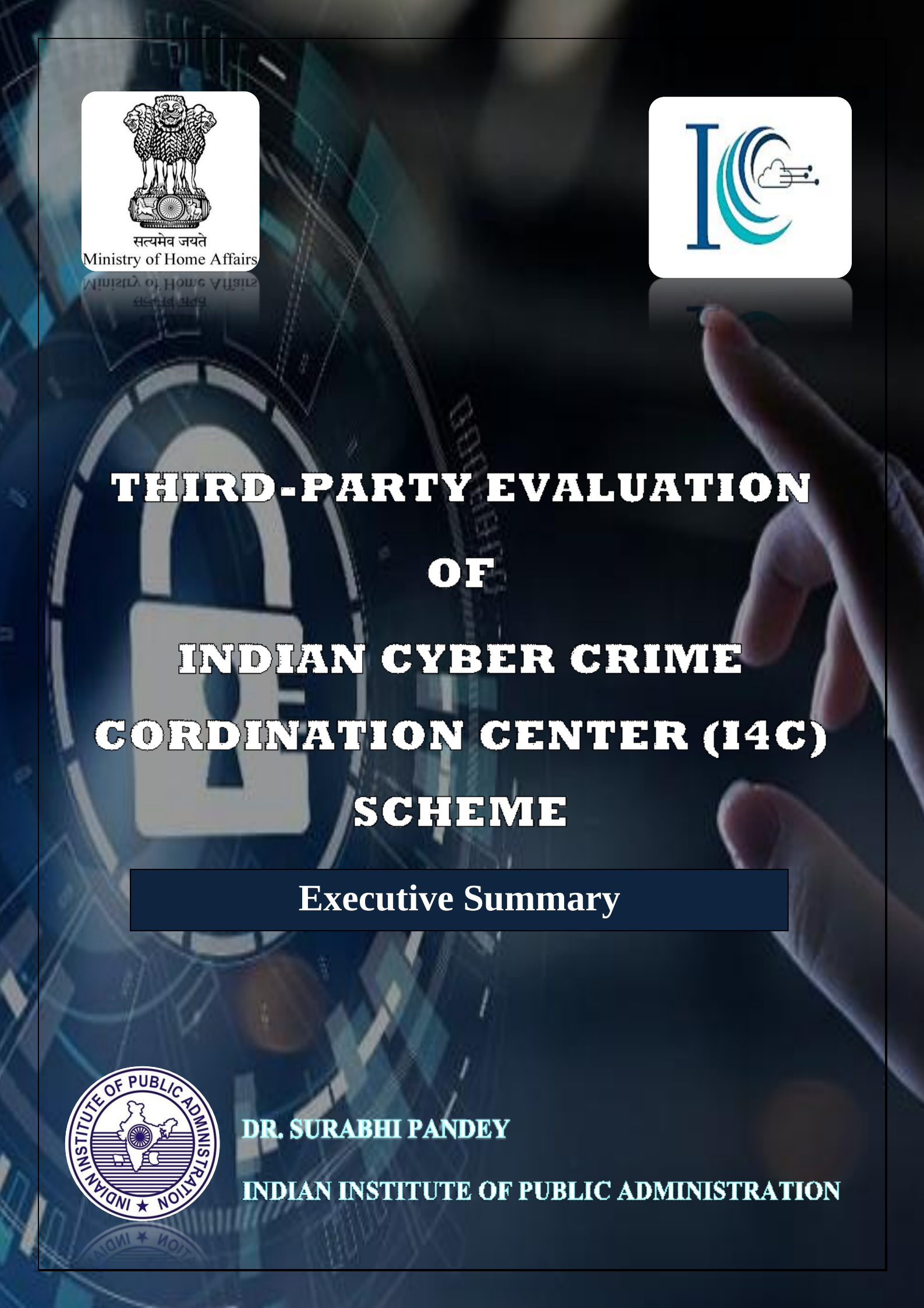

THIRD-PARTY EVALUATION OF INDIAN CYBER CRIME CORDINATION CENTER (I4C) SCHEME

Executive Summary

DR. SURABHI PANDEY

INDIAN INSTITUTE OF PUBLIC ADMINISTRATION

Executive Summary

of

Report on

Third Party Evaluation of Indian Cyber Crime Coordination Centre (I4C) Scheme

Project Head

Dr. Surabhi Pandey

Research Officers

Munisha Chauhan
Surabhi Khullar
Shaurya Singru

Sponsored by

सत्यमेव जयते
Ministry of Home Affairs

Ministry of Home Affairs
Government of India

Conducted by

Indian Institute of Public Administration
New Delhi- 110002

EXECUTIVE SUMMARY

Ministry of Home Affairs (MHA) entrusted to **IIPA** the **Third-Party Evaluation of Indian Cyber Crime Coordination Centre (I4C) Scheme** of the **Cyber and Information Security (C&IS) Division** of the Ministry. The terms of reference for this evaluation study, as mandated by MHA are as below:

TERMS OF REFERENCE

The Evaluation study is expected to assess:

1. Implementation mechanism and progress,
2. Performance of the scheme,
3. Training/Capacity building of administrators/facilitators,
4. Asset/Service creation & its maintenance plan,
5. Coverage of beneficiaries,
6. IEC activities,
7. Need for extension of the implementation period and required time frame,
8. Justification for restructuring of scheme to support setting up of regional cybercrime coordination centers,
9. Achievement of deliverables,
10. Gaps in achievement of outcomes,
11. Key Bottlenecks & Challenges,
12. Input Use Efficiency,
13. Vision for the future, and
14. Recommendation for Scheme with reasons.

INDIAN CYBER CRIME COORDINATION CENTRE SCHEME

The **Indian Cyber Crime Coordination Centre (I4C)** is a crucial element of the **Cyber and Information Security (C&IS) Division** of **Ministry of Home Affairs, Government of India**. With the aim of combating cybercrime in an effective and organized manner, GOI initiated a seven-pronged Scheme for strengthening the cyber ecosystem and infrastructure of India. The scheme with its seven components enables I4C, MHA to be the nodal agency in fighting against cybercrime in the country.

The sub-components of I4C and their salient features are as the following:

1. **National Cybercrime Threat Analytics Unit (TAU)**
    - Platform for analysing all pieces of puzzles of cybercrimes.
    - Produce cybercrime threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions.
