EXHIBIT 2

http://www.forbes.com/2007/08/06/security-hacking-challenge-tech-cx_ag_0806toughhack.html

Middle America, Meet The Hackers
Andy Greenberg, 08.07.07, 6:00 AM ET

Don't try to hack the hackers.

That's what *Dateline NBC*'s Associate Producer Michelle Madigan learned at this year's DefCon, the largest gathering of hackers, crackers and security professionals in the world. Going undercover, she hoped to reveal cybercriminals talking openly about their illegal exploits. Instead, the sting backfired: A conference organizer outed her in a room filled with thousands of her would-be targets.

The crowd, usually a friendly group despite some vampirish clothes and complexions, wasn't pleased. As a few chanted "burn the witch," Madigan scurried out of the Riviera Hotel to her car, with about 150 hackers-turned-hecklers in pursuit.

DefCon's inhospitable treatment of Madigan wasn't just because she was missing a press badge, says one conference spokesman who goes by the handle "Priest." She had also missed the point. By focusing on the bad apples, Priest says, Madigan was glossing over DefCon's true spirit: smart people getting together to mess around with technology.

"Middle America thinks we're stealing your social security numbers, raping your children and breaking into your bank account," he says. "The reality is, we are the ultimate explorers. We see a technology, and we want to know how it works."

That exploration goes well beyond invading the closed corners of the Internet. DefCon's more than 6,000 attendees hack everything: their cars, to increase horsepower and remove pesky safety and emissions controls; their brains, using biofeedback receptors attached to videogames to relieve anxiety disorders; even the war in Iraq. One Navy engineer gave a presentation detailing the nine months he spent hacking insurgent bombs, jamming their radio frequencies to prevent detonation.

"The people who built the Mars rovers are hackers," says Jeff Moss, also known as "Dark Tangent," the hacker who has organized DefCon for the last 15 years. "We generally like hacks that aren't nefarious, that involve figuring something out from the ground up. That's what we try to reward here."

That kind of harmless hacking was channeled into a variety of competitions at the conference, including a lockpicking contest and a game of capture the flag, in which teams earned points by stealing bits of each other's data.

Of course, DefCon still attracts some true "black hat" hackers, bent on learning the newest tools for illegal intrusion, sabotage, espionage and credit card theft. And what attracts cybercriminals

also attracts cybercops; any attendee who can verify the identity of an undercover cop wins an "I Spotted the Fed" T-shirt.

But as the danger of online crime shifts from amateur hackers to organized cybergangs in Eastern Europe and Asia, the Feds are increasingly cooperative with DefCon's shenanigans. This year, at least six federal employees revealed themselves in press conferences and panel discussions. More bizarrely, two federal agents were married during the conference's closing ceremony.

In fact, DefCon's species of armchair hackers are more of a distraction for law enforcement than a real menace, says Jim Christy, director of future exploration at the Department of Defense's Cyber Crime Center. He's more focused on the potential for major attacks on critical infrastructure or government Web sites, like the kind that rattled Estonia's government Web sites in May, or the "Titan Rain" attacks that penetrated the U.S. Department of Commerce and Department of State computers in past years.

"Run-of-the-mill individual hackers are just noise as we try to focus on the real problem," he says. "We have to investigate every threat, but we're often dealing with ankle biters."

When DefCon's hackers do venture into the illegal, it's often based on impulses that are more libertarian than malicious, says a hacker known as "Dead Addict," another of DefCon's organizers. "We simply don't take the law as a moral compass," he says.

Dead Addict, a lanky 34-year-old dressed in all black and a bowler hat, points out that he began using the Internet in the early '90s, even before the advent of Internet service providers. At the time, only users with university connections could legally connect. He, and many others without university accounts still found ways to borrow access, essentially breaking the law. In that sense, Dead Addict argues, Internet culture has always bent, and sometimes broken, the legal rules.

That's not to say that true cybercrime doesn't hold a certain temptation. Though Dead Addict now works for a major technology company, he says he was once offered a job with a so-called "online pharmacy."

"I politely declined," he says. "But if I'd taken that job, I'd probably be basking on some tropical beach right now."

Dead Addict says that many of the hackers that gave DefCon its renegade reputation in earlier days have now grown up and, like himself, launched legitimate careers in security with big-name tech companies. But a lucrative day job leaves DefCon's hackers to focus on what Dead Addict says is the original sense of hacking.

"It's about a passion for technology. It's thinking about what technology can do, rather than what it was originally intended to do," he says. "It's about a bunch of people with time on their hands saying, 'Wouldn't it be cool if ...?'"