Centre for Air Power Studies (CAPS)
Forum for National Security Studies (FNSS)
36/20

INDIA'S FORTHCOMING NATIONAL CYBER SECURITY STRATEGY

Analysing the Past to Predict the Expected Outcome

Dr.E.Dilipraj
Research Fellow, CAPS

Keywords: National Cyber Security Strategy, National Cyber Security Policy 2013, India's cyber security, MeitY

During his speech, on India's 74th Independence Day on August 15, 2020, Prime Minister Narendra Modi announced from the ramparts of the Red Fort that the country would soon release its National Cyber Security Strategy (NCSS).[1] While the cyber community of the country were already aware about the drafting of the strategy document, such an announcement from the PM during his national address has put the document in limelight both at the domestic and international level and the expectations from it have increased manifold.

A flourishing smart phones market and affordable internet tariffs have enabled the cyberspace of the country to expand multi-fold in the recent past. This expansion, coupled with the Central Government's push for its scheme of "Digital India," has created a culture of dependency on virtual communications and transactions in the minds of the people of the country. Additionally, the lockdown due to COVID-19 pandemic has further increased the dependency on digital platforms, which has further expanded the span of usage of the country's cyberspace. This puts a premium on ensuring the security of the national cyberspace an ultimate necessity in the coming years.

The security aspects of the virtual domain are yet to catch up with the technological growth and usage seen in this sector. This is evident from the numerous cyber security threats and the threat landscape that the country faces every day resulting in huge loss of data and money. For instance, the extrapolated data from NortonLifeLock report states that Cyber criminals have stolen Rs.1.2 trillion from Indians in 2019 alone.[2] Experts believe that this loss is only the tip of the iceberg and hence the magnitude of loss necessitates stringent counter measures in the form of enhanced security posture in the country's cyberspace. It can be inferred that the formulation of the new cyber

security strategy is aimed at achieving this objective.

The existing National Cyber Security Policy (NCSP), which was released in 2013, has long outlived its expected lifetime and is due for natural evolution in the form of NCSS. The NCSP 2013 has had its share of ups and downs in shaping the cyberspace of the country and a critical analysis of its achievements and shortfalls in contributing towards guiding the cybersecurity of the country in the past would in a way set the tone for the kind of expectations that the forthcoming NCSS has.

The NCSP 2013 highlighted 14 different objectives with almost 50 different strategies to achieve them. Table 1 charts out the Objectives of NCSP 2013 and the Milestones achieved.

Table 1: Objectives of NCSP 2013 Vs Milestones achieved

S.No.	Objective	Milestones
1	To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace and thereby enhance adoption of IT in all sectors of the economy	• Office of **National Cyber Security Coordinator** established in National Security Council Secretariat (NSCS) with the appointment of National Cyber Security Coordinator. • All Government Ministries/ Departments/ Organisations have **CISOs appointed**. Appointment of CISOs in Private sector also promoted. • All Government Ministries/ Departments/ Organisations **earmark specific budgets for cybersecurity** every year.
2	To create an assurance framework for design of security policies and for promotion and enabling actions for compliance to global security standards and best practices by way of conformity assessment (product, process, technology & people).	• **Cyber Crisis Management Plan** prepared by MeitY and circulated to all Government Ministries/ Departments.
3	To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem	-NIL-
4	To enhance and create National and Sectoral level 24 x 7 mechanisms for obtaining strategic information regarding threats to ICT infrastructure, creating scenarios for response, resolution and crisis management through effective predictive, preventive, protective, response and recovery actions.	• **Computer Emergency Response Team-In (CERT-In)** functions as the 24X7 National mechanism for responding to cyber incidents. • Several sectors such as Telecom (**T-CERT**), Power (**Power CERT**), Banking (**Banking CERT**), etc have established CERTs at sectoral levels. • **National Critical Information Infrastructure Protection Centre (NCIIPC)** established as the nodal agency responsible for the protection of Critical