    - Create multi-stakeholder environment for bringing together law enforcement specialists and industry experts.

2. **National Cybercrime Reporting Portal**
    - Facilitate reporting of all types of cybercrime incidents with special focus on cybercrime against women and children.
    - Automated routing to concerned State/UT based on information furnished in the reported incident for appropriate action in accordance with law.
    - Facilitate complainants to view status of action taken on the reported incident.

3. **Platform for Joint Cybercrime Investigation**
    - To drive intelligence-led, coordinated action against key cybercrime threats and targets.
    - Facilitate the joint identification, prioritization, preparation, and initiation of multi-jurisdictional action against cybercrimes.

4. **National Cybercrime Forensic Laboratory (NCFL) Ecosystem**

   - Forensic analysis and investigation of cybercrime because of new digital technology and techniques.
   - A centre to support investigation process. NCFL and associated Central Forensic Science Laboratory to be well-equipped and well-staffed to engage in analysis and investigation activities to keep-up with new technical developments.

5. **National Cybercrime Training Centre (NCTC)**

   - Standardization of course curriculum focused on cybercrimes, impact containment and investigations, imparting practical cybercrime detection, containment, and reporting trainings on simulated cyber environments.
   - Development of Massive Open Online Course on a cloud-based training platform.
   - National Cybercrime Training Centre to also focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes.

6. **Cybercrime Ecosystem Management Unit**

- Develop ecosystems that bring together academia, industry, and government to spread awareness n cybercrimes, establish standard operating procedures to contain the impact of cybercrimes and respond to cybercrimes.
- Provide support for development of all components of cybercrime combatting ecosystem.

7. **National Cyber Crime Research and Innovation Centre**

   - Track emerging technological developments, proactively predict potential vulnerabilities, which can be exploited by cybercriminals.
   - To leverage the strength and expertise of all stakeholders, be it in academia, private sector, or inter-governmental organizations.

