



World Faces 'Cyber Cold War' Threat

November 29, 2007

By Reuters , [Publish](#)

A "cyber cold war" waged over the world's computers threatens to become one of the biggest threats to security in the next decade, according to a report published on Thursday.

About 120 countries are developing ways to use the Internet as a weapon to target financial markets, government computer systems and utilities, Internet security company McAfee said in an annual report.

Intelligence agencies already routinely test other states' networks looking for weaknesses and their techniques are growing more sophisticated every year, it said.

Governments must urgently shore up their defenses against industrial espionage and attacks on infrastructure.

"Cybercrime is now a global issue," said Jeff Green, senior vice president of McAfee Avert Labs. "It has evolved significantly and is no longer just a threat to industry and individuals but increasingly to national security."

The report said China is at the forefront of the cyber war. It said China has been blamed for attacks in the United States, India and Germany. China has repeatedly denied such claims.

"The Chinese were first to use cyber-attacks for political and military goals," James Mulvenon, director of the Center for Intelligence and Research in Washington, was quoted as saying in the report.

The report was compiled with input from academics and officials from Britain's Serious Organised Crime Agency, the U.S. Federal Bureau of Investigation and NATO.

Cyber-attacks on private and government Web sites in Estonia in April and May this year were "just the tip of the iceberg", the report warned.

Estonia said thousands of sites were affected in attacks aimed at crippling infrastructure in a country heavily dependent on the Internet.

The attacks appeared to have stemmed initially from Russia although the Kremlin denied any wrongdoing.

"The complexity and coordination seen was new," the report quoted an unnamed NATO source as saying. "There were a series of attacks with careful timing using different techniques and specific targets."

EU Information Society commissioner Viviane Reding said in June that what happened in Estonia was a wake-up call. NATO said "urgent work" was needed to improve defenses.

The McAfee report predicted that future attacks would be even more sophisticated.

"Attacks have progressed from initial curiosity probes to well-funded and well-organised operations for

political, military, economic and technical espionage," it said.

The report is available [here](#).

Copyright (c) 2008Ziff Davis Enterprise Inc. All Rights Reserved.