

WRAP Exams · wrapexams.com

Prelims PYQ, Mains model answers, and copy evaluation. Write to the desk for this paper, a doubt, or the AI waitlist.

ask@wrapexams.com · +91 85951 84903 · wrapexams.com

Q20

Considering the threats cyberspace poses for the country, India needs a "Digital Armed Forces" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation.

UPSC Civil Services Mains 2015 · GS III · 12 marks · Cyber Security and Money Laundering

Challenges to internal security through communication networks, role of media and social networking sites in internal security challenges, basics of cyber security; money-laundering and its prevention.

Core demand of the question

- Critically evaluate the **National Cyber Security Policy, 2013** against India's cyberspace threats
- Outline implementation challenges and whether a Digital Armed Forces idea is needed

Revision summary

NCSP 2013 sought a secure IT environment, 24×7 response, CERT and critical-infrastructure protection, skills, and public-private sharing.

Those aims match the threat; a policy paper did not automatically fund staff, a chain of command, or modern law.

Private owners of power and finance still need mandatory standards, not only partnership language.

A Digital Armed Forces idea is valid as a trained defence and CI cadre with a fusion centre, not as militarising all cyber crime.

Implementation needs statute, a career service, supply-chain rules, and drills.

Flow diagram

Cyberspace threats -> NCSP 2013
 NCSP 2013 -> CERT-In NCIIPC skills PPP-In NCIIPC skills PPP
 Law command workforce supply chain -> NCSP 2013
 Digital cadre fusion -> Defence CI
 Digital cadre fusion -> CERT-In NCIIPC skills PPP police crime
 Defence CI -> Resilient cyberspace
 CERT police crime -> Resilient cyberspace

Conclusion

- Update the 2013 policy with **binding sectoral regulations**, breach-notification, and supply-chain rules.
- Build the missing **career cyber service** and national range for live-fire drills.

- Clarify encryption and agency lanes so firms are not complying with five contradictory letters.
- Keep citizen security and **privacy** in the same design, or a Digital Armed Force will lose the public it claims to protect.

The **National Cyber Security Policy, 2013** correctly named CERT, critical infrastructure, skills, and public-private work. It did not by itself create law, a commander, or a retained workforce, so implementation is the real gap. India needs professional digital forces for defence and critical systems, not a slogan that turns every cyber crime into a military parade. The 2013 map still holds if it is given statute, staff, and drills.

Facts & figures

National Cyber Security Policy, 2013

Union policy framework for a secure cyberspace, CERT strengthening, critical infrastructure, R&D, and human resources.

CERT-In

Indian Computer Emergency Response Team, the national civilian agency for cyber incidents under the IT Act framework.

NCIIPC

National Critical Information Infrastructure Protection Centre, focused on strategic and essential sectors' cyber protection.

IT Act, 2000

Principal Indian law on electronic crime and intermediary rules; often criticised as incomplete for state-level cyber conflict.

Critical information infrastructure

Systems in energy, finance, transport, government, and communications whose failure would hit national security or public life.

WRAP Exams · Write. Read. Analyse. Practice. · <https://wrapexams.com/upsc/mains-answers/gs-3/2015/considering-the-threats-cyberspace-poses-for-the-country-india-needs-a-digital-armed-forces-to-prevent-crimes-critically-evaluate-the-national-cyber-security-policy-2013-outlining-the-challenges-perceived-in-its/> · ask@wrapexams.com · wrapexams.com