Joint Doctrines - Defence

Recently, the Chief of Defence Staff (CDS) General Anil Chauhan formally released the declassified versions of the Joint Doctrines for Cyberspace Operations and Amphibious Operations during the Chiefs of Staff Committee meeting in New Delhi. These doctrines aim to standardise tri-service operations, improve interoperability, and enhance India's readiness for multi-domain threats.

Joint Doctrine for Cyberspace Operations

The primary objective is to create a unified and coordinated approach to protect and advance India's national interests in cyberspace. It integrates both offensive (cyberattacks, disruption of adversary networks) and defensive (network protection, malware removal) cyber capabilities into a cohesive operational framework. It enables synchronised cyber operations across the Army, Navy, and Air Force, ensuring that cyber defence and attack plans are harmonised with broader military objectives. Emphasis is placed on threat-informed planning—operations are designed based on real-time intelligence about adversary cyber capabilities and intent.

The doctrine seeks to integrate real-time cyber threat intelligence into the decision-making process for faster, more effective responses.

It promotes the development of joint cyber capabilities, including unified infrastructure, tools, and skillsets for tri-service cyber missions.

Joint Doctrine for Amphibious Operations

The doctrine provides a framework for integrated maritime, air, and land force operations in littoral (coastal) and island environments. It focuses on building interoperability between naval, air, and ground forces so they can operate seamlessly in coastal missions. It establishes procedures for rapid deployment of amphibious task forces, enabling swift response to emergencies, humanitarian crises, or hostile actions in coastal or island regions. It highlights the use of joint force projection from sea to shore to influence or dominate operations on land.

Cyberspace Operations

Cyberspace is the interconnected network of IT systems, communication systems, and embedded devices, forming a largely non-physical domain. It is a critical operational environment where both military and civilian activities take place to ensure freedom of action for one's side and deny the same to adversaries.

Characteristics of Cyberspace

1.Cross-Domain Impact

Cyber effects can have direct consequences in the physical world (e.g., power grid shutdowns) and in the cognitive sphere (e.g., misinformation).

2.Civil-Military Overlap

The interconnected nature of civilian and military networks means that attacks often impact both sectors simultaneously.

3. Kinetic Potential

Cyberattacks can cause physical damage to equipment, infrastructure, or critical systems.

4. Attribution Difficulty

Tracing the real source of an attack is challenging, complicating retaliation or legal action.

5.Neutrality Issues

Attackers often route operations through infrastructure in neutral countries to avoid direct attribution.

6. Asymmetry

Even relatively weaker actors can cause disproportionate damage through cyber means.

Measures Taken for Strengthening India's Cyberspace Capabilities

1. National Cyber Security Policy

Establishes national objectives for protecting cyberspace, improving prevention, response, and coordination across agencies.

2. Digital Personal Data Protection Act, 2023

Regulates how personal data is used, mandates explicit consent, enforces security measures, and sets up a Data Protection Board.

3. National Cyber Coordination Centre (NCCC)

Acts as a central control hub to scan national cyberspace and detect threats in real time.

4. Indian Cyber Crime Coordination Centre (I4C)

Provides a nationwide platform for law enforcement to address cybercrime, including analytics, training, and forensics.

5. National Critical Information Infrastructure Protection Centre (NCIIPC)

Protects essential sectors like power, telecom, and banking from cyberattacks.

6. Cyber Swachhta Kendra

Detects and cleans botnet infections, helping individuals and organisations secure their devices.

7. Defence Cyber Agency (DCyA)

Conducts tri-service cyber operations, including hacking, surveillance, and counter-cyber measures.

8. Cyber Diplomacy Division (MEA)

Handles India's international negotiations and collaborations on cyberspace issues.

Amphibious Operations

Amphibious operations involve naval forces transporting and supporting land forces ashore, often with air support, to achieve military objectives on land. They require extensive planning and joint integration of the three Services for success. Such operations offer strategic flexibility, allowing forces to open new fronts or bypass heavily defended areas.

Characteristics of Amphibious Operations

1. Complex Coordination – Demands a unified chain of command to integrate naval, air, and land components.
2. Scalable – Can range from small tactical raids to large-scale strategic invasions.
3. Specialised Assets – Requires landing ships, amphibious vehicles, and interoperable support systems.
4. Multinational Scope – May involve allies or coalition partners due to evolving geopolitical needs.
5. Maritime-Land Linkage – Acts as a bridge between sea-based strike capability and ground objectives.

