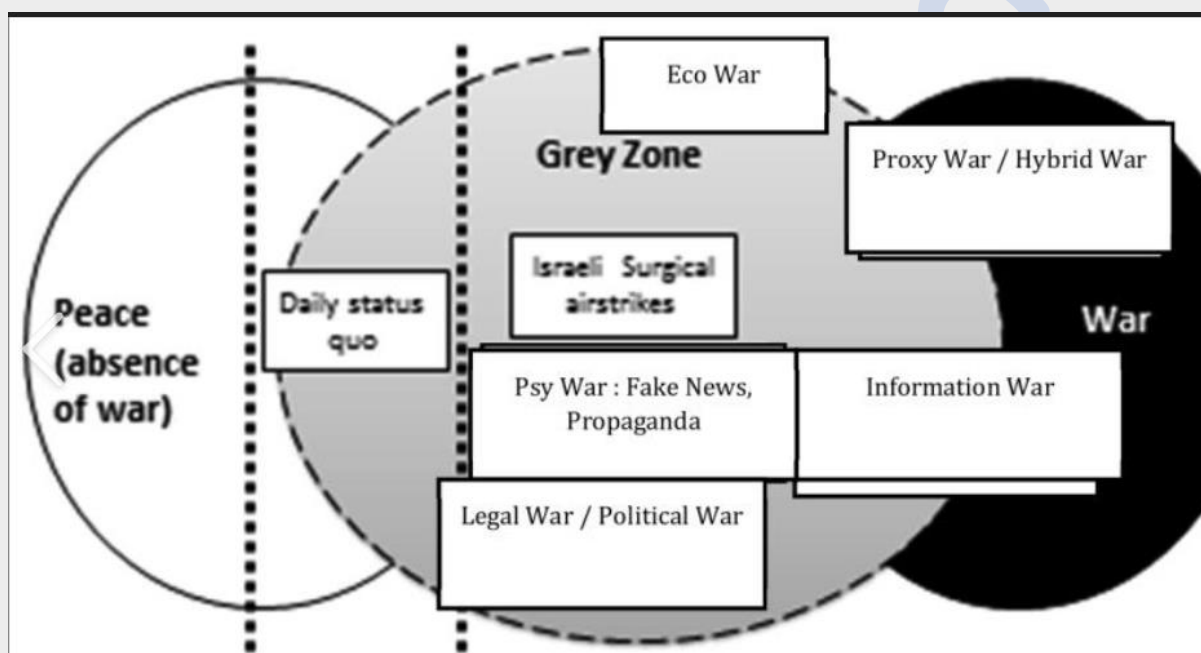


To receive Daily news juice pdf on your WhatsApp, send name and city through WhatsApp on 75979-00000.

1. What is grey zone warfare, mentioned by India's Chief of Defence Staff recently?

Why in News?

On the last day of the 2024 Raisina Dialogue (February 24), India's Chief of Defence Staff General Anil Chauhan said that "grey zone warfare" is the latest in informal warfare.



What does grey zone warfare mean?

Grey zone warfare generally means a middle, unclear space that exists between direct conflict and peace in international relations.

A multitude of activities fall into Grey zone — from nefarious economic activities, influence operations, and cyberattacks to mercenary operations, assassinations, and disinformation campaigns." Other experts include economic actions too, such as debt traps and economic sanctions.

What grey zone warfare looks like

Experts from the US and Europe have characterised certain Russian and Chinese actions of late as examples of grey zone warfare. It includes the Chinese military's presence in the South China Sea.

The Philippines is one of the countries which has challenged China's claims, extending over around 80 per cent of the region. In December 2023, it termed the presence of more than 135 Chinese maritime militia vessels near a disputed reef as "illegal".

It accused China of firing water cannons at its boats and ramming into others, while the Chinese coast guard blamed the Philippines for hitting Chinese boats.

Another example can be that, "Taiwan has complained for four years of stepped-up Chinese military action, such as fighters regularly flying over the strait as part of a 'grey zone' strategy to wear down Taiwan with activities that stop short of a full-blown conflict."

