16th Anniversary of 26/11 Attacks

For Prelims: Indian Navy, Coast Guard, Territorial Water, Unlawful Activities Prevention Act, 1967 (UAPA), Intelligence Bureau, National Investigation Agency (NIA) Act, 2008, National Security Guard (NSG), FATF.

For Mains`: Strengthening of counter-terrorism measures.

Source: TOI

Why in News?

On **26th November 2008**, **Lashkar-e-Taiba**, a Pakistan-based terror group, carried out attacks at the **Taj Mahal Palace Hotel, Nariman House, Oberoi Trident, and Chhatrapati Shivaji Railway Station** in Mumbai.

- The attacks revealed significant **vulnerabilities** in India's **security infrastructure,** prompting urgent reforms in **counter-terrorism measures.**

What were Indian Security Vulnerabilities Exposed by 26/11 Attacks?

- **Intelligence Failures:** The failure to **share intelligence in real-time** between various security agencies allowed the terrorists to **operate undetected** for a significant period before the attack.
- **Maritime Security:**
  - **Porous Coastal Borders**: The attackers hijacked an **Indian fishing trawler** after traveling on a Pakistani-flagged cargo ship, then used **inflatable boats** to land on Indian shores without raising suspicion.
  - **Lack of Coordination**: The **lack of clear command and control** structures among **Indian Navy, Coast Guard, Marine Police** led to inefficiencies in securing the **coastal areas**, making them vulnerable to exploitation.
- **Digital Vulnerabilities**: India's inability to counter **digital propaganda** and **online radicalisation** led to **local support** through **logistical assistance**.
- **Lack of Specialised Training**: India's security forces were **not adequately trained** to handle the new type of **urban terror attack** with multiple sites targeted simultaneously as seen in **26/11.**
- **Slow Response:** The **delayed response** from security forces, combined with a lack of **rapid deployment and tactical coordination**, allowed the terrorists to hold out for several hours.
- **Inadequate Cyber Security Measures:** The 26/11 attackers used advanced communication tools, including **satellite phones,** to stay in constant contact with their handlers in Pakistan.

What Steps Were Taken to Strengthen Security after 26/11 Attacks?

- **Maritime Security Revamp:** The Indian Navy was made responsible for **overall maritime security,** while the **Indian Coast Guard** managed **territorial waters** and coordinated with **new marine police stations** along the coastline.

    - The Indian Navy established the **Sagar Prahari Bal** to enhance **coastal patrolling** and rapid response capabilities.
    - Regular **coastal security exercises** are conducted across all states, in collaboration with the **Coast Guard, State and Central Government agencies** for improving coordination.
    - All vessels longer than **20 meters** were made to install the **Automatic Identification System (AIS)** to transmit **identification** and other critical information.
- **Intelligence Coordination:** The **Intelligence Bureau's Multi-Agency Centre (MAC)** was strengthened to improve the **coordination of intelligence sharing** among central agencies, the armed forces, and state police.
    - MAC's charter was **expanded** to cover new areas, such as **analysing and addressing radicalisation** and terrorism networks more effectively.
- **Institutional Measures:**
    - **National Counter-Terrorism Centre (NCTC)** was established to **draw up plans and coordinate action** for counter-terrorism with other stake holders including anti-terrorist organisations in states.
    - **Crime and Criminal Tracking Network and Systems (CCTNS)** was started to **inter-link all police stations** under a common application software for the purpose of **investigation, data analytics, research, and policy making.**
    - **National Intelligence Grid (NATGRID)** is an integrated **IT platform to help access data** gathered from various databases such as **credit and debit cards,** tax, telecom, immigration, airlines and railway tickets, passports, driving licenses among others to tackle crime and terror threats in the country.
- **Legal Reforms:** The **Unlawful Activities Prevention Act, 1967 (UAPA)** was amended to broaden the definition of **terrorism** to take more proactive steps against terrorist activities.
    - The **National Investigation Agency (NIA) Act, 2008** was passed to create a **federal investigation agency** with the authority to handle terrorism cases **across states.**
- **Modernisation of Police Forces:** The Ministry of Home Affairs allocated more funds to state governments to **upgrade police stations, equip them with modern technology, train officers** for modern challenges like terrorism, and provide better weapons.
    - Emphasis was given to the creation of **crack commando** teams among all police forces.
    - The **National Security Guard (NSG)** established four regional hubs across the country at **Chennai, Hyderabad, Kolkata and Mumbai** for rapid deployment.
- **International Cooperation:** The biggest impact of the 26/11 attacks was the **willingness of the West, especially the US**, to cooperate with India on matters of security.
    - The US provided **real-time information** during the attacks and helped gather **prosecutable evidence** through the FBI that helped **isolate Pakistan globally.**
    - In **2018**, global pressure led to **Pakistan** being placed on the **FATF** grey list, forcing action against terror groups like **Lashkar-e-Taiba (LeT) and Jaish-e-Muhammad (JeM).**
- **Sensitisation Campaigns**: These drives aim to sensitise **local populations** about the risks posed by **maritime threats** and to encourage them to report **suspicious activities.**

