Propaganda & Warfare in Cyber World: Pakistan's weak flank

By: Farzana Shah

After sea, land and air warfare, traditional arch rivals India and Pakistan are now facing each other in another arena. With the help of Israelis, Indians have launched another war on a new axis against Pakistan – Cyber Warfare.

In certain aspects, cyber warfare is complex, more penetrating and detrimental to the national security than conventional warfare. It is fought on the cyberspace using weapons like Cyber espionage, web vandalism, gathering data, Distributed Denial-of-Service Attacks (DDOS), equipment disruption, attacking critical infrastructure, compromised counterfeit hardware, virus and worm release. Potential targets include;

- Emergency services
- Financial markets and bank systems
- Power grids
- Water and fuel pipelines
- Strategic Weapons systems
- Communication networks (Military / Civil)
- Industrial and Engineering Complexes
- E-Government services (internet based utility services, web servers)

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.

Global Cyber Wars:

China and US are spearheading cyber war at global level with dozens of cyber attacks on each other's critical IT infrastructure. Both countries are spending millions every year in order to fight against cyber attacks.

Lethality of cyber warfare becomes palpable by the fact that till April 2009, Pentagon had spent more than 100 million dollars in just 6 months to fight against cyber attacks on its different systems. Money spent on propaganda operations are apart from this. In October 2010, US army created its first ever US army Cyber Command headed by a 3 star General.

ARCYBER headquarters will be located in the National Capital Region and will realign soldiers and civilians into essential ARCYBER headquarters positions. ARCYBER is the Army's service component command to US Cyber Command, a sub-unified command under US Strategic Command to operate the Defense Department's information resources of 15,000 computer networks across 4,000 military bases in 88 countries. The total command strength of 21,000 soldiers and civilians will be located around the globe.

Not only US army but US navy and air force have also setup their respective cyber commands to tackle cyber threats from hostile enemies (read China).

This aggressive cyber warfare capability build-up by US has triggered serious restiveness among Chinese intelligentsia and media. The People's Daily, a Chinese government-run newspaper, said in an editorial:

"The US was the first country in the world to introduce the concept of cyberwar; it has introduced and developed a new kind of army, a cyber army, and even set up a hacker brigade. US intelligence agencies can, through technical means, fully monitor, follow and erase online information harmful to the US' national interest. It is really ridiculous that under such circumstances, it demands other countries to allow the free flow of information on the net."

From Pakistan's perspective, unlike any other conventional threat, cyber warfare is rather a new battle field for Pakistani government, its intelligence agencies and citizens. Pakistan is not geared nor prepared to respond to this latest threat. India has all the reasons and resources to use this as a weapon against Pakistan, but more recently Israel has joined hands with Indians increasing the threats for Pakistan.

Cyber espionage, web vandalism and information gathering are known cyber threats to its security establishment and government. Apart from these cyber threats, recently cyber world has been used ruthlessly as a part of propaganda warfare by Indo-Israel alliance. As per various media reports one can be sure that Indians 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 Indians wanted to gain an edge in cyber warfare technology is evident from what Indian Naval Chief Admiral Sureesh Mehta told to Start Post;

"The Indian Armed Forces are increasingly investing in networked operations, both singly and in 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,"

Maj. Gen. Rhett A. Hernandez assumed command of the US Army Cyber Command from Lt. Gen. Kevin T. Campbell, who is also the commanding general of US Army Space and Missile Defense Command, as well as US Army Forces Strategic Command.

Statement of Indian Naval Chief is an endorsement to the media reports that India has offensive cyber warfare plans. Pakistan is the natural target though Indian military establishment and political leadership used Chinese threat as an excuse for introducing this new war theatre in the region.

Indian endeavor:

Recently in August this year (2010) the Indian government decided to recruit and form cyber army of software professionals to spy on the classified data of hostile nations (read Pakistan and China) by hacking into their computer systems.

A strategy was drafted for this purpose earlier in a high level security meeting on July 29, 2010, chaired by Indian National Security Advisor Shiv Shankar Menon and attended by the director of Indian Intelligence Bureau (IB) as well as the senior officials of the telecom department, IT ministry and RAW.

US army cyber command centers

According to the strategy drafted in the meeting, India will recruit IT professionals and hackers who will be assigned to be on the offensive or to launch pre-emptive strikes by breaching the security walls of enemy's computer systems. The most important factor to note is the involvement of the Indian National Technical Research Organization (NTRO) along with the Defense Intelligence Agency (DIA) which will be responsible for creating these cyber-offensive capabilities. It is to be noted that NTRO is a key government agency of India that gathers technical intelligence while DIA is tasked with collating inputs from the Navy, Army and the Air Force.

