Cyberspace-A new front of war

The incidents of war happened in the real world is mirrored in cyber space, given the recent incidents of hacking of government websites by state or non state group of hackers for political, military, espionage purposes. As the world becomes increasingly dependent on the internet and increasingly connected through it, another threat is beginning to loom large – Hacking and defacement of Government website and other cyber infrastructure. Recently, a hacker group from Pakistan calling itself as 'Pakistan Cyber Army' made a mockery of the country's cyber security by infiltrating into the CBI website supposed to be one of the most secure websites as it is maintained by National Informatics Centre, reported to be employing strict cyber security measures.

Today the CBI's website, connected to the command centre of world police organisation — Interpol — 24×7 has been hacked, but what about tomorrow? What is the guarantee that next cyber attack may take place on something more critical, like the power grid?

The hacking of Government websites is not new and in past too the hackers group with patronage of government establishment successfully penetrated the highly secure websites belonging to Government of India. However, it is not a one sided affair as there are hacker group from either side who in retaliation or out of political or strategic compulsion hack each other websites. It is no more a secret that our neighbors with whom we have troubled relations find it politically and strategically useful to have arms-length relationship with hackers. One blogger has written that the hackers claim that they are sometimes paid secretly by the Chinese government — a claim the Beijing government denies. There is a number that circulates the web (not confirmed data) that the Chinese government pays to up to 50,000 highly skilled military hackers to use the Internet for specific purposes that are defined by the government officials (cyber expert James Mulvenon told a congressional commission in 2008). The hacker community is diverse with different purposes, for example; (a) Script-kiddies – people, teenagers who are doing it for fun or to show off or to see what they can actually accomplish (b) Criminal Hackers-criminals who are just hacking for financial gains, (c) Patriotic hackers – people that hack websites out of a kind of nationalistic feeling (d) Government backed hackers; There are hackers that are probably employed by the government, probably by the military and the security agencies that are used to attack specific targets for political reasons and last but not the least there are hackers in the military that are thinking about how cyber would be used in an actual military conflict.

The category to which the Pakistani Hackers group who hacked the CBI website is not difficult to imagine. The Pakistan Cyber Army, claim that the Indian Cyber Army had allegedly hacked into the oil and gas regulatory website in Pakistan. The Pakistan Cyber army in retaliation has therefore also hacked the website of CBI. So, the group clearly fall under point (c) mentioned above i.e. patriotic hackers, however it is equally true that they have the government sponsorship too.

As far as the law is concerned, we have Information Technology Act, 2000 on statute book which deals with hacking, particularly the government owned website, say Section 66 (punishing the offence of hacking) read with Section 70 Information Technology Act (punishing access or attempt to access the protected systems). However, these sections are not effective as far as cross border cyber crimes are concerned, more so if one traces the digital footprints of hacking to hostile countries with which we have troubled relations and do not have bilateral treaty. The only solution seems to be is to first identify the critical and vulnerable cyber infrastructure, upgrade their security, setting up of a cyber command structure with experts in cyber security and warfare to continuously look at the cyber security aspects

and suggest measures to upgrade the security, make preemptive cyber attacks against enemy cyber infrastructure and last but not the least thwart any similar cyber attacks emanating from foreign land.

The need for international cooperation on these critical issues and the role that international law can play in containing the threat cannot be undermined. As far as the cyber espionage is concerned, there is no known international treaty on this issue, however, on the criminal front there is a convention on cyber-crime drawn up by Council of Europe which is the first international treaty seeking to address Computer crime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. However, the problem with this convention or treaty is that most of the major players including India itself have not signed it which could have gone a long way consistent legal enforcement standards across national borders about dealing with instances of cross border cyber crimes. As an alternative to the aforesaid convention, as a short time security measure we can enter into treaty with the Pakistan and China like the one we have with Pakistan to not attack each other nuclear installations, in similar manner we can agree to not launch cyber attacks on each other identified critical cyber installations.