Headline	Collaboration, info sharing make good defence		
Date	20. Oct 2008	Language	ENGLISH
Media Title	New Straits Times	Page No	5
Section	Tech & U	Article Size	482 cm2
Circulation	158042	Frequency	Daily
Readership	512000	Color	Full Color
		AdValue	9953.34

Collaboration, info sharing make good defence

Boosting cyber warfare capabilities has become a key component of the defence strategy for many countries to protect their critical information infrastructure. But with technology advancements, keeping cyber attackers at bay is easier said than done. **Izwan Ismail** talks to two industry players.

■ **Professor Dr Mohamed Ridza Wahiddin, head of information security cluster, Mimos**

There is currently no foolproof system to combat cyberwar effectively. This is why some e-government and defence systems are still prone to attacks, despite the high protection systems put in place.

At Mimos, we are researching and developing a comprehensive solution to counter cyber attacks effectively. The project is called Ultimate Digital Fortress. It comprises the defence in-depth (layer-by-layer protection) method to protect information at rest, in motion and in use.

Besides that, Malaysia has already placed a strategy to maintain the country's e-sovereignty such as the existing National Cyber Security Policy to address the protection of Malaysia's CNII (Critical National Information Infrastructure). The implementation and co-ordination of this policy, which involves key national bodies and agencies, will offer the best protection.

Mimos is responsible for driving the NCSP Thrust 5 initiative, which is an R&D (research and development) for self-reliance, and also leads and co-ordinates national R&D information security activities with universities, which include developing and updating the national R&D information security roadmap, building bridges between local universities and relevant local industries, and promoting *Buy Malaysia First* efforts.

■ **Tom Fernandez, public sector director, Unisys**

The cyber warfare threat is no different from any other open economy threat. In fact, the impact is much greater to countries like Malaysia, which is outward-looking and an export-oriented economy.

The ugly side of cyber warfare is that one cannot really stop an attack. Unlike in the physical space, one cannot see the attacker coming in from afar and take the necessary precautions or security measures before the attack happens.

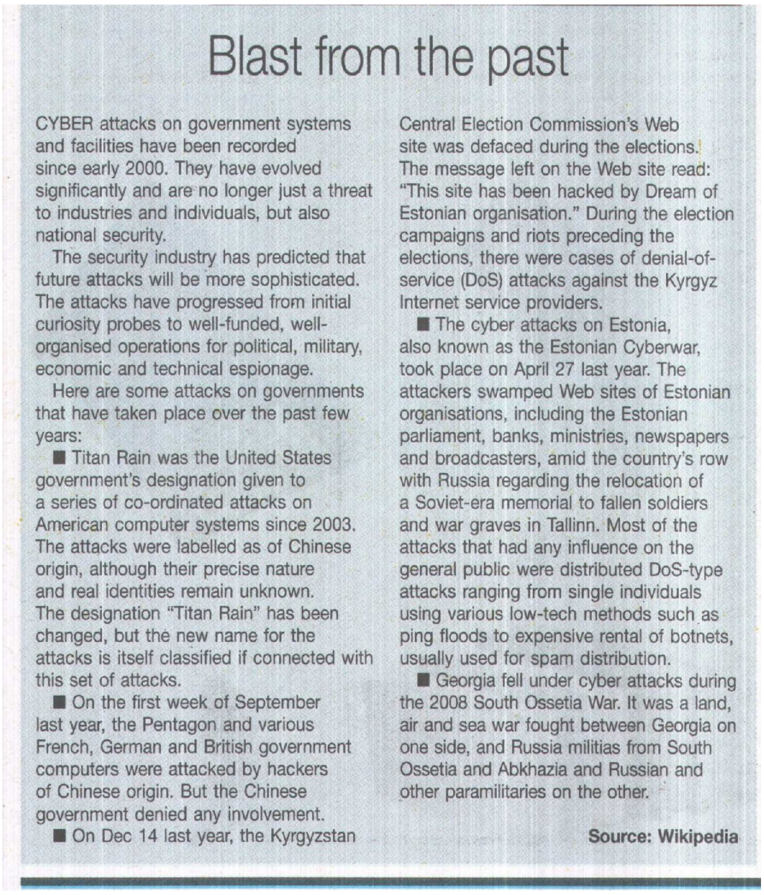
If one takes a look at cyber attacks, most always exploit loopholes that have existed for many months or years. One never sees attacks on new vulnerabilities. Often, negligence and the failure to address long-term loopholes have resulted in serious exploitations.

For Malaysia, there is a need to ensure co-ordinated multi-agency responses. Information or intelligence should be shared among all Government departments Oversight needs to be reduced and governance audits have to be carried out regularly to ensure all organisations running critical systems adopt the right protective measures.

Collaboration and information sharing at the international level is also key towards putting in place an effective early response system to counter the cyberwar threat.

Mohamed Ridza says Mimos' Ultimate Digital Fortress project aims to protect information at rest, in motion and in use.

Headline	**Collaboration, info sharing make good defence**
Date	**20. Oct 2008**
Media Title	**New Straits Times**



Blast from the past

CYBER attacks on government systems and facilities have been recorded since early 2000. They have evolved significantly and are no longer just a threat to industries and individuals, but also national security.

The security industry has predicted that future attacks will be more sophisticated. The attacks have progressed from initial curiosity probes to well-funded, well-organised operations for political, military, economic and technical espionage.

Here are some attacks on governments that have taken place over the past few years:

■ Titan Rain was the United States government's designation given to a series of co-ordinated attacks on American computer systems since 2003. The attacks were labelled as of Chinese origin, although their precise nature and real identities remain unknown. The designation "Titan Rain" has been changed, but the new name for the attacks is itself classified if connected with this set of attacks.

■ On the first week of September last year, the Pentagon and various French, German and British government computers were attacked by hackers of Chinese origin. But the Chinese government denied any involvement.

■ On Dec 14 last year, the Kyrgyzstan Central Election Commission's Web site was defaced during the elections. The message left on the Web site read: "This site has been hacked by Dream of Estonian organisation." During the election campaigns and riots preceding the elections, there were cases of denial-of-service (DoS) attacks against the Kyrgyz Internet service providers.

■ The cyber attacks on Estonia, also known as the Estonian Cyberwar, took place on April 27 last year. The attackers swamped Web sites of Estonian organisations, including the Estonian parliament, banks, ministries, newspapers and broadcasters, amid the country's row with Russia regarding the relocation of a Soviet-era memorial to fallen soldiers and war graves in Tallinn. Most of the attacks that had any influence on the general public were distributed DoS-type attacks ranging from single individuals using various low-tech methods such as ping floods to expensive rental of botnets, usually used for spam distribution.

■ Georgia fell under cyber attacks during the 2008 South Ossetia War. It was a land, air and sea war fought between Georgia on one side, and Russia militias from South Ossetia and Abkhazia and Russian and other paramilitaries on the other.

Source: Wikipedia