OBJECTIVE OF THE STUDY

The key objectives of the evaluation study are as follows:

- To evaluate the provision of financial assistance for creation and strengthening of the cyber security ecosystem and infrastructure of states across all the 6 geographical zones of the country,
- To evaluate the implementation progress of I4C across all the seven sub-components of the scheme,
- To evaluate the achievements of deliverables vis-à-vis the sub-components of the scheme,
- To assess the deliverables provided by MHA for evaluation of the scheme,
- To assess the existing constraints faced by the implementing agencies in the implementation of projects under the I4C scheme, and
- To study to aspect of economic, social, and political infrastructure required for the cyberspace industry and suggest programs/schemes/interventions for the government to cater to the necessary measures for the way forward.

METHODOLOGY

1. Scope of Study

The scope of the study encompasses evaluation of the efficacy of I4C as a scheme. For the study of impact analysis, all the seven sub-components vis-à-vis the LEAs in terms of their objectives, implementation mechanism, achievements and suggestions at a national level have been studied.

2. Methodology

The study team applied a balanced combination of quantitative and qualitative tools of data collection. The research study encompassed the identification of primary and secondary sources of information.

The detailed evaluation pertaining to research methodology followed by the study team, are as under:

A. Collection of Secondary Data

The study team collected secondary information from the following sources:

1) Reports, notifications, and other documents as provided on the official websites of MHA and sub-components of I4C.
2) Other relevant information mentioned on the websites, such as, NCRP, MeitY, NCTC, and NITI Aayog among the others.
3) Copies of relevant documents provided by I4C Department of MHA.
4) Copies of relevant documents provided by the components of I4C.
5) I4C Scheme guidelines, project status in terms of its implementation and other relevant information of the scheme.

B. Collection of Primary Data

1) Considering the evaluation study was carried out during the pandemic, interviews took place on digital platforms. The proposal of roster meetings that took place with the respective Law Enforcement Agencies for the study is enclosed in Appendix 1.1.
2) Presentations by the respective agencies and components of I4C, as made in accordance to the agenda points designed by study team.

3. Process Steps of Evaluation Study

This research assesses the I4C scheme, its progress, and prospects, and thereby the extent of its presence and awareness among the public sector, private sector, and civil society of the country since the inception of the Scheme that took place in October 2018.

The following process steps were carried out to study this Scheme:

A. Identification of the Scheme

The scheme guidelines and documents provided by the MHA were analysed and parameters were formulated. Based on the parameters the questionnaire was prepared and data was collected through the annual progress report and personal interview methodology.

B. Designing of Questionnaires based on following parameters:

i) Implementation Mechanism
ii) Operational Issues, Manpower Analysis
iii) Fund and Budget Allocation
iv) Scheme Achievements/Contribution of Scheme
v) Gaps in Achievements of Outcomes
vi) Challenges faced during implementation
vii) Vision for the future

C. Meetings and Visits with respective Components of I4C.

4. Data Analysis

The subsequent information entails the qualitative and quantitative aspects of the methodology used for the study.

A. Qualitative Analysis

- The qualitative analysis of I4C Scheme was performed, by evaluating the I4C related documents provided by I4C/MHA and the other LEAs namely, BPR&D, NCRB and Delhi Police.
- The Agenda Points, Presentations and discussions carried out by the respective dignitaries of the departments were also a part of the analysis made by the study team.

B. Quantitative Analysis

- The quantitative analysis of the Scheme was done based on the data provided by team I4C. This included financial data of all the components as well as some specific data provided by TAU and NCFL.
- In addition, a ranking model was designed to assess the performance of each component and rank them based on the presentations provided by each component over video conferences. The model assessed the completion of objectives, response to challenges faced, future cyber initiatives, and proportion of expenditure by each component to ascertain a degree of accomplishment.

5. Limitations of the Study

The following were a few of the limitations of this study:

I. Given, the study took place during the Covid-19 pandemic, lack of field visits attribute to one of the major limitations of the study

II. Considering, the scheme is in its nascent stage, limited data is available and perhaps the study is limited in terms of evaluating the cyber ecosystem of the country at large

III. Lastly, Lack of interaction with all the stakeholders of the steering committee of I4C has inhibited the holistic evaluation of the study.

