



The Cold War Moves To Cyberspace

Charles Cooper: There Are Battles Being Waged Online Between The U.S., China And Russia

April 22, 2009

Somewhere deep in Washington's national security apparatus, more than a few old-timers surely pine for the clarity of the Cold War. Black versus white, American versus Russian, spy versus spy - the good old days.

Now, however, they face more ephemeral threats from shadowy foes that prefer to cloak their identities. "There's a cyber war going on," said Ed Giorgio, who spent nearly 30 years with the National Security Agency before starting an IT security consultancy in 2007. The problem, he says, is that identifying an online adversary isn't as easy as pinpointing an enemy tank formation.

"Adversaries are just as likely to be nationalists as they are likely to be countries," said Giorgio, echoing a theme that cyber security experts say is likely to shape the Pentagon's approach to building Internet defenses in an increasingly networked world. The extent of the problem was hinted at earlier in the day by Defense Secretary Robert Gates. In an upcoming 60 Minutes interview, Gates told CBS News anchor Katie Couric that the United States is "under cyber-attack virtually all the time, every day" and that his department will more than quadruple the number of experts to battle cyber attacks.

Gates' comments came only hours after the Wall Street Journal reported that cyber spies had breached the DOD's Joint Strike Fighter project and also had penetrated the Air Force's air-traffic-control system. The Journal did not have details on the identities of the intruders but many industry experts are pointing fingers at China.

If true, that should not surprise anyone, says security analyst Richard Stiennon. In fact, he says, cyber probes from China have become more frequent since a U.S. Navy EP-3 was forced down by a Chinese fighter plane over the South China sea in 2001.

That incident led to a brief diplomatic row as well as a surge in of cyber attacks against U.S. Web sites. What's more, only a couple of years earlier, Chinese hackers attacked private and government Web sites in the U.S. in retaliation after NATO accidentally struck the Chinese embassy in Belgrade during the Kosovo crisis.

But finding out who orchestrated the attacks remains a mystery. "I talked to IT administrators who said that if you were running Microsoft IIS, (server software for the Internet) then you were getting hacked," Stiennon said. "That was the beginning of the Chinese attacks....but it had plausible deniability. That's the beautiful thing about attributing the source of the attacks."

Dmitri Alperovitch, who specializes in threat research at the software security firm, McAfee, offers a more blunt assessment of what's happening on the ground. He says the U.S. is "in the midst of a cyber Cold War" and that the roster of potential foes could lengthen as more countries acquire more sophisticated knowledge about how to conduct cyber warfare.

He said that Russia defines cyber war as a force multiplier while China views cyber war as a way to get control of an enemy without the need for engaging on a physical field of battle. "It's straight out of Sun Tzu," he said.

That's the rub. Even in cases where a hack attack seems clearly linked to a government sponsor, experts say it's still hard to conclude the identity beyond a shadow of a doubt. In March 2007, Estonian Web sites got knocked out after the regime decided to move a Soviet statue from one park to another. Last August, when Russian tanks rolled across the border, Georgia's government ministries also got overwhelmed by a coordinated cyber attack.

U.S. and NATO officials don't seem to have any confusion about who was behind the attacks. In fact, NATO has since created a cyber defense center in Tallinn, Estonia. But in the absence of a smoking gun, this remains an unanswered question. Indeed, defenders of Russia attribute the brief cyber war to nationalists acting independently.

Same goes for the Chinese, who are assumed to be behind the recent "GhostNet" attacks involving targets in the Tibetan community. "Even if an attack comes from Beijing, it doesn't mean that it comes from the Chinese government," said Ed Skoudis, the founder of the security consultancy, InGuardians. "You can't jump to that automatic conclusion."

The only clear conclusion is that this sort of activity is likely to become increasingly common. That's why Secretary Gates and his team are about to wade through lots of resumes in the coming weeks and months.

By Charles Cooper

© MMIX, CBS Interactive, Inc. All Rights Reserved.