**Combating Cyber Terrorism**

Some problems that threaten the security of the individual and the State arise with the rapid growth of information technology. The focus has to be turned on the Critical Infrastructure Protection by all nations.

Common among the infrastructures are the essential services like electricity, telephone connections, railway and traffic control, gas or oil transportation and so on. As infrastructures depend on IT their vulnerability has increased manifold.

As a concept Critical Infrastructure Protection or CIP was projected first in the USA in 1996 by the President, Bill Clinton, as a result of a high level commission report. The report proved the susceptibility and necessity of taking a closer look at protection provided to high priority infrastructures. George Bush was set up a special board after the September 11 attack on the World Trade Centre of USA.

Most of the developed and developing nations all over the world have woken up to the situation now and several countries like Canada, Sweden, Germany, Holland and Switzerland are falling in line with the US. There is a wing under the Defence and Intelligence Ministries of our Government and a special task force has been created for the purpose of counteracting cyber terrorism. Some of the Governments have multilateral agreements with other nations for sharing the resources. Although there is no global forum to tackle such issues our country has an exclusive forum to consult USA and fight back the menace of cyber terrorism. But the European Union Countries have a common federation.

Our country has earlier faced a problem with Pakistan when Pakistan-backed defence hackers jammed our troop movement

Communication system, giving false commands. Hence we need to set up an action plan on a war footing. The national security council is already in touch with several ministries to draw up plans. But the gap between our planning and implementation has always been long. Cyber space surveillance is on top priority. The paramilitary forces should be trained to provide security to agencies developing critical software applications. The vulnerability of cyber attacks and the cascading effect of critical interdependence infrastructures falling prey to this menace needs to be guarded against. All such organizations need to coordinate their cyber protection security and work in tandem.

We are country which has already left its mark in the software world and our software prowess should be geared up for research and analysis. An emergency response strategy should be set up and it should be activated in case of need. We have a very advanced set-up in the Pune- Centre for development of advanced Computing (CDAC), which has successfully developed a parallel computer. This set-up should be the model agency and it should be given charge for developing critical software to tackle cyber terrorism. Terrorism is any mode and method needs to be given a deathblow. What is needed is a unified effort to combat cyber terrorism.