SUMMARY OF FINDINGS

1. Visibility of the Scheme

There have been efforts taken by the I4C to proliferate visibility about the threats on cybercrime to the citizens. I4C components have introduced online portals and conducted webinars to reach out to more people.

2. Cyber Awareness

There have been mechanisms implemented by I4C particularly the Cyber Crime Ecosystem Management Unit component have undertaken various initiatives to create Cyber Awareness. Cy-Train (NCTC) and other platforms have initiated bringing awareness about the cyber Crimes. This process has been helpful to a large extent for both the LEAs and common citizens. Some more combined efforts and better coordination between the State's agencies are required. A twitter handle CyberDost is also being operated by I4C for creating awareness.

3. Financial Support

I4C and its components have received financial support on a regular interval of time. The Budgetary allocation and expenditure have been enhanced according to the expenditure requirement of the components.

4. Inter-Agency Coordination

Multiple institutions have been established at varied locations. This results in time-consumption and creates problem in effective coordination, for instance, differences between Centre and different States nodal agencies and their workings creates delays.

5. Manpower Strength

I4C has been going through a crisis in recruiting professional manpower for many of its components. Professional manpower for malware analysis and other areas has been a major challenge which I4C has been trying to overcome.

6. Duties and Responsibilities

Each component in the I4C has their defined duties and responsibilities and the LEA's are performing the task allocated to them. The task of Joint Cybercrime is yet to be fully functional to its capacity.

7. Shortage of Professionals

There is a limited availability of experienced professionals in area of cybercrime. During the discussion it was highlighted that the cyber safety infrastructure needs well trained and skilled professionals. The process of recruitments needs a boost.

8. Scheme Achievements

I4C has achieved success to a larger extent in processing cases related to cybercrime. Each component of I4C has been effective in their working. The units have been able to gain a remarkable amount of achievements in a short period of time since the scheme inception.

The main highlights of all the components-wise achievement are summarised below:

I4C-TAU

- A new concept of Regional Cyber Crime Coordination Center has been adopted as part of I4C involving all the states. As of now 28States/UTs have given their consent to setup R4C in their states and will actively collaborate with I4C for preventing cybercrime.
- Over 20000 suspect mobile numbers have been shared with DoT based on cybercrime portal analytics.
- 09 mobile apps have been shared which are being used by militants to share information bulletin during internet shutdown in J& K region.
- A total of 134 IoCs received from Cert In has been analysed by I4C.
- Started sharing reports on Cyber Incidents with NSCS.
- Open source Threat Analytics and other documents for internal use in I4C.
- NCCC, NCIIPC and CERT-In have started sharing CMTX alert and other information with I4C.
- *PM Cares fund fraud case:* I4C has shared fake UPI ID of PMCARES with NPCI for its blocking and monitoring. NPCI has blocked 239 VPAs.

- 239 UPI handles like **pmcares@sbi** also shared with Delhi Police.
- I4C proactively advised payment operators for taking necessary steps including awareness campaigns to prevent financial frauds while making digital payments in view of COVID-19.

NCFL

- Installation of Damaged Hard disk Recovery/Forensics Lab
- Installation of Advanced Mobile Forensic Lab
- Installation of Image & Video Enhancement/ Forensics Lab
- Installation of Malware Forensics Lab
- Installation of Crypto-Currencies Forensics Lab
- Upgradation of Existing Memory Forensics Lab with latest Forensics workstations
- Upgradation of Existing Mobile Forensics Lab with latest software

