



**BAJIRAO IAS ACADEMY**

# THE HINDU ANALYSIS

**21th JANUARY 2026**



**DIGITAL FRAUD & CYBER  
ARREST**

**The importance of Pax Silica for India**

**Kill switch, insurance as tools to fight digital arrest**

**Trump slams U.K.'s move to Hand over Chagos island**

# The importance of Pax Silica for India

## The importance of Pax Silica for India

The Pax Silica initiative seeks to reduce coercive dependencies, secure global tech AI supply chains, and build trusted digital infrastructures. India seeks to build a strong, digital infrastructure, and a secure, secure supply chain.

**THE GIST**

On December 18, 2023, the United States (U.S.) announced the launch of the Pax Silica initiative to secure the supply chain of critical minerals and technologies, and to build trusted digital infrastructures. India seeks to build a strong, digital infrastructure, and a secure, secure supply chain.

**THE GIST**

On December 18, 2023, the United States (U.S.) announced the launch of the Pax Silica initiative to secure the supply chain of critical minerals and technologies, and to build trusted digital infrastructures. India seeks to build a strong, digital infrastructure, and a secure, secure supply chain.



**THE GIST**

On December 18, 2023, the United States (U.S.) announced the launch of the Pax Silica initiative to secure the supply chain of critical minerals and technologies, and to build trusted digital infrastructures. India seeks to build a strong, digital infrastructure, and a secure, secure supply chain.

**THE GIST**

On December 18, 2023, the United States (U.S.) announced the launch of the Pax Silica initiative to secure the supply chain of critical minerals and technologies, and to build trusted digital infrastructures. India seeks to build a strong, digital infrastructure, and a secure, secure supply chain.

## Overview

### What is Pax Silica?

Pax Silica is a US-led strategic initiative to build a secure, prosperous, and innovation-driven silicon supply chain

### Participating countries

Japan, Republic of Korea, Singapore, the Netherlands, the UK, Israel, the UAE, and Australia

**Aim:** The initiative responds to the growing demand to deepen economic and technological cooperation with the US





## Understanding Pax Silica

- Pax Silica is a multilateral initiative launched by the United States in December 2025 to secure supply chains of critical technologies such as semiconductors, artificial intelligence (AI), and rare earth elements (REEs).
- The term “Pax” denotes peace, while “Silica” refers to silicon-based semiconductor technologies, symbolising a stable and cooperative global technology order.

### The Pax Silica Declaration emphasises three core objectives:

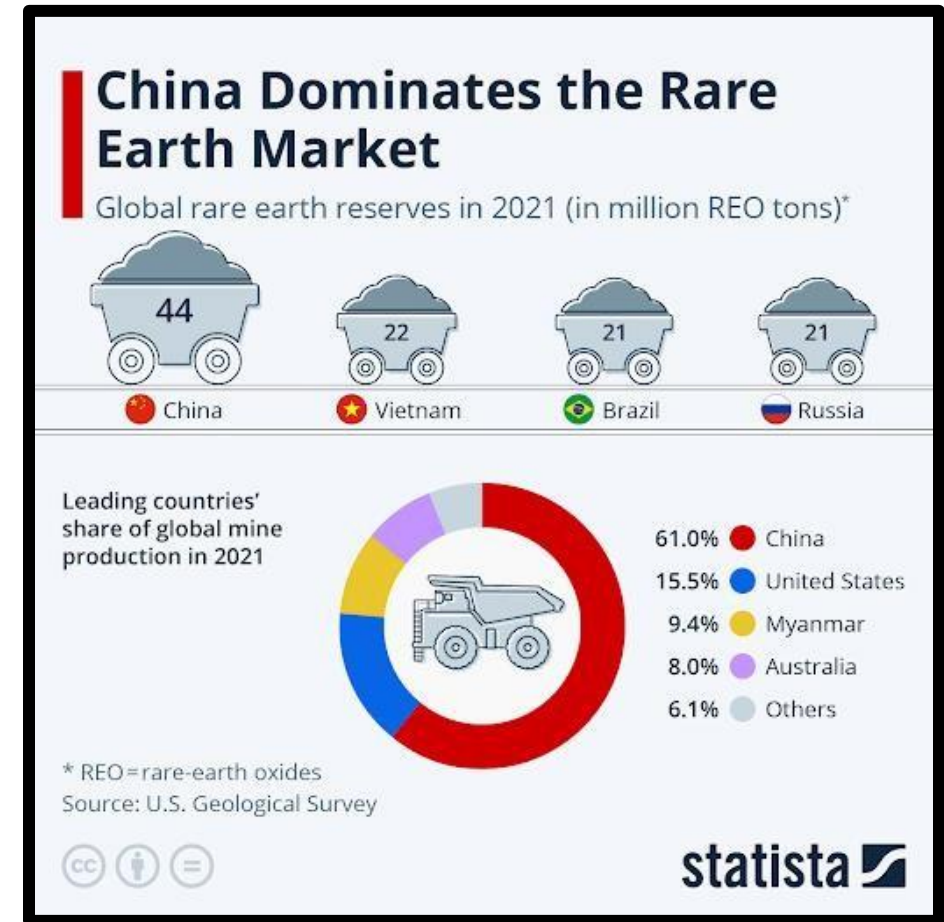
- Reducing coercive economic dependencies,
- Ensuring secure global technology and AI supply chains, and
- Building trusted digital infrastructure.

