# C Y B E R S E C U R I T Y

# A WAKEUP CALL

**by**
**Prof. Dr.-Ing. Jameel Ahmad Khan**
*Former Chairman, Pakistan Engineering Council*
*Former Vice Chancellor, NEDUET*
**E-mail: profjakhan@yahoo.com**

If the president of United States complains that the growing number of attacks on their cyber networks has become **"one of the most serious economic and national security threats their nation faces"**, it certainly carries lot of weight. It reflects the stark truth that when technology is available, it could be used by any body.

In the recent past some extremely critical incidents took place in Pakistan demonstrating a complete break down of the cybersecurity. More alarming, however, is the deliberately installed hush-hush culture, which very successfully conceals the facts from the nation. In reality, it is simply a cover-up of the incapacities of our system. Are we prepared to learn?

It was disappointing to note that the 5 Member Abbottabad Commission constituted by the government regarding US incursion into Abbottabad on May 2, 2011 had no **subject matter expert** on board. There is a general impression that its long awaited report will remain shrouded in mystery. The hypothesis is that the key issue of cybersecurity management will remain unaddressed. Complete absence of any reaction on the part of the Ministry of Information technology and the National Response Centre for Cyber Crises, managed by the FIA, was extremely disappointing (Interestingly FBI of USA has been training FIA to combat cyber crimes).

The world has already ushered into an era of the so called **"Information Confrontation"**. This is strongly evidenced by the fact that even a country like US, occupying the **Information High Ground**, has been conducting several in depth studies such as

- Cyber Warfare – An Analysis of the Means and Motivation of Selected Nation States, Dec. 2004. (Pakistan has been covered in this study. However, it mentions that the Pakistani Military has not released any official publication on cyber warfare.
- Capabilities of the Peoples Republic of China to conduct Cyber Warfare and Computer Network Exploitation, Oct., 2009.
- Chinese Capabilities for Computer Network Operations and Cyber Espionage, March, 2012.

Additionally, US Homeland Security has come out with a series of reports and guidelines. These efforts are being adequately and timely supported by a chain of legislative exercises such as the Federal Information Security – Management Act of 2002 (FISMA). Organisations such as US – Computer Emergency Response Team (US – CERT) are in place to effectively manage cybersecurity. India has also realized that there is an immediate threat to their burgeoning IT industry and to their supervising of data acquisition company programmes that control national security – related industries, such as nuclear installations. The Indian Defence Information Agency (DIWA) was formed in 2003.

There is no dearth of material available in public domain related to cybersecurity, which patently indicates that the issue is multi-dimensional and has become a paramount global concern. **Where do we stand? Have we got a national strategy to secure our cyberspace? Have we got a programme aimed at cyber warfare?** In the face of the opaque conduct

observed by our government, it is very unlike by that these key questions will be answered satisfactorily. Therefore, there should be a move in the national parliament to discuss the subject threadbare. The evolution of information protection technology is galloping at a very fast pace. Private companies and individuals own a large percentage of the Internet and related business. It would be indispensable to develop a partnership between the government and private sector regarding “cybersecurity”. Their intimate cooperation will be vitally required for overseeing and monitoring the task of **continued vigilance**.

A common **Information Technology Platform** needs to be installed at the earliest as a **Cybersecurity Initiative** on the part of the government. The Draft National Policy (Revised) 2012, issued by the Secretary IT, Ministry of Information Technology, and posted on its website for comments, does mention that Overriding Principles used include preservation of National Security, Confidentiality and Integrity. Surprisingly, this formal statement has not been supported by any identifiable milestones or goals. Infact the subject of security of our national cyberspace should be assigned top priority, and treated exclusively with utmost seriousness, it urgently deserves.

**How long have we to wait?**