Cybercrime Ecosystem Management Unit

- Total 587 cybercrime awareness tips tweeted on @CyberDost Twitter handle: over 1.93 lakh followers.
- Over 50 crore cybercrime awareness SMSs sent to mobile customers.
- 9 FM radio spots on cybercrime awareness released.
- Created awareness brochures on Financial frauds, Matrimonial frauds, Job frauds and Safe use of Social Media Platform and Cyber Crime Awareness Booklet on Cyber Security Awareness.
- On initiative of I4C, NCERT has published a cyber safety handbook for students of Secondary and Senior Secondary Schools.
- 13 Central Ministries, 06 CAPFs have designated nodal officers for I4C.
- Raised the security concerns with the Ministry of Road Transport and Highways (MoRTH) regarding the security data and misuse of FASTag for cheating users.
- Follow up with MeitY, CERT-In NIC, NIXI, and CIS division regarding the use of domain names like government domain (dot)gov(dot)in and (dot)nic(dot)in for fraudulent activities.
- Development of short films/videos on cybercrime awareness and its prevention for children and the general population by BPR&D/NCRB.

NCTC

- Work completed on MOOC Platform, and Pilot testing has been done by more than 350 Police Personnel
- Content development for 'Responder Track': Developed 28 videos which were prepared through local vendor
- MoU with CEC for sharing of Cybercrime related course contents. These contents have been uploaded on the NCTC MOOC Platform.
- MoU with NeGD for development of NCTC.
- Conducting Cybercrime investigation training at NCRB under NCTC banner: Six (06) Classroom Courses conducted at NCRB HQ and total 143 trainees are trained on NCTC MOOC Platform.
- Setting up of Cyber Lab by C-DAC
- RFP for managed services for maintenance of MOOC platform
- Procurement of furniture and IT Infrastructure for Cyber Lab of an estimated amount of Rs. 1.05 Crores has been initiated through GeM
- Course content development: Technical bids are under examination
- Development of Virtual Classroom at NCRB: Preparation of RFP is in Final Stage
- Meeting for Collaboration with National & International Agencies/Institution for collaborative development of simulated course contents on Cybercrime investigations
- Launch of NCTC MOOC platform namely CyTrain portal
- More than 850 Police Officers across the country have enrolled different courses on CyTrain Portal.

NCRP

- More than 49 Million visitors, 105171 complaints filed, 1402 FIRs lodged, 248 NC registered, 413 notice issued as on 15th May 2020,
- Total 79 Advisories has been uploaded on the Cyber Police Portal.
- Total 2654 unique mobile numbers of the suspects involved in frauds have been shared with Department of Telecommunication for appropriate action.
- Daily cybercrime trends are also being generated with the help of National Cyber Crime Reporting Portal and same is being shared with LEAs.

NCR&IC

- Under NCR&IC, a lab has been instituted in Hyderabad that entails several forensic tools, 31 workstations – for the students.
- There are 3 more labs wherein third-party tools are used. Currently, NCR&IC is recommending work threat stations.
- SOP for Joint Investigation Platform Centre has been proposed and submitted to MHA. Post approval, its functioning will begin.
- Concept of Smart Policing (SMART India) is being put into practice.
- NCR&IC has benchmarked the best practices being followed in collaboration with foreign vendors and indigenous players.
- Increase in efficient professional hiring to combat the existing challenges.

Platform for Joint Cybercrime Investigation Team: Draft SoP for the same has been prepared and circulated to all states for their comments and feedback.

RECOMMENATION AND SUGGESTIONS BY I4C COMPONENTS

Based on the interactions with officials of I4C components and subsequent observations made by the study team, key recommendations and suggestions made by I4C components are enlisted below.

A. Delegation of Power and Authority to a Dedicated Workforce

It is suggested that with delegation of power and authority, wherein the agencies are given a free hand in implementing the project, the process of attaining the deliverables will become easier and more effective. Regular Post of DG (I4C) is much needed at this juncture to take I4C to next level.

Another important suggested measures by I4C to mitigate the existing issue of trained workforce is by giving designated time to the personnel for enhancing their technological skills. Considering, multiple tasks are assigned to Government officers and police force; they do not have the time to take up these courses. Hence, they should be given designated time

with incentive to encourage the workforce. Longer work tenure for professionals and consultants will also be beneficial in providing continuity in the work.

B. Hiring of Trained Professionals

Considering, cybercrime is a global phenomenon; it is imperative for worldwide collaboration wherein effective measures for combating cyber-led crimes can be achieved. In the given scenario, I4C is suggested to continue collaboration with national and international agencies for adoption of best practices. To attain the same, it is also suggested that professional hiring for the purpose of benchmarking needs to be given consideration. As a result, trained manpower will assist in benchmarking against best global practices and optimum utilization of resources.

