14C A New Cyber Initiative- By Government of India in 2020

– Subodh Kesharwani
Associate Professor, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0001-8565-1571 skesharwani@ignou.ac.in

– Shailza
Research Scholar, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0001-5414-2467 shailza509@gmail.com

– Jyoti
Research Scholar, SOMS, IGNOU, New Delhi
https://orcid.org/0000-0002-1945-3005 jyotiningania@gmail.com

Article History
Paper Nomenclature:
Argument Based Credentials (ABC)
Paper Code: CYBNMV1N6NOV2019ABC3
Submission Online: 02-Nov-2019
Manuscript Acknowledged: 11-Nov-2019
Originality Check: 13-Nov-2019
Originality Test Ratio: 20% **(Disclaimer)**
Peer Reviewers Comment: 15-Nov-2019
Blind Reviewers Remarks 20-Nov-2019
Author Revert: 21-Nov-2019
Camera-Ready-Copy: 23-Nov-2019
Editorial Board Citation: 24-Nov-2019
Published Online First: 22-Jan-2020

The scheme to set up I4C was approved on October 2018 at an estimated cost of around 416 crore rupees to deal with all types of cyber-crimes in a comprehensive and coordinated manner in an Indian jurisdiction or the cross border. At the initiative of Home Ministry, 15 States and UTs have given their consent to set up Regional Cyber Crime Coordination Centres to deal with the matters relating to Cyber Security, Cyber Crime, National Information Security Policy & Guidelines (NISPG) and implementation of NISPG, NATGRID etc.

Keywords : Cyber Crime | Cyber Security | Cyber Law | 14C | Cyber Attacks | Citizens

Introduction:

On January 10, 2020 Government of India inaugurated the Indian Cyber Crime Coordination Centre (I4C) and a National Cyber Crime Reporting Portal. I4C is a seven-pronged scheme to fight against cybercrimes which is facilitated by National Cyber Crime Reporting Portal where people can report cybercrimes online.Over a period of time, there has been a phenomenal increase in use of computers, smart phones and internets. With this increase, cybercrimes have emerged as a major challenge for law enforcement agencies. The cybercrime cases are of varied types. These range from defacement of government websites, online financial frauds, online stalking and harassment, data thefts Phishing, scanning or probing, website intrusions and defacements, to virus or malicious. Each requires specialised investigative skill sets and forensic tools. Cybercrime cases pose technical, legal and administrative challenges in investigation which require strengthening of the institutional mechanism. Cyberattacks that target the infrastructure or underlying economic well-being of a nation state can effectively reduce available state resources and undermine confidence in their supporting structures. A cyber related incident of national significance may take any form such as an organized cyberattack, an uncontrolled exploit such as computer virus or worms or any malicious software code, a national disaster with significant cyber consequences or other related incidents capable of causing extensive damage to the information infrastructure or key assets. Large-scale cyber incidents may overwhelm the government, public and private sector resources and services by disrupting functioning of critical information systems. Complications from disruptions of such a magnitude may threaten lives, economy and national security. 14C is launched with a vision to build a secure and resilient cyberspace for citizens, businesses and government altogether. It will assist in centralizing cyber security investigations, priorities the development of response tools and bring together private companies to contain the menace. Operationalization of National Cybercrime Reporting Portal is to deal with all types of cybercrimes. The earlier Cybercrime Reporting Portal www.cybercrime.gov.in was for filing of cybercrime complaints pertaining to Child Pornography (CP)/ Rape Gang Rape (RGR)/ Obscene Content only, however, the National Cybercrime Reporting Portal facilitates filing of all types of cybercrimes with special focus on the cybercrime against women and children. 14C has got various objectives as explained further in the article.

CYBER AND INFORMATION SECURITY (C&IS) DIVISION

*Courtesy: Ministry of Home Affairs (MHA), government of India

Source: https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division

Mission of 14C:

14C is launched with a prime mission to protect information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities and minimize damage from cyber incidents through a combination of institutional structures, people, processes, technology and cooperation.

