Is there really a cyberwar? Term might be misused

May 5 2010, By JORDAN ROBERTSON , AP Technology Writer

(AP) -- Is there really a "cyberwar" going on? Some officials and computer security companies say yes, arguing that armies of hackers are stealing online secrets and using the Internet to attack infrastructure such as power grids.

However, some security analysts said at a conference this week that "cyberwarfare" is such a broadly used term that it might be hurting efforts by countries to agree how to cooperate on Internet security.

For instance, last month the United Nations rejected a Russian proposal for a new treaty on cybercrime. That highlighted a schism with the U.S. and European countries, which support a 2001 treaty that Russia claims gives foreign governments too much leeway to electronically pursue criminals across borders.

"Lots of times, there's confusion in these treaty negotiations because of lack of clarity about which problems they're trying to solve," said Scott Charney, vice president of Microsoft Corp.'s Trustworthy Computing Group, before a speech at the Worldwide Cybersecurity Summit.

The conference was sponsored by the EastWest Institute think tank and assembled about 400 security officials and industry executives from dozens of countries.

Cyberwar is a catchall phrase: It's often used to refer to everything from purely financial crimes to computer attacks that could kill people by

blowing up an oil pipeline. Last year came revelations that spies had hacked into the U.S. electric grid and left behind computer programs that would let them disrupt service.

Bruce Schneier, chief security technology officer at British telecommunications operator BT and an influential security blogger, noted that attacks last summer that knocked out service to government Web sites in the United States and South Korea - and were suspected but never proven to have originated in North Korea - were also widely called acts of cyberwar, even though they were essentially harmless.

The White House's cybersecurity coordinator, Howard Schmidt, has called "cyberwar" an inaccurate metaphor, given that many computer attacks are criminal acts aimed at stealing money.

If the "war" metaphor is problematic, there could be an important consequence. It might shift responsibility onto the government, in the minds of some in private industry, for fighting the attacks. Instead, experts at the Dallas summit said, it should be a joint effort, particularly when it comes to control systems for critical infrastructure.

"As soon as you say `war,' people think, `That's a government problem,'" said James Isaak, president of the IEEE Computer Society. "And if that's not the nature of the problem we're dealing with, that's a disservice."

Charney, of Microsoft, believes cyber threats should be better differentiated. He proposes four categories: conventional computer crimes, military espionage, economic espionage and cyberwarfare. That approach, he argues, would make it easier to craft defenses and to discuss international solutions to each problem.

However, even in Charney's framework, "cyberwarfare" remains tricky to define and deal with. One reason is that the nature of the Internet

makes it possible that "a nation-state might well find itself `at war' with a single individual," Charney wrote in a paper accompanying his talk.

As a result, he wrote, new rules for such combat have to be considered.

"If the concern is an electronic Pearl Harbor, perhaps part of the response is an electronic `Geneva Convention' that protects the rights of noncombatants."

More information: Scott Charney's paper: http://bit.ly/a7UOF1

Citation: Is there really a cyberwar? Term might be misused (2010, May 5) retrieved 18 April 2024 from https://phys.org/news/2010-05-cyberwar-term-misused.html