What are the Persistent Lacunas in Indian Coastal Security?

- **Challenge of Monitoring**: India's **7517 km-long coastline**, including the mainland (5423 km) and the Andaman & Nicobar Islands (2094 km).
    - The vast coastline, with thousands of fishing boats and dhows, makes **monitoring and patrolling potential threats challenging.**
- **Lack of Comprehensive Coverage**: The provision to install **Automatic Identification Systems (AIS)** for boats over 20 meters in length, limits the scope of maritime surveillance, especially when many **smaller boats (under 20 meters)** could be used for illegal activities such as **smuggling or infiltration.**
- **Diverse Threat Landscape:** The varied nature of threats **(Terror Attacks, Smuggling, and Illegal Migration)** highlights the complexity of the security challenges.
    - Migrants, particularly from **Bangladesh and Sri Lanka**, may pose security risks, either **inadvertently or deliberately.**
- **Over-reliance on Local Communities:** Fishermen are crucial for **coastal security**, but relying solely on them for intelligence is risky due to potential non-cooperation from fear, lack of awareness, or distrust.

- **Poor Infrastructure:** State police forces continue to remain **ill-equipped and poorly trained** with continued political interference hampering overall coordination.

Way Forward

- **Deterrence and Offensive Strategies**: India's recent responses to cross-border terrorism, including **surgical strikes and airstrikes** should be **institutionalised** as part of India's long-term **counterterrorism policy**, aiming to deter terrorism by demonstrating the country's resolve to respond decisively.
- **Multi-Agency Training and Exercises**: The NSG's model of **multi-agency exercises,** where various security forces train together, should be scaled up nationwide.
    - These exercises should include **local law enforcement, paramilitary forces, and intelligence agencies** to ensure all parties are well-prepared for coordinated action during attacks.
- **Coordination with Specialised Forces**: The local police must maintain a close working relationship with national counterterrorism units such as the **NSG** to ensure smooth coordination in the event of an attack.
- **Empowering Decision-Makers**: Decision-makers at various levels (from local police to national security agencies) should be empowered with **greater discretion to act quickly and decisively** during emergencies.
- **Urban Disaster Management Plans**: Cities need to have **disaster management plans** that focus not only on natural disasters but also on **man-made threats** such as terrorist attacks.
- **Building Cybersecurity Expertise**: Multi-disciplinary training in **cyber and physical security** should be integrated.
- **Establishing 'Awake Cells'**: Community-based **'Awake Cells,'** made up of youth and citizens, can bridge the gap between the **public and security agencies** by reporting suspicious activities and providing real-time intelligence.

Drishti Mains Question:

What reforms were introduced in India's security apparatus post the 26/11 attacks to enhance counter-terrorism capabilities?

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Mains

Q. The scourge of terrorism is a grave challenge to national security. What solutions do you suggest to curb this growing menace? What are the major sources of terrorist funding? (2017)

Q. Religious indoctrination via digital media has resulted in Indian youth joining ISIS. What is ISIS and its mission? How can ISIS be dangerous to the internal security of our country? (2015)

Q. Cyber warfare is considered by some defence analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. (2013)