FT-14-0632

Cyberwarfare: Your Business Is the New Battleground

Published: 3 July 2001

Analyst(s): Vic Wheatman

Although the threat of state-sanctioned cyberwarfare is real and should not be underestimated, bigger and more immediate realities are likely to come in the form of organized fraud and espionage.

News Analysis

Event

On 25 June 2001, the Joint Economic Committee of the U.S. Congress was told that Russia and China were developing computer-based technologies capable of attacking and harming the U.S. economy. Lawrence Gershwin, the national intelligence officer for science and technology, said cyberattacks would be part of the "next wave of military operations."

Analysis

Although computer hackers can do considerable harm to Internet sites and connected networks, they pose little threat to national infrastructures such as transport and power. The view of many experts is that hackers acting alone lack either the skills or the desire to carry out the sustained attacks necessary to cause any major or lasting economic damage. However, nation-against-nation cyberwarfare could cause devastating and long-term damage to crucial infrastructures, particularly with the use of more controllable, precise and predictable computer viruses. These would become, in effect, weapons of war.

Gartner believes the potential for cyberwarfare between nations is real and the interconnected world of business puts enterprises on the front line. China and Russia are often named as nations most capable of launching a cyberwar. Realistically, the threat could come from any nation opposed to the United States. Still, government-led initiatives don't pose the largest, overt threat to enterprises. The main threats are:

- The growing base of underemployed technology workers using covert operations for online fraud and financial gain (whether state-sponsored or not)
- Technological espionage by all nations for commercial and intelligence-gathering purposes

All enterprises must protect crucial computer networks and data using a cohesive and intelligent strategy based on appropriate levels of information security policies, products and procedures. The minimum standards are:

- Firewalls
- The use of intrusion detection technology
- Data and e-mail encryption
- Strict monitoring of user activity

Enterprises considering investments or partnerships in countries that are capable of cyberwarfare with the United States should also:

- Ignore the daily ups and downs in relations between these countries and the United States, and remember the basics
- Not let political risk stop any investment decisions if those investments are appropriate to the enterprise's and the nation's size and market opportunities
- Hedge political risks by finding a knowledgeable local operator who can help with contacts at all levels of government; at every level, enterprises should make political risk an explicit topic for discussion and should negotiate specific ways to mitigate these risks
- Not assume situations in a particular country will remain in the long run as they are today
- Remember that it is possible for some countries, such as China and Russia, to remain remarkably stable despite long periods of torrid economic growth and disorienting social change

Analytical Source: Vic Wheatman, Information Security Strategies

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp