PrepAlpine

The Next-Generation UPSC Institution

Where Research Meets Mentorship & Precision

Preparation Meets Precision

A Next-Generation Learning Institution

Disclaimer

The information contained in this book has been prepared solely for educational purposes. While every effort has been made to ensure accuracy, PrepAlpine makes no representations or warranties of any kind and accepts no liability for any errors or omissions. The use of any content is solely at the reader's discretion and risk.

DAILY CURRENT AFFAIRS DATED 27.05.2026

GS Paper II: International Relations

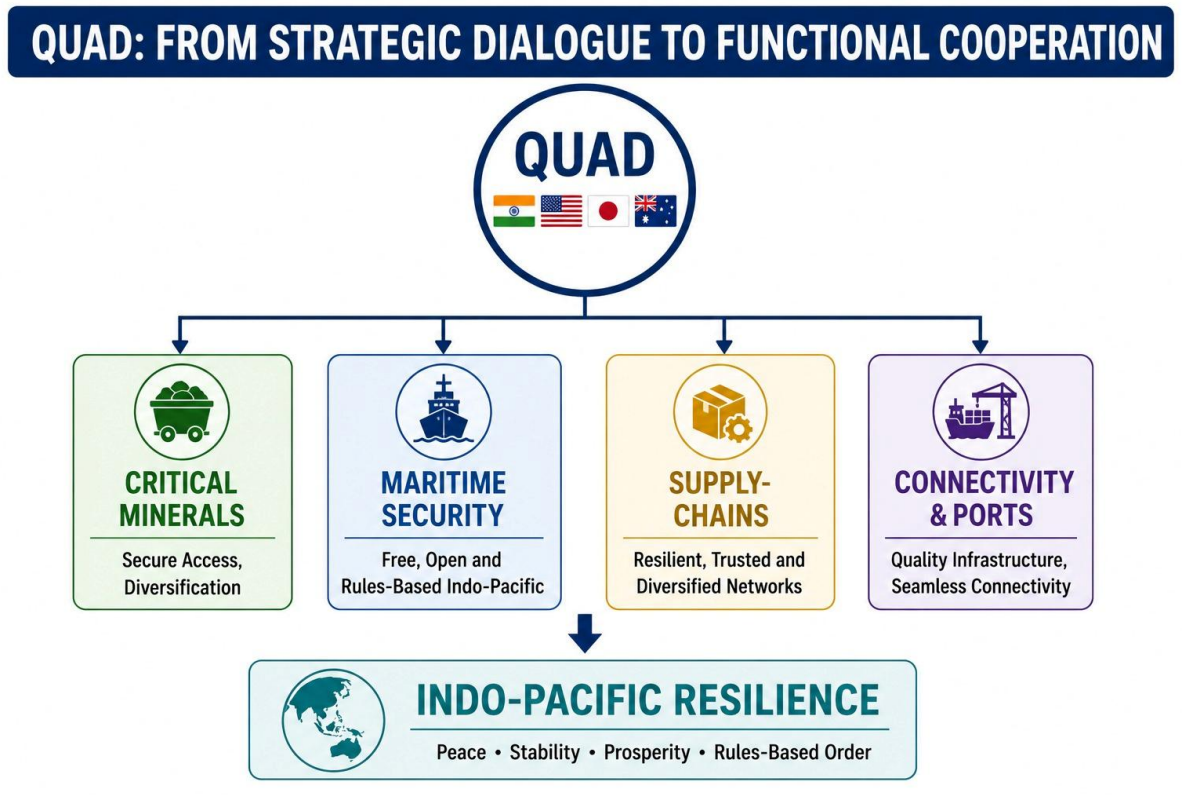
1. Quad Initiatives on Critical Minerals, Maritime Security and Indo-Pacific Connectivity

a. Introduction

The Quad countries, India, the United States, Japan and Australia, have announced new initiatives on energy security, critical minerals, maritime surveillance, maritime domain awareness and port infrastructure in Fiji. Alongside this, India and the United States have signed a bilateral framework on critical minerals to secure mining, processing and supply chains of critical minerals and rare earth elements.

