Kiwi experts raise fears of cyber warfare

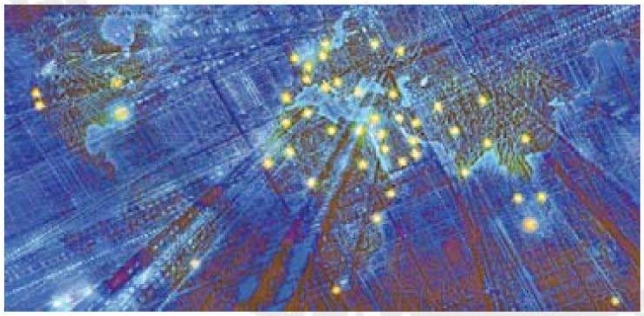
By LOIS CAIRNS

TWO NEW Zealand-based cyber warfare experts believe 2012 could be the year that attacks on information technologies cause global military conflicts and severe civilian suffering.

And they are warning that New Zealand needs to be better prepared.

Dr Andrew Colarik and Associate Professor Lech Janczewski, from Auckland University's Business School, have told an international information assurance conference in Malaysia that comprehensive national strategies must be mobilised so modern societies don't implode in the face of a cyber attack by other nations or terrorists.

In their paper, ''Developing a Grand Strategy for Cyber War'', the two say internet and communication technologies are particularly vulnerable, with a deployment window dramatically different from traditional conflicts. They say a cyber attack could be quickly prepared by a small group, be launched without warning from anywhere in the world, and escalate in a matter of minutes to shut down national infrastructures.



Cyber warfare: We need to be better prepared say two Kiwi experts.

That could include banking systems, water, power, transport, supply chains and commerce, leading to severe deprivation of basic facilities.

The pair, Department of Information Systems and Operations Management researchers, say attacks on such systems and infrastructures by third-party cyber criminals or state sponsors could spark full-scale military conflict if a Cyber War Doctrine is not developed.

''It sounds like a Space Invader type of thing . . . but the truth is that we are so reliant on technology that if anyone chooses to deliberately tamper with it, the effects can be catastrophic. And the longer we wait, the more likely it is that something will occur,'' Colarik said.

No country was properly prepared to handle the eventuality.

''There is no comprehensive national strategy in the world for handling a cyber war that brings the civilian infrastructure into alignment with military operations in a collaborative environment. It is imperative that governments, business and professional organisations are brought together, because they are responsible for a country's cyber infrastructure and national security.

''That, unfortunately, includes New Zealand, and a cyber war affecting even us in a little corner at the bottom of the world could happen at any time – even in 2012.

''We need to talk about the risks and come up with a plan for how we would respond. And we can't leave it all to the government because there are so many stakeholders who would be affected.''

Colarik said growing dependence on technology had created a fundamental weakness.

''Modern nations today are lacking a grand strategy for handling cyber attacks that co-ordinates all resources towards defending mutual security and prosperity. That's why we are urging the development of a doctrine that is inclusive of all stakeholders, can bring a decisive conclusion when attack happens, and will serve to deter future conflicts through a unified national security policy.''