One of the suggested measures by I4C to mitigate the existing issue of trained workforce is by giving designated time to the personnel for enhancing their technological skills. Considering, multiple tasks are assigned to Government officers and police force; they do not have the time to take up these courses. Hence, they should be given designated time with incentive to encourage the workforce. Longer tenure of professional and consultants will provide continuity and the workforce will be more effective.

C. Knowledge Repository

To fasten the working process, creating a large mainframe structure and a better log system over the investigation would enhance the cyber defense mechanism and speeding of the investigation process. In simpler terms, it may be stated that adoption of a sound knowledge repository will enable smooth functioning of the cybercrime ecosystem by leveraging the tasks performed by the respective workforce.

D. Training and Awareness Programmes

An increase in awareness of training courses offered by the training division of BPR&D will mitigate the existing issue of lack of trained personnel along with keeping the professionals updated with latest technological trends.

E. Subjective Benchmarking

The practice of subjective benchmarking will facilitate NCR&IC to bring all the diverse stakeholders on common ground. This will in turn smoothen out the functioning of this sub-component of I4C. Supplementing the suggestion of increased trained professionals, the adoption of benchmarking against the best practices will stimulate the functioning of cyber security architecture of the country in the global paradigm of cyber safety measures.

F. Accreditation and Certification

As expressed by NCTC, establishment of accreditation and certification system for various training institutes, organizations and individuals working in the field of cybercrime should be given importance. Several measures to attain the same are being taken place. As suggested, establishing standard SOPs for the same is being sought of.

G. International Collaborations

Collaboration of I4C –TAU with international organizations like Interpol , USA Cybercrime coordination center, Europe cybercrime coordination center, UNODC will help I4C to leverage its potential to the fullest as there will be exchange of latest information , best practices adopted for prevention of cybercrime and getting data from International ISP will become more easy.

RECOMMENDATIONS AND SUGGESTIONS BY IIPA

The team of IIPA is of the viewpoint that the functioning and implementation of Indian Cyber Crime Coordination Centre (I4C) scheme has been effective and satisfactory. Based on the observations made by the study team, certain suggestions and recommendations have been put forward as enlisted below.

1. **Immediate Appointment of Officials at Senior Posts**

   Currently, the posts of Directors across all the sub-components of I4C are vacant. It is suggested that appointment of Directors and Under Secretaries vis-à-vis the seven sub-components of the scheme along with support staff for Director/ other officers should be given consideration on an urgent basis. It is also suggested that a post of **Director General** may be created to synergize the prevention, detection, investigation and prosecution activities undertaken by States/UTs and to provide strategic direction to I4C by identifying strategic priorities and define the strategic roadmap for achieving the objectives set for I4C. Also, lead and guide other functional heads of seven components.

2. **Technical Manpower**

   It is suggested to increase the employment of technical manpower in all the sub-components, along with contract professionals with 3-year term in addition to govt officials, respectively. The need of addressing this issue has been expressed by the LEAs. In addition, it is suggested to encompass a trained and professional workforce that will be allocated to each of the sub-components in a dedicated and strategic manner. Therefore, the ratio of manpower in LEA to combat cyber-attacks should be increased for all the components.

   In support to the suggestion, a well-established accreditation and certification system for various training institutes, organizations and individuals working in the field of cybercrime should also be laid emphasis on.

3. **Regular Budgeting:**

I4C is mandated to deal with cybercrimes in a coordinated and comprehensive manner and to act as Nodal agency to deal with cybercrimes of India, It is recommended that instead of scheme , regular budget based on annual Plan should be there as it is now an ongoing activity.

4. **Special Financial Allowances:**

To adhere the level of motivation it is suggested that a special allowance should be given to I4C officials being a specialist Centre

5. **Enhancement of Centre-State Coordination on Cybercrime**

To effectively implement the mechanism that has been constituted to combat cybercrime threats and attacks, an integrated approach wherein center-state coordination is strengthened will yield productive outcomes.