This development is significant because the Quad is gradually moving beyond broad strategic statements towards practical cooperation in areas where Indo-Pacific countries face real vulnerabilities. Critical minerals, maritime security and resilient connectivity are now central to economic security, defence preparedness and technological sovereignty. For India, these initiatives are closely linked with clean energy transition, defence modernisation, supply-chain diversification and its larger Indo-Pacific strategy.

Thus, the Quad's recent initiatives should be understood as part of a wider shift from diplomatic signalling to functional cooperation in the Indo-Pacific.



b. Key Features of the Quad Initiatives

- **Indo-Pacific Maritime Surveillance:** The Quad has agreed to launch an Indo-Pacific Maritime Surveillance Corporation to strengthen maritime surveillance and expand Maritime Domain Awareness in the Indo-Pacific region. Maritime Domain Awareness means the ability to understand and monitor activities at sea, including shipping movement, illegal fishing, suspicious vessels, grey-zone activity and threats to sea lanes.
- **Port Infrastructure in Fiji:** The Quad will also support port infrastructure in Fiji, indicating a growing focus on Pacific Island countries. This is important because Pacific Island states

occupy strategically located maritime spaces and are increasingly becoming sites of geopolitical competition.

- **India–United States Critical Minerals Framework:** Separately, India and the United States have signed a framework on critical minerals and rare earths. This framework covers mining, processing, recycling, investment, financing and diversified supply chains. The aim is to reduce vulnerability to single-source monopolies, especially China's dominance in rare earth processing and critical mineral supply chains.

Taken together, these initiatives show that the Quad is trying to address the economic, technological and maritime vulnerabilities of the Indo-Pacific in a practical manner.

c. Strategic Significance of Critical Minerals

- **Meaning and Importance:** Critical minerals are minerals that are essential for modern industry, clean energy, defence and advanced technology, but whose supply chains are vulnerable to disruption. Rare earth elements are especially important for permanent magnets, electric vehicles, wind turbines, missiles, aircraft, electronics and advanced defence systems.
- **Link with Twenty-First Century Economy:** The strategic significance of these minerals has increased because the twenty-first century economy depends heavily on clean technologies and digital systems. Electric vehicles require batteries and magnets. Semiconductors require specialised materials. Defence systems require advanced alloys, sensors and electronic components. Renewable energy systems require mineral-intensive supply chains.
- **China's Dominance and Supply-Chain Risk:** China's dominance in the processing of rare earths and some critical minerals has made this a major geopolitical concern. Even countries that have mineral deposits may remain dependent on China if they lack refining and processing capacity. Therefore, the real challenge is not only mining minerals, but building complete supply chains from extraction to processing, recycling and final manufacturing.
- **Relevance for India:** For India, securing critical minerals is essential for electric mobility, semiconductor ambitions, battery manufacturing, renewable energy expansion and defence indigenisation.

This makes critical minerals a strategic economic issue rather than a narrow mining or trade concern.

d. Importance for India's Strategic Economy

- **Link with Domestic Industrial Goals:** India's economic and strategic ambitions increasingly depend on secure access to critical minerals. The country is trying to expand domestic manufacturing in electric vehicles, electronics, solar energy, batteries, defence systems and semiconductors. All these sectors require reliable mineral inputs.
- **Complementarity Within the Quad:** A trusted supply-chain network with the United States, Japan and Australia can reduce India's dependence on China-dominated mineral networks. Australia has mineral resources, Japan has technological and industrial capabilities, the United States has financing, strategic reserves and advanced research capacity, while India offers a large market and growing manufacturing base.
- **Support for Resilient Manufacturing:** Such cooperation can support India's goal of becoming a resilient manufacturing hub. It can also strengthen India's position in global value chains by reducing the risk of supply disruptions, export controls and geopolitical pressure.

Thus, critical mineral cooperation directly supports India's larger objectives of Atmanirbhar Bharat, supply-chain diversification and strategic autonomy.

e. Maritime Dimension of the Quad

- **Importance of the Indo-Pacific:** The maritime initiatives are equally important. The Indo-Pacific is central to global trade, energy flows and strategic competition. Major sea lanes pass

through this region, carrying energy supplies, manufactured goods and raw materials. Any disruption in maritime routes can affect global and Indian economic security.