In a paper from the foreign policy research institute Pacific Forum, titled 'The Gray Zone Issue: Implications for US-China Relations', a researcher argued that the US has also engaged in similar tactics. These include its economic sanctions against China and imposition of duties on Chinese imports to the US, along with maritime reconnaissance.

Why is grey zone warfare seen as a separate category of action?

Firstly, the challenges that grey zone warfare poses differ from those of an open conflict. Here, action is often covert or indirect, meaning a country's response needs to be appropriate in terms of its scale.

Relevance: GS Prelims & Mains Paper II; Bilateral Relations

Source: The Indian Express

2. Apple's PQ3 post-quantum cryptographic protocol seeks to protect messages on iMessage from hackers using quantum computers. The protocol can protect communications against current and future decryptions

Why in news?

On February 21, Apple announced PQ3, a post-quantum cryptographic protocol, to encrypt conversations in iMessage. The company called it the "first messaging protocol to reach Level 3 security" and claimed it can defend "highly sophisticated quantum attacks." As per Apple, this protocol's security layer will surpass those available in all widely used messaging apps.

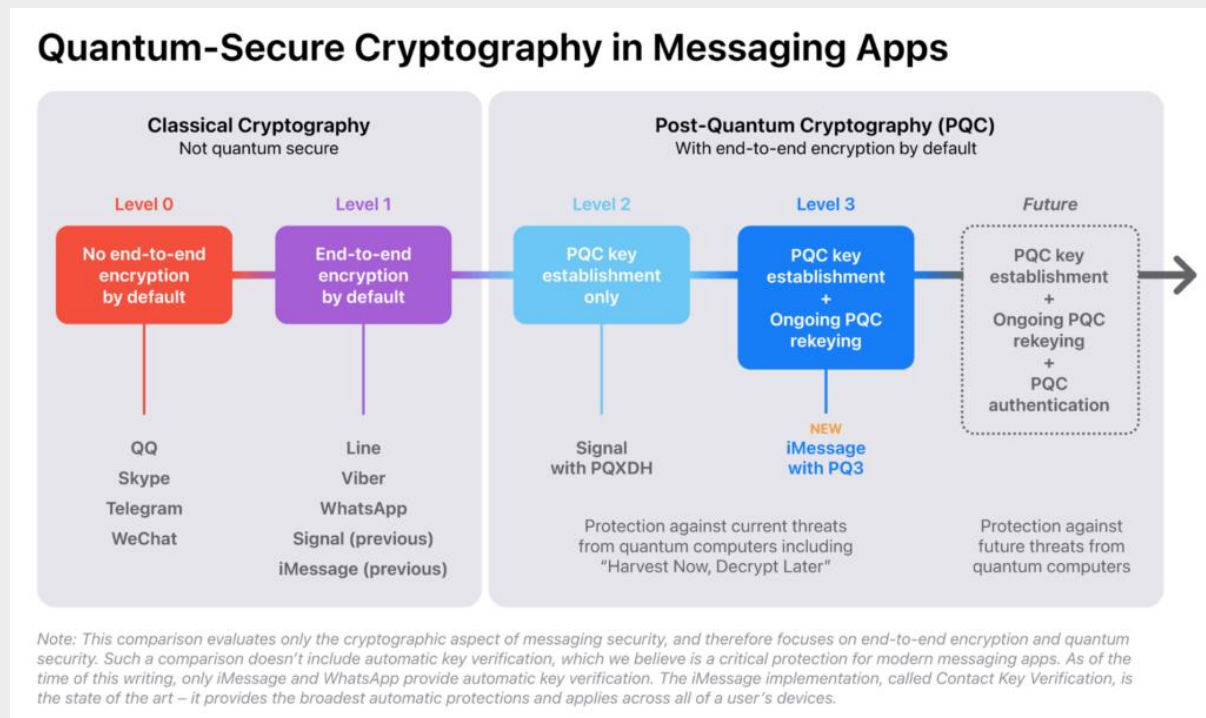
What is the PQ3 protocol, and how does it work?

