Advanced Persistent Threats (APT) are types of cybercrime threat actors that aim to gain unauthorised access to, and remain in, systems as a long term presence staying undetected for as long as possible.

They are often but not always nation state sponsored criminals targeting a country's critical infrastructure, intellectual property, or networks.

An APT may be involved in cyber espionage to steal:

- military information about the target country,
- intellectual property such as trade secrets or patents, or
- information about key personnel involved in government or research.

An APT may be involved in compromise, destruction or disruption of critical infrastructure such as:

- Water treatment plants,
- Communications networks, or
- Power grids.

An APT may target employee information to steal or disrupt such as:

- Identity information,
- banking data, or
- research databases.

An APT may seek to gain funds to further their activities by using:

- Business Email Compromise scams,
- Ransomware,
- Investment scams,
- Cryptojacking.