S.No.	Objective	Milestones
		Information Infrastructures and Protected Systems of the country and Phase 1 successfully completed.
5	To enhance the protection and resilience of Nation's critical information infrastructure by operating a 24x7 National Critical information Infrastructure Protection Centre (NCIIPC) and mandating security practices related to the design, acquisition, development, use and operation of information resources.	• **National Critical Information Infrastructure Protection Centre (NCIIPC)** established as the nodal agency responsible for protecting the Critical Information Infrastructures and Protected systems of the country **24X7** and Phase 1 successfully completed. NCIIPC has published the following guidelines: ○ Guidelines for Protection of CII ○ Evaluating Cyber Security in CII ○ SOP: Incident Response ○ SOP: Audit of CII/Protected Systems ○ Rules for the Information Security Practices and Procedures for the Protected System
6	To develop suitable indigenous security technologies through frontier technology research, solution oriented research, proof of concept, pilot development, transition, diffusion and commercialisation leading to widespread deployment of secure ICT products / processes in general and specifically for addressing National Security requirements.	**Make in India** programme initiated in September 2014 by the Central Government for encouraging development of products in India.
7	To improve visibility of the integrity of ICT products and services by establishing infrastructure for testing & validation of security of such products	**Standardisation, Testing and Quality Certification (STQC)** established under Ministry of Electronics and Information Technology (MeitY) provides quality assurance services in the area of Electronics and IT through countrywide network of laboratories and centres. The services include Testing, Calibration, IT & e-Governance, Training and Certification to public and private organizations.
8	To create a workforce of 500,000 professionals skilled in cyber security in the next 5 years through capacity building, skill development and training.	MeitY conducts the **Information Security Education and Awareness (ISEA)** initiative and has conducted a number of education, awareness and training programmes as part of the initiative. As on November 2020, **299458** participants have taken part in **education programme**, **170418** participants have taken part in **awareness programme** and **10789** participants have taken part in **training programmes**

S.No.	Objective	Milestones
		organised through the ISEA initiative.
9	To provide fiscal benefits to businesses for adoption of standard security practices and processes.	-NIL-
10	To enable protection of information while in process, handling, storage & transit so as to safeguard privacy of citizen's data and for reducing economic losses due to cyber crime or data theft.	• The **Personal Data Protection Bill** was fielded in the Parliament in December 2019 for the House's approval. The bill is currently under examination by the Joint Parliamentary Committee. • MeitY has formulated an **Expert Committee** in September 2019 for devising a **Framework for regulating Non-Personal Data** of citizens. The Committee submitted its initial report on the Non-Personal Data Governance Framework in September 2020.
11	To enable effective prevention, investigation and prosecution of cyber crime and enhancement of law enforcement capabilities through appropriate legislative intervention.	• **Indian Cyber Crime Coordination Centre (I4C)** established in 2018 with an overlay budget of Rs 415.86 Crores. • Several States and Union Territories have established **Cyber Crime Cells** as part of their respective State/UT **Police Department**.
12	To create a culture of cyber security and privacy enabling responsible user behaviour & actions through an effective communication and promotion strategy.	• Under the **ISEA initiative** run by MeitY, **170418** participants have taken part in **awareness programme**, which focuses on imparting a culture of cyber security and privacy. • Ministry of Home affairs runs a series of Online and Offline campaigns under the name of '**CyberDost**' with the agenda to sensitise citizens about culture of cyber security and privacy.
13	To develop effective public private partnerships and collaborative engagements through technical and operational cooperation and contribution for enhancing the security of cyberspace.	• MeitY has formulated "**Guidance Notes for IT PPP Projects**" in 2017. • **Microsoft & Data Security Council of India** joined forces under the aegis of the MeitY Initiative - Information Security Education & Awareness (ISEA) and launched Project **CyberShikshaa** for skilling women engineering graduates in the niche field of Cyber Security. As part of this program, C-DAC, MeitY's premier R&D institution for the design, development and deployment of electronic and ICT technologies, conducts training programs exclusively for women and also making them Industry ready by imparting the requisite technical skills in the domain of Cyber Security, in association with National