Objectives of 14C:

- To act as a nodal point in the fight against cybercrime
- To prevent misuse of cyber space for furthering the cause of extremist and terrorist groups
- To suggest amendments, if required, in cyber laws to keep pace with fast changing technologies and International cooperation
- To coordinate all activities related to implementation of Mutual Legal Assistance Treaties (MLAT) with other countries related to cybercrimes in consultation with the concerned nodal authority in MHA.
- To create a secure cyber ecosystem in the country, generate adequate trust & confidence in IT systems and transactions in cyberspace
- To create a culture of cyber security and privacy enabling responsible user behaviour& actions through an effective communication.
- To identify the research problems/ needs of LEAs and take up R&D activities in developing new technologies and forensic tools in collaboration with academia / research institutes within India and abroad
- To strengthen the Regulatory framework for ensuring a Secure Cyberspace ecosystem

Working of the Portal:

- This portal facilitates a person to report any kind of cybercrime under various available category and sub-category, including cybercrimes affecting women and children.
- There is a dedicated section 'Learn about Cybercrime' on the home page of cybercrime.gov.in portal under which the description of various type of cybercrime that can be reported through this portal can be found.
- Assignment of a reported complaint to a State/UT is done on the basis of the address of the complainant.
- For future tracking of the complaint, the complainant will receive a complaint ID on the registered mobile number and e-mail address. This complaint ID is not a FIR number but is a confirmation of registration of complaint on the portal.

- The jurisdictional State/UT law enforcement agency will also send the update of action taken on the registered mobile number and e-mail ID.
- In case complainant is not satisfied with the action taken by the State/ UT law enforcement agency he/ she can reach out to grievance officers of the concerned State/ UT.
- The complainant can track status of his/her reported complaint by logging into the account user manual for national cybercrime reporting portal.

Other Ministry functioning against Cyber Attacks:

Apart from MHA various other ministries with some special divisions and units as given below are also working to tackle the cybercrimes:

- **Ministry of Finance (MOF):** Cyber security wing for financial frauds-Fin-Cert
- **Ministry of Electronics and Information Technology (MeitY):**
- CERT-in (Computer Emergency Response Team);
- National Cyber coordination Centre (NCCC) as part of CERT-in for e surveillance;
- Computer & information Security Advisory Group
- **Ministry of external Affairs (MEA):** Cyber Diplomacy Division
- **National Technical Research Organisation (NTRO):** National critical information infrastructure protection Centre

**Source: ET prime research*

Steps taken by the MHA to tackle increasing Cyber Crime:

- This division will deal with matters relating to security clearances, Cyber Security, Cyber Crime, national information security policy & Guidelines (NISPG) and implementation of NISPG etc.
- It will act as a dedicated wing to track and counter online fraud, hacking, identity theft, dark net, trafficking and cyberattacks on critical infrastructure.
- The CIS division will have four wings namely Security Clearance, Cyber Crime Prevention, Cyber Security and Information Security Wings each headed by an Under-Secretary level Officer.
- It will coordinate with state governments/ UTs and closely monitor cyberspace and social media with due emphasis on vernacular content.
- It will also block those websites which flout Indian laws and circulate child pornography and communally and racially sensitive content.

Components of Indian Cyber Crime Coordination Centre:

Indian Cyber Crime Coordination Centre will be set up under the newly created Cyber and Information Security (CIS) division of the MHA. It has seven components as discussed below:

1. **National Cyber Crime Threat Analytics Unit**

- This unit provides a platform to work collaboratively to the different stake holders such as Law enforcement persons from private sector, academia and research organizations in order to deal with the cybercrimes.
- It shall also produce cybercrime threat intelligence reports and organize periodic interaction on specific cybercrime centric discussions.
- For bringing together law enforcement specialists and industry experts, it creates multi-stakeholder environment.

2. **National Cyber Crime Reporting Portal**

- This unit will work in tandem with already established investigation units at state and central levels as well as experts from different spheres to create expert investigation teams.
- It Will be capable of answering in real time basis for the rapidly emerging cyberthreats and also to collaborate with partners to investigate cyber related issues.

Figure : *Components of Indian Cyber Crime Coordination Centre*

3. **National Cyber Crime Training Centre**

- It will standardize the 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 to be delivered on a cloud based training platform.
- It will also focus on establishing Cyber Range for advanced simulation and training on cyber-attack and investigation of such cybercrimes.

