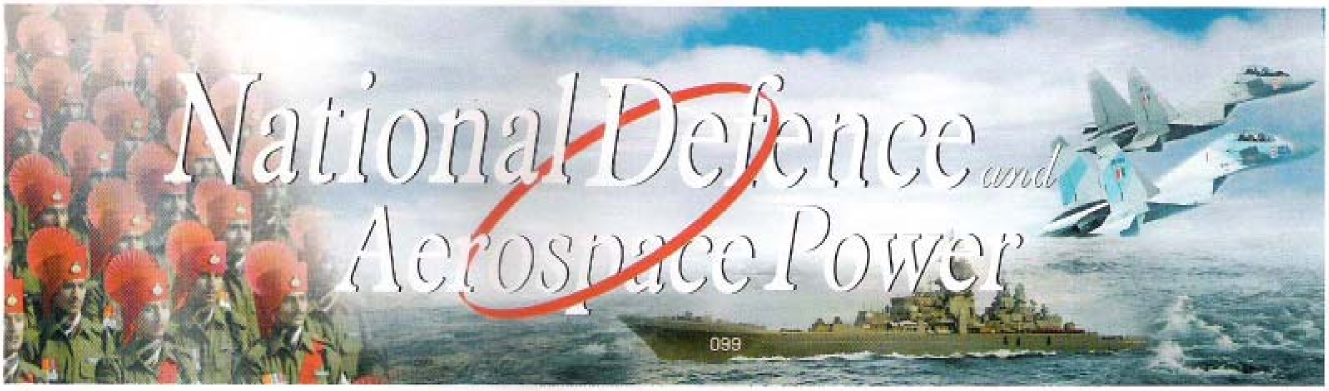


Centre for Air Power Studies
ISSUE BRIEF
80\12
24 December 2012

PPP: OPENING OF A NEW AVENUE IN INDIA'S CYBER SECURITY

E. Dilipraj
Research Associate, Centre for Air Power Studies, New Delhi

The recent experiences of a propaganda threat in the cyber space, led to the exodus of North East population from their place of work to their homelands. This also resulted in a huge chaos in the political scenario which once again stamped its need for the security of the cyber space in India. Cyber space is being considered to be the fourth front of warfare in the future, which makes the scenario worse due to the unorthodox methods of offensive practises involved in it.

India ranks third in the list of countries with high freedom on internet and it is a country which has a high dependency on IT sector for its national economy. Aware of these factors,India has carried out security measures in securing the cyber space of the country in the past and as a next step in the direction, it has recently come out with a plan to have a joint venture with the private sector to effectively counter the future threats in the cyber arena.

The Public-Private Partnership(PPP) in the field of cyber security is a long anticipated approach from the government of India to safeguard the information infrastructures, networks and data centres of both government and private sectors. This PPP model of security to the national Cyber Spaceis already prevalent in countries like the USA, UK, Australia, Sweden, Switzerland, Germany, France, Estonia, etc.[1] The feasibility of such a partnership was given a structural dimension in the recent report from the 'National Security Council Secretariat', and was released under the title 'Recommendations of Joint Working Group on Engagement with Private Sector on Cyber Security'. This was an ambitious project of the Deputy National Security Advisor, Ms. Latha Reddy, and the study was conducted Data Security Council of India (DSCI)[2], in order to analyse and frame a structural organisation for a Joint working Group (JWG) consisting of both public and private members, that would focus on the area of cyber security of the country. During the release of the report, Ms Reddy stated that:

India has carried out security measures in securing the cyber space of the country in the past and as a next step in the direction, it has recently come out with a plan to have a joint venture with the private sector to effectively counter the future threats in the cyber arena.

"The recommendations are the outcome of extensive and in-depth discussions with the industry."[3]

The Report was resealed on 15th October 2012 by the National Security Advisor of India, Mr. Shiv Shankar Menon. During his address Mr Menon said:

"The unique nature of cyberspace and its potential for damage has propelled the government and private sector to work together" [4]

"We all have seen social media disseminating information to wreck communal harmony. This kind of phenomenon is something we need to learn to deal with. This is something new. The important thing for a democratic society like us is how to do it while maintaining democratic freedom." [5]

While mentioning the kind of approach India needs to take in securing its IT sector, Me Menon emphasied:

"If India has to grow its IT industry, we also have to maintain our reputation of being safe, secure partners with whom everybody can work with. We need to be more secure than we are and we have a sense of the kind of steps we need to take for the future."[6]

It was obvious from Mr. Menon's speech that the Public-Private Partnership would be an indispensible venture in the Cyber space in order to maintain a secured environment and to tackle the complex situations that are existing and also which might occur in the future challenging the security to the cyber world.

