical information infrastructures of the country and providing the guidelines specifically to every aspect individually.

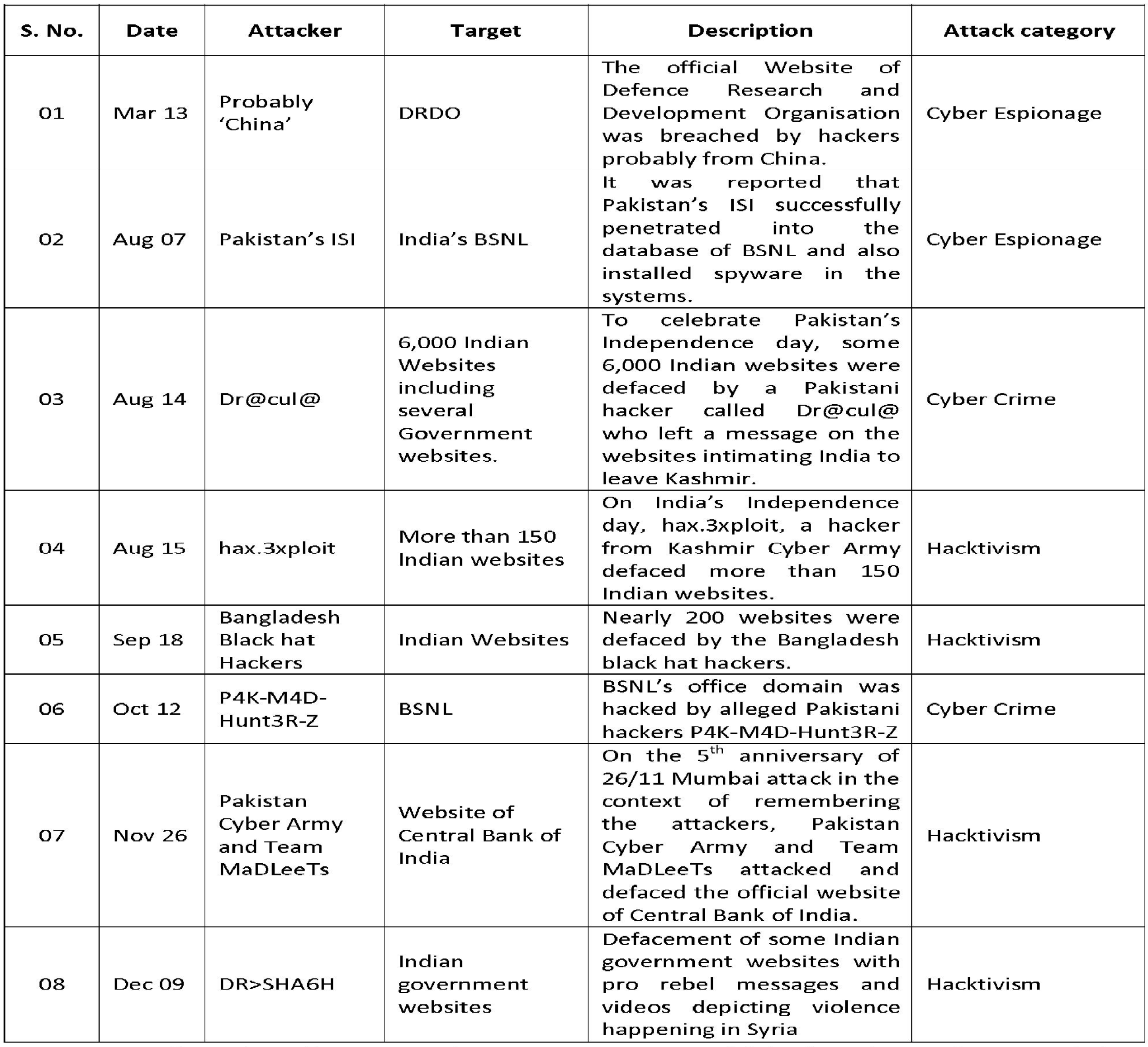
In addition, in September 2013, India crossed one more milestone in the field of cyber security by becoming an 'Authorising Nation' for IT products from its previous status of a mere 'Consuming nation'.[3] In less academic terms, it can be stated that all those IT products that are certified in India are now authorized to be used in the 26 member countries of Common Criteria Recognition Arrangements (CCRA) without having them retested. The fact that testing in Indian labs has a distinctive cost advantage might help India become one of the major hub for IT product testing in the near future. Also, due to low cost for testing the production of IT products may also see an increase in India which would eventually increase the export of these products.

Apart from these advancements in the field of cyber security within the country, another notable event was India taking pioneer step in suggesting to set up a Joint Cyber Security Portal with the US in order to check cyber crime and misuse of social media platforms between the two countries. In December 2013, during the two day conference of police chiefs of India and the US which was held in New Delhi, the idea of setting up a portal was suggested by the Indian delegation for which a positive response was given from the US side. The Indian side had also made a suggestion for setting up web servers in India to make it easy for the intelligence agencies to legally intercept communications in real time when need arise.[4] As the world of internet is growing globally, it is a general feeling that the service providers need to venture out of US and set regional servers especially in India where the number of users are increasing day by day.