4. **Cyber Crime Ecosystem Management Unit**

- It will provide a platform for academia, industry and government to operate and investigate a cybercrime basis established standard operating procedures
- It will be able to provide incubation support for development of all components of cybercrime combatting ecosystem.

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

- It keeps a check on emerging technological developments toforecast potential vulnerabilities, that can be exploited by cybercriminals.
- It will leverage the strength and expertise of all the stakeholders such as academia, the private sectors or inter-governmental organizations.
  - It creates strategic partnerships with all such entities in the area of research and innovation focused on cybercrimes, cybercrime impact containment and investigations.

6. **National Cyber Crime Forensic Laboratory Ecosystem**

- It will assist in forensic analysis and investigation of cybercrime.
- It will provide a well-equipped and well-staffed centre in order to support investigation process.

7. **Platform for Joint Cyber Crime Investigation Team**

- It aims at driving intelligence-led, coordinating action against key cybercrime threats and targets.
- It will facilitate the joint identification, prioritization, preparation and initiation of multi-jurisdictional against cybercrimes.

Need for surveillance:

India is the region most targeted by cyber-attackers, resulting in significant economic losses. As the region continues to play a key role in the global economic market, these cyber threats are expected to increase. Over 460 million people in India currently use the internet, leaving them vulnerable to online criminals – both individuals and organized syndicates. It has been observed that India has been ranked 2nd amongst the countries exaggerated by cyber-attacks between 2016-2018? According to a source, there was a 22% rise in cyber-attack in India on IoT deployments. India has faced the most number of attacks in the IoT department this year. In fact, India has been consecutively facing cyber-attacks, the second time in the row!

Curtain raiser about Cyber Security scenario in India:

- India ranks 3rd in terms of the highest number of internet users in the world after USA and China, the number has grown 6-fold between 2012-2017 with a compound annual growth rate of 44%. (NITI Aayog)
- As per a report by Indian Computer Emergency Response Team (CERT-In), more than 53,000 cyber security incidents took place in India in 2017
- As per the data by NCRB (National Crime Record Bureau), 12317 cases related to cybercrime were registered in 2016.
- India ranked 23rd out of 165 nations in the second Global Cybersecurity Index (GCI)

Organization Structure of CIS Division:

CIS-I Desk: Co-Ordination Wing

- Co-ordination within the Division.

CIS-II Desk: Cyber Crime Wing

- Indian Cyber Crime Co-ordination Centre (I4C) Scheme.
- Schemes on prevention of Cyber Crime against women and children.
- Central Cybercrime portal.
- Capacity building – Setting up of Cyber investigation labs.
- Best Practices compilation and dissemination on cyber Crime.

Some facts and figure of India attacks:

•	In a recent study, it was discovered that out of 15 Indian cities, Mumbai, New Delhi, and Bengaluru have faced the maximum number of cyber-attacks.
•	In the Annual Cyber Security Report by CISCO, 53% of cyber-attacks caused more than $600K of financial loss to organizations.
•	Cyber-attacks in India have risen up to such an extent that our country ranks fourth out of the top 10 targeted countries in the world.
•	According to the Economic Times, 96% of data breaches successfully take place through emails.
•	About 90% of cyber-attacks happen because of employee negligence and around 30k websites are hacked on a daily basis

- Cybercrime complaints.
- Dealing with cyber threat inputs and dissemination thereof.
- Coordination and Guidelines/ Advisory to States/UTs.
- Budget Matters.
- Annual Action Plan.
- Grievances, RTI, court cases including prajjwala court case, Parliament Questions and other matters connected with above.

