Cyber terrorism

Continued from Page 1

Info. Tech. Dawn 10.2.02

Chivalry dictates that war should be waged "in accord with well-recognized formalities and courtesies". This rule allows ruses, but prohibits perfidy, which raises questions of whether modifying information in an enemy's computer which leads to casualties would be considered tactic or treachery. Moreover, neutrals are required not to yield telecommunications systems to either belligerent, a task which would be difficult to accomplish because the Internet and telecommunications systems for the entire world often rely on crucial 'breakpoints' which cannot be shut down.

While today's world is only marginally vulnerable to disturbances caused by cyber terrorists and information warriors, the real danger lies in violations of copyright law. The state of Massachusetts, for example, earns $9.4 billion in revenue each year from software development, but it loses $562 million to software piracy.

According to the Business Software Alliance (BSA), annual estimated loss due to piracy is $13.1 billion worldwide, with a loss of $2.9 billion in the United States alone. China hosts hundreds of state-of-the-art facilities which manufacture in bulk compact discs containing expensive software, leading to rock-bottom retail prices. For example, a programme that would sell for $500 or more in the US retails for only $3 in Asia and none of this revenue ever reaches the rightful developer. The Internet is an active vehicle for delivery because almost any software programme imaginable can be downloaded using free programmes such as Kazaa and Grokster. Moreover, software pirates use the Internet to coordinate activities with skilled crackers to break the layer of protection surrounding commercial software so it can be copied illegally.

It is not difficult to imagine that a developed nation could declare illegal copying of software to be a form of information warfare because it causes irreparable economic damage. The legal ramifications of such a move would be serious — it may force users of illegal programmes as well as their illicit manufacturers to pay hefty fees in reparations.

Like China, the government of Pakistan needs to incorporate the cost of purchasing and maintaining software in its budgets. Such actions are needed not only to avoid legal pitfalls, but also to encourage foreign financiers to invest in Pakistani software development firms. Moreover, the threat posed by software piracy to the global economy needs to be emphasized and a culture of honesty and fair play needs to be introduced for the benefit of this industry in Pakistan.

Terrorism will no doubt remain a scourge in the world, but until countries use mature, large-scale techniques to disrupt enemy communication, economy and governance, cyber terrorism and info warfare cannot come to the fore. Until that happens, Pakistan needs to realize that its bright young computer aces need protection, guidance and, occasionally, legal checks and balances in an increasingly networked world.

The future of information technology in our country could be brightened by building a framework for ensuring its commercial success and our integration into the global economy by increasing awareness and implementation of software copyright laws. ■