Failures

However, all the above mentioned policy level and strategic developments in the cyber security arena of India could not shadow the fact that India's cyber security was compromised during many instances especially with the cyber snooping of the US on India through the PRISM program which involved Data Mining and Cyber Espionage operations. The PRISM program which began in 2007 was the mass electronic surveillance and data mining program conducted by the US on almost all the countries of the world. Since 2007, Indian telecommunication networks were spied upon in all possible ways by the US and it is ranked as the fifth most snooped country by this program, yet, the Indian government's response for the program was defensive rather than condemning it. Although it is rumored that India's response was defensive for the program because it is also developing a similar espionage program on the lines of PRISM, it however, need not stop India to show its protest against US when there is a question of sovereignty encroachment.

Apart from this one major incident where India's cyber security was totally compromised by the US, there are few other incidents in much lesser scale where individuals or a group of people have tested India's capability in securing its various cyber networks. A few such incidents are tabled as follows:



S. No.	Date	Attacker	Target	Description	Attack category
01	Mar 13	Probably 'China'	DRDO	The official Website of Defence Research and Development Organisation was breached by hackers probably from China.	Cyber Espionage
02	Aug 07	Pakistan's ISI	India's BSNL	It was reported that Pakistan's ISI successfully penetrated into the database of BSNL and also installed spyware in the systems.	Cyber Espionage
03	Aug 14	Dr@cul@	6,000 Indian Websites including several Government websites.	To celebrate Pakistan's Independence day, some 6,000 Indian websites were defaced by a Pakistani hacker called Dr@cul@ who left a message on the websites intimating India to leave Kashmir.	Cyber Crime
04	Aug 15	hax.3xploit	More than 150 Indian websites	On India's Independence day, hax.3xploit, a hacker from Kashmir Cyber Army defaced more than 150 Indian websites.	Hacktivism
05	Sep 18	Bangladesh Black hat Hackers	Indian Websites	Nearly 200 websites were defaced by the Bangladesh black hat hackers.	Hacktivism
06	Oct 12	P4K-M4D-Hunt3R-Z	BSNL	BSNL's office domain was hacked by alleged Pakistani hackers P4K-M4D-Hunt3R-Z	Cyber Crime
07	Nov 26	Pakistan Cyber Army and Team MaDLeeTs	Website of Central Bank of India	On the 5th anniversary of 26/11 Mumbai attack in the context of remembering the attackers, Pakistan Cyber Army and Team MaDLeeTs attacked and defaced the official website of Central Bank of India.	Hacktivism
08	Dec 09	DR>SHA6H	Indian government websites	Defacement of some Indian government websites with pro rebel messages and videos depicting violence happening in Syria	Hacktivism

Source: Collected from various reports published in the website [URL]:http://hackmageddon.com/

What Waits Ahead?

In this age of Information, it should be accepted that a virtual world is taking shape and expanding rapidly parallel to the physical world and that the safety of it is comparatively essential for a safe living, because the wars of the future will be first fought in the virtual world before coming into the physical World.

India is undoubtedly a strong military power in the physical world. But its capacity to secure its virtual/ cyber arena is low compared to other major powers of the world. Nevertheless, in the recent years, awareness has aroused in the Indian society regarding cyber security of the country, and, it is very much evident from all the policy documents that were published in the year 2013. Yet India faces few challenges in the cyber security platform which needs immediate attention especially in the context of:

- Swift implementation of the National Cyber Security Policy.

- Setting up a national level architectural framework for Cyber Security. Most probably by setting up an independent nodal agency and by bringing in all the different stake holders in the field from both government and private under its purview.

- Building up an efficient Cyber Security workforce to the desired numbers. India is lacking in the number of Cyber Security experts which are not more than 10000 personnel at present. As this field requires personnel with real technical expertise and to get the desired number of 500,000 personnel in the next 5 years[5] is a real challenge for the country.

- Increasing both Offensive and Defensive cyber capabilities of the country by enhancing the capabilities of the agencies involved in it like NTRO and CERT-In.

- On the defence services part, to commission an effective Cyber Command which can conduct large-scale offensive operations as well safeguard the defence networks of the country is a mandatory requirement.

Addressing these immediate challenges would help India to catch up with other major powers of the world in the cyber space. In addition to this, as a long time strategy, India should also work on enhancing the country's cyber laws, which is in an infant stage today to the next level that would cater the needs of future generations to make India a force to reckon with even in the cyber world.

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] Chakrobarthy, Rakhi." NTRO releases guidel ines to protect against cyber attacks" , Times of India, July 20, 2013 at http://articles.timesofindia.indiatimes.com/ 2013-07-20/india/40694913_1_cyber-attacks-ntro- guidelines

[3]. "India became the 17th Authorizing Nation under CCRA" ,Standardisation Testing and quality certification directorate, Department of Electronics and Information Technology, Ministry of communication and Information Technology, Government of India at http:// www.stqc.gov.in/content/india-became-17th- authorizing-nation-under-ccra

[4]. "India favours setting up of portal with US to check webcrime" *Z News*, December 22, 2013 at http:// zeenews.india.com/news/net-news/india-favours-setting-up-of-portal-with-us-to-check-webcrime_898534.html

[5] "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.

Centre for Air Power Studies

The Centre for Air Power Studies (CAPS) is an independent, non-profit think tank that undertakes and promotes policy related research, study and discussion on defence and military issues, trends, and development in air power and space for civil and military purposes, as also related issues of national security. The Centre is headed by Air Cmde Jasjit Singh, AVSM, VrC, VM (Retd)

Centre for Air Power Studies
P-284, Arjan Path, Subroto Park, New Delhi 110010
Tel: +91 11 25699130/32, Fax: +91 11 25682533

Editor: Dr Shalini Chawla e-mail: shaluchawla@yahoo.com

The views expressed in this brief are those of the author and not necessarily of the Centre or any other organisation.