> **States Acquiring Offensive Cyber Capabilities**
> Several countries have established institutions to develop offensive cyber capabilities. United States has raised US Cyber Command (USCYBERCOMM) for offensive capabilities. Consequently, South Korea created a Cyber Warfare Command in 2009. This was also in response to North Korea's creation of cyber warfare units. The British Government Communications Headquarters (GCHQ) has begun preparing a cyber force, as also France. The Russians have actively been pursuing cyber warfare. In 2010 China overtly introduced its first department dedicated to defensive cyber warfare and information security in response to the creation of USCYBERCOM. The race is thus on across the world.

Lately, **advanced persistent threats (APTs)** have wholly transformed the threat landscape. These are the state – sponsored campaigns targeted against Critical information infrastructure, especially communication network. APTs are sophisticated, targeted and prolonged attempts of intrusion and information theft using a wide variety of techniques, including SQL injection, malware, spyware, phishing and spam. Attacks led by the APTs infiltrate into sensitive systems, such as email servers, and they are designed to remain undetected or hidden from the administrators— sometimes for years. Since APTs are highly advanced, planned and executed meticulously, they hardly leave any trace, and therefore render traditional means of security and forensics incapacitated. The APTs can be used to disruption of industrial operations or even destruction of industrial equipment.

5. Importance of Securing Communication Networks

- The communication networks **form the basis of digital ecosystem**. For ensuring **overall cyber security**, it is imperative to secure communication networks from all types of possible threats – human as well as natural.
- **National Security**: Disruption of communication networks can disturb stability of country especially if communication networks supporting critical sector are targeted. The failure of communication network has potential to cripple security agencies rendering them ineffective. This can be understood by following-
  - Security agencies follow hierarchy and have certain chain of commands. For exchange of information such as intelligence– both horizontally and vertically, the security forces and agencies use communication technologies such as wireless handsets. The working of these devices requires robust communication network infrastructure. The attacks on such communication infrastructure could have far reaching implication on capabilities of securities agencies.
  - The gathered intelligence by local intelligence officer cannot be communicated to competent decision-making authorities in wake of such failure. The resulting delay in decision making would prevent forces and authorities taking timely corrective actions.

> **Case of Estonia**
>
> The intensity of the impact of communication network failure in Estonia which is one of the most densely connected countries and has pioneered facilities such as e-government, Internet voting and online banking transactions (98 percent). India is also aspiring to follow the same path.
>
> In 2007, Estonia witnessed massive Internet traffic, which brought down the networks of its banks, broadcasters, police, parliament and ministries. The scale and timing of this attack targeted at the core of its information infrastructure. It practically brought Estonia to a standstill.

- **Growing Interdependencies:** All the critical sectors, such as transportation, communications and government services, depend upon the power/electricity sector for their basic requirement of electricity supply, which powers the railways, airports and communication systems such as switching centres or telephone exchanges. In an interdependent function, the power/electricity sector itself depends on transportation for