CIS-III Desk: Cyber Security / NISPG Wing

- Implementation of information security policy as per NISPG in MHA
- NATGRID
- Data Protection framework.
- Blocking of websites and regulation of intermediaries and coordination with MeitY
- Cyber Security policy, intelligence report on cyber security breach of organizations and government officials.
- International conventions on Cyber security and cyber- crime (inputs of CIS-II Dsk will be taken as per need).
- Coordination with CERT-In, NCSC, National Critical Information Infrastructure Protection Centre, MEA, IB, Deity, Defence etc.
- NISPG policy and its implementation / compliance in other government organizations
- Administration & Monitoring of Network Operations Centre and Security Operation Centre of MHA
- Regular information security audits (internal and external).
- Co-ordination with NIC for administration of IT assets, monitoring of traffic and logs.
- Assessing security risks, planning and implementing steps to counter threats
- Cyber awareness programs and skill building of MHA officials.
- Overall supervision of NIC Unit in MHA.
- Related grievances, RTI and parliament questions etc.

CIS-IV Desk: IS / CISO Wing

- Policy on lawful interception.
- Co-ordination for Centralized Monitoring System.
- Secured communication systems like RAX, SDCN etc.
- Audit of monitoring facilities, policy related issues of DoT.
- Related grievances, RTI and parliament question.

How 14C is going to help Indian citizens in the long run?

- Cybercrime Reporting Portal will empower citizens to report online content pertaining to Child Pornography (CP)/ Child Sexual Abuse Material (CSAM) or sexually explicit content.
- Through the portals the cybercrime related complaints will be accessed and addressed by the concerned law enforcement agencies in the States and Union Territories for taking action as per law on immediate basis.
- It will assist to provide and create an ecosystem for dealing with cybercrimes in a comprehensive & coordinated manner. In future, this portal will provide for a chatbot for automated interactive assistance system to the public for guidance on cybercrime prevention and how to report incidents on the portal.

Way Ahead:

Cybercrimes being the emerging issues needed to be dealt with promptly. According to NCRB (National Crime Research Bureau), 2017, the cybercrimes has doubled in India. The government of India has decided to hire IT experts from premier public and private institutes, including IITs, to help fight new age crimes like online fraud, hacking, identity theft, dark net, trafficking, child pornography, online radicalization and cyber-terrorism. Apart from I4C, the central government has also launched NIC-CERT (National Informatics Centre-Computer Emergency Response Team). The centers are highly important for India to achieve its 5 trillion-dollar economy by 2024. This is because, Indian Power sector alone faces at least 30nevents being reported daily. 14C, will undoubtedly help the citizens to timely reporting to crimes and will also assist in proper address to them.

Conclusion:

Cyber criminals have different motives, but they can command the resources to create attack vectors in order to achieve the results they want. They may commit fraud, identity theft, steal money, and commit robbery against corporations, banks, nations, regions and even individuals. They may try to blackmail them, too. The initiative taken by the government will empower the citizens to do the timely reporting of the cybercrimes and get appropriate support from government machinery to deal with them.

Disclaimer/Declaration by the authors:

This is an excerpt from the government of India portal and used as a suggestive measure. The contents are wholly owned with the Government of India and its counterpart and vested with the original copyrighter. The purpose behind throwing a light on this thought is to make readers and learners aware to the scheme and its implications.

For more details please https://mha.gov.in/division of mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme. The purpose behind floating this thought in a magazine cybernomics is to make learner familiar about the law and take precautionary measure.

References:

- https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india
- https://www.dailypioneer.com/2020/india/shah-launches-cyber-crime-reporting-portal--14c.html
- https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
- https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184
- https://currentaffairs.gktoday.in/tags/indian-cyber-crime-coordination-centre
- https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf
- https://www.thehindu.com/news/national/govt-to-set-up-apex-cybercrime-coordination-centre/article22540882.ece
- "Time for parliamentary oversight over intelligence agencies". Deccan Herald.
- The Role and Impact of Forensic Evidence in the Criminal Justice Process by Joseph Peterson, Ira Sommers, Deborah Baskin, and Donald Johnson, 2010
- Digital Forensics in Law Enforcement: A Needs Based Analysis of Indiana Agencies by Teri A. Cummins Flory (Purdue University),2016.
- Standard operating procedure of digital evidence collection (Digital Forensics Department, CyberSecurity Malaysia)
- Forensic Examination of Digital Evidence: A Guide for Law Enforcement, National Institute of Justice, Apr. 2004, https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
- "Take steps to make intelligence agencies accountable to Parliament: Team Anna". Times Of India
- "Spooks Under Scrutiny". India Today.
- "India Unprepared For Cyber Warfare". Business Insider.
- "National Cyber Security Policy-2013". Department Of Electronics And Information Technology.
- "India to Beef Up National Cyber Defense". Softpedia News.
- "Govt plans to set up Rs 800 crore cyber intelligence centre". Firstbiz.
- "Centre to shield India from cyber attacks proposed". Hindustan Times.
- "Super cyber intelligence body soon, announces IT Minister". The Hindu.
- "Rs 1,000 cr set aside for cyber shield". Business Standard.
- "Minister's response in the LokSabha to a question on the operationalization of the NCCC" (PDF). LokSabha.
- "Big brother is watching you?". Hindustan Times.
- "Cyber Crime Prevention Strategy will be Strengthened: Home Minister ShriRajnath Singh". Press Information Bureau, Government of India, Ministry of Home Affairs.
- "Exempted Organisations From Applicability Of Right to Information Act 2005". CIC Online.