- **Maritime Domain Awareness:** Expanded Maritime Domain Awareness can help track illegal fishing, piracy, smuggling, unregulated shipping, grey-zone activities and coercive maritime behaviour. Grey-zone activities refer to actions that are aggressive or coercive but remain below the threshold of open war, such as maritime militia activity, intimidation of smaller states and disputed presence near sensitive waters.
- **Significance for India:** For India, maritime surveillance cooperation strengthens its role as a net security provider in the Indian Ocean and supports a wider Indo-Pacific presence. It also improves coordination with like-minded partners in identifying threats to sea lanes, maritime resources and regional stability.

Therefore, the maritime component of the Quad strengthens both regional security and India's own maritime strategic posture.

f. Focus on Fiji and the Pacific Islands

- **Strategic Importance of Pacific Island States:** The Quad's decision to support port infrastructure in Fiji reflects its growing interest in the Pacific Islands. These island states may be small in population, but they occupy vast maritime zones and are strategically located across important sea routes.
- **China Factor and Alternative Connectivity:** China has been expanding its presence in the Pacific through infrastructure financing, security agreements and diplomatic engagement. In response, the Quad is trying to provide alternatives that are transparent, climate-resilient and respectful of local sovereignty.
- **Developmental Relevance:** Port infrastructure in Pacific Island countries can improve trade, disaster response, connectivity and maritime safety. However, such projects must be designed carefully. Pacific Island states are highly vulnerable to climate change, sea-level rise and extreme weather. Therefore, infrastructure cooperation must be climate-resilient and development-oriented, not merely strategic.

This focus on Fiji shows that Indo-Pacific strategy must address the developmental priorities of smaller island states if it is to gain wider legitimacy.

g. Quad as a Provider of Public Goods

- **Public Goods Approach:** The new initiatives show that the Quad is trying to project itself not merely as a security grouping, but as a provider of public goods in the Indo-Pacific. Public goods in this context include maritime safety, resilient supply chains, transparent infrastructure, disaster response, climate adaptation and technology cooperation.
- **Relevance for Smaller States:** This is important because many countries in Southeast Asia and the Pacific do not want to be forced into a binary choice between China and the Quad. They prefer practical cooperation that supports their own development priorities.
- **Legitimacy Through Delivery:** Therefore, the Quad's success will depend on whether it can deliver useful outcomes rather than only strategic messaging. If it helps smaller countries improve ports, monitor maritime zones, respond to disasters and access resilient technology, it will gain greater legitimacy.

Thus, the Quad's future relevance will depend on its ability to provide inclusive and development-oriented solutions, not merely balance China militarily.

h. Challenges in Implementation

- **Long Gestation in Critical Minerals:** Despite its promise, the Quad's agenda faces several challenges. Critical mineral supply chains require long-term investment. Mining projects take years to develop and face environmental, regulatory and community-related concerns.

Processing capacity is even more difficult because it requires technology, environmental safeguards and large capital investment.

- **Need for Private Sector Participation:** Private sector participation is essential, but companies will invest only if there is policy certainty, financing support and assured demand. Without risk guarantees and technology partnerships, critical mineral cooperation may remain limited to diplomatic announcements.
- **Trust and Data-Sharing in Maritime Cooperation:** Maritime cooperation also requires data-sharing, interoperability and trust. Different countries have different legal frameworks, technological systems and strategic sensitivities. Sharing maritime information with smaller countries must be done in a way that respects sovereignty and avoids the impression of surveillance dominance.
- **Perception Challenge:** Another challenge is perception. If the Quad is seen only as an anti-China platform, some Indo-Pacific countries may hesitate to engage deeply with it. Therefore, the grouping must present itself as inclusive, development-oriented and supportive of regional stability.

