Steven M. Bellovin
Columbia University

Military Cybersomethings

You can hardly read the news without seeing dire warnings of national security problems lurking in our computers. If it isn't some country stealing some other country's commercial secrets—just who's the victim and who's the thief varies with the teller, of course—it's the threat of a "cyber Pearl Harbor" or "cyberterrorism" or "cyberwarfare" or "cyberespionage" or "cyber disturbing the peace" or cybersomething-or-other. What are all of these things? Are they real? And what should "we"—one nation, or the whole world—do about them?

Let's start by defining some terms. My metric is very simple: if the same activities were done without computers, what would we call them? This in turn means that context and scale matter. One person crossing a border illicitly might be a refugee, a smuggler, a spy, a scout for an invasion, or simply the first soldier in a large unit. Even that latter example doesn't always mean war; it might be a limited duration, cross-border raid. No, these terms aren't precisely defined, but like Justice Potter Stewart, we generally know it when we see it, and broadly speaking, we do have a rough shared understanding of these terms.

The same, of course, is true in the digital realm, although the categories are somewhat different. Just as we have spies in the physical world, we have espionage online; that it's called "cyberexploitation" when done by governments doesn't change the underlying reality. Similarly, just as spying on businesses can be done by governments or by rival companies, cyberespionage can be done by either. The presence or absence of the "cyber" prefix doesn't change anything.

What about physical damage to something? Is it an act of war? A warlike but limited incident? Sabotage? Terrorism? Again, the means—an airstrike, some plastique, some malware—doesn't matter; what does matter is the larger context and the effect. Was it truly a civilian group or something government directed? Again, this isn't new; false fronts and letters of marque and reprisal are ancient.

Certainly, there are differences. It's hard to imagine what a cyberrefugee might be; conversely, in the absence of Internet border controls and customs inspection, cybersmuggling is hard to distinguish from an international file transfer, even assuming that the participants can tell if a border crossing is involved. More ominously, in cyberspace, a country can "prepare the battlefield": deploy malware that will act destructively on command but wait quietly until hostilities break out.

Can there be cyberwar? Are we at risk of a cyber surprise attack? What about cyberterrorism? Let's delete the prefix and ask again: Can there be a war? Are we at risk of a surprise attack by a hostile nation? What about terrorism? Asked this way, we can see that the questions boil down to motive and capability. Are there nations or groups who might start a war, with or without a surprise attack? Are there terrorists?

Now the answers seem a lot clearer. A cyberattack, of any of these types, can happen if and only if the attacker can gain more than it loses, even in the face of a kinetic response. This in turn reduces the questions to enemy capability, the potential for serious damage from a cyberattack, and the risk of retaliation. In other words, things aren't quite that bad. Really damaging attacks aren't that easy; perpetrating one at a large scale requires many trained people and a fair amount of luck. Small differences in configuration make a very big difference in how an attack must be launched; the attacker needs really good intelligence and weapons customized for each target.

Cyberexploitation—spying—happens now, and it matters. But a war? If there is one, there will undoubtedly be a cyber component, but the Internet doesn't seem to make it more likely or more serious. ■

Steven M. Bellovin is a professor of computer science at Columbia University and chief technologist of the Federal Trade Commission (FTC). Opinions are solely his, and not necessarily those of the FTC. Contact him via www.cs.columbia.edu/~smb.

Copublished by the IEEE Computer and Reliability Societies