Auckland graduate warns over possible 'cyber-jihad' attack
By Darren Greenwood
Computerworld, July 16, 2007
http://computerworld.co.nz/news.nsf/news/146450CACF6D47B9CC2573170010008D

The US business community is under threat from Islamic "cyberjihadis" and New Zealand is also at risk, claims Andrew Colarik

New Zealand companies and government face a small but growing risk of ‘cyber terrorism,’ and IT managers must prepare for it, warns Auckland-educated information security expert Andrew Colarik.

Ohio-based Colarik, who gained a PhD in informations systems security from the University of Auckland, believes the US business community and government is under threat from Islamic “cyber-jihadis” and claims New Zealand is also at risk.

Colarik was quoted in the US magazine InformationWeek this month, in a story concerning the programme for “electronic jihad” on the jihadi website Al-Jinan.org that uses the internet for online attacks and offers “cyberterrorism for the masses”.

However, the professors that taught him at Auckland University — Associate Professor Lech Janczewski and Professor Clark Thomborson — are divided over the actual threat organisations face, while noted sceptic George Smith points to similar warnings that have never eventuated.

Colarik says the ability of terrorist organisations to “retaliate via electronic warfare is growing significantly”.

“The reality is significant harm will occur to the New Zealand economy if it were digitally isolated from the rest of the world, even if for a short period of time,” he told Computerworld last week.

Colarik says cyber-terrorism uses the same methods as hacking. Economic terrorism is real and governments must make people aware of this reality so they react. This means government working with business to ensure systems are secure and IT managers are accountable.

“The key to all the discussions about cyberterrorism lies in the ability to replicate and automate new attack methods. One skilled person can create the tools for tens of millions to launch attacks of all kinds against Western civilisation.

“Politically, economically or pure hate-motivated digital attacks can be triggered by an ultra-minority of people in the world. Everyone needs to take this seriously or our troubles will only increase geometrically,” Colarik says.

However, the sceptical George Smith says people spreading news of electronic jihadists exaggerate the threat to attract attention to themselves and sell a product or service.

“It’s business-motivated,” the founder of the US-based internet company Globalsecurity.org told Computerworld.Even the reported cyberattacks against Estonia earlier this year were a non-event, he says, with nobody starving, getting shot or running out of money.

Associate Professor Lech Janczewski, of Auckland University, backs his former student, even co-writing a book on the subject with him, noting attacks from China against the US several years ago. While New Zealand was not in the front line, cyber-terrorists might use an open country such as ours for launching such an attack, he says.

Professor Clark Thomborson, a Professor of Computer Science at Auckland, stresses he is no security expert but doubts jihadis will target New Zealand, unless as a first-step to warn “larger, antagonistic nations.”

Instead, local IT managers must safeguard their businesses against “greedy attackers” whose damage could be “catastrophic to any business.” By securing systems against these, you likewise guard against jihadis, he says.

In his Dick Destiny blog (dickdestiny.com), Smith recently noted the constant warnings of cyber-attacks that never seem to happen, calling them “electronic Pearl Harbour” stories.

“The necessity for good network patches hasn’t changed,” he says. “Internet and network security remain important, but they’re a completely separate issue from terrorism in the real world. Pretending jihadis can make any kind of contribution to real world terrorism by downloading some point-and-click kiddie tool from a website is delusional,” Smith says.

Delusional or not, jihadist or greedy, in March 2008, New Zealand will join the international Cyber Storm 2 cyber security simulation, aimed at testing our critical infrastructure, including utilities, central government and telecommunications networks. It is organised by the US Department for Homeland Security, and also involving Australia, Canada and the United States.