Steven M. Bellovin
Columbia University

Dr. Strangecode

We all know what nuclear bombs do: they make a really big blast, emit prompt radiation, and perhaps create a lot of fallout. People who study the field—and not just government specialists toiling in the bowels of the Pentagon but uncleared civilians who are willing to put in some effort—know far more, such as the differing effects of high-altitude EMP blasts versus "bunker busters." There are entire books devoted to nuclear targeting strategies, a subject that has been discussed openly for more than 50 years. The result has been vigorous public debate about issues like MIRVs, antiballistic missile systems, and more.

I bring this up because it isn't true of cyberwar. There has been almost no public discussion of weapons, doctrines, tactics, or policy. If this doesn't change, we're headed for trouble, fighting battles we don't want in places we don't want them fought. The only thing worse than accidental cyberwar is losing an accidental cyberwar.

In the 1950s, US nuclear strategy called for bombing cities, a choice dictated by the small number of weapons and the inaccuracy of the bombers and missiles of the era. Later on, when those constraints disappeared, there was a shift to a strategy that targeted the Soviet military. Is that better? It's arguably more moral, but it requires vastly more warheads, which carries its own risks, up to and including nuclear winter.

A more recent (and to some extent ongoing) example is the controversy over the proposed antiballistic missile system. Even assuming it could work (it couldn't), would it be a good thing? Or was it destabilizing because it let one side conduct a first strike on the other while remaining relatively immune to counterattack? Again, this issue could be discussed widely because the fundamental characteristics of the weapons are publicly understood.

Corresponding discussions about cyberweapons have yet to take place. Suppose that some country develops the tools to take out an enemy's power grid. Is this good or bad? Ethically, we might want to ask how selective it is—is the target the entire power grid of a region or country, or just the part feeding military bases and munitions plants? Given how porous computer defenses are, should we assume that any weapon that one side develops will soon be possessed by the other? This might not be all bad—it's good for each side to know the other's abilities—but it moves us back into the realm of mutually assured destruction. Is this where we want to go? It's a debate we can and should have.

Defensive strategies have implications for domestic politics. Assume that a cyberattack is believed to be imminent. Should a country disconnect from the Internet? It's easier for, say, China than it is for the US, but simply having that ability implies the ability to do surveillance and even censorship of international traffic. Is this a good or a bad thing?

Many more questions need to be answered: Where is the line between cyberespionage and cyberattacks? Is "preparing the battlefield"—hacking now to create access points in the event of a future conflict—legitimate? Under what conditions will a country respond with kinetic weapons to a cyberattack? What's the general nature of offensive capabilities? How selective is targeting? How much collateral damage is acceptable? How should lines be drawn between state, state-tolerated, and purely private action? What jurisdiction do various countries claim?

The world needs answers, and soon. Otherwise, it's time to grab my cowboy hat: "Gentlemen, you can't hack in here; this is the Internet." ■

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

Copublished by the IEEE Computer and Reliability Societies
1540-7993/14/$31.00 © 2014 IEEE