Currently, most messaging apps have standard encryption methods which use public and private keys to securely deliver messages. There are two encryption methods. In the public key encryption method, a user's message is encrypted by the public key before transmission and then the private key is used to decrypt messages. In the private key method, while both keys are required, they are basically the same, and both the sender and the recipient are allowed to encrypt or decrypt the message.

Apple's PQ3 protocol uses a hybrid design combining traditional encryption methods with post-quantum encryption both during the initial key establishment between devices and during rekeying, which essentially rechecks the cryptographic keys between devices to ensure continued protection.

Under the PQ3 protocol each device generates public keys locally and then transmits them to Apple servers as part of the iMessage registration process using the Module Lattice-based Key Encapsulation Mechanism or ML-KEM. This enables the sender device to get the receiver

device's public keys and generate post-quantum encryption keys for the first message. Apple has also included a periodic post-quantum rekeying mechanism within the conversation which is capable of self-healing from key compromise and safeguarding future messages.



Why is Apple shifting to PQ3 protocol?

Currently, Apple's iMessage supports end-to-end encryption by default. This mode of protection relies on mathematical problems that could potentially be solved by powerful quantum computers.

Over the years, Apple has made improvements to encryption, enhancing its platform's overall protection against hackers. However, current cryptographic problems can be solved by quantum computers, though such computers are still in the works. Apple says extremely well-resourced attackers can mount attacks by taking advantage of the drop in data storage costs. Essentially, attackers can store large amounts of today's encrypted data and file it for future reference. And though attackers may not be able to decrypt this data today, they can retain it until it can be decrypted at a later date by making use of a quantum computer.

Are other messaging services also using methods like PQ3?

Currently in beta, PQ3 will start to roll out with the public release of iOS 17.4, iPadOS 17.4, macOS 14.4, and watchOS 10.4. However, this is not the first time a tech company has announced post-quantum encryption protocols.

Earlier in September 2023, Signal announced advancements in quantum resistance for the Signal Protocol.

The upgrade called PQXDH added a layer of protection against the threat of quantum computers being built for the future. The upgrade used a new post-quantum cryptosystem

that implemented one-way functions that cannot be advantageously reversed by a quantum computer.