These challenges show that the Quad's functional agenda will require sustained financing, patient diplomacy and credible implementation mechanisms.

i. Way Forward

- **Build End-to-End Critical Mineral Supply Chains:** The Quad should build end-to-end critical mineral supply chains covering exploration, extraction, refining, processing, recycling, stockpiling and final manufacturing. The focus should not remain limited to mineral access; it must include value addition and industrial capability.
- **Encourage Private Sector Participation:** Private sector participation must be encouraged through financing, risk guarantees, technology partnerships and long-term purchase agreements. This will make critical mineral projects commercially viable.
- **Align with India's Domestic Industrial Strategy:** India should align critical minerals cooperation with its policies on electric vehicles, semiconductors, batteries, renewable energy and defence manufacturing. This will ensure that external partnerships directly support domestic industrial strategy.
- **Expand Maritime Domain Awareness to Smaller States:** Quad maritime domain awareness should be expanded to include smaller Indo-Pacific states. Such cooperation must help them monitor illegal fishing, protect maritime resources, respond to disasters and strengthen maritime governance.
- **Ensure Climate-Resilient Port Infrastructure:** Port infrastructure in Fiji and other Pacific Island countries should be transparent, climate-resilient and financially sustainable. It should avoid debt stress and respect local priorities.
- **Maintain an Inclusive Approach:** The Quad must also maintain an inclusive approach. Its initiatives should be framed around development, resilience and regional public goods rather than narrow military competition. This will make cooperation more acceptable to Southeast Asian and Pacific countries.

A successful Quad strategy must therefore combine strategic purpose with developmental credibility and practical delivery.

Conclusion

The Quad's focus on critical minerals, maritime surveillance and Pacific connectivity marks a shift from strategic dialogue to functional cooperation. These initiatives show that economic security, technological resilience and maritime stability are now central to the Indo-Pacific order.

For India, the initiatives strengthen supply-chain resilience, support defence and clean-energy ambitions, improve maritime security and expand Indo-Pacific outreach. However, their success will depend on sustained financing, technology partnerships, private sector participation and the ability to offer credible alternatives to China-dominated networks.

The Quad's future relevance will be determined not only by its strategic intent, but by its capacity to deliver practical, inclusive and development-oriented outcomes in the Indo-Pacific.

GS Paper III: Security

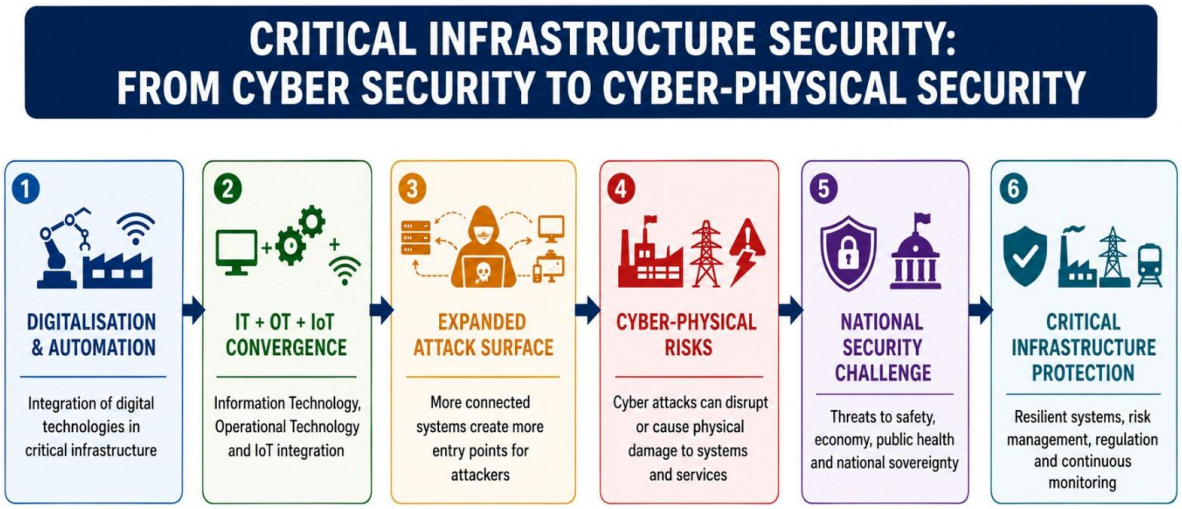
2. Security of India's Critical National Infrastructure

a. Introduction

India's critical national infrastructure is becoming increasingly digital, automated and interconnected. Sectors such as energy, transport, water supply, banking, communications, healthcare and defence now depend on sensors, automation systems, artificial intelligence, GPS-based monitoring, Internet-connected devices and remotely managed control systems.

