


John Arquilla: Go on the Cyberoffensive

By Noah Shachtman  09.21.09



Wired's Smart List 2009

The Pentagon already employs legions of elite hackers trained in cyberwarfare. But they mostly play defense, and that's what Naval Postgraduate School professor [John Arquilla](#) wants to change. He'd like the US military's coders to team up with network specialists abroad to form a global geek squad. Together, they could launch preemptive online strikes to head off real-world battles.

Armies (even guerrilla armies) are so dependent on digital communications these days that a well-placed network hit could hobble their forces. Do these cyberattacks right—and openly—and the belligerents will think twice before starting trouble. Arquilla calls his plan "a nonlethal way to deter lethal conflict."

Sure, it's risky. A misinterpreted or misattributed attack could inflame tensions. Or you might fritz the good guys and civilians by mistake. But Arquilla says this "kinder, gentler deterrence" is better than threatening to strangle an adversary's economy or reduce its cities to radioactive cinders. Here are three scenarios in which preemptive cyberattacks could prevent bloodshed.

Scenario: Defusing South Asia

Situation: Pakistan and India are massing armies on their shared border.

Solution: Take out the command-and-control networks on both sides before these nuclear-armed foes can go to war for a fifth time. In the 1951 film *The Day the Earth Stood Still*, Arquilla notes, a benevolent alien shuts down the machines of Earth's superpowers before they can spread nukes to other planets. Here, US- led hackers play the ET role to put the conflict on ice.

Scenario: Disconnecting al Qaeda

Situation: Intelligence sources report that al Qaeda is about to launch another 9/11.

Solution: Track down militants online and let them know we're watching. Spy agencies already eavesdrop on al Qaeda's networks and occasionally take down its Web sites. But to really disrupt increasingly Web-dependent terror groups, you have to convince them they're not safe anywhere on the Net. Set up online honeypots—like a fake jihadist discussion forum—to lure in and bust wannabe Osamas. And even if you break up terror cells by other

means, give public credit to your online spadework. A little fudging is acceptable if it keeps killers from clicking for the cause.

Scenario: Restraining Russia

Situation: Russia is mobilizing its troops for another showdown with Georgia.

Solution: Deploy a US-led or NATO-sponsored cyberdeterrent squad to disrupt the Russian military's communication networks, forcing the Kremlin to delay an attack on the former Soviet republic. The intervention would buy time for diplomacy to work. Arquilla says, "I like the idea of cyberdeterrence being used against anyone who would start a war"—even, he muses, the US.

Note:

The article above was written in 2009. Since then we have recently all heard about PRISM - which is the US system designed to save all our online activity for any future investigation of any individual. People do not want to be watched and have their privacy invaded.

Is this different from what this article proposes or just another side of the whole Internet controversy?

Does his system create the potential for total world domination by a supersmart hacker?