Internet Revolution—World Wide War

by Peter R. Taffae

Editor's note: *This article is copyrighted by e-perils.com™ . This article also appeared in the April 2001 issue of* Loss Control Section Quarterly, *published by the CPCU Society, Malvern, PA.*

Peter R. Taffae *is president and CEO of e-perils.com™, a division of Worldwide Facilities, Inc., specializing in cyber, D&O, EPLI, crime, and E&O insurance for corporate and financial institutions. He can be reached at (213) 251-2427 or PeterT@eperils.com.*

More than 40 years ago Che Guevara, Fidel Castro, and Camilo Cienfuegos came marching down from the Sierra Maestra Mountains into Havana and ousted President Batista. The rest is history. Castro has ruled Cuba ever since. In 1949 it was guns and political outrage; today's wars are being raged on the Internet. Are today's Gates, Cases, and Linus Torvalds yesterday's Ches, Castros, and Camilos? Did anyone anticipate the Internet Revolution would include political revolutions?

This new high technology revolution is not only occurring in the country of Cuba but recently in China, Kosovo, East Timor, and the Middle East. This is the beginning of a new era in rebellions.

These new rebels are known as Internet guerrillas. They represent the new resistance to governments in power via the Internet. Internet guerrillas' attacks have resulted in e-mail flooding, denial of service attacks, and hacking of web sites worldwide. Often the guerrillas test their abilities on innocent targets first via third-party servers as relays for their attacks. This results in legal liability for those innocent servers and web sites. The most vulnerable to these malicious attacks are small and mid-size companies that cannot afford to employ the personnel that have the necessary security experience to halt these attacks. There are already many examples of American universities and commercial sites that have been used as third-party conduits.

The fact that information is freely exchanged globally at little or no cost has allowed and even encouraged opposing parties to dissimulate and gather sometimes-secretive information to assist their causes. In some countries, and Cuba in particular, the Internet threatens the government's control of information. Its monopoly of information is now being challenged. War is won via information and there is no easier, quicker, and less expensive information than the Internet has to offer. **Some compare today's Internet guerillas to World War II's French resistance role in war.**

In Cuba the state-owned news agency distributes information that it feels is relevant to the people of the country. The idea of someone being able to log onto CNN's web site and see the world contradicts the monopoly that the government has had all these years. The Internet is uncontrollable, which is exactly why it can easily crumble the leaders of a controlled environment. For the very reason the Internet has lead the developed countries into a new economy, the speed and efficiencies of the Internet will play a larger and larger role in developing countries' political environments.

In late December, China made it a crime to use the Internet as a way to further Taiwan's independence. China has said it will attack Taiwan if the island declares its independence since the civil war of 1949 when the island became a breakaway province. The Standing Committee of the National People's Congress passed a resolution stating, among other things, that spreading computer viruses and breaking into national defense networks are criminal activities. Many of the resolutions' "new" laws mirror existing laws that are used to arrest dissidents and members of opposing political groups but for the first time the Congress addressed "criminal activities" specifically arising out of the Internet.

Recently, across the globe from Cuba and China, in the Middle East we have seen how the Internet is being used to further opposing political views. The Anti-Defamation League web site was attacked the end of December by anti-Israeli Internet guerillas. The site was taken over for about 30 minutes where the attackers posted threats to Israelis and other pro-Palestinian opinions. Other sites that have been hit by Internet guerillas include: Bank of Israel,

Continued on page 2

Internet Revolution—World Wide War

Continued from page 1

the Tel Aviv Exchange Market, Palestinian National Authority, and the Palestinian's Hamas' site.

As recently as mid-January 2001, hackers calling themselves Pentaguard hit a series of Australian, U.S. and UK government web sites. These sites were replaced with home pages and links with Pentaguard's logo. **Pentaguard is believed to be based in the United States and claims to be running a World Wide Web War (WWWW).** Many security experts believe that if groups like Pentaguard can break into a government site with such ease then commercial sites are very accessible to unauthorized access.

The FBI has issued a warning to the U.S. government and corporate America that their web sites are potential targets for Internet guerillas:

> Based on FBI investigations and other information, the NIPC has observed that there has recently been an increase in hacker activity specifically targeting U.S. systems associated with e-commerce and other Internet-hosted sites.
>
> –www.nipc.gov

It is important to understand that companies with sales to clients based in the Internet war territories are vulnerable to cyber attacks. Already there have been reported incidents with U.S. firms conducting business in Israel being hacked. Many of these attacks will come via innocent third parties. By using "conduits," hackers disguise their identity and make capture almost impossible. One good example of an innocent third party involved was the denial of service attacks on some of the largest B2C web sites on February 9, 2000, when the University of California at Santa Barbara was covertly used as a conduit for the attacks.

At the end of the day there are no measures that can stop all politically motivated Internet warfare. **Governments as well as companies are wrestling with how to protect their technology boundaries.** For now, there are a few steps corporations need to take to minimize their veniality and protect themselves from Internet guerillas.

Every company with an Internet presence should seriously consider a comprehensive security assessment. The level of assessments can be tailored to a firm's financial budget. It is an excellent process because of the diversity of issues/concerns that will be addressed.

Equally important is cyber insurance to protect senior management and the company's balance sheet. The perils arising from the Internet need to be addressed, as are the traditional perils of fire, flood, etc. There are a number of insurance contracts that have been specifically designed to protect against the numerous perils arising out of the World Wide Web. Knowing the good ones from the bad is the trick in this ever-changing, quick-moving environment. ■