The initiative reflects growing concerns that over-dependence on a single country for critical inputs can expose economies to geopolitical coercion.



## Global Context Behind Pax Silica

- The global economy is witnessing a shift where advanced technologies such as AI, semiconductors, and digital infrastructure are becoming central to economic and strategic power.
- At the same time, supply chains for rare earths and critical minerals remain highly concentrated.
- China currently dominates the global supply of rare earth elements and processing capabilities.
- In recent years, it has used export restrictions as a strategic tool, including suspending REE exports following tariff disputes with the U.S. India too faced disruptions in rare-earth magnet supplies, affecting its automobile and electronics industries.
- The COVID-19 pandemic further exposed vulnerabilities of globally fragmented and concentrated supply chains, prompting countries to pursue diversification and resilience strategies.



## Key Members of Pax Silica

- The Pax Silica grouping brings together technologically advanced and resource-rich countries.
- Key participants include the United States and Japan as technology leaders; Australia as a major lithium and rare-earth exporter; the Netherlands for advanced lithography technologies; South Korea for memory chip manufacturing; and Singapore for semiconductor fabrication.
- Israel contributes expertise in AI software, defence technologies, and cybersecurity, while the United Kingdom hosts one of the world's largest AI markets.
- Gulf countries such as Qatar and the UAE add financial strength through sovereign investment funds.
- Canada, the European Union, OECD, and Taiwan currently participate as observers.

## Pax Silica: The New Tech Alliance & Why India's on the Sidelines

A US-led initiative to build a secure global silicon supply chain and counter China's tech dominance, with India as a notable absentee.

### WHAT IS PAX SILICA?

#### A US-Led Strategic Alliance

An initiative to build a secure and innovative global silicon supply chain.

#### Primary Goal: Counter China's Dominance

Aims to reduce "coercive dependencies" and protect materials foundational to AI.



#### The Founding Members

Includes the US and 8 allies like Japan, South Korea, and the Netherlands.

### INDIA'S POSITION

#### A Developing Supply Chain

Experts cite India's less-evolved semiconductor sector as a reason for its exclusion.



#### Strengths

Strong in chip design



#### Weaknesses

Lacks capacity for high-grade silicon processing



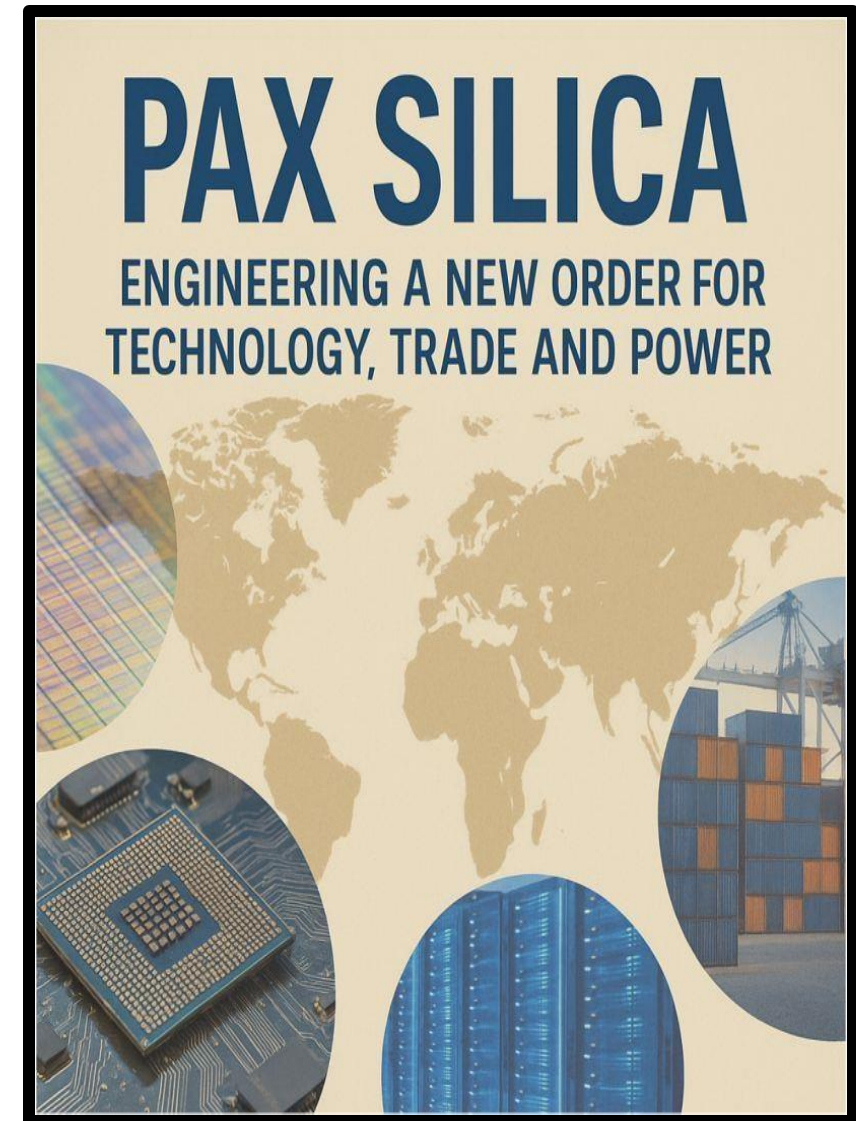
#### Path to Future Membership

India could join later, similar to its delayed entry into the Minerals Security Partnership.



## India's Strategic Relevance

- India is not yet a formal member but is expected to be invited soon.
- India brings several strengths to Pax Silica.
- It has one of the world's most robust digital public infrastructures, a rapidly growing AI market, and a large pool of skilled technology professionals.
- The Government of India has also launched the India Semiconductor Mission and national AI initiatives with significant financial support.
- Investments by Indian firms such as the Tata Group and foreign companies like Micron indicate growing confidence in India's semiconductor ecosystem.
- Additionally, a steady return of skilled Indian professionals trained abroad could strengthen domestic capabilities.



## Kill switch, insurance to fight digital arrest

### INTER-DEPARTMENTAL COMMITTEE

# Kill switch, insurance as tools to fight digital arrest

High-level panel weighs options to deal with growing menace

Soumyendra Barik & George Mathew  
New Delhi, Mumbai,  
January 20

A HIGH-LEVEL committee constituted by the Ministry of Home Affairs (MHA) to look into the menace of 'digital arrest' is considering the idea of a

'kill switch' that will allow users at the receiving end of a potential digital scam to immediately stop all financial transactions from their accounts, *The Indian Express* has learnt.

An insurance mechanism to cover fraud-related losses in the banking system may also be on the anvil as rising digital-age frauds force commercial banks to rethink their risk-mitigation frameworks to better protect customers and the wider financial system, according to officials involved in the proposal.

The proposal for a kill switch, which is being

—CONTINUED ON PAGE 2

## Digital arrest fight looks at kill switch, insurance

examined by an inter-departmental committee formed in late December, envisages, among other possibilities, an emergency button integrated into payment applications of lenders that can instantly freeze all banking operations when a user suspects he or she is being targeted by a fraudster.

"The idea is, can a user's payments application, like the UPI app or bank app, have a kill switch, and the moment the user presses that button, no bank transaction will be possible," a senior government official said, requesting anonymity.

"The committee is also looking if it is possible to identify transactions that may be fraudulent, and if there is a way to ensure that if such a transaction takes place, it cannot immediately be split into multiple mule accounts," the official said.

In digital arrest scams, fraudsters impersonate law enforcement officials from the police, or other law enforcement agencies, via video calls, claiming victims are under investigation for serious crimes. Using leaked personal data for credibility, they create fear and urgency, keeping victims on calls for hours with fake IDs and arrest warrants. Victims are coerced into transferring large sums to avoid arrest. Victims across India are believed to have collectively lost nearly Rs 3,000 crore to digital arrest scams, prompting the Supreme Court to take suo motu cognizance of the issue last October.

The high-level inter-departmental committee (IDC) of the MHA was formed in December, and has officials from multiple agencies to comprehensively examine all facets of the issue of digital arrests. Last week, a status report submitted in the Supreme Court stated that the IDC has held a few meetings where extensive deliberations have taken place on the issues outlined in the court.

The committee has been constituted under the chairmanship of the Special Secretary (Internal Security), MHA, with representation at the level and above of Joint Secretary of- ficers from the Ministry of Elec- tronics and Information Tech- nology (MeitY), Department of Telecommunications (DoT), Ministry of External Affairs (MEA), Department of Financial Services (DFS), Ministry of Law & Justice (MoJ), Ministry of Consumer Affairs (MoCA), Reserve Bank of India (RBI), Central Bureau of Investigation (CBI), National Investigation Agency (NIA), Delhi Police, and the Indian Cyber Crime Coordi- nation Centre (I4C), with the CEO, I4C acting as Member-Sec- retary.

The MeitY is learnt to have convened another meeting with IT intermediaries on January 6 this year. It was attended by the amicus curiae and representa- tives of I4C, MHA, Depart- ment of Telecom, Google, WhatsApp, Telegram, and Microsoft.

Queries sent to the MHA, Finance Ministry, IT Ministry, and Department of Telecommuni- cations by *The Indian Express* remained unanswered until publication.

According to another official

involved in the exercise, an in- surance mechanism to cover fraud-related losses in the bank- ing system is also on the table.

As digital transactions, mo- bile banking and online inter- faces expand rapidly across In- dia's banking ecosystem, fraud risks have grown more sophis- ticated and pervasive. Cyber-en- abled frauds, digital arrests, phishing attacks, account take- overs, mule accounts and com- plex third-party breaches have become harder to detect and prevent. While traditional inter- nal controls, audits and com- pliance systems remain essen- tial, the RBI has indicated that these measures alone may no longer be sufficient to address the evolving threat landscape.

At a financial sector event re- cently, RBI Deputy Governor T Rabi Sankar raised the question whether existing risk-trans- fer tools are adequate and whether there is scope for insurance against frauds, sparking dis- cussions on the potential for in- surance to play a more formal role in bank risk management.

RBI officials have already dis- cussed the issue with various stakeholders, sources said.

Meanwhile, sources said a formal fraud insurance propos- al is yet to reach top insurance companies. "We have not re- ceived any formal proposal from regulators about this issue. The IRDAI will have to take the lead in this matter," said an of- ficial of a public sector insurer.

The RBI's suggestion signals a broader shift in thinking - from viewing fraud solely as a compliance issue to treating it as a balance-sheet and systemic

risk. Collaborative efforts be- tween banks, insurers and regu- lators could lead to innovative products tailored to evolving fraud profiles, strengthening the resilience of India's fast-dig- itising financial system.

