26– 04 – 2023

News: Operation Kaveri

- India has started 'Operation Kaveri' to evacuate its nationals owing to the Current Crisis in Sudan.
- Around 3,000 Indians are stuck in various parts of Sudan, including capital Khartoum and in distant provinces like Darfur.

Operation Kaveri

- Operation Kaveri is a codename for India's evacuation effort to bring back its citizens stranded in Sudan amid intense fighting between the army and a rival paramilitary force there.
- The operation involves the deployment of Indian Navy's INS Sumedha, a stealth offshore patrol vessel, and two Indian Air Force C-130J special operations aircraft on standby in Jeddah.
- There are about 2,800 Indian nationals in Sudan, and there is also a settled Indian community of about 1,200 in the country.

Current Crisis in Sudan

Background

- The conflict in Sudan has its roots in the overthrowing of long-serving President Omar al-Bashir by military generals in April 2019, following widespread protests.
- This led to an agreement between the military and protesters, under which a power-sharing body called the Sovereignty Council was established to lead Sudan to elections at the end of 2023.
- However, the military overthrew the transitional government led by Abdalla Hamdok in October 2021, with Burhan becoming the de-facto leader of the country and Dagalo his second-in-command.

Tussle between Army and RSF

- Soon after the 2021 coup, a power struggle between two military (SAF) and paramilitary (RSF) generals arose, interrupting a plan to transition to elections.
- A preliminary deal was reached in December 2021 for a political transition, but negotiations hit a roadblock over the integration of the paramilitary Rapid Support Forces (RSF) with the Sudanese Armed Forces (SAF), due to disagreements over the timetable and security sector reforms.

- Tensions escalated over the control of resources and RSF integration, leading to clashes.
- There was disagreement over how the 10,000-strong RSF should be integrated into the army, and which authority should oversee that process.
- Also, Dagalo (RSF general) wanted to delay the integration for 10 years but the army said it would take place in the next two years.

Rapid Support Force (RSF)

- The RSF is a group, evolved from Janjaweed militias, which fought in a conflict in the 2000s in the Darfur region in West Sudan nearing the Border of Chad.
- Over time, the militia grew and made into the RSF in 2013, and its forces were used as border guards in particular.
- In 2015, the RSF along with Sudan's army began sending troops to fight in the war in Yemen alongside Saudi and Emirati forces.
- In addition to the Darfur region, the RSF was deployed to states such as South Kordofan and the Blue Nile, where it was accused of committing human rights abuses.
- In a 2015 report, Human Rights Watch described its forces as "men with no mercy".

News: LockBit Ransomware

- Recently, it has been found that LockBit ransomware was found to be targeting Mac devices.

LockBit Ransomware

- LockBit Ransomware, formerly known as “ABCD” ransomware, is a type of computer virus that enters someone's computer and encrypts important files so they can't be accessed.
- The virus first appeared in September 2019 and is called a "crypto virus", because it asks for payment in cryptocurrency to unlock the files.
- LockBit is usually used to attack companies or organizations that can afford to pay a lot of money to get their files back.
- The people behind LockBit have a website on the dark web where they recruit members and release information about victims who refuse to pay.
- LockBit has been used to target companies in many different countries, including the U.S., China, India, Ukraine, and Europe.

Modus Operandi

- It hides its harmful files by making them look like harmless image files. The people behind LockBit trick people into giving them access to the company's network by pretending to be someone trustworthy.

- Once they're in, LockBit disables anything that could help the company recover their files and puts a lock on all the files so that they can't be opened without a special key that only the LockBit gang has.
- Victims are then left with no choice but to contact the LockBit gang and pay up for the data, which the gang may sell on the dark web - whether the ransom is paid or not.

LockBit Gang

- The LockBit gang is a group of cybercriminals who use a ransomware-as-a-service model to make money.
- They create custom attacks for people who pay them and then split the ransom payment with their team and affiliates.
- They are known for being very prolific and avoiding attacking Russian systems or countries in the Commonwealth of Independent States to avoid getting caught.

Why is LockBit targeting macOS?

- LockBit is targeting macOS as a way to expand the scope of their attacks and potentially increase their financial gains.

- While historically ransomware has mainly targeted Windows, Linux, and VMware ESXi servers, the gang is now testing encryptors for macOS.
- The current encryptors were not found to be fully operational, but it is believed that the group is actively developing tools to target macOS.
- The ultimate goal is likely to make more money from their ransomware operation by targeting a wider range of systems.
-