NEW STRAITS TIMES

Tuesday, August 28, 2012

Cyber warfare is no laughing matter

By Elina Noor

GAME ON: A country's right to self-defence will be challenged by questions like what responses are appropriate

Anyone with a computer and Internet connection can do some cyber damage

Elina Noor is ISIS Malaysia assistant director, foreign policy and security studies

COUNTRIES still fight over real things: oil and gas, nuclear warheads and barren rocks in the ocean barely visible at high tide. Sometimes, these tensions simmer. Sometimes, they threaten to grow into full-blown conflicts.

Always, countries reserve for themselves the full arsenal of situation-management options: diplomatic negotiations, economic sanctions and, if necessary, use of military force.

Increasingly, however, that list has begun to include an emergent, amorphous means; the cyber domain as a form of tactical and strategic weaponry in times of war and even in peace.

Cyberspace is the perfect extension of warfare for several reasons.

FIRST, the proliferation of network access nodes and faster connection speeds means that not only is it an expanding battlefield but it is one conducive for quick, agile and dynamic manoeuvres.

Because there is as yet no verifiable identification mechanism, it also offers the elements of stealth, anonymity and surprise.

SECOND, a cyber attack recruits an army beyond the uniformed but risks no boots on the ground.

Given the right price, a cyber war can in theory be waged by even script kiddies or hackers for hire (in reality, this is unlikely to happen given the sensitivity of national security operations). Even unwitting computer users can end up being part of a "botnet", or a zombie army (a network of Internet-connected computers whose security defences have been breached), to be commanded and controlled remotely to join a cyber attack.

THIRD, though itself intangible, the cyber domain is capable of effecting mass kinetic and physical destruction when a country's critical infrastructure is targeted. Imagine the consequences of a cyber attack that disables the air traffic control system or emergency services of a major city let alone a whole country, if only temporarily.

Sceptics play down the threat of a cyber war having the same devastating effects of a nuclear attack because any damage, death or injury would be indirect. The simple rejoinder is that it should not matter whether wide-scale damage or destruction is direct or indirect.

In the same manner that chemical, biological, radiological, and nuclear weapons provide a tactical means of destroying life or property, so, too, does the cyber domain afford another delivery system of warfare. Magnitude may not be an impressive measure of the potential of a cyber war right now but the same could be argued of the weaponisation of chemical or biological toxins in 1948 when the United Nations Commission on Conventional Armaments produced its authoritative definition of weapons of mass destruction.

There are undoubtedly many problems surrounding cyberspace and its application to warfare. For one, it is hard to define and terminology proliferates.

In the early days, there were "information operations", "computer network attacks", "computer network defence", and "computer network exploitation". Now, as this piece shows, the buzzwords are "cyber attack", "cyber war", and "cyber domain". The interpretation of each remains elastic.

That ambiguity ties into the blurred distinction between civilian and military application in cyberspace. The Internet, of course, came about with major involvement from the United States' defence research organisation, Defence Advanced Research Projects Agency.

Today, it is a common platform for information and interaction for about 2.5 billion people. The overlap pervades even the software market where programmes written primarily for the commercial market are tweaked for specific use by key government installations and systems.

The latter are often "air-gapped", or isolated from normal network vulnerabilities, but as any information security specialist will confirm, human beings are the weakest link and all it takes is a CD or USB stick to breach that buffer.

It is also true that the barriers of entry for a post-Apocalyptic vision of a cyber war remain very high. But remember Stuxnet?

The US-Israeli venture was, in the words of former CIA chief, Michael Hayden, "the first attack of a major nature in which a cyber attack was used to effect physical destruction". Someone, he said, had crossed the Rubicon.

In tests conducted on models of Iran's Natanz nuclear plant, the computer worm that was to be Stuxnet managed to reduce to rubble a replica of Iran's P-1 nuclear centrifuge by instructing it to slow down or speed up unpredictably.

There are conflicting reports as to how much the Iranian nuclear programme was set back by Stuxnet because the operation is still ongoing. While there have been no reports of wholesale physical destruction of a centrifuge yet, only that at least 1,000 centrifuges were disabled, the modelling tests showed that possibility remains.

It is a possibility that will continue to be tested, judging by the number of countries that have set up cyber warfare units in recent years. The United States now has USCybercom; China, a blue army; Germany, a top secret unit; Iran, the Passive Defence Organisation; and Israel, its Unit 8200.

Countries that have not yet organised an equivalent or are in the process of doing so recognise cyberspace as a priority national security agenda. And we talk about an arms race in this region.

As weapon and warfare, means and method, cyberspace is the ultimate dual-use technology. Crucially, it is also internationally unregulated.

What international lawyers already grapple with in relation to conventional armaments, cyberspace obfuscates 50 shades greyer. The scope of a country's right to self-defence will further be challenged by questions like what constitutes a cyber war and what kinds of responses are appropriate.

It is time for an international legal regime on cyber warfare and all its attendant precepts. The future is already present.