Dr. Subodh Kesharwani is an academician with a bronze medal in his post graduate and Doctorate in ERP System in 2002 from Allahabad University. He is one of the researchers who had concentrated his research on Total Cost of Ownership [TCO] & Critically evaluate ERP vendors including SAP. Dr.Kesharwani is presently an Associate Professor, School of Management Studies with a total 20 years of hardcore teaching and research in Information System and its linkages with various domains of management at Indira Gandhi National Open University, New Delhi

✉ skesharwani@ignou.ac.in

Miss Shailza is a Research Scholar at SOMS (IGNOU), New Delhi. She has done her B.Com (H) from Vivekananda College and M.Com from Delhi School of Economics, University of Delhi and qualified UGC- NET JRF twice. She has been a part of various Seminars, Paper Presentations, Faculty Development Programme and National and International Conferences. She is a hardcore believer to work on her own initiative and also as a part of team. She excels in her analytical skills with a global outlook and foresightedness which is the need of hour.

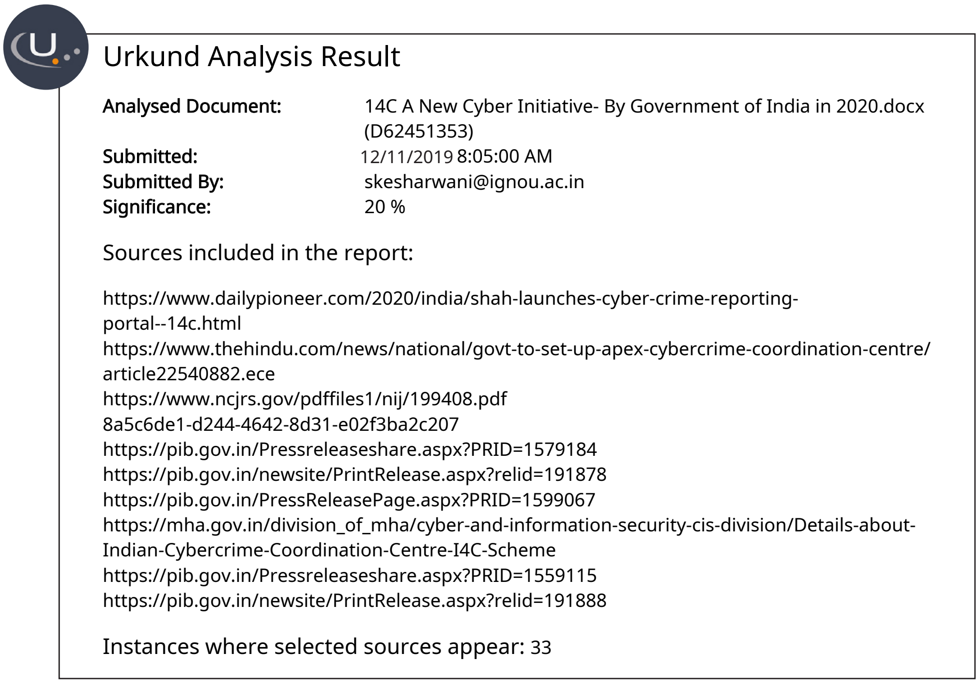
✉ shailza509@gmail.com

Miss Jyoti is currently pursuing her Doctoral Research study from SOMS (IGNOU), New Delhi. She has done her B.Com (H) and M.com from University of Delhi and qualified UGC- NET JRF. She has been a part of various Seminars, Paper Presentations, Faculty Development Programme and National and International Conferences. She is an enthusiastic learner who believes in maintaining and maximizing the quality of life by implementing her skills, and experience gained through education, hard work and dedication.