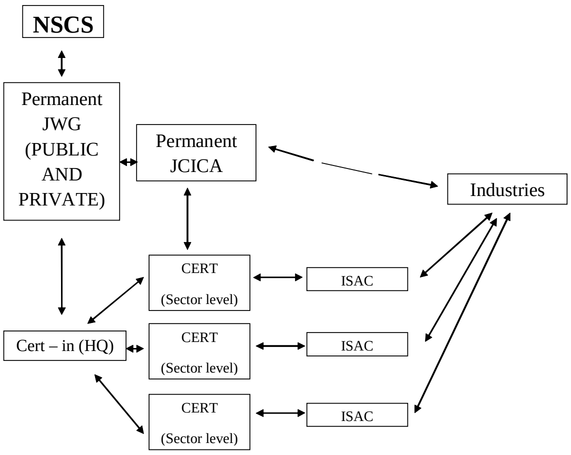
Critical areas would be identified where capacity building can take place in Cyber Security, both for the public and private sector, along with which policy and legal frameworks can be drafted to ensure fulfilment with Cyber Security efforts.

The recommendations released by the National Security Council Secretariat (NSCS) has some salient features stated in the report,[7] which deals in framing a broad model for government engagement with private sector on Cyber Security. The first feature identifies the issue of Cyber Security as an important task to be performed in order to ensure the security of the computer networks and systems of both government as well as industries. The report states that the Cyber Security cannot be achieved in isolation by either government or industry alone. It is for this reason that after deliberations with representatives of the private sector, it decided to set up a Joint Working Group (JWG), under the chairpersonship of Deputy National Security Advisor, to work out the details of the roadmap for Cyber Security cooperation that needs to be evolved. It was also stated that this JWG would consist of representatives from both government and the private sector.

A temporary JWG was constituted and five sub groups were also formed under the JWG to carry out the study for a partnership among the Public and Private sector on Cyber Security and the details furnished by those five groups on 16th August, 2012, were taken into consideration for preparing the report. The JWG even observed some guiding principles that would fortify the Public-Private partnership in Cyber Security. The JWG believes that the institutional mechanism that is to be set up should promote union of efforts both in public and private sector due to varied stakeholders in the field. It is for this reason the already existing institutions and organisations which are working for Cyber Security both in public and private sector should be included in future institutional mechanism. Furthermore, new institutions can be created only to fill the gaps where ever necessary to enhance the effectiveness. However, this mechanism that is to be set should be of permanent in nature and there it is also necessary to find capable bodies that would play a major role in funding and also in the process of implementation in the public-private sector. It is also reported that critical areas would be identified where capacity building can take place in Cyber Security, both for the public and private sector, along with which policy and legal frameworks can be drafted to ensure fulfilment with Cyber Security efforts. It is also observed that promotion of active PPP in the international forums would be given a considerable importance along with formulating India's position on global Cyber Security policies with the aim of establishing India as a global hub of development of Cyber Security products, services and manpower, where promotion would be mostly concentrated on indigenization and joint R&D projects to meet the need of Cyber Security of the country.

The next salient feature identified by the JWG was the Roadmap for PPP on Cyber Security in which it gives an institutional framework that would work on the guiding principles of the JWG. The upper structure or the policy framing body would be headed by NSCS, under which the JWG would operate with representatives from both public and private sector. Furthermore, this JWG would act as an advisory body and coordinate PPP on Cyber Security taking inputs, whenever necessary from the Joint Committee on International Cooperation and Advocacy (JCICA), which would also be a permanent advisory committee of JWG to promote India's national interest at various international forums on Cyber Security. The business associations belonging to the private sectors would be consulted by JWG and JCICA, in order to finalise any of their compositions. At the lower level or on the operational level the private sector would set up Information Sharing and Analysis Centres (ISACs), which would cooperate with the respective sectors of Computer Emergency Response Team (CERTs) of the government, to increase the efforts on Cyber Security.

The proposed structure of institutional framework according to the report would work as follows:



Moreover, it is been observed that capacity building would be the next major task to ensure Cyber Security for which the first identified area is to fill the shortage of Cyber Security professionals, that would be tackled by innovative recruitment and placement procedures along with specialised training forthe existing manpower. It is been observed that the country would need at least 5 Lakh experts in the Cyber Security arena. Currently, it is surviving with just a few thousands.[8]Nonetheless, the report states that, the Ministry of Communication and Information Technology (MCIT) and the Ministry of Human Resource Development (MHRD) would have to play a major role in the capacity building efforts in association with the private sector. The report also states that a competency framework should be established to assess the required skills, identify gaps, and device strategies and programs for capacity building. In addition, MCIT in collaboration with private sector can conduct awareness campaigns for the general public on Cyber Security and it can setup training facilities for Law Enforcement Agencies (LEA) in collaboration with MHRD to train them on cyber forensics and cyber crime. The Private sector can play their part in this by establishing the training facilities and also by providing basic level of professional and advanced level training to the LEAs. The next task in capacity building would be to establish a multi-disciplinary Centre of Excellence (COE),which would focus on the study about the best practices and forensics involved in cyber crime investigation and studies and research related to international frameworks/institutions. In short, the COE would act as a think-tank for the PPP to study and analyse the latest developments in the field of Cyber Security.