This technological transformation has improved efficiency, transparency, predictive maintenance and real-time monitoring. However, it has also created new security risks. The protection of critical infrastructure can no longer be limited to traditional cyber security measures such as firewalls, antivirus systems and data protection. It must now include the security of physical control systems, sensors, connected devices, software supply chains and industrial networks.

The issue is therefore central to India's internal security, economic security and national resilience.



b. Understanding the Key Concepts

- **Information Technology:** Information Technology refers to systems that handle data, servers, software, digital communication and enterprise networks. These are the conventional targets of cyberattacks, where attackers may steal information, disrupt websites, encrypt data or compromise communication systems.
- **Operational Technology:** Operational Technology refers to systems that monitor and control physical processes. These include refineries, power plants, transport networks, water systems, industrial machinery and manufacturing lines. Unlike ordinary information systems, operational technology directly affects physical infrastructure.
- **Internet of Things:** Internet of Things refers to Internet-connected devices such as cameras, sensors, GPS trackers, controllers, smart locks, surveillance devices and industrial monitoring tools. These devices connect the physical world with digital networks.
- **SCADA Systems:** Supervisory Control and Data Acquisition systems, commonly called SCADA systems, are used to monitor and control industrial processes. They are widely used in power grids, oil and gas facilities, water systems, transport operations and other critical sectors.
- **Convergence as the Core Challenge:** The real security challenge arises because these systems are increasingly connected with each other. This convergence of information technology, operational technology and Internet-connected devices has expanded the attack surface of critical infrastructure.

c. Why Critical Infrastructure Is Becoming More Vulnerable

- **Shift from Isolated Systems to Connected Networks:** Earlier, many industrial and infrastructure systems were isolated and locally controlled. A refinery, power plant or water treatment system could function through closed internal networks with limited exposure to the Internet. Today, however, centralised monitoring, remote maintenance, predictive analytics and real-time dashboards have become common.
- **New Pathways for Intrusion:** This improves efficiency, but it also creates pathways for remote intrusion. If a connected device, sensor, controller or software platform is compromised, an attacker may gain access to systems that were earlier physically isolated.
- **Cyber-Physical Consequences:** The risk is especially serious because attacks on operational technology do not merely affect data. They can disrupt physical processes. A compromised server may lead to data loss, but a compromised industrial controller can affect electricity supply, fuel movement, transport safety or water distribution.

Thus, critical infrastructure protection has moved from the domain of cyber security alone to the wider field of cyber-physical security.

d. IT, OT and IoT Convergence as a Security Challenge

- **Layered Vulnerability:** The convergence of information technology, operational technology and Internet-connected devices creates a layered vulnerability. A conventional cyberattack may target a software system or database. However, if that system is connected to operational networks, the attack may move deeper into physical infrastructure.
- **Examples of Cyber-Physical Risks:** For example, a weak GPS tracking device used in fuel transportation may provide incorrect location data. A compromised electronic lock may be remotely opened or disabled. A manipulated sensor in a power plant may send false readings. A vulnerable camera or industrial router may act as an entry point into a larger network.
- **Hidden and Persistent Risk:** Such risks are especially dangerous because they may not be immediately visible. A system may appear to function normally while hidden vulnerabilities remain embedded in devices, firmware or remote-access pathways.
- **Need for Advanced Security Architecture:** This makes critical infrastructure security more complex than ordinary cyber security. It requires device-level assurance, network segmentation, continuous monitoring, supply-chain verification and sector-specific technical expertise.

The convergence of these systems therefore demands a shift from perimeter-based protection to layered, continuous and risk-based protection.

e. Supply-Chain Security and Imported Devices

- **Risk from Global Supply Chains:** A major concern relates to supply-chain security. Many sensors, cameras, GPS trackers, controllers, communication modules and smart devices used in critical sectors are imported or assembled through global supply chains. If these devices are deployed without rigorous security testing, they may contain hidden vulnerabilities, unauthorised data-sharing mechanisms or remote-control pathways.
- **Strategic Trust Deficit:** This concern becomes more serious when devices are sourced from countries with strategic tensions or weak trust frameworks. A device may be inexpensive and technically functional, but it may create long-term security risks if its hardware, firmware, software updates or cloud communication channels are not verified.
- **Atmanirbhar Bharat as Security Requirement:** Therefore, Atmanirbhar Bharat in critical technology sectors is not only an economic objective. It is also a national security requirement. Indigenous capability in trusted devices, secure firmware, certified hardware, encryption systems and industrial cyber security can reduce strategic dependence and improve resilience.
- **Need to Verify Domestic Claims:** However, self-reliance should not be reduced to mere assembly in India. Claims of domestic manufacturing must be verified through design origin,

manufacturing origin, component security and software control. A product assembled domestically but dependent on unverified foreign firmware may still create vulnerability.

