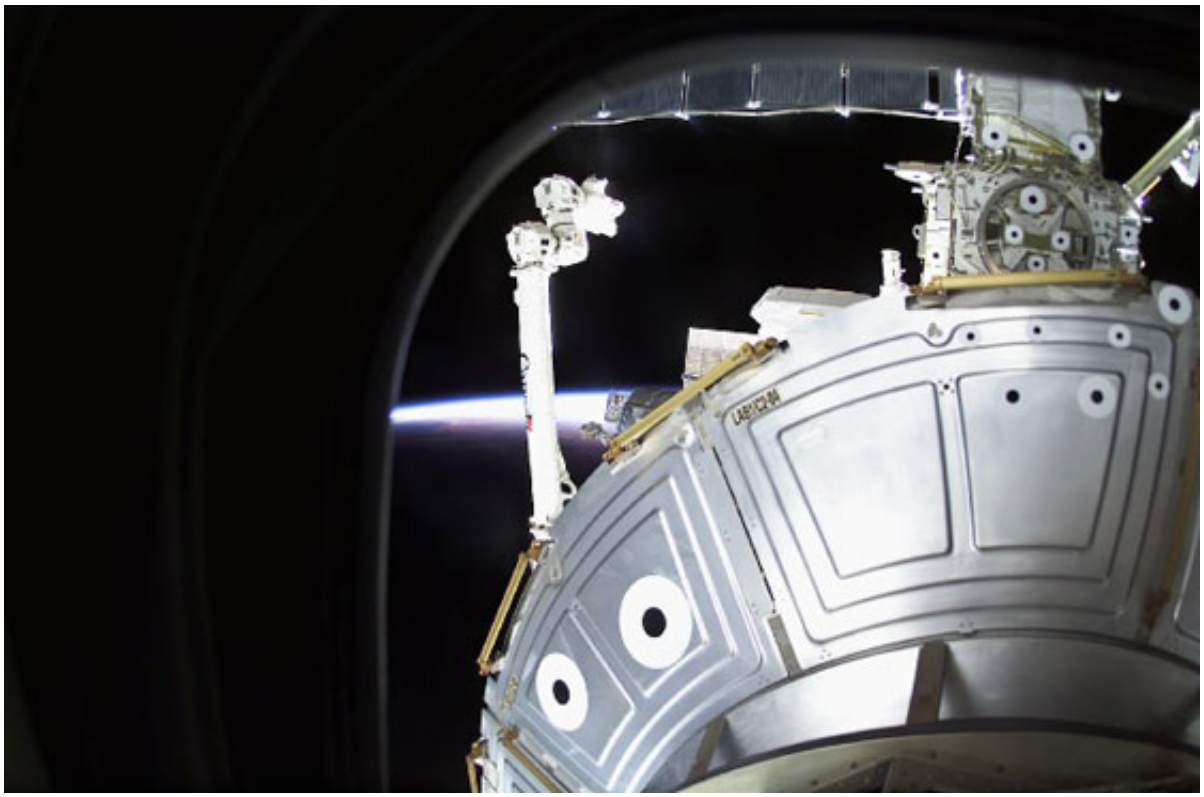
CYBERWAR: MYTH OR REALITY?

The biggest problems in discussing cyberwar are the definitions. The things most often described as cyberwar are really cyberterrorism, and the things most often described as cyberterrorism are more like cybercrime, cybervandalism or cyberhooliganism - or maybe cyberespionage.



At first glance there is nothing new about these terms except the “cyber” prefix. War, terrorism, crime and vandalism are old concepts. What is new is the domain; it is the same old stuff occurring in a new arena. But because cyberspace is different, there are differences worth considering.

Of course, the terms overlap. Although the goals are different, many tactics used by armies, terrorists and criminals are the same. Just as they use guns and bombs, they can use cyberattacks. And just as every shooting is not necessarily an act of war, every successful Internet attack, no matter how deadly, is not necessarily an act of cyberwar. A cyberattack that shuts down the power grid might be part of a cyberwar campaign, but it also might be an act of cyberterrorism, cybercrime or even - if done by some 14-year-old who does not really understand what he is doing - cyberhooliganism. Which it is depends on the attacker’s motivations and the surrounding circumstances, just as in the real world.

For it to be cyberwar, it must first be war. In the 21st Century, war will inevitably include cyberwar. Just as war moved into the air with the development of kites, balloons and aircraft, and into space with satellites and ballistic missiles, war will move into cyberspace with the development of specialized weapons, tactics and defenses.

I have no doubt that smarter and better-funded militaries are planning for cyberwar. They have Internet attack tools: denial-of-service tools; exploits that would allow military intelligence to penetrate military systems; viruses and worms similar to what we see now, but perhaps country- or network-specific; and

Trojans that eavesdrop on networks, disrupt operations, or allow an attacker to penetrate other networks. I believe militaries know of vulnerabilities in operating systems, generic or custom military applications, and code to exploit those vulnerabilities. It would be irresponsible for them not to.

The most obvious attack is the disabling of large parts of the Internet, although in the absence of global war, I doubt a military would do so; the Internet is too useful an asset and too large a part of the world economy. More interesting is whether militaries would disable national pieces of it. For a surgical approach, we can imagine a cyberattack against a military headquarters, or networks handling logistical information.

Destruction is the last thing a military wants to accomplish with a communications network. A military only wants to shut down an enemy's network if it isn't acquiring useful information. The best thing is to infiltrate enemy computers and networks, spy on them, and surreptitiously disrupt select pieces of their communications when appropriate. The next best thing is to passively eavesdrop. After that, perform traffic analysis: analyze the characteristics of communications. Only if a military can not do any of this would it consider shutting the thing down. Or if, as sometimes but rarely happens, the benefits of completely denying the enemy the communications channel outweigh the advantages of eavesdropping on it.

Cyberwar is certainly not a myth. But you have not seen it yet, despite the attacks on Estonia. Cyberwar is warfare in cyberspace. And warfare involves massive death and destruction. When you see it, you will know it.

http://www.schneier.com/essay-201.html
This essay first appeared on Information Security as the second half of a point/counterpoint with Marcus Ranum (which can be found at
http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1280052_idx1,00.html)
This article was republished with the author's permission.

* Bruce Schneier is an internationally renowned security technologist and author. Described by The Economist as a "security guru", he is the author of Applied Cryptography, Secrets and Lies, Beyond Fear and Schneier on Security. Regularly quoted in the media - and subject of an Internet meme - he has testified on security before the United States Congress on several occasions and has written articles and op eds for many major publications, including The New York Times, The Guardian, Forbes, Wired, Nature, The Bulletin of the Atomic Scientists, The Sydney Morning Herald, The Boston Globe, The San Francisco Chronicle, and The Washington Post. Schneier also publishes a free monthly newsletter, Crypto-Gram, with over 150,000 readers. In its ten years of regular publication, Crypto-Gram has become one of the most widely read forums for free-wheeling discussions, pointed critiques, and serious debate about security. Schneier is the Chief Security Technology Officer of BT.
More from the author can be found at www.schneier.com