Currently, a hierarchical structure of monitoring cybercrime related cases vis-à-vis the complaints lodged is taking place. In the given light, it is suggested that surveillance of Information System in a horizontal and vertical manner should be laid emphasis upon.

6. **Capacity Building at Block Level (emphasis on Rural India)**

To spread awareness among the mass citizens, broadcasting can be done with the help of All India Radio, Doordarshan that will enable in attaining mass outreach on areas related to awareness of cyber security and safety. For the masses living in the rural India, awareness program can be carried with the help of Block Development Officers and Panchayats.

In addition to this, capacity building can be bolstered by incorporation of a course on cyber safety in educational curriculum at initial levels of education (primary and secondary level) of education.

7. **Center of Excellence (CoE)**

To support the functioning of cyber ecosystem at large it is suggested to develop Centre of Excellence (CoE) for the study of best practices in cyber security and institutionalize the development, sharing, collation and implementation of best practices across

country. This will also progressively develop the skilled and trained personnel on matters related to cyber safety and security.

8. **Involvement of NGOs and Women Empowerment in Cyber Safety Programmes**

To strengthen the cyber ecosystem at large it is suggested to increase the involvement of NGOs wherein programmes on cyber safety and security, participation of women will also escalate. As observed during the study, rape threats, women safety and child pornography have been among the major concern area of I4C. This is evidently witnessed on NCRP platform wherein the sub-component has received major issues related to cybercrime on women. It is therefore recommended to increase the strength of NGOs for women and holistic empowerment at large.

9. **Institutional Repository**

It is suggested to lay emphasis on establishing a sound institutional knowledge repository of cyber security and measures and other remedial initiatives. The repository will work as knowledge bank – a centralized database for all seven sub-components.

10. **Developing effective Public Private Partnership (PPP) Model**

Incorporation of Public Private Partnerships will create an environment for enhancing trust between the industry and government. It is notable to state that Government and industry cannot overcome the cyber security challenge in isolation; the imperative is to work together in a trusted and collaborative environment, leveraging each other's strength to strengthen the cyber security posture and hygiene of the country and take lead in global cyber security efforts. Internal Security, Banking and Technology should tie up with government agencies working for cyber system to strengthen total security of the country. The tie-up and collaboration of these verticals has been effective in many advanced countries, owing to their best ratings in cyber security.

11. **Standardization of Cyber safety Programmes**

It is recommended to standardize cyber awareness programmes by benchmarking against the best global practices. To enhance cyber courses standard, the concept of "Cyber Belt" should be given consideration like six sigma certification courses. This will enhance the standard of cyber security knowledge base with benchmarking.

12. **Contribution in Global Dialogues on Cyber Norms and laws**

Regular consultation with the identified groups such as Government agencies, academia, NGOs, private players, and technical companies at both, national and international level should be given importance in a regular manner. The Intersection of law, policy and strategy in the international cyber security dialogue is important to laid emphasis on more systematic and structured way of formulating national strategy pertaining to cyber norms.

13. **Integration of e-Court Services for Cybercrime Cases**

In Cybercrime portal there is already provision of repository of court cases related to cybercrime cases and judgments. Integration of e-Court Services with TAU platform will aid in resolving procedural issues of registered cybercrime cases and can be used as reference case in judiciary. Furthermore, integration of e-court services for speeding up the increasing log of existing cases will bolster the process of proactive identification of cyber threats and organized criminal groups that the government is currently working on.

14. **Competency Framework:**

A Competency framework can be designed and implement for building adequate cyber security workforce. The competency framework will assess the technical skills set requirement, identifying current existing gaps, define major competency areas across the components with defined roles and devise strategies and programme for building and trained the required capacity.

15. **Building lawful Interception Capabilities:**

Emphasis will be given to build lawful interception capabilities for providing balance national security and economic growth by establishing a national center for performing research in cryptography and cryptanalysis.

16. **Joint Approach to Deal with Cyber Fraudsters:**

I4C Initiative of Platform for Joint Cybercrime Investigation is going to be a great help to jointly deal with cybercrime cases at state and UT levels.