* Global meet on criminal finances

- 4th Global Conference on Criminal Finances and Cryptocurrencies (virtual) → 132 countries
- Organised by Interpol, Europol & Basel Institute of Governance
- 2016 → Working Group on Cryptocurrencies & Money Laundering established

Objective: Strengthening knowledge & expertise for solutions against the criminal use of cryptocurrencies

Since then regular meetings held

- Agenda -
  - Trends & investigations on cryptocurrency related offences
  - Exploring criminal flows and operations in dark market
  - Ransomware & Sextortion case studies
  - Money laundering involving virtual assets
  - Transfer of drug proceeds using cryptocurrencies

* India must raise bar on AML systems

- AML → Anti Money Laundering
- FATF will undertake its once-a-decade evaluation of India's AML regime in 2021
  - ↳ comprises of peer reviews of each member
  - ↳ assesses implementation of its recommendations
  - ↳ analyses of country's system for preventing criminal abuse of financial system
- Major challenge for India
  - Identifying suspicious transactions in the sheer volume
    - ↳ SBI itself has 43 crore account
    - ↳ with 15-20 crore transactions per day
  - Immense load
    - ↳ quality of transaction monitoring suffers
- Measures
  - Indian banks using AI & ML tools to identify transactions that dont follow the usual pattern.
  - Improve compliance culture. Eg: KYC

— FATF work on Pak

- FATF able to do what UNSC could not
  - ↳ tamed financing of terror activities in Pakistan
- Put Pak on a tight leash
- Pak forced to put main terrorist leaders behind bars

* Crackdown on fake medicines

- Operation Pangea XIV
  - ↳ by Interpol
  - ↳ coordinated with many national nodal bodies, like CBI in India
  - ↳ 1st Operation Pangea in 2008
- Results of the operation:
  - 1.13 lac weblinks removed against sale of fake and illicit medicines, etc
  - Seizure of potentially hazardous pharmaceuticals
    - ↳ worth over $23 mn.
    - ↳ mainly fake COVID-19 test kits
  - UK
    - ↳ 3 mn. fake medicines & devices ⇒ $13 mn
  - Venezuela
    - ↳ e-commerce website developer arrested
    - ↳ sold illicit medicines
  - Italy ⇒ 5 lac fake surgical masks.
  - Qatar ⇒ Nerve pain tabs hidden in tins of beans.
- Pandemic forced criminals to move to online modes.

India signed 26 pacts to fight drug menace

–(MHA) reply in the Lok Sabha on the measures taken to combat drug trafficking in India.

–International level:

1.India is signatory to

- UN Single Convention on Narcotics Drugs 1961
- Convention on Psychotropic Substances, 1971
- Convention on Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 1988

2. India has signed 26 bilateral pacts, 15 MoUs and 2 agreements on security cooperation with different countries for combating drug trafficking

–Domestic level:

- Narcotics Drugs and Psychotropic Substances (NDPS) Act, 1985.– is the basic legislative instrument.
- Narco Coordination Centre (NCORD)– For better coordination among various Central and State agencies.
- The NCORD system has been further extended into a four-tier scheme up to the district level.

- A Joint Coordination Committee was set up to monitor the investigation into cases involving large seizures.
- The MHA has launched an e-portal called 'SIMS' (Seizure Information Management System) for digitisation of pan-India drug seizure data.

1,000 held in 20 countries in financial crime crackdown

Recently, Interpol coordinated an operation with enforcement agencies in more than 20 countries highlighting the global threat of cyber-enabled financial crime.

Cyber-enabled financial crime:

- Ransomware, sextortion scams, identity theft, money laundering, and other financial crimes are examples of cyber-enabled financial crime.
- It's not about draining bank accounts or bitcoin wallets; it's about stealing IP.

Threats from cyber-enabled financial crime:

- Social engineering (e.g. phishing email) might be used to launch a cyber-enabled financial assault from the outside.
- Insider threats - criminally motivated workers attempting to obtain access to cash - are also a concern.

The following are the four most prevalent components of these attacks:

- Distributed Denial of Service (DDoS) smokescreens: Coordinated denial of service attacks on financial institutions are common, and they often appear to be aimed solely to impair the usage of online banking assets.
- Transactional based network penetration:
- Data theft based network penetration: Hackers continue to try to hack into processor and other systems in order to obtain client data
- Conventional remote banking fraud: The latest wave of cyberattacks is notable for combining any or all of the above-mentioned attacks with traditional internet, mobile, phone payment, and card attacks.

Global Efforts to Prevent Cyber-enabled financial crime:

'HAECHI-II': -

- The operation codenamed 'HAECHI-II' was conducted by INTERPOL saw police arrest more than 1,000 individuals underlining the global threat of cyber-enabled financial crime.

- Specialised police units from 20 countries, including Hong Kong and Macau, took part in the exercise to target specific types of online fraud, such as "romance" scams.
- It is the second such operation in a three-year project launched to tackle cyber-enabled financial crime.

Anti-Money Laundering Rapid Response Protocol (ARRP)

- The Anti-Money Laundering Rapid Response Protocol (ARRP) has been vital to effectively intercepting illegal payments in various HAECHI-II situations.
- The findings revealed that the increase in crimes caused by the COVID-19 epidemic had not subsided.

Purple Notices from Interpol

- Based on the findings during the operation, the Interpol published multiple Purple Notices – police alerts that seek or provide information on modus operandi, objects, devices and concealment methods used by criminals.