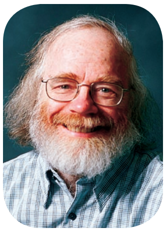
The Government and Cybersecurity



Steven M. Bellovin
Microsoft

We all realize that computer security is a serious problem. But who should solve it? More precisely, who should be responsible for coping with computer insecurity—governments or the private sector? To some extent, the answer depends on how we view the problem.

Most classic hacking was treated as petty crime, but attacker motives today have changed. Most hacking is done for pecuniary reasons, but a noticeable amount seems to be done to advance national goals. The different scenarios pose different questions.

In the US, at least, responsibility for protection against ordinary criminal behavior is split between the government and private citizens. While investigation, apprehension, prosecution, and punishment or retribution are generally governmental roles, individuals are expected to take reasonable steps to protect themselves: houses have locks, keys shouldn't be left in cars, and so on. That said, beyond a certain point, most people expect the government to take over.

Jurisdictional issues add to the muddle. Even if counterhacking is legal in the victim's locale, it might not be in the attacker's. Is hot pursuit legal in cyberspace? Across national boundaries? Can the victim even tell where the attacker is? Botnets, reflector attacks, and stepping stones aside, IP geolocation is inherently imprecise.

Simply put, reality is different in cyberspace. Although it might have a similar legal regime, the law's deterrent ability is almost nil. People aren't expected to live inside bank vaults, but many advocate running computer networks that way. Even Texas doesn't seem to permit it today, but in the absence of effective law enforcement, should this change? The difficulty of accurate attacker identification is, of course, a complicating factor.

The situation is more complex in attacks by nation-states. In general, individuals have little expectation that they should be able to protect themselves against foreign governments, the 1950s craze for fallout shelters notwithstanding. Do we expect people to protect themselves against other governments? Is this a reasonable expectation?

The nature of a governmental response is even less clear. Are such attacks espionage, whether directed against the private sector or the government? If so, the response would normally involve counterintelligence units and the legal process. But if we consider them physical intrusions, akin to reconnaissance aircraft, is a direct response—cyber or physical—justified?

The theoretical answer, although not the reality, is rather clearer in the event of officially sponsored attacks of certain types. It matters little if hostile forces destroy an electrical generator via a kinetic weapon or by taking over a control computer; either way, it could be considered an act of war. But who launched the attack? A garden-variety hacker? A foreign military? Private parties acting at the direction—or with the tacit approval—of a foreign government? The answer to the core question is generally quite unclear, as in the recent denial-of-service attacks against Estonia, Georgia, and Kyrgyzstan. Perhaps there's historical precedent: are officially sponsored cyberattacks the latter-day equivalent to letters of marque and reprisal? Do we want to return to those days?

To complicate matters further, even financial crime can be tied to other governments. Repeated reports indicate that some countries are willing to tolerate any sort of fraud and hacking as long as it's aimed externally. Indeed, it was deemed newsworthy that the recent Conficker/Downadup worm didn't infect machines with a Ukrainian keyboard. Is this *casus belli*?

None of these questions have pat answers. Even if current laws can be stretched to answer them, those laws probably still couldn't give the right answer. Essentially, we need an international answer because there's no 12-mile limit in cyberspace. The discussion needs to begin sooner rather than later. □

***Steven M. Bellovin** is a professor of computer science at Columbia University. Contact him via www.cs.columbia.edu/~smb.*