Foreign spies 'penetrate' US military networks

BBC News 23 March 2012

Foreign spies should be assumed to have penetrated the computer networks of the US military, American politicians have been told.

Security experts testifying to the Senate Armed Services Subcommittee said the penetration was likely so complete that attempts to curb it should stop.

Instead, cyberdefence should be about protecting data not controlling access.

The experts said the US should look into ways to retaliate against nations that had access to its networks.

In an open session, experts from the US National Security Agency and government labs said America had to change the way it thought about protecting Department of Defense (DoD) computer networks.

"We've got the wrong mental model here," said Dr James Peery, head of the Information Systems Analysis Centre at the Sandia National Laboratories. "I think we have to go to a model where we assume that the adversary is in our networks."

'Delayed drowning'

That change would mean spending less time shoring up firewalls and gateways and more time ensuring data was safe, he said.

Dr Kaigham Gabriel, current head of the Defence Advanced Research Projects Agency, likened the current cybersecurity efforts of the US DoD to treading water in the middle of the ocean.

All that did was slightly delay the day when the DoD drowned under the weight of maintaining its network defences, he said. The DoD oversees 15,000 networks that connect about seven million devices.

"It's not that we're doing wrong things, it's just the nature of playing defence in cyber," Dr Gabriel said.

The poor defences that the US military could muster were made weaker by its hiring system, said Dr Michael Wertheimer, director of research and development at the NSA.

Low pay, delays over promotion and wage freezes made it very hard for the US government to attract and keep talented computer security staff, he said.

The open session was followed by a closed debate about the capabilities the US was developing to hit back against those who had won access to sensitive networks.