This shows that trusted technology requires not only domestic production, but also end-to-end control over design, software, firmware and supply-chain integrity.

f. Procurement Weaknesses

- **Limits of Paper-Based Compliance:** Another major problem lies in procurement practices. Public agencies and infrastructure operators often rely on template-based compliance. Vendors may be asked to submit general certificates, declarations or standard cyber-security clauses. However, such paperwork may not involve deep technical evaluation.
- **Need for Technical Evaluation:** Critical infrastructure procurement requires much stricter standards. Devices must be tested for hidden communication pathways, firmware vulnerabilities, weak encryption, insecure update mechanisms, default passwords, remote access risks and data leakage.
- **Risk of Lowest-Cost Procurement:** The lowest-cost procurement model can become risky when applied to sensitive infrastructure. A cheaper device may create hidden security costs if it exposes an entire fuel network, power system or transport chain to cyber-physical disruption.

Therefore, security must become a core procurement criterion, not an afterthought.

g. Fuel Transportation as an Example

- **Benefits of Connected Devices:** The use of Internet-connected devices in fuel transportation shows both the benefits and risks of technology. GPS tracking and electronic locking systems can reduce pilferage, improve route monitoring, prevent unauthorised access and increase accountability in fuel supply chains.
- **Risks of Compromise:** However, if these devices are poorly certified or remotely compromised, the same systems can become a vulnerability. False location data may hide diversion. Electronic locks may be manipulated. Central monitoring systems may be disrupted. In a sector as sensitive as fuel supply, such vulnerabilities can affect economic activity, public services and national security.
- **Wider Lesson:** This example shows a broader principle. Technology improves governance only when the technology itself is secure. Otherwise, digitisation may convert an old physical problem into a new cyber-physical risk.

Thus, the security of connected devices is not a technical detail, but a precondition for safe digital governance in critical sectors.

h. Limitations of Existing Frameworks

- **Progress in Cyber Security:** India has taken several steps in cyber security through CERT-In, cyber incident reporting rules, sectoral guidelines and device certification mechanisms. These are important developments.
- **IT-Centric Nature of Existing Frameworks:** However, existing frameworks remain more focused on information technology systems than on the full range of operational technology and Internet-connected infrastructure. Certification mechanisms exist for some devices, but coverage remains limited, slow and uneven across sectors.
- **Need for OT and IoT-Specific Standards:** Many sectors still lack clear standards for industrial cyber security, device-level testing, secure procurement and incident response in operational environments.
- **Higher Stakes in Critical Infrastructure:** Critical infrastructure requires a higher level of assurance because even a small compromise can affect public safety, economic stability and national security. A cyber incident in an ordinary office network may disrupt services, but a

cyber incident in a power grid, refinery, transport network or hospital system may directly endanger lives.

These limitations show the need for a specialised critical infrastructure security framework rather than relying only on general cyber security norms.

i. National Security Implications

- **Critical Infrastructure as National Backbone:** Critical infrastructure is the backbone of national functioning. Power supply, fuel movement, water systems, telecommunications, banking, transport, healthcare and defence logistics support both civilian life and state capacity.
- **Grey-Zone Threats:** If adversaries can disrupt these systems during a crisis, they can weaken national response without launching a conventional military attack. This is especially relevant in the age of grey-zone conflict, where hostile actors use cyberattacks, disinformation, economic coercion, infrastructure disruption and deniable operations to weaken a country below the threshold of open war.
- **Beyond Technical Responsibility:** Therefore, critical infrastructure protection must be treated as part of national security planning. It is not merely a technical responsibility of information technology departments.

