Cyberterrorism is a controversial term with no clear definition yet. However, it can be understood as the use of the Internet to carry out violent activities that result in or threaten the loss of life or substantial physical injury to accomplish political or ideological advantages through threat or intimidation

Threats posed by cyber terrorism:

cyber terrorism poses critical security threats to the world. The CIs, like nuclear installations, power grids, air surveillance systems, stock markets and banking networks, are dependent upon cyberspace. This functional dependence has made CIs vulnerable to Cyber terror attacks and increased the scope for Cyber terror footprints exponentially. Most CIs globally are poorly protected. Therefore, Cyber terror attacks on CIs can cause egregious damages to the society. Further, today there is a persistent threat of sensitive information of national interests being stolen by terrorists, destruction of computer networks or systems superintending the functioning of CIs.

Objectives of Cyber Terror Attack:

Cyber terrorism is based on specific objectives, such as:

1. Like, air traffic, military networks, financial and energy systems, telecommunications and others, to cause physical devastation.
2. Cause disruptions sufficient to compromise the industrial and economic operations of a country. A Cyber terror attack thwacks a large part of the world population and causes monetary disorder and loss of data.
3. Cause physical injuries, loss of lives, explosions, crashing of aircraft and other aerial vehicles, theft of technology and privileged information.
4. Move beyond the realms of destruction and send a signal of ferocious disruption and fear to governments.