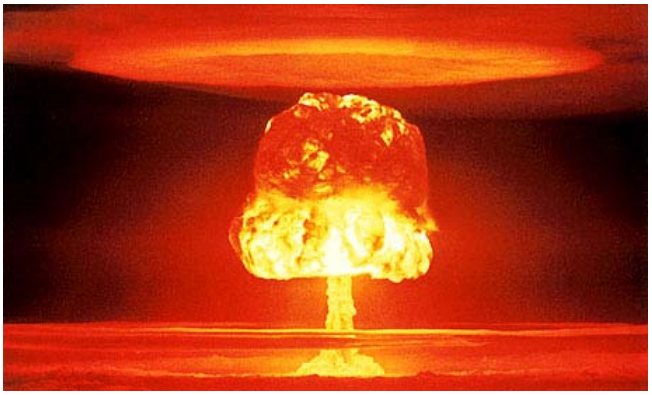
guardian.co.uk

Terrorists could use internet to launch nuclear attack: report

The risk of cyber-terrorism escalating to a nuclear strike is growing daily, according to a study

Bobbie Johnson
guardian.co.uk, Friday 24 July 2009 13.01 BST



Photograph: U.S. Department of Energy-Nevada/Corbis

Terrorists groups could soon use the internet to help set off a devastating nuclear attack, according to new research.

The claims come in a study commissioned by the International Commission on Nuclear Non-proliferation and Disarmament (ICNND), which suggests that under the right circumstances, terrorists could break into computer systems and launch an attack on a nuclear state – triggering a catastrophic chain of events that would have a global impact.

Without better protection of computer and information systems, the paper suggests, governments around the world are leaving open the possibility that a well-coordinated cyberwar could quickly elevate to nuclear levels.

In fact, says the study, "this may be an easier alternative for terrorist groups than building or acquiring a nuclear weapon or dirty bomb themselves".

Though the paper admits that the media and entertainment industries often confuse and exaggerate the risk of cyberterrorism, it also outlines a number of potential threats and situations in which dedicated hackers could use information warfare techniques to make a nuclear attack more likely.

While the possibility of a radical group gaining access to actual launch systems is remote, the study suggests that hackers could focus on feeding in false information further down the chain – or spreading fake information to officials in a carefully orchestrated strike.

"Despite claims that nuclear launch orders can only come from the highest authorities, numerous examples point towards an ability to sidestep the chain of command and

insert orders at lower levels," said Jason Fritz, the author of the paper. "Cyber-terrorists could also provoke a nuclear launch by spoofing early warning and identification systems or by degrading communications networks."

Since these systems are not as well-protected as those used to launch an attack, they may prove more vulnerable to attackers who wish to tempt another nation into a nuclear response.

Governments around the world have recently stepped up their commitment to increasing cyber-defence, after a number of high-profile incidents in which hackers launched attacks on foreign nations. Recent online conflicts, as well as reported attacks on government computer systems in the US, UK and elsewhere have increased the stakes.

In Britain, Gordon Brown recently announced plans to step up online intelligence operations – while in the US, President Obama has said he intends to appoint a cyber-security tsar to ensure that protecting America's computer systems "will be a national security priority".

"Cyberspace is real, and so is the risk that comes with it," he said in May, adding that online attacks are "one of the most serious economic and national security challenges we face".

However, the study suggests that although governments are increasingly aware of the threat of cyberwar with other nations, action to bolster those defences does not alleviate the threat of a rogue group that circumvented the expected strategies for online warfare.

"Just as the 9/11 attacks were an unprecedented attack with unconventional weapons, so too could a major cyber attack," it says.