Cyberassault on Estonia

Estonia recently survived a massive distributed denial-of-service (DDoS) attack that came on the heels of the Estonian government's relocation of a statue commemorating Russia's 1940s wartime role. This action inflamed the feelings of the substantial Russian population in Estonia, as well as those of various elements in Russia itself.

Marc Donner
Associate Editor in Chief

Purple prose then boiled over worldwide, with apocalyptic announcements that a "cyberwar" had been unleashed on the Estonians. Were the attacks initiated by hotheaded nationalists or by a nation state? Accusations and denials have flown, but no nation state has claimed authorship.

It's not really difficult to decide if this was cyberwarfare or simple criminality. Current concepts of war require people in uniforms or a public declaration. There's no evidence that such was the case. In addition, there's no reason to believe that national resources were required to mount the attack. Michael Lesk's piece on the Estonia attacks in this issue (see the Digital Protection department on p. 76) include estimates that, at current botnet leasing prices, the entire attack could have been accomplished for US$100,000, a sum so small that any member of the upper middle class in Russia, or elsewhere, could have sponsored it.

Was there national agency? It's highly doubtful that Russian President Vladimir Putin or anyone connected to him authorized the attacks. If any Russian leader had anything to say about the Estonians, it was more likely an intemperate outburst like Henry II's exclamation about Thomas Becket, "Will no one rid me of this troublesome priest?"

We can learn from this, however: security matters, even for trivial computers. A few tens of thousands of even fairly negligible PCs, when attached by broadband connections to the Internet and commanded in concert, can overwhelm all modestly configured systems—and most substantial ones.

Engineering personal systems so that they can't be turned into zombies is a task that requires real attention. In the meantime, the lack of quality-of-service facilities in our network infrastructure will leave them vulnerable to future botnet attacks. Several avenues are available to address the weaknesses in our current systems, and we should be exploring all of them. Faced with epidemic disease, financial panic, and other mass threats to the common good, we're jointly and severally at risk and have a definite and legitimate interest in seeing to it that the lower limits of good behavior aren't violated.

From the Estonia attacks, we've also learned that some national military institutions are, at present, hard-pressed to defend their countries' critical infrastructures and services. Historically, military responses to attacks have involved applying kinetic energy to the attacking forces or to the attackers' infrastructure. But when the attacking force is tens or hundreds of thousands of civilian PCs hijacked by criminals, what is the appropriate response? Defense is left to the operators of the services and of the infrastructure, with the military relegated to an advisory role—something that both civilians and military must find uncomfortable. Of course, given the murky situations involved in cyberwar, we'll probably never fully learn what the defense establishments could or did do.

Pundits have dismissed this incident, arguing that this is a cry of "wolf!" that should be ignored (see www.nytimes.com/2007/06/24/weekinreview/24schwartz.html). Although it's true that we're unlikely to be blinded to an invasion by the rebooting of our PCs, it's naïve to suggest that our vulnerability to Internet disruptions has passed its peak. Cyberwar attacks, as demonstrated in 2003 by Slammer, have the potential to disable key infrastructures. To ignore that danger is criminally naïve.

Nevertheless, all is not lost. Events like this have been forecast for several years, and as of the latest reports, there were no surprises in this attack. The mobilization of global expertise to support Estonia's network defense was heartening and will probably be instructive to study. Planners of information defenses and drafters of future cyberdefense treaties should be contemplating these events very carefully. This wasn't the first such attack—and it won't be the last. □