RBI's Report on Trend and Progress of Banking in India says there were 23,879 fraud cases involving an amount of Rs 34,771 crore as of 2024-25. The RBI's Payment Vision 2025 re- port, on the other hand, has pro- posed studying the feasibility of setting up a Digital Payment Protection Fund (DPPF) to pro- vide security cover to defrauded customers and payment instru- ment issuers.

While several insurance models are available, experts prefer an insurance pool - backed by contributions from banks, insurers and potentially supported by regulatory frame- works - that could spread fraud risk across the system, similar to terrorism insurance pools in several countries. Such a struc- ture would help manage tail risks while keeping premiums affordable.

Ranjith Bellary, Partner, EY Forensic and Integrity Services- Cyber Forensics, said existing cyber insurance does not ad- equately cover first-party fraud losses, especially those arising from customer manipulation rather than system compro- mise.

"Insurance companies can form a fraud insurance pool like a terror pool, and this idea has been internally mooted by the Reserve Bank to tackle the rising surge of digital frauds, including 'digital arrest' scams," he said.

## Digital Arrest

- India is witnessing a sharp rise in digital frauds, particularly the phenomenon of "digital arrest" scams, leading to massive financial losses and erosion of trust in digital payments.
- In response, a high-level inter-departmental committee (IDC) constituted by the Ministry of Home Affairs (MHA) is examining systemic solutions, including a transaction "kill switch" and a fraud insurance mechanism..



## Digital Arrest' Scams Meaning

- **Cyber-enabled fraud:** Fraudsters impersonate law enforcement officials via video calls.
- Victims are shown fake IDs, arrest warrants, and threatened with arrest. Leaked personal data is used to build credibility.
- **Social engineering:** Victims are kept under psychological pressure for hours and coerced into transferring money to mule accounts.
- **Estimated losses:** Victims across India are believed to have collectively lost nearly Rs 3,000 crore to digital arrest scams, prompting the Supreme Court to take suo motu cognizance of the issue.

## What exactly is 'Digital arrest'?

- New **cyber fraud**
- Accused video call and **pose as law enforcement agency officials, like CBI or customs officials**
- They **give threats of arrest in the name of fake international parcels of banned drugs**
- **Organised economic crime** operated by **cross-border crime syndicates**



## Key Proposals Under Consideration

- **Transaction ‘Kill Switch’:** An emergency button embedded in UPI apps, and banking/payment applications.
- Once activated all banking and financial transactions are instantly frozen, preventing further outflow of funds during suspected fraud.
- It aims to create last-mile consumer protection, and real-time intervention in fraud scenarios.
- **Tracking and blocking fraudulent transactions:** Exploring systems to identify suspicious transactions, prevent instant splitting of funds into multiple mule accounts, and address rapid laundering techniques used by fraud networks.
- **Fraud insurance mechanism:** Proposal to introduce insurance coverage for fraud-related losses in banking.
- Driven by increasing scale and sophistication of digital frauds, and recognition that traditional audits and compliance are insufficient.



## Key Challenges and Way Ahead

- Operational complexity: Avoiding misuse or accidental triggering of the kill switch.
- Technology-based safeguards - AI-driven fraud detection and transaction velocity checks.
- Interoperability: Uniform adoption across banks, UPI platforms, and fintech apps.
- Strengthened coordination - Banks-Insurers-Regulators-Tech platforms partnership.
- Moral hazard: Risk of reduced consumer vigilance if insurance is guaranteed.
- Consumer awareness - Nationwide campaigns on digital arrest scams.
- Regulatory coordination: RBI, IRDAI, MeitY, and banks must act in sync.
- Regulatory clarity - Clear SOPs for kill switch activation and reversal.
- Legal backing - Amendments to IT and banking regulations for rapid response.
- Coverage gaps: Current cyber insurance inadequate for social engineering frauds.



