



Powered by Clickability

Click to Print

[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

U.S. at risk of cyberattacks, experts say

- Story Highlights
- Experts say the recent computer attacks on Georgia signal a new kind of cyber war
- The U.S. is not fully prepared for a large-scale, coordinated attack, experts say
- Such attacks can be mounted anonymously and cheaply from anywhere in the world
- A cyberattack on the U.S. could hobble utilities, transportation and other infrastructure

By Brandon Griggs
CNN

(CNN) -- The next large-scale military or terrorist attack on the United States, if and when it happens, may not involve airplanes or bombs or even intruders breaching American borders.

Instead, such an assault may be carried out in cyberspace by shadowy hackers half a world away. And Internet security experts believe that it could be just as devastating to the U.S.'s economy and infrastructure as a deadly bombing.

Experts say last week's attack on the former Soviet republic of Georgia, in which a Russian military offensive was preceded by an Internet assault that overwhelmed Georgian government Web sites, signals a new kind of cyberwar, one for which the United States is not fully prepared.

"Nobody's come up with a way to prevent this from happening, even here in the U.S.," said Tom Burling, acting chief executive of Tulip Systems, an Atlanta, Georgia, Web-hosting firm that volunteered its Internet servers to protect the nation of Georgia's Web sites from malicious traffic.

"The U.S. is probably more Internet-dependent than any place in the world. So to that extent, we're more vulnerable than any place in the world to this kind of attack," Burling added. "So much of what we're doing [in the United States] is out there on the Internet, and all of that can be taken down at once." [Watch experts discuss threat »](#)

"This is such a crucial issue. At every level, our security now is dependent on computers," said Scott Borg, director of the United States Cyber Consequences Unit, a nonprofit research institute. "It's a whole new era. Political and military conflicts now will almost always have a cyber component. The chief targets will be critical infrastructure, and the attacks will emerge from within our own computer systems."

Hackers mounted coordinated assaults on [Georgian](#) government, media, banking and transportation sites in the weeks before Russian troops invaded. Known as distributed denial of service, the attacks employ multiple computers to flood networks with millions of simultaneous requests, overwhelming servers and crippling Web sites.

Hackers shut down the Web site of the Georgian president, Mikheil Saakashvili, for 24 hours and defaced the Georgian parliament site with images of Adolf Hitler. Saakashvili blamed Russia for the attacks, although the Russian government said it was not involved.

Web sites and computer networks have been targeted by hackers for decades, although large-scale, coordinated cyberattacks are still a relatively new phenomenon. Some [Internet-security](#) experts believe that the Georgia conflict marks the first time a known cyberattack has coincided with a ground war, but others said that similar computer attacks have accompanied military operations in the Middle East and elsewhere.

The challenge to U.S. security experts is that such attacks can be mounted anonymously, and relatively cheaply, from anywhere in the world. Georgia's attackers employed "botnets," or malicious automated programs that take root undetected in far-flung computers and barrage their targets with useless data. By last Friday, some of those botnets were originating from Comcast Internet addresses in the United States, Burling said.

"It only takes a couple of experts; it doesn't take a whole cyber infantry division to pull something like this off," said Don Jackson, director of threat intelligence for SecureWorks, an Atlanta-based computer security firm. "For a very small investment in resources, you can have a huge impact."

In the United States, government computer networks parry millions of attempted intrusions every day, Internet-security experts say. The [U.S. Department of Homeland Security](#) created a National Cybersecurity Center this year to coordinate federal cyberdefense

efforts and quicken responsiveness. However, a recent Homeland Security Department intelligence report, obtained by The Associated Press, concluded that there are no effective means to prevent a coordinated attack on U.S. Web sites.

"When it comes to our government IT security, we're pretty strong in protecting against [attacks]," Homeland Security spokesman William R. Knocke told CNN. "But I wouldn't say ... we're 100 percent impenetrable."

So what would a cyberattack on the United States look like? And where is the U.S. most vulnerable? It depends on who you talk to.

Borg does not believe that the U.S. is susceptible to the kind of attacks launched at Georgia.

"We can command so much bandwidth that it's hard to overwhelm our servers," he said. "We are vulnerable to more sophisticated attacks, but right now most of the people who want to do us harm don't have those capabilities."

The Web sites of key government security agencies, such as the Pentagon and the Central Intelligence Agency, are difficult to bring down, experts said. So are the computer networks of large American banks. But experts say a successful, large-scale attack on U.S. computer systems could hobble electric-power grids, transportation networks and industrial-supply chains.

"You'd see some disruption of essential services, like electricity. You'd definitely see espionage," said James A. Lewis, a senior fellow at the Center for Strategic and International Studies in Washington. "Would it be decisive? No. Nobody's going to win a conflict with the United States in cyberspace. But would it be disruptive and irritating? Yes."

Federal researchers who launched an experimental cyberattack last year in Idaho caused a generator to self-destruct, prompting fears about the effect of a real attack on the nation's electrical supply.

And a May report by the Government Accountability Office found that the Tennessee Valley Authority, which supplies power to almost 9 million people in the southeastern U.S., had not installed sufficient cybersecurity measures. Spokesman Jim Allen said the TVA, the nation's largest publicly owned utility company, is "on track" to correct the problems.

What frustrates computer-security experts is that the features that make the Internet such an invaluable resource -- its openness and interconnectedness -- also make it easier for hackers to do harm. As a staple of 21st-century warfare, cyberattacks will become increasingly sophisticated, forcing governments and private industry to build ever-stronger firewalls and other defenses, experts said.

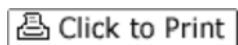
Also, vague international laws and a lack of accountability will continue to make tracking down and prosecuting cyberattackers difficult.

"We don't know quite what the rules are for this kind of conflict. If it's spying, it's illegal. But is it an act of war? And who do you arrest?" Lewis asked. "We're much safer [in the U.S.] than we were a year ago. But we still have a long way to go."

All About[U.S. Department of Homeland Security](#) • [Republic of Georgia](#) • [Computer Security](#)

Find this article at:

http://www.cnn.com/2008/TECH/08/18/cyber.warfare/index.html?eref=rss_tech



[SAVE THIS](#) | [EMAIL THIS](#) | [Close](#)

Check the box to include the list of links referenced in the article.