Capacity building would be the next major task to ensure Cyber Security for which the first identified area is to fill the shortage of Cyber Security professionals.

As the issues of framework and capacity building have been addressed the next issue identified by JWG, is the standard of security and audits, which would help in enhancing the level of preparedness and assurance in Cyber Security. The private sector is being proposed as the active player in this part of the process where a cyber audit would be made a compulsory by appropriate amendment in the listings required under the companies act. The private sector along with MCIT would have to define the basic standards and guidelines for the critical sector organisations both in public and private sectors. There is also a proposed plan to establish an Institute of Cyber Security Professionals of India which would act as an autonomous institution under the guidance of MCID.

The final issue highlighted in the report was with regard to the measures to enhance testing and certifying facilities to address the growing concerns relating to supply-chain vulnerabilities, where the main aim was to establish a National Testing and Certification Scheme, under the supervision and oversight of MCIT and to establish an independent government certification body for IT products under MCIT. For the private sector, a plan is proposed for establishment of testing labs owned by private firms which would be duly accredited and funded by government. Finally, the key agenda is to enhance India from a 'Common Criteria Certificate Consuming Nation' to that of 'Common Criteria Certificate Authorizing nation'. Common Criteria Certificate (CCRA) is an arrangement which shares a set of agendas which ensures Quality, Security, Non-duplicity, Enhanced Effectiveness and cost-Effectiveness of IT products in the global scenario. At present, the countries with authorizing status in CCRA are: Australia, Canada, France, Germany, Italy, Japan, Malaysia, New Zealand, Netherlands, Norway, South Korea, Spain, Sweden, Turkey, United Kingdom and the United States of America. Whereas, India being a huge producer and consumer of IT products, remains a consuming member in CCRA along with Austria, Czech Republic, Denmark, Finland, Greece, Hungary, Israel, Pakistan and Singapore.

After having identified the guiding principles for PPP in Cyber Security and the various roadmaps to achieve these principles by forming institutional framework, capacity building, increasing the security standards and audits and by developing the testing and certification standards the JWG has finally revealed its four pilot projects as a first step towards the implementation of its recommendations. This includes:

- The setting up of a pilot testing lab
- Conducting a test audit for some selected targets
- To study vulnerabilities in a sample Critical Information Infrastructure
- To establish a multi-disciplinary Centre of Excellence (COE).

The report finally stated that the Permanent JWG to be constituted under the guidance of NSCS, would work out the action plan for all the recommendations stated in this report.

Conclusion

PPP is not a new module that is adopted by India as countries like Austria, Australia, Belgium, Switzerland, Germany, Spain, Finland, Estonia, France, Italy, Netherlands, Sweden, UK and the US are already practicing it at various levels of compositions. But, what makes it special in India, is the fact, that India is a country with high Internet independence and with a population that is highly concerned about Privacy, Interception, Surveillance, Blocking and takedown, which the PPP has to keep in mind. Moreover, there is no time limitations specified for implementation of any of the recommendations mentioned in the report. Furthermore, it is not sure which private sector concerns would participate in the proposed PPP and up to which level. There was no role specified in the report for the countries defence forces in the PPP. As of now, it is unpredictable to state the kind of participation that would take place from both the public and private sector, when PPP is constituted in reality.But if this partnership catapults, then it will open a new area for the Public and the Private sector to cooperate in the field of security, along with the traditional ones like the manufacture/supply of arms, military vehicles and equipment.On the whole, this report by Joint Working Group on Recommendations on engagement of private sector on Cyber Security is a broad approach which tries to interlink the highly advanced IT industry of India and relatively not so advanced government IT sector on a common platform that would address the issue of security.

Notes:

[1] Cooperative Models for Effective Public Private Partnerships Desktop Research Report, European Network and Information Security Agency, 2011.

[2] www.dsci.in/

[3] "National Security Advisor Releases Joint Working Group Report on Cyber Security, Says Urgent Need to Address Risks from Cyberspace", Ministry of Communication and Information Technology, October 15, 2012.

[4] ibid

[5] n. 3

[6] ibid

[7] "Recommendations Of Joint working group On Engagement with private sector On cyber security", Ministry of Communication and Information Technology, Government of India.

[8] "Govt to set up working group to check cyber crimes; spend Rs 300 cr on security", *Business Line, The Hindu*, October 16, 2012.

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.