✉ jyotiningania@gmail.com

Annexure I

Submission Date	Submission Id	Word Count	Character Count
12 Nov 2019	D62451353 (urkund)	3441	22347



Urkund Analysis Result

Analysed Document:	14C A New Cyber Initiative- By Government of India in 2020.docx (D62451353)
Submitted:	12/11/2019 8:05:00 AM
Submitted By:	skesharwani@ignou.ac.in
Significance:	20 %

Sources included in the report:

https://www.dailypioneer.com/2020/india/shah-launches-cyber-crime-reporting-portal--14c.html
https://www.thehindu.com/news/national/govt-to-set-up-apex-cybercrime-coordination-centre/article22540882.ece
https://www.ncjrs.gov/pdffiles1/nij/199408.pdf
8a5c6de1-d244-4642-8d31-e02f3ba2c207
https://pib.gov.in/Pressreleaseshare.aspx?PRID=1579184
https://pib.gov.in/newsite/PrintRelease.aspx?relid=191878
https://pib.gov.in/PressReleasePage.aspx?PRID=1599067
https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
https://pib.gov.in/Pressreleaseshare.aspx?PRID=1559115
https://pib.gov.in/newsite/PrintRelease.aspx?relid=191888

Instances where selected sources appear: 33

Note: Cybernomics runs an Urkund plagiarism tool for the originality check of an article before publication. Urkund is developed by Prio Infocenter AB based in Stockholm, Sweden.

Disclaimer: All Views expressed in this paper are my own, which some of the content are taken from open source website for the knowledge purpose. Those some of i had mentioned above in references section.

Reviewers Comment

Reviewer Comment 1: Cybercrimes exist in variety of forms and they are of greater concern to be dealt with. The article is very well structured to educate readers about Indian Cyber Crime Coordination Centre (I4C) and a National Cyber Crime Reporting Portal to fight the emerging cybercrimes.

Reviewer Comment 2: With the digital transformation everyone seems to be fascinated by and engaged in cyberspace and very easily they fall prey to the cyber attackers. In such a scenario 14C in a way empowers the people the article very well familiarize the readers with it.

Reviewer Comment 3: The article focuses on the needs to take precautionary measures again the cyber-attacks that can lead to the huge financial as well as non -financial damage to the citizens of the country.

Editorial Excerpt

This article is an excerpt from the government of India portal and is used as a suggestive measure with an objective to make learners familiar about the law. All the authors (Subodh, Shailza and Jyoti) have given an undertaking in disclaimer at the end of the article. The paper has gone through some modifications with the preliminary stage remarks and minor revision as and when suggested by the editorial board and blind reviewers at the successive stages. The comments related to this manuscript are noteworthy and related to the "**14C a new cyber initiative 14C taken By Government of India in 2020 to fight the emerging cybercrimes**". The article provides an overview of Indian Cyber Crime Coordination Centre (I4C) and a National Cyber Crime Reporting Portal to fight the emerging cybercrimes. Cybercrimes exist in various forms and they are of greater concern to be dealt with. All the comments had been shared at variety of dates by the authors in calculation. By and large all the editorial board and reviewers' suggestions had been incorporated in the article and the manuscript had been earmarked and finalized to be published under "**Argument based credential**" category.

Citation

Subodh Kesharwani, Shailza and Jyoti
"14C A New Cyber Initiative- By Government of India in 2020"
Volume-1, Issue-6, Nov 2019. (www.cybernomics.in)

Frequency: Monthly, Published: 2019
Conflict of Interest: Author of a Paper had
no conflict neither financially nor academically.

Scholastic Seed Inc.
www.scholasticseed.in