Security Class 04

18th March, 2024 at 1:00 PM

LINKAGES BETWEEN ORGANISED CRIME (OC) AND TERRORISM IN INDIA (01:10 PM):

- In 2014, naxalism in India was reported to be a 1500 crore extortion business.
- This mostly involves the kidnapping of businessmen, contractors, and even public servants and seeking ransom.
- Naxalites also resort to taking "protection money" as a tribute for allowing business operations/governance to continue undisturbed in areas controlled by them.
- In Punjab, one person in 65% of families is addicted to drugs.
- The reasons primarily involve cultural and geographical proximity to Pakistan.
- Drying up of funds for terror organizations in Pakistan since 2001.
- In the North East, especially in Manipur and Nagaland, there are areas controlled by local militia which involve themselves in human/arms/drug trafficking.
- In Jammu and Kashmir, terrorist operations are primarily sponsored by external State actors and there is an involvement of OGW (over-ground workers) which act as a front for terror organizations to secure finances, especially since the ban on Jamaat-e-Islami.
- **Challenges with respect to organized crimes and terrorism in India (01:55 PM):**
- a) Inadequate Legal framework:
- Although the Unlawful Activities Prevention Act (UAPA) came into existence in 1967, a dedicated chapter for preventing terrorist activities was added in 2004.
- Until then terrorism was primarily being dealt with by the now repealed Terrorist and Disruptive Activities (Prevention) Act (TADA) and Prevention of Terrorism Act (POTA).
- b) Only a few States like Maharashtra, Karnataka, Gujarat, etc. have dedicated laws against organized crime.
- c) Weak enforcement agencies:
- Particularly the State police forces which lack both in terms of arms and ammunition and also training.
- d) Lack of coordination amongst security agencies.
- e) The role of technology:
- Technology poses a significant challenge, especially with security agencies lacking the capacity to combat new-age organized crimes involving cyberspace.
- f) Lack of public awareness and glorification of OC in popular media and cinema attracts youth to such organizations.
- **Question (02:18 PM):**
- 1. What is the way forward for breaking the crime-terror nexus in India?
- 2. Find examples of OC in India (i.e. Matka).

CYBER SECURITY (02:40 PM):

- *Securing a nation's political and socio-economic interests from cyber threats.*
- *First generation warfare - Firearms, line arrangements.*
- *2nd generation warfare - Artillery, cavalry, infantry, steam engine (ships, rail), and total warfare.*
- *3rd generation warfare - Storm tactics/Blitzkrieg, nuclear capabilities.*
- *4th generation warfare - Unconventional warfare, irregular warfare, hybrid warfare.*
- **Different types of warfare:**
- a) Unconventional Warfare (UW):
- UW refers to the use of an indirect or covert approach to conduct activities such as establishing resistance movements, insurgency, etc. to coerce, disrupt, or even overthrow a Government of the adversary.
- For instance, the use of proxy forces, underground armies, or use of surrogates, use of psyops (psychological operations), etc.
- For example, ISIS supports Khalistani Movement.
- b) Irregular Warfare:
- It is considered the oldest form of warfare wherein a significant proportion of those fighting are not a part of conventional security forces. Wagnor group used by Russia.
- For example, the Chinese Revolution and the Operation Gulmarg.
- It is generally protracted and the main aim is not territorial but acquiring influence over people.
- c) Hybrid Warfare:
- It is a combination of both conventional and unconventional warfare.
- It seeks to exploit all vulnerabilities of the opposition which include diplomatic, intelligence, military, economic, financial, legal, informational, and political vulnerabilities (DIMEFLIP).
- **Note** - Cyberspace has added another dimension to unconventional warfare (i.e. Fifth dimension of warfare).
- **Need for Cyberwarfare/Motivation Behind Cyberwarfare (03:19 PM):**
- ***Challenges** of Kinetic Warfare:*
- *Deterrence distance.*
- *Asymmetry in terms of cost and impact.*
- *Retaliation.*
- *Preference to offense.*
- *Conventional status apparatus.*

- **The advantages of cyberwarfare mainly stem from the disadvantages of conventional/kinetic warfare**.
- a) Conventional warfare in contemporary times will beget heavy sanctions and costs.
- b) Furthermore, the "deterrence distance" created by the introduction of nuclear technology makes it prohibitively expensive (both in terms of life and property) to engage in conventional war.
- In this respect, cyberwarfare offers the following advantages:
- i) **Asymmetricity**:
- Cyberwarfare is asymmetric in terms of its cost, impact, and response.
- It can be conducted at the State level and the non-state level.
- It can be both long-term (i.e. cyber espionage) and short-term.
- For example, a targeted attack on a country's smart grid network is a short-term attack while cyber espionage can be long-term.
- A dozen hackers ,cheaply equipped can bring an economy's entire digital infrastructure down.
- ii) **Plausible Deniability**:
- Cyber conflicts are usually low-intensity and non-lethal, hence they don't attract retaliation using conventional State instruments.
- In addition, since actors can be non-state and attacks can be made to appear as though they originated from a different jurisdiction, it becomes extremely difficult to trace the origin and establish capability***.
- iii) **Combined Warfare**:
- It is very easy to combine cyber capabilities with conventional military capabilities that both can go simultaneously and cyber attacks can even be conducted during peacetime.
- iv) **Preference to Offense:**
- The Internet is designed to be a collaborator and hence "zero-day vulnerabilities" will always remain.
- Hence, what matters in cyber warfare is speed, not deterrence.

THE TOPIC FOR THE NEXT CLASS - DEFINITION OF CYBER ATTACKS AND THE DIFFERENT TYPES OF CYBER ATTACKS.