Cyberpolice wrestle with command and control

By Liz Tay on Dec 6, 2010
http://www.scmagazine.com.au/Tools/Print.aspx?CIID=240622

No neutral parties in dynamic online world.

Traditional "command and control" strategies may be insufficient to combat cybercrime in today's dynamic online world, international law enforcement agencies heard this week.

Despite various efforts to facilitate international collaboration, high-tech crime fighters were challenged by jurisdictional boundaries and access to information.

Queensland-based political scientist Sohail Inayatullah said regulators were challenged with balancing the speed of progress and civil liberties - such as individuals' rights to privacy - with law enforcement needs.

In Sydney to address the Virtual Global Taskforce conference today, Inayatullah questioned the role of internet service providers, non-governmental organisations and the community in policing the internet.

Inayatullah disputed ISPs' claims that they were politically neutral information conduits. Former VGT chair Jim Gamble also said that technology was neutral earlier in the conference.

"The internet is just another public space," Gamble told the conference's 240 attendees from 23 countries.

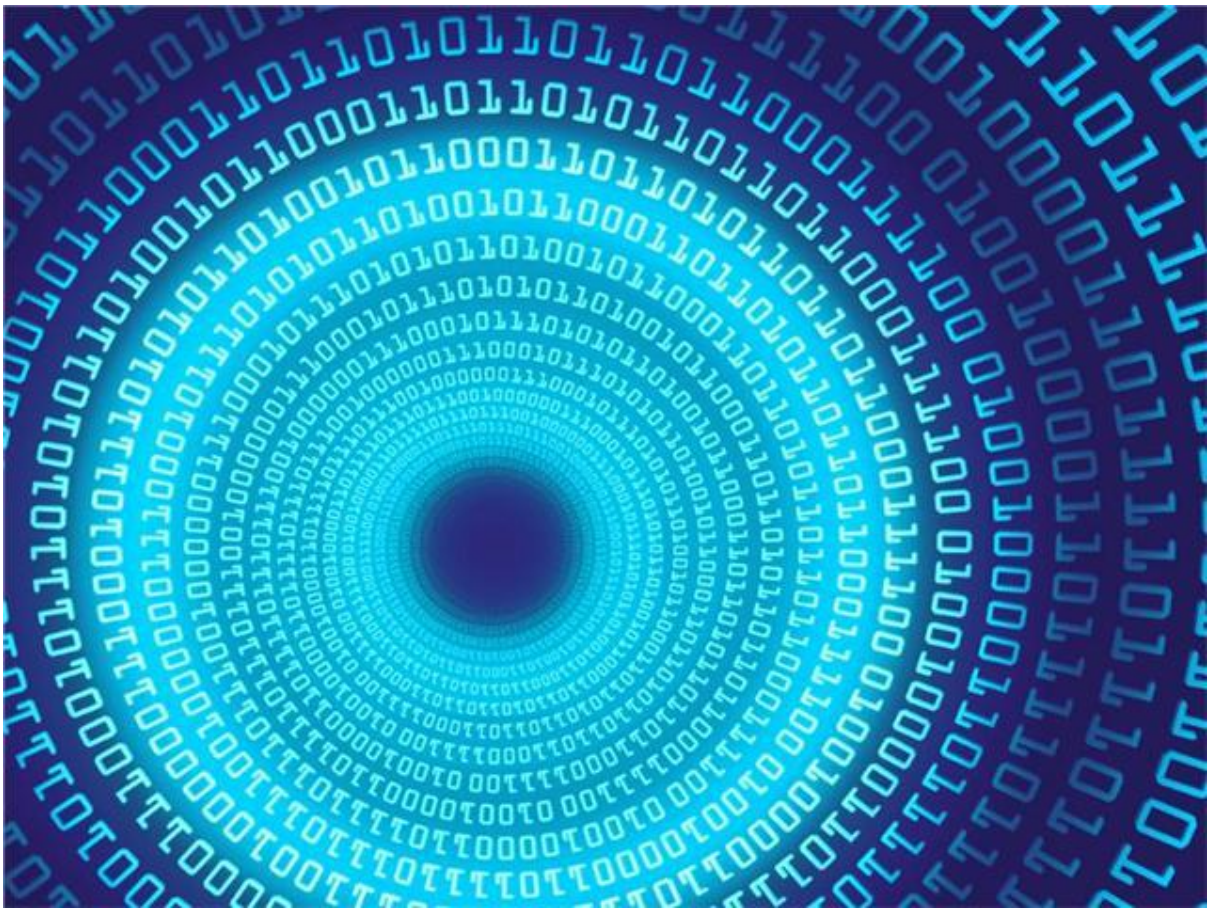
"The technology itself is neutral ... the defining character is the people that occupy it,"

But Inayatullah argued that cybercrime was "everyone's problem", likening the existence of malware-ridden - or otherwise unsavoury - pockets of the internet to the risk of inhaling second-hand cigarette smoke.

"Getting the balance right is very important," he told *iTnews*, declining to comment specifically on Labor's ISP-level internet filtering proposal. "I don't want a Big Brother society, but I don't want us to sink."

"Many service providers say, 'We're just the highways, not content providers,'" he said, arguing that roads still needed to be regulated to reduce the number of traffic accidents that occurred.

"They [ISPs] should be part of the solution. No technology is neutral; every space has politics in it."



http://www.itnews.com.au/Topic/233773,scitech-with-liz-tay.aspx

VGT attendees agreed that authorities needed to work closely with industry and international counterparts to combat crimes like the online sexual exploitation of children.

On Wednesday, the Australian Federal Police announced that VGT partners in six countries, software developers and Australian telecommunications companies had successfully shut down 230 child exploitation websites.

The so-called Operation Basket identified 30,000 customers in 132 countries, and led to hundreds of convictions in the US, 11 arrests in Belarus, and the arrests of five key members of a criminal organisation in the Ukraine.

Education and criminal psychology were also key strategies discussed at the conference. Australian Home Affairs Minister Brendan O'Connor highlighted the ThinkUKnow internet safety program for parents, carers and teachers of primary and secondary school students.

Gamble, who led the UK Child Exploitation and Online Protection (CEOP) Centre, blamed the initial explosion of cybercrime on a perception of law enforcement's technological incompetence.

He said online child sex offenders had no "fear of consequence" until initiatives like Operation PIN, for which the VGT set up a site purporting to host child abuse images.

Visitors who attempted to download images from the site were notified that they had committed an offence and that their details may have been captured and passed on to relevant authorities.

The site was uploaded to various addresses and taken on- and offline sporadically, Gamble said, explaining that its key purpose was to instil doubt in criminals' minds.

After Operation PIN was publicly announced in the UK, Gamble said several, worried anonymous callers contacted police, claiming to have stumbled on the site.

That was impossible, as Operation PIN was not actually active at the time, he said.