

1. One of the key components of the strategy to counter the threat emanating from a China-Pakistan axis is to strengthen border infrastructure. Do you agree? Substantiate your views.

Approach

Candidates need to highlight threats related to China and Pakistan and highlight on China Pakistan axis. Also write about the importance of Border security infrastructure to tackle the China Pakistan axis.

Introduction

Relationship between China and Pakistan developed over the 1970s and '80s. Countering India was one of the key pillars. It opens a two-front war possibility for India to tackle it India should strengthen its security apparatus on borders.

Body

Threat to India's security ecosystem on borders:

- Pakistan is able to sustain cross-border terrorism despite a domestic Balance of Payments crisis, using Chinese funds and material (including Chinese-made grenades).
- They're able to combine their efforts in destabilizing border management by exploiting open & porous borders with Myanmar and Bangladesh.
- Passing of CPEC through POK affects the sovereignty and territorial integrity of India.
- Pakistan is all set use BeiDou for both military purposes on borders, ending their dependence on the US-based Global Positioning System.

Strengthening border infrastructure to tackle China Pak axis:

- Border road infra helps in maintaining peace and stability by controlling the security concerns related to inter-region and intra-region issues.
- Creating infrastructure: India is also constructing some critical bridges to cut down time for troop movement such as Dhola – Sadiya bridge.
- India has joined hands with Japan to aggressively develop infrastructure projects in North east to contain China.
- To increase capability tender for purchase of six Border Surveillance Management Systems (BSMS) to cater to the needs of Indian Army's peace time requirements for countering the infiltration attempts from Pakistan.
- BOLD-QIT is a project to install technical systems under the Comprehensive Integrated Border Management System (CIBMS), which enables the BSF to

equip Indo-Bangla borders with different kinds of sensors in the unfenced riverine area of Brahmaputra and its tributaries.

- The UAVs and other surveillance gadgets already under installations have significantly reduced the incidents taking place due to human error.
- The mini UAVs are also intended to carry out reconnaissance in Jammu and Kashmir for counter insurgency along with the LoC with Pakistan and the Line of Actual Control with China.

Conclusion

The traditional approach to border management on Pakistan and China borders, i.e. focussing only on border security, has become inadequate. India needs to not only ensure seamlessness but with the adoption of new technologies for border control and surveillance and the development of integrated systems for entering, exchange and storage of data, will facilitate the full proof border security without endangering security personnel and internal security of India.

2. How do you define terrorism? How is it related to organised crime? Has the linkage between organised crime and terrorism evolved in recent years? If yes, how? Discuss

Approach

Students are expected to give basic information of both organized crime and terrorism and explain how both are interlinked and related to each other in many cases. Also discuss whether this type of linkage are recent phenomenon or not.

Introduction

Organised crime is a category of transnational, national, or local groupings of highly centralised enterprises run by criminals who intend to engage in illegal activity, most commonly for money and profit. While terrorism is a Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organisations or nations (state-sponsored).

Body

Nexus between organised crime and terrorism

- Terrorist groups need arms and money to fight against security forces. The organised criminals and terrorist groups become clients of each other.

Organised criminals groups smuggle arms, drugs, cattle, humans to generate money for terrorist groups.

- Terrorist groups always try to destabilise the country and bring down the morale of security forces. When the terrorist groups are unable to confront the security forces directly, they turn towards organised criminals. Thus organised criminals indirectly help these terrorist groups.
- Organised criminal groups generally establish a strong communication network. These organised groups act as eyes and ears of the terrorist groups.
- Terrorist organisations in India, especially in the northeast, mobilise funds by becoming couriers of illegal drugs and arms and at times even human beings from one point to another within the country.
- Terrorists are always in need of money. As they fail to mobilise large amounts of money, they take the help of organised criminals to exchange counterfeit currency with arms.

Penetration of Organised crime and its link with terrorism:

- Besides Kashmir and the northeast, sporadic incidents in other parts of India like the Bombay blasts, for instance, have exposed the connection between terrorism and organized crime.
- This is distinct from the traditional linkages flourishing between organized crime syndicates and local criminals.

Conclusion

There is a need to develop effective and tailor-made responses to the organised crime and terrorism, which address the underlying causes of the convergence at all levels, based on strong evidence, engagement with local actors, good governance, enhanced services delivery and capacity building and the incorporation of normative frameworks.

3. Examine the significance of robust intelligence for internal security. What are the key elements for the success of intelligence agencies? Discuss.

Approach-

Candidates need to examine the significance of robust intelligence for internal security. Also discuss the key elements for the success of intelligence agencies.

Introduction:

Any fight against terrorism, insurgency and internal security would be incomplete without a strong and a robust intelligence network, feedback or its analysis.

The significance of robust intelligence for internal security

- In India there is a thin line between external security threat and internal security threat. We live with an aggressive neighbourhood.
- National Intelligence Grid (NATGRID) was created in 2012 and due to some circumstances, it slowed down. The present government is reviving it to give it a practical shape. This is known to be a robust intelligence gathering mechanism.
- By recognizing patterns on the network and clustering them, AI proceeds to detect any deviations or security incidents from the norm before responding to them.
- Potential threats with similar traits to those recorded get blocked early enough.
- The fact that AI keeps learning makes it difficult for hackers to beat its intelligence.
- All the intelligence agencies in the country sit together, coordinate and analyse all the intelligence information available and analyse the real threat and pass on to agencies which are required to take counter action.
- Technology that uses AI, such as a residential proxy, can help you to transfer data.
- It can also detect and identify any threats hidden in the sea of chaotic traffic
- The present scenario of the country is that the threat from outside is not only along borders but anywhere in the country. All the states have to remain alert and they have to coordinate and share the intelligence gathered. In the same manner centre should also share the intelligence with the states.

The key elements for the success of intelligence agencies

For the success of intelligence agencies, the following key elements are generally required:

- No counter terrorism programme in the world would be complete without use of the latest technology.
- With the coordination of Technology intelligence and human intelligence we can get real time information which is required for action against the terrorist threat or any other threat to the country.
- The robust intelligence that tips off to an impending cyberattack or any attack on internal security should be timely. Putting together the indications that an attack was coming after it already happened is not.
- At its core, intelligence must be of value to the end consumer. In order to achieve that goal, it must be actionable, timely, and relevant. Data feeds are

often timely, but because they are predicated on volume, they are rarely actionable or relevant.

- The foundation of the threat intelligence ecosystem is, and always will be, data. No intelligence program can survive without data.

Conclusion

The increasing rate of cyber-attacks has posed a great challenge in the recent times. AI gives the much-needed analysis and threat identification that can be used by security professionals to minimize breach risk and enhance security posture. AI can help discover and prioritize risks, direct incident response, and identify malware attacks before they come into the picture. So, even with the potential downsides, AI will serve to drive cybersecurity forward and help organizations create a more robust security posture

