Argue A Case In Favour of An Evolved National Critical Information Infrastructure Framework in The Domain of Cyber Intelligence. (250 Words / 15 M) (GS-3 Cyber Security)

Approach:

1. Introduction
2. Define the concept of Critical Information Infrastructure.
3. Discuss the existing institutional & legal infrastructure.
4. Why a broader framework is needed ?
5. Conclusion

The quest for ***National Critical Information Infrastructure Framework*** for India seems essential. When it comes to dealing with Critical Information & its associated Infrastructure, it is often looked at with the perception of National Security and intelligence, especially, the ever-growing domains of ***cyber intelligence***.

Critical Information Infrastructure deals with ***physical and cyber systems*** that are essential to a nation in their capabilities to ***govern the broader security scenario*** and any damage to it, would have a devastating effect on national security, political, economic and social welfare. With such an important role, it's the need of the hour to see into the present framework and also look into the measures that would strengthen national critical information infrastructure. CIIs include *strategic services, power and energy, financial services, emergency services etc.*

COVID – 19 has played a vital role in shifting these attacks to major information grids, the ever-evolving nature of ***complex cyber-attacks*** also is a major challenge, the new techniques of sensing & communication poses yet another challenge.

India's existing infrastructure : India's present apparatus includes the ***National Critical Information Infrastructure Protection Centre*** (NCIIPC) under NTRO, set up in 2014 for regulation & supervision of our nation's critical assets. Moreover, CIIs were also defined in ***Information Technology Act, 2000*** as vital resources to national security. All the CII organizations are therefore bound to operate under the guidelines of NCIIPC, covering various aspects of the cybersecurity life cycle and its effective implementation. ***CERT-in*** Response Team plays a nodal role in responding to cybersecurity threats on a national level and hence coordinates with NCIIPC.

National Cyber Security Coordinator (NCSC) under National Security Council Secretariat also coordinates with all agencies for the protection of critical infrastructure. ***MHA's newly formed division*** known as ***Cyber and Information Security*** (CIS) is also responsible for effective implementation, coordinating such threats at all source domain. For situational awareness, ***National Cyber Coordination Centre*** enables timely information sharing for protective measures. Recently, MHA also launched ***Cyber Volunteer Program*** for better assistance against Cybercrime under the supervision of the Indian Cyber Crime Coordination

Centre. Moreover, the present apparatus also includes ***Cyber Swachhta Kendra*** for detecting malicious software and provide effective safety measures. The present apparatus is well equipped with dealing with critical threats, yet it needs a fluent framework to have greater implementation & efficiency.

Need for a broader framework : The government's execution for this particular setup needs to include ***greater international cooperation***, training & awareness programs, certification of protection mechanisms of critical information infrastructure, building ***greater cyber workforce*** and also an ***integrated supply chain security objective*** for operational efficiency. This particular broader framework includes the supervision of NTRO (National Technical Research Organization) in all the domains of NCIIPC. ***NTRO's supervision*** ensures ***all-around technical supervision*** of such critical infrastructure.

This broader framework should include ***effective feedback*** from all agencies such as the CERT-in and CIS division of MHA, along with National Cyber Security Coordinator and National Cyber Coordination Centre. NSC Secretariat will play a crucial role as well in the policy decisions. Overall, ***India needs a broader framework*** where ***National Critical Information Infrastructure Protection Centre*** plays a ***nodal role*** with ***multi-staged coordination*** from all agencies working in this domain. NCIIPC's existence & coordination along with NCSC and CERT-in plays a vital role in the protection of nationally critical information infrastructure, thus paving the way for more effective measures to national security.

New Amendments to IT Act can also be very beneficial in governing a better framework and its effective implementation. India has an apparatus, a better fluent communication nodal implementation and a feedback framework covering all respective agencies would pave an effective step to enhanced national security.