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

The most interesting aspect of this exercise was that Indian Military simulated a scenario in which China launches a nuclear attack on India somewhere in 2017. The purpose of the exercise was to describe how China will launch a cyber attack on India before the launch of the actual nuclear strike.

Chinese were not amused by this Indian war gaming and simulation.

"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's spokesman Qin Gang expressed his views on the Indian cyber warfare exercise. But recently the Indian Army chief and the ex-chief has clearly threatened that there can be a nuclear war in the region (a veiled message and threat to both Pakistan and China).

Indo-Israeli Cyber nexus against Pakistan:

Though no large scale cyber attack has been reported yet in Pakistan but limited cyber skirmishes have already taken place between Indian and Pakistani hackers in the recent years. In 2008 a group of Indian hackers defaced a Pakistani website of Ministry of Oil and Gas. Pakistani hackers, in retaliation, attacked and defaced many Indian websites. This year also many websites were defaced by hackers on both sides.

This is where the interests of both India and Israel converged. According to reports, Israel has recently established a cyber task force for Cyber Warfare against Islam and Pakistan, besides harming the 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 against Pakistan.

Propaganda warfare and Cyber Space:

In a new development, Israel has also setup a huge workforce of writers on the internet and is still increasing its strength. Primary task of this force would also be to wage propaganda war against Pakistan and its nuclear weapons and armed forces. Israelis are waging a net based disinformation and psychological war against Pakistan since long. Hebrew websites and magazines have been targeting Pakistan by orchestrating near to impossible scenarios about vulnerability of Pakistani nukes and the

"possibility" of their falling into 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 the ministry of foreign affairs of Israel, through www.giyus.org (Give Israel Your 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 the extent to give written messages which were to be posted on the aforementioned websites as if they were the personal responses or views of the citizen of any country.

Israeli lobbies have been heavily exploiting their clouts in US and UK to wage propaganda wars against Pakistan's nuclear program through satellite news channels (like BBC, FOX, SkyNews) and news papers (New York Time, Washington Post). Disinformation campaign was also launched from US and Western media when operation Rah-e-Rast was initiated in Swat and Malakand regions. Taliban threat was so exaggerated that the perception was created as if Islamabad was about to fall to the Taliban! Indian government also took active part in this campaign. Indian premier took this disinformation war to new heights by saying that some of the Pakistani nuclear installations are already in Taliban control!

Israeli cyber operations were resolutely countered by the young Palestinian bloggers by posting thousands of pictures and footages from GAZA over the internet.

Final Thoughts:

In Pakistan, where billions are being spent on conventional forces and strategic nuclear assets, it is alarming to see the absence of any serious threat perception in the theatre of cyber warfare. The government as well as the armed forces have neglected this threat too long and now are hopelessly unprepared to respond to the new challenges. Pakistan will now have to respond to this threat on literal war footings.

There is absolutely no coordination, planning or understanding within various civil and military

A hacked Indian website

organizations and intelligence agencies responsible for cyber war and perception management through propaganda wars in cyber space. The whole existing system and organizations have failed to deliver in these times of great crisis and threats in the arena of cyber warfare due to reliance on old fashioned methods of information collection and processing. This should be clearly understood that in the modern world only those nations would have the advantage on the battle field, in both conventional and unconventional wars, which have fought and won the war in the cyber world first. The entire military equation in a war can be changed dramatically without even firing a shot, by controlling the critical infrastructure and perception of the target population through propaganda war in cyber world.

Weapons like E-bombs have emerged as a new threat to cripple the military communication infrastructure by producing massive electromagnetic pulse. Pakistan must start work on Transient Electro Magnetic Pulse Emanations Standards, known as TEMPEST in military parlance to counter electromagnetic-pulse bombs that can interrupt wireless signals.

Since Pakistan had faced interception of its vital highly secret data on military operations in FATA by India through its assets in the area therefore, it's a must that we should work on TEMPEST making it difficult for a cyber spy to hack into our systems minimizing the chances of interception of data transferred by defense agencies.

Pakistan now urgently needs to create a new centralized, aggressive and pro-active Command for Cyber and Information warfare under the office of Chairman Joints Chief of Staff. It is not too late yet. An entire flank of Pakistan's defense has been left unguarded and unprepared.