JENNIFER S. GRANICK

strike back

Jennifer Stisa Granick joined Stanford Law School in January 2001 as a lecturer and is Executive Director of the Center for Internet and Society (CIS). She teaches, speaks, and writes on the full spectrum of Internet law issues, including computer crime and security, national security, constitutional rights, and electronic surveillance, areas in which her expertise is recognized nationally.

jennifer@granick.com

SEVERAL COMPANIES ARE DEVELOPING interesting new programs system administrators can use to disable remote machines that are sending damaging packets to their computer systems. These technologies—often called "strike back" or "active defense"—foment a lot of interest among those of us fed up with an avalanche of unending worms and viruses.

But are strike-back technologies legal? The law simply hasn't developed to the point where there's a clear answer, but sysadmins resorting to strike-back are playing with legal fire.

strike-back technologies are designed to locate the source of unwanted or harmful Internet connections and shut those machines down. For example, one such program responds to the Code Red worm by identifying the machine sending the worm, and using a back door left by the worm itself to install and execute code that stops the attacking machine from transmitting the worm.

Many critiques of strike-back focus on the risk of retaliating against the wrong machines. IP spoofing can mask the true origin of unwanted packets. Also, an attack may come from an unwary third party's machine that is itself the victim of an attack. Disabling that machine may cause the innocent owner serious problems. At the very least, the owner will realize that the strike-back program has altered his or her system and will need to investigate to determine exactly what happened.

Even if a strike-back program accurately targets the source of the attack, state and federal laws prohibit unauthorized access to and modification of networked computers. These laws not only outlaw the transmission of worms and viruses but also prohibit victims of attacks from themselves intruding on their attacker's systems, regardless of motive. Any unauthorized access to a networked computer that causes damage of $5000 or more (which includes the costs of investigating the access) violates federal law. "Unauthorized access" currently means connecting to the computer without the permission of the system owner. Most state laws prohibit unauthorized access whether or not it causes damage. Users of strike-back technology may be buying themselves a civil suit or, worse, criminal prosecution.

In time, legal rules may embrace strike-back. Congress could decide to give system owners the right to disable attacking machines, as it recently proposed doing for intellectual property owners who discover their copyrighted information on peer-to-peer networks. Or

judges confronting strike-back cases may decide to extend traditional legal excuses such as self-defense or defense of others to this new situation.

The doctrine of self-defense or defense of others permits the use of otherwise illegal force to prevent harm to oneself or to others under certain circumstances. The precise definition of self-defense differs from state to state, but as a general rule, self-defense applies only if the force used to repel the harm is necessary, reasonable, and proportional. As applied to strike-back, a judge might think disabling a system from sending Code Red packets is self-defense, but completely paralyzing the system or reformatting the hard drive is not.

The excuse of self-defense usually applies only if you have no other means of protecting yourself. Some states even require you to retreat if possible, to leave the scene of the problem, before resorting to self-defense measures. There are usually alternatives to strike-back, whether it's taking your system offline (a digital form of retreat, perhaps), firewalls, or comprehensive patching. Perhaps a court will find that self-defense is never a valid excuse, because the first line of defense is to secure the system properly, not to strike back against attackers.

It's folly to ask judges or juries to calculate whether a digital retaliation is necessary, reasonable, and proportional when the security community itself doesn't yet agree on best practices. But in light of the interest in strike-back technology and the eagerness of sysadmins to deploy it, it won't be long before judges have to decide whether strike-back is self-help or vigilantism.