CYBER TERRORISM

World **W**ide **W**eaponisation!

Amaresh Pujari, IPS
Inspector general of police (Training) ,
Tamilnadu Police, Chennai

==========

"An invasion by armies can be resisted but not an idea whose time has come. In fact, nothing is more powerful than an idea whose time has come. "

- -Victor Hugo

"Cyber Terrorism" is an idea whose time has surely come !

The excitement was palpable in Football's very own country this year after Brazil pipped USA to host the Olympics in 2016. The Brazilians could feel their country moving up quite a few notches in the comity of nations after their successful bid to host the games . The entire country was enveloped in the luminous afterglow of its stupendous success in bringing the games to the country for the first time ever. And then, it happened.. As if to extinguish the afterglow, the main power grid of the country crashed plunging more than half of Brazil into complete darkness. The outage, worst in the country's history, made millions of people suffer without electricity, especially in the major southern cities including Sao Paulo and Rio de Janeiro. Thousands of people found themselves trapped in immobile elevators and subway trains. Cars were forced to nose through intersections made dangerous by non functioning traffic lights. Police was called up and deployed to combat widespread nocturnal crime wave.

What caused the outage ? The Brazilian energy officials had no ready answers. Even though some officials tried to blame it on weather, the electricity companies were not in agreement as no physical damage to the grid could be detected. Further investigation revealed that the national grid had become short of 14,000 megawatts suddenly leading to the blackout though the officials were at a loss to explain as to how did it happen. Cyber security experts, however, recalled that in 2005 and 2007 the country had faced power outages due to the disruption of national grid caused by cyber attacks . They concluded after their investigation that the recent outage was also a result of sophisticated cyber attacks by hackers . What the world witnessed was the latest (and surely not the last) act of "Cyber Terrorism" ! US President Barack Obama, while recently launching a new Cyber Security Initiative (CSI) said without naming Brazil , "*We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness*" The American President also said in the same speech "*It is now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation*."

Just a few days before, CBS in USA broke the news story of penetration of top secret Military Network of Pentagon by some unknown persons/groups after bypassing the state of the art firewalls and encryption codes ! The story, which has not been denied by Pentagon has caused widespread alarm amongst military and cyber security experts .

In 2007, when inspite of opposition by a powerful neighbouring country, Estonian government relocated a War Memorial from a prime place to an obscure one, hackers presumably based in the neighbouring country, totally disrupted the functioning of Estonia's Internet for two weeks by launching massive cyber attacks .

There have been several instances of official and government websites of India having been defaced by some terrorist groups inimical to India , to propagate their aims.

From that fateful day in 1973 when two scientists Vinton Cerf and Robert Kahn working in ARPA (Advanced Research Project Agency) of US Military established a communication link between two computers, thus gifting humanity the Internet (it was called ARPANET then) the Internet has surely come a long way . And so have the criminals and terrorists who misuse this great technological marvel for their own selfish and nefarious purposes, making the world loose billions of dollars annually to cyber criminals and endangering the lives and properties of millions of people by acts of cyber terrorism.

The word "Cyber Terrorism" is of recent vintage and was coined by computer whiz Barry C. Collin. A widely acceptable definition of cyber terrorism is " a criminal act perpetrated by the use of computers and telecommunication capabilities resulting in violence, destruction and/or disruption of services to create fear within a given population with a goal of influencing a government or population to conform to a particular political, social or ideological agenda." According to the U.S. Federal Bureau of Investigation, " Cyber terrorism is any premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by sub-national groups or clandestine agents."

Can all cyber crimes be called as cyber terrorism ? Not really. It is pertinent to note that while all cyber terrorism cases are cyber crimes, not all cyber crimes can be called acts of cyber terrorism ! Only those cyber crimes which are politically or ideologically motivated qualify to be called as acts of cyber terrorism In the year 2000, an engineer working in Maroochy Shire Waste Water Plant , Sunshire Coast City, Australia subverted the computers of the company which controlled its operations , to vent out his feelings of frustration with the company's promotion policies. The result was release of millions of tons of sewage water into parks and seacoast of the city causing massive environmental damage. As the act was not ideologically or politically motivated , it was not, rightly so, called an act of cyber terrorism. It was a grave cyber crime, never the less !

The main aim of cyber terrorists today is to cripple critical infrastructure of a country by cyber attacks to further the causes they espouse for as a terrorist group. In their wish lists are critical infrastructure like telecommunications, electric grids, transportation networks, banking & finance, water supply , fuel production & supply chains, military complexes , government operations .and emergency services.

In order to wreck havoc with the critical infrastructure of a country, the cyber terrorists use a variety of sophisticated tools to perpetrate their attacks. As discussing the technical

details of such tools shall be beyond the scope of the present article, I shall refrain from doing so. However, it shall be worth mentioning that cyber terrorists are increasingly making use of tools like DDOS (Distributed Denial of Service), Phishing, Vishing (VOIP Phishing) , Buffer Overflow, IP Spoofing etc. Out of these tools, DDOS is emerging as a favourite tool of the perpetrators. In the last few years, the cyber attacks have grown both in sophistication and geographical reach. There has been a massive surge in the number of attacks as well. There are several reasons for this. Many terrorist groups view these attacks as an asymmetric, low cost & low risk warfare against powerful nations. The easy availability of malicious software in the Net, increasing technological skills of terrorist groups, anonymity provided by the Internet and ever increasing networking of critical infrastructure in developed and developing countries are some other reasons for the massive upsurge witnessed in cyber attacks in the last few years.

The question most often asked is how vulnerable are we to the threat of cyber terrorism. A country's vulnerability to cyber threat is directly proportional to the dependency of its critical infrastructure on networks. In India, our critical infrastructure like power grids, telecommunication, banking etc is already highly network dependent and hence quite vulnerable. Many terrorist groups are in pursuit of capabilities of penetrating these networks . According to a report submitted by CRS (Congress Research Service) to US Congress, " *the terrorists are exhibiting similar level of web knowledge as by US government agencies*. " The same report mentions that Al-Qaeda has opened web forums for its cadres to impart knowledge in hacking of computers ! The use of cyber technologies by intelligence agencies of some countries for not only snooping but also for compromising the critical infrastructure of other countries adds an entirely new dimension to cyber terrorism.

What can be done to counter the grave threat that looms large on us ? A comprehensive Cyber Security Audit of our critical infrastructure shall be a good step to begin with . This shall help us in identifying our vulnerabilities and thus in plugging the same. Designing and implementing more stringent Access Control Systems and Encryption Standards, augmenting our Tech-Int capabilities to thwart a cyber attack before it happens and educating the users of critical infrastructure for adopting safe practices are some ways to combat the threat. However, we need to remember that while we have to confront the entire range of security vulnerabilities, the cyber terrorist has to exploit just one vulnerability and achieve his mission !

The time of cyber terrorism has come . And so has the time for us to combat it by all the means at our disposal. Let's watch out _ the next act of terrorism may not involve a bomb but a byte !

AMARESH PUJARI
amarpujari.ips@gmail.com

Article Published in the TN Police Sesquicentennial Anniversary Souvenir