## Trump slams U.K.'s move to hand over Chagos Island

### Trump slams U.K.'s move to hand over Chagos Islands

**Associated Press**  
LONDON

A startled British government on Tuesday defended its decision to hand sovereignty of the Chagos Islands to Mauritius, after U.S. President Donald Trump attacked the plan, which his administration had previously supported.

Mr. Trump said that relinquishing the remote Indian Ocean archipelago, home to a strategically important American naval and bomber base, was an act of "stupidity" that shows why he needs to take over Greenland.

"Shockingly, our brilliant NATO Ally, the United Kingdom, is currently planning to give away the Island of Diego Garcia, the site of a vital U.S. Military Base, to Mauritius, and to do so FOR NO REASON WHATSOEVER," he said in a post on his social media platform Truth Social. "There is no doubt that China and Russia have noticed this act of total weakness."

"The U.K. giving away extremely important land is an act of GREAT STUPIDITY, and is another in a very long line of National Security reasons why



**Ground zero:** An aerial view of the Diego Garcia island. Thousands of Chagos islanders were evicted to make way for the U.S. base. AP

Greenland has to be acquired," Mr. Trump said.

#### 99-year lease

The United Kingdom and Mauritius signed a deal in May 2025 to give Mauritius sovereignty over the Chagos Islands after two centuries under British control, though the U.K. will lease back Diego Garcia where the U.S. base is located, for at least 99 years.

The U.S. government welcomed the agreement at the time, saying it "secures the long-term, stable, and effective operation of the joint U.S.-U.K. military facility at Diego Garcia."

In recent years, the United Nations and its top court have urged Britain to return the islands to Mauri-

itius, and the British government says it's acting to protect the security of the base from international legal challenge.

But the deal has met strong opposition from British opposition parties, which say that giving up the islands puts them at risk of interference by China and Russia.

The U.K. kept control of the Chagos Islands after Mauritius gained independence from Britain in the 1960s. But it evicted thousands of Chagos islanders, who have since mounted a series of legal claims for compensation in British courts. Over 10,000 displaced Chagossians and their descendants now live primarily in Britain, Mauritius and the Seychelles.

### Trump Attacks UK's Chagos Islands Sovereignty Decision

- Former U.S. President **Donald Trump** criticised the **United Kingdom's decision** to transfer sovereignty of the **Chagos Islands** to **Mauritius**, despite earlier U.S. support, arguing it undermines **national security** and risks strategic advantage to **China and Russia**.

## Trump's Critique and Strategic Narrative:

- **Donald Trump** termed the U.K.'s move an act of “**great stupidity**“, questioning the rationale behind relinquishing control of a **strategically vital Indian Ocean territory**.
- He highlighted the presence of a **major U.S. naval and bomber base** on **Diego Garcia**, calling it indispensable for American and allied military operations.
- Trump argued that the decision signals **strategic weakness**, potentially emboldening rivals such as **China** and **Russia**.
- Linking the issue to his Greenland remarks, Trump suggested that such geopolitical missteps justify stronger territorial control to protect **national security interests**.
- His comments, posted on **Truth Social**, surprised British officials, as his administration had earlier **backed the agreement**



## UK–Mauritius Agreement and Political Fallout

- The **United Kingdom** and **Mauritius** signed a deal in **May 2025**, ending over **200 years of British sovereignty** over the Chagos Islands.
- Under the agreement, Mauritius gains **formal sovereignty**, while the U.K. leases back Diego Garcia for **at least 99 years** to ensure continuity of the **joint U.S.-U.K. military base**.
- The base hosts around **2,500 personnel**, mostly Americans, and plays a key role in **Indo-Pacific power projection**.
- British opposition parties criticised the move, warning it could expose the islands to **foreign interference** and weaken the U.K.'s strategic posture.
- The **U.S. government** initially welcomed the deal, stating it secures the **long-term, stable, and effective operation** of the military facility.







# Thank you

## Address

**B-47, Main Road Shivalifi Enclave,  
Blocfi- B, Shivalifi Colony, Malviya  
Nagar, New Delhi-110017**

**Phone Number +t1 8178833167**