Relevance: GS Prelims; Science & Technology

Source: Indian Express

3. What is the Punjab-Himachal dispute over the Shanan hydropower project

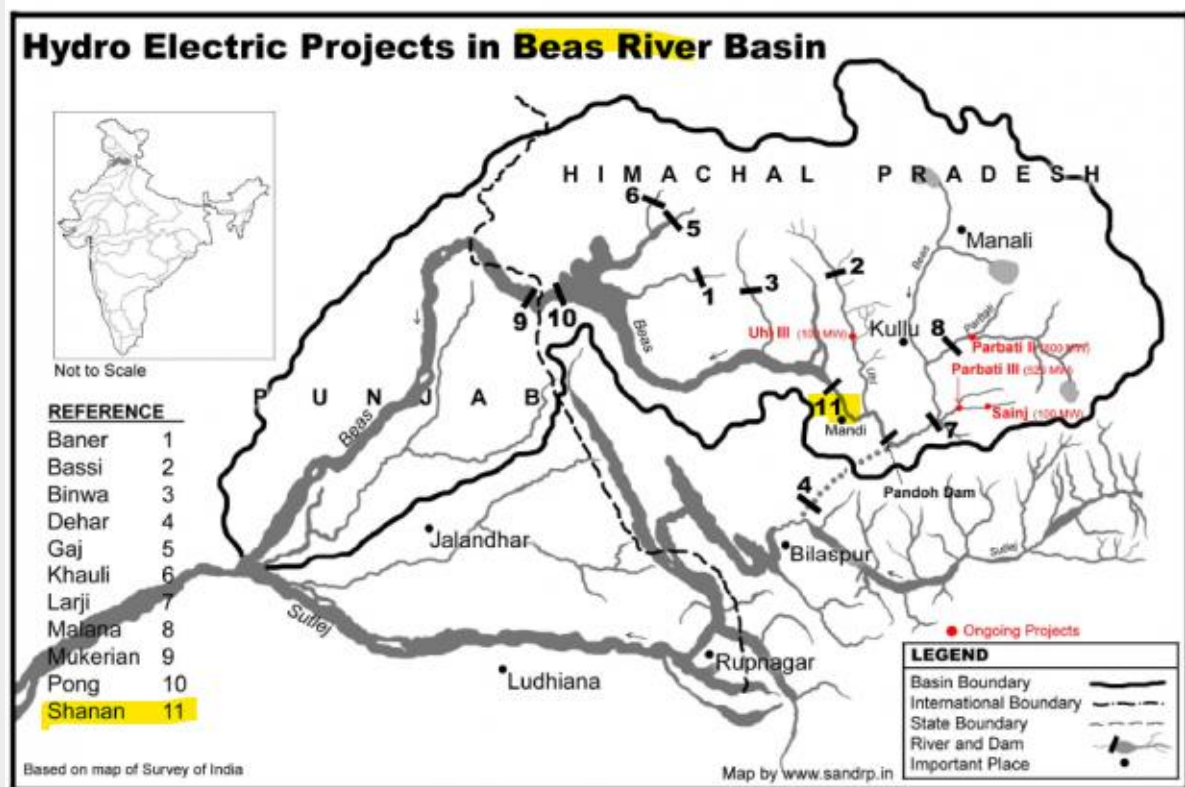
Why in News?

The Centre ordered that status quo be maintained on the Shanan hydropower project, over which Punjab and Himachal Pradesh have made competing claims. Punjab has moved the Supreme Court over the issue.

What is the issue?

The British-era 110-MW hydel project, situated at Jogindernagar in Mandi district, was leased to Punjab in 1925. The lease agreement was signed between the then ruler of Mandi, Raja Joginder Bahadur, and Col BC Batty, a British representative and Chief Engineer of Punjab. The 99-year-old lease came to an end on March 2.

In the past few years, Himachal has contended that the project should stay with it once the lease ends. State Chief Minister Sukhvinder Sukhu had stated they would not allow Punjab to stake claim on the project after the lease period. He had written to his Punjab counterpart Bhagwant Mann last year and also taken up the issue with the Union ministry of power.



What claims does Punjab have over the Shanan project?

The project used to feed the undivided Punjab and Delhi before Independence. After partition, supply to Lahore was discontinued and its transmission line was stopped at Verka village in Amritsar.

During the reorganisation of states in 1966, the hydel project was given to Punjab, as Himachal Pradesh was then a Union Territory. It was allocated to the state by a central notification issued on May 1, 1967 by the Union ministry of irrigation and power. This stated that Punjab's legal control over the project was under the provisions of the Punjab Reorganisation Act, 1966 read along with the 1967 notification.

The Himachal government has alleged that the project is in a poor condition as Punjab is not repairing or maintaining it.

What did Punjab say in the SC plea?

In its suit in the SC, Punjab has contended that it is the owner and is in lawful possession of the Shanan Power House Project, with all assets currently under formative control of the state government through the Punjab State Power Corporation Ltd (PSPCL).

The government has sought a "permanent Prohibitory Injunction" restraining the Himachal Pradesh government from disturbing the "lawful peaceful possession and smooth functioning" of the project. The state has also made the Centre a party.

What has the Centre done?

A day before the 99-year-old lease was to come to an end, the Centre ordered status quo on the project as an interim measure to keep the project working.

The orders have clearly stated that "The issuance of this order is entirely in the nature of the interim measure and shall not be treated as a basis of any claim or interest and parties are expected to proceed further on all matters concerning the settlement of the dispute in such manner as they may deem fit and within such legal framework as may be appropriate."

Relevance: GS Prelims & Mains Paper III; S&T

Source: The Indian Express