Need for Joint Doctrines for Cyberspace & Amphibious Operations

1. Unified Command & Coordination – Ensures that all three Services operate under a common operational framework for multi-domain missions.
2. Cyber Threat Readiness – India faces persistent threats such as Chinese group APT10 targeting vaccine firms (2021) and cyber incidents like the 2020 Mumbai power outage.
3. Standardisation of Procedures – Establishes uniform tactics and interoperability protocols across Services.
4. Capability Development – Guides resource allocation, training, and procurement for long-term readiness.
5. Deterrence & Rapid Response – Enhances India's ability to respond swiftly to physical and cyber threats.
6. International Cooperation – Creates a basis for joint exercises and intelligence sharing with partner nations.

Challenges in Indian Military Coordination

1. Operational Jointness – Service HQs remain separate, limiting unified operational control; CDS has limited direct authority.
2. Organisational Jointness – Bureaucratic silos and overlapping responsibilities reduce efficiency.
3. Professional Military Education – Joint training institutions are limited; most training remains service-specific.
4. Doctrinal Gaps – Existing joint doctrines lack consistency and are often biased towards individual Services.
5. Cybersecurity Limitations – Defence Cyber Agency not yet upgraded to a full Cyber Command.
6. Resistance to Reform – Institutional reluctance to transition to integrated theatre commands.
7. Amphibious Capability Gaps – Shortage of ships and landing craft for large-scale missions.
8. Shortage of Specialised Personnel – Few trained experts in cyber warfare and amphibious operations.
9. Foreign Technology Dependence – Reliance on imports creates vulnerabilities in equipment supply and maintenance.
10. Operational Integration Issues – Real-time synchronisation of land, air, sea, and cyber elements remains challenging.

Initiatives for Jointness & Integration

1. Tri-Service Exercises – Such as AMPHEX for amphibious training and combined cyber drills.
2. Common Logistics – Shared depots, maintenance, and fuel facilities for cost efficiency.
3. Digital Integration – Unified battlefield communication systems like Defence Communication Network (DCN)
4. Standardised Equipment – Joint procurement for interoperability.
5. Integrated Commands – Examples include Andaman & Nicobar Command.
6. Joint Training Institutions – Modelled on NDA for higher-level joint war colleges.
7. Combined Planning Units – Led by DMA for unified operational planning.

8. Shared Human Resources – Cross-service deployment of medical, logistics, and cyber units.

Major Government-Led Efforts

1. Chief of Defence Staff (CDS) – Central authority to enhance jointness and resource optimisation.
2. Integrated Theatre Commands (ITCs) – Geographical/function-based commands for multi-domain efficiency.
3. Department of Military Affairs (DMA) – Integrates procurement, staffing, and restructuring for joint operations.
4. Inter-Services Organisations Act, 2023 – Gives tri-service commanders authority over mixed personnel.
5. Joint Logistics Nodes (JLNs) – Provide integrated logistics in key locations.
6. Joint Training & Exercises – Includes tri-service war games and advanced training courses.
7. Technology Integration – Secure communication and real-time control systems like IACCS.
8. Year of Defence Reforms – 2025 – MoD initiative to modernise and integrate Armed Forces for multi-domain readiness.

Way Forward

1. Build Integrated Capabilities – Establish a dedicated cyber command; expand amphibious lift assets and unmanned capabilities.
2. Enhance Interoperability – Standardise communication, tactics, and equipment across all Services.
3. Boost Indigenous R&D – Increase defence R&D spending to 2% of GDP; encourage private and start-up innovation.
4. Strengthen Human Capital – Develop specialised cadres for cyber and amphibious warfare with advanced training.
5. Upgrade Strategic Infrastructure – Improve DCN resilience; develop forward bases in critical coastal and island zones.
6. Deepen Global Partnerships – Expand joint exercises and intelligence-sharing with friendly nations.

Conclusion

The release of these joint doctrines is a transformative step in India's defence preparedness, ensuring a unified approach to emerging threats. By focusing on integration, capability development, and partnerships, India can effectively counter both conventional and unconventional challenges in the coming decades.

Source: https://timesofindia.indiatimes.com/india/forces-release-joint-doctrines-for-cyberspace-amphibious-operations/articleshow/123176697.cms