This wider national security perspective is essential because future conflicts may target networks, systems and infrastructure before conventional military escalation begins.

j. Way Forward

- **Develop a Critical Infrastructure IoT Security Framework:** India should develop a dedicated Critical Infrastructure Internet of Things Security Framework covering devices, networks, software, cloud services, firmware, procurement and supply chains. This framework must be sector-specific because the risks faced by power systems, transport networks, fuel supply chains, hospitals and telecom infrastructure are not identical.
- **Mandate Rigorous Certification and Testing:** Rigorous certification and security testing should be mandatory for operational technology and Internet-connected devices used in sensitive sectors. Testing should include hardware security, firmware analysis, software vulnerabilities, data flows, remote access pathways and update mechanisms.
- **Promote Trusted Indigenous Technologies:** Procurement policies should give preference to trusted and verified indigenous technologies in critical infrastructure. However, such preference must be linked with genuine security assurance, not only domestic branding.
- **Strengthen Inter-Agency Coordination:** Coordination must be strengthened among CERT-In, sectoral regulators, public sector undertakings, defence agencies, intelligence institutions and private infrastructure operators. Many critical assets are operated by a mix of public and private entities, so isolated security planning will not be sufficient.
- **Conduct Regular Audits and Red-Team Testing:** Regular vulnerability audits, red-team testing and incident-response drills should be conducted. Red-team testing refers to simulated attacks carried out by authorised experts to identify weaknesses before real adversaries exploit them.
- **Verify Make in India Claims:** Make in India claims should be verified through design-origin, manufacturing-origin and security-origin checks. This will ensure that critical systems are not dependent on unverified foreign hardware, firmware or software control.
- **Create Sector-Specific Standards:** Sector-specific standards should be created for energy, transport, telecommunications, healthcare, water supply, banking and fuel supply chains. Each sector should have clear norms for device certification, network segmentation, incident reporting, recovery planning and continuity of operations.
- **Build Skilled Manpower:** India must also build skilled manpower for operational technology security, industrial cyber security and Internet of Things risk assessment. Traditional information technology security skills are not enough for protecting power plants, refineries, transport systems and industrial networks.

A strong way forward must therefore combine trusted technology, strict procurement, technical testing, skilled manpower and coordinated national security planning.

Conclusion

India's critical infrastructure is becoming more connected, automated and efficient, but also more vulnerable to invisible digital threats. The security challenge now extends beyond computers and data. It includes sensors, controllers, GPS devices, electronic locks, industrial systems, supply chains and remotely connected operational networks.

A secure critical infrastructure ecosystem requires trusted technology, rigorous certification, indigenous capability, skilled manpower and coordinated governance. Protecting such infrastructure is essential for national resilience, economic security, public safety and internal security.

As India deepens digitisation and automation, the guiding principle should be clear: efficiency must not come at the cost of strategic vulnerability.

Reader's Note — About This Current Affairs Compilation

Dear Aspirant,

This document is part of the PrepAlpine Current Affairs Series — designed to bring clarity, structure, and precision to your daily UPSC learning.

While every effort has been made to balance depth with brevity, please keep the following in mind:

1. Orientation & Purpose

This compilation is curated primarily from the UPSC Mains perspective — with emphasis on conceptual clarity, analytical depth, and interlinkages across GS papers.

However, the PrepAlpine team is simultaneously developing a dedicated Prelims-focused Current Affairs Series, designed for:

- factual coverage
- data recall
- Prelims-style MCQs
- objective pattern analysis

This Prelims Edition will be released separately as a standalone publication.

2. Content Length

Some sections may feel shorter or longer depending on topic relevance and news density.
To fit your personal preference, you may freely resize or summarize sections using any LLM tool (ChatGPT, Gemini, Claude, etc.) at your convenience.

3. Format Flexibility

The formatting combines:

- paragraphs
- lists
- tables
- visual cues

—all optimised for retention.

If you prefer a specific style (lists → paras, paras → tables, etc.), feel free to convert using any free LLM.

4. Monthly Current Affairs Release

The complete Monthly Current Affairs Module will be released soon, optimized to a compact 100–150 pages — comprehensive yet concise, exam-ready, and revision-efficient.