S.No.	Objective	Milestones
		Institute of Electronics & Information Technology (NIELIT).
14	To enhance global cooperation by promoting shared understanding and leveraging relationships for furthering the cause of security of cyberspace.	Government of India has **MoUs/ Agreements with 42 Countries** (as mentioned below) on various aspects of Cyber Security including Information Sharing and Capacity Development. Australia; Bangladesh; Belgium; Brazil; Brunei; Canada; Colombia; Croatia; Dominica; Egypt; Estonia; Finland; France; Germany; Indonesia; Israel; Italy; Japan; Kazakhstan; Kenya; South Korea; Malaysia; Mauritius; Mongolia; Myanmar; New Zealand; Portugal; Qatar; Russia; Saudi Arabia; Serbia; Singapore; Sweden; Thailand; Tunisia; United Arab Emirates; United Kingdom; United States of America; Uzbekistan; Vietnam.

Source: Data compiled by the author.

While it may seem that, a considerable number of milestones have been achieved by the efforts of various organisations and agencies of the Government, there are certain fundamental shortfalls to the NCSP 2013 that are elucidated below:

1. ***Lack of Timeframes and Action Plan.*** NCSP 2013 specifies no timelines for accomplishing any capabilities or tasks. In addition, it is not an action-oriented document and hence the strategies highlighted in the document have not resulted in their full implementation. For instance, the policy identified that the country would require 500000 cyber security professionals by 2018, but did not provide any road map/ action plan for achieving these numbers. As a result, the country still lacks, by a huge margin, requisite number of cyber security professionals.
2. ***Roles and Responsibilities.*** The document lacked requisite detailing and remains only as a broad guideline document. It does not delineate any responsibility to any cyber security organisation or agency for the implementation of the strategies, which can be attributed as the main reason for its own non-implementation in full measure. All the milestones achieved have been the result of voluntary commitment by the respective Ministry/ Organisation/Agency to undertake the specific task and such actions would have taken place even without the existence of NCSP 2013.
3. ***No Governance Framework.*** The country's cyberspace was rapidly expanding even while the 2013 Policy was being formulated and yet, the policy failed to visualise a

unifying governance framework for the country's cyberspace. This has resulted in the existing scattered approach towards cyberspace governance in the country where cyber security organisations are often involved in duplication of work due to lack of clarity in fundamental responsibilities.

4. ***Void of Financial Commitments.*** Cyberspace is a rapidly expanding and evolving domain, which requires substantial funds for its effective governance and maintaining security. While the NCSP 2013 proposed various objectives and strategies for cyber security of the country, it remained silent about the financial requirements that would be needed to execute the strategies. Additionally, the policy did not suggest any road map for government spending in the field of cyber security in order to achieve the objectives and strategies. This lack of financial commitments towards cybersecurity in general, and the 2013 policy in particular, has resulted in non-implementation of the policy as well as side-lining of cyber security issues.

Despite these inherent shortfalls, NCSP 2013 has served as the guiding light for activities in the budding cyberspace of India. With a vision to ensure a safe, secure, trusted, resilient and vibrant cyberspace for our Nation's prosperity, the NCSS is expected to chart out various strategies under three pillars namely: Secure, Strengthen and Synergise.[3] However, there is a pressing need for the forthcoming NCSS to address the fundamental shortfalls of NCSP 2013 (highlighted above) by being an actionable document, with committed financial support from the Government and clear-cut delineation of roles & responsibilities of various stakeholders; only then will it fulfil its objectives and live up to expectations placed on it.

(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])

Notes

[1] "English rendition of Prime Minister Shri Narendra Modi's address to the Nation from the ramparts of the Red Fort on the 74th Independence Day- August 15, 2020", *Press Information Bureau*, Delhi, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1646045, accessed on November 18, 2020.

[2] Riju Mehta, "Cyber criminals stole Rs 1.2 trillion from Indians in 2019: Survey", *The Economic Times*, April 13, 2020, https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019-survey/articleshow/75093578.cms?from=mdr, accessed on November 18, 2020.

[3] http://ncss2020.nic.in/, accessed on August 16, 2020.