

Indo-Israeli Cyber Warfare Against Pakistani Nuclear Program

Farzana Shah | BrassTacks

After sea, land and air warfare, traditional arch rivals India and Pakistan are now facing each other in another arena. With evolution of technology over the period another kind of war has been started by Indians with Israeli help against Pakistan since last few years and that is Cyber warfare.

Cyber warfare is complex, more penetrating and detrimental than conventional warfare, fought on cyberspace using different tactics like Cyber espionage, Web vandalism, Gathering data, Distributed Denial-of-Service Attacks, Equipment disruption, attacking critical infrastructure, Compromised Counterfeit Hardware etc. The Internet security company McAfee stated in their 2007 annual report that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

Like any conventional threat, cyber warfare is rather new battle field for Pakistani government and people alike. India has all the reasons to use this as a weapon against Pakistan, but more recently Israel has joined hands with Indians in this war against Pakistan.

Propaganda, Cyber espionage, Web vandalism and information gathering are known cyber threats for Pakistani security institutes and government offices. Now there are reports emerging that Indian and Israelis are taking these known cyber threats to next level by using money, talent and technology to defame Pakistan and its nuclear program.

How eagerly Indian wanted to gain an edge in cyber warfare technology is evident from what Indian Naval Chief Admiral Sureesh Mehta told StartPost; “The Indian Armed Forces are increasingly investing in networked operations, both singly and a joint fashion. We cannot, therefore, afford to be vulnerable to cyber attacks. Information Technology is our country’s known strength and it would be in our interest to leverage this strength in developing a formidable ‘offensive’ and ‘defensive’ cyber warfare capability. Harnessing the gene pool available in academia, private industry and the younger generation of talented individuals is imperative.”

Statement of Indian Naval Chief is a further endorsement of our assessment about Indian designs against Pakistan and its security establishment. Clearly India has offensive cyber warfare plans. Naturally these plans will be against Pakistan (as the history of both the countries proves), although Indian military establishment and political leadership used Chinese threat as an excuse for introducing new war tactics and systems in Subcontinent.

The Indian Army conducted a war game called Divine Matrix in March 2009.

The most interesting aspect of this exercise was the scenario simulated by Indian military in which China launches a nuclear attack on India somewhere in 2017. The purpose of the exercise was to describe that how China will launch a cyber attack before actual nuclear attack to take on India. On the other hand Chinese were astonished by the simulated Chinese nuclear attack on India. "We are surprised by the report. Leaders of China and India had already reached at consensus that the two countries will not pose a threat to each other but rather treat each other as partners." Foreign Ministry spokesman Qin Gang expressed his views on Indian cyber warfare exercise.

In reality both China and India have been in negotiations since 2004 to boost their economic trade and cooperation in various other fields including defense. Both countries have also conducted military exercises as well. In the backdrop of all this and renewed cooperation between two countries it is very unlikely China would go for a war and that too a nuclear one whereas Pakistan is the only country against whom India has any possibility to go for a nuclear war over any of multiple disputes like Indian water aggression against Pakistan and Kashmir issue.

Limited cyber skirmishes have already taken place between Indian and Pakistan in 2008 when a group of Indian hackers defaced Pakistani website of ministry of oil and gas, government of Pakistan. Pakistani hackers in retaliation defaced many Indian websites. After these counter cyber attacks now Indians are looking to adopt "joint fashion" for cyber warfare against Pakistan with help of Israel.

According to reports Israel recently established a cyber task force for cyber warfare against Islam and Pakistan, besides harming Palestinian cause. A budget of \$ 1,50,000,00 has been also allocated to this force to carry out various digital espionage and information gathering operations from various strategic offices of government of Pakistan.

Breaching network security is one aspect of all this cyber war against Pakistan. In a new development Israel has also setup a huge workforce of writers on internet and is still increasing its strength by appealing more persons to join in. Primary task of this force would be to wage propaganda war against Pakistan and its nuclear weapons and armed forces.

Israelis are doing it since long time. Hebrew websites and magazines have been targeting Pakistan by orchestrating near to impossible scenarios about Pakistan's nukes to deceive world that these are going to fall in the hands of Al-Qaeda. Israelnationalnews.com, IsraelNN.com, and Arutz-7's Hebrew newsmagazine are few to name among these media outfits where Israelis are spiting their venom against Pakistan.

Israeli government first tested these cyber propaganda tools during operation Cast Lead (brutal military operation in Gaza in 2008) when bloggers, surfers and writers were asked by ministry of foreign affairs of Israel, through www.giyus.org (Give Israel You United Support), to promote words like "holocaust", "promised land" and "murder of jews" on social networking and blogging websites like Face book, Twitter, MySpace, BlogSpot, wordpress etc. Israeli government went to an extent to give written messages which were

to be posted on aforementioned websites as if they were personal responses or views of citizen of any country.

Israeli lobbies in US and UK waged similar agenda against Pakistan's nuclear program in the past through satellite news channels (like BBC, FOX) and news papers (New York Time, Washington Post). New tactics of using social networking and blogging websites on internet has certainly more probability to shape people's opinion about Pakistan's nuclear weapons as unsafe. This campaign was also launched from US and Western media when operation Rah-e-Rast was initiated in Swat and Malakand region. The target in that particular campaign was to defame Pakistani government and security institutions as inept and incapable to save the nation from terrorists.

Israeli cyber operation was resolutely counter by young Palestinian bloggers by posting millions of pictures and footages from GAZA over the internet. These photos and footages revealed evil deeds committed by Israeli forces in Gaza during operation Cast Lead. However these Israeli and Indian cyber evangelists were successful in scaring ordinary masses in and outside Pakistan by posing Taliban threat to taking over Islamabad out of proportion. The real intention behind all this Taliban Hoopla was to tell the world that Pakistani nuclear weapons are about to fall into Taliban's hand.

Like their Israeli counterpart, Indian government also took part active part in this campaign against Pakistan. Indian premier went on saying that some of Pakistani nuclear installations are already in Taliban control. This further sanctioned scare created by "paid" surfer of internet.

Israel helps India against Pakistan and Indians are also waging this propaganda war against Pakistan but on different axes. India's current focus, after Pakistan's security establishment, is to deceive and confuse locals of Pakistan's Northern Areas where Pakistan is about to build three mega dams to fulfill its needs. Indian think tanks, websites and discussion forums are constantly pointing out that Pakistan is going to build dams in disputed territory in Diamir, Bonji etc. whereas the matter of fact is India is building dams illegally on Pakistani rivers whereas Pakistani plans are all about Pakistan's own river.

Apart from all this Cyber espionage, Web vandalism, propaganda enemies of Pakistan are adopting more complex to beat cyber operations like information gathering and equipment disruption. US pressurized Pakistan to take dubious Permissive Action Link boxes to be put on its nuclear program to prevent "unauthorized" detonation of bombs but Pakistan quite sensibly refused these locks which are said to be impossible to beat. This is one example of extent to which Pakistan's enemies are pushing against its nuclear program in Cyber warfare.

Lethality of cyber warfare become palpable by the fact that till April 2009, pentagon has spent more than 100 million dollars in 6 months to fight against cyber attacks on its different systems. Money spent on propaganda operations are apart from this.

Pakistan must build a dedicated professional force to fight against all Cyber warfare tactics. A special wing inside armed forces must also be raised to counter advanced Cyber threat from Israel, India and US.

www.pakistanyouthmovement.com