

Cyberweapons: A Bad Idea

Neil C. Rowe
U.S. Naval Postgraduate School
ncrowe at nps.edu
February, 2010

Cyberweapons have recently been subject of much discussion. The U.S. has, for instance, publicly expressed lack of interest in developing treaties outlawing their use. This is a foolish position.

Cyberweapons are software that exploits bugs or flaws in other software. Such bugs and flaws are present because it is difficult for software vendors to find and remove all of them. Strong incentives to make software needlessly complicated (as with the most recent versions of the Windows operating system) and needlessly diverse (as with the superfluity of networking protocols) also increase the number of bugs and flaws. While techniques of good software engineering can reduce their numbers, these methods are not always cost-effective for the vendor. And while there are ways to reduce the harms of bugs and flaws by access controls, network monitoring, and vulnerability scanners, these ways hurt friendliness of systems and many computer users will not accept this. We cannot depend on free-market mechanisms to improve things because computer software tends towards monopolies like those of Microsoft and Google.

A weapon that critically depends on bugs and flaws in something else will be a temperamental and unreliable weapon. For one thing, bugs and flaws can get fixed, and then the weapon will fail. They are getting fixed all the time as they are discovered in software by a large community of system administrators and information-security personnel that freely shares information through a wide range of Web sites. Furthermore, cyberweapons themselves are software and subject to bugs and flaws of their own. In fact, they will have higher rates of bugs and flaws than the software they attack because it is difficult to test them adequately. Cyberweapon effectiveness depends upon small details of the victim computer systems, and it is hard to duplicate these conditions exactly to properly test the cyberweapon.

The dependence of cyberweapons on bugs and flaws also means that cyberweapons will quickly stop working after their first use, since information-security experts can usually quickly figure what bug or flaw the attack is exploiting and then fix it. So cyberweapons are prohibitively expensive to develop in terms of cost-benefit ratio. This means that only large and powerful countries and organizations have the resources to develop significant numbers of them. But large and powerful countries also have the most cyberinfrastructure, and have the most to lose by an attack on themselves. Using a cyberweapon is the best incentive possible for a victim to use a cyberweapon in response, and even a weak country can get lucky and hit upon a powerful cyberweapon by random search. So any attempt a powerful nation like the United States to use cyberweapons is likely to backfire and hurt the United States worse than it hurts the other country.

Proponents of cyberweapons claim they are relatively benign as nonlethal weapons. But this is not clear. Cyberweapon effects can cover an enormous range, much greater than that of explosives technology, depending on their targets and methods. Cyberweapons can target any computer system including those of critical infrastructure, and networks make societies increasingly connected so that attacks can spread. The unreliability of cyberweapons means that attacks could easily attack unintended targets with unnecessarily powerful force. Furthermore, unreliability encourages attacks to attempt overkill of a target in the hope of ensuring at least some damage. Overkill on incorrect targets is a recipe for high collateral damage with cyberweapons. Since we depend so much upon computer technology, uncontrollability could harm people and even cause death when it effects medical, food, or habitation infrastructure.

The damage of cyberweapons can be highly persistent because it can be hard to localize within code or data. Changes to a few bits in code leave no clues. Reinstalling software or copying data from backup is possible, but for many systems, it is very time-consuming and expensive. That means damage to computer systems can persist for long periods of time in victims without the necessary technical resources and personnel to figure out what has happened to them and fix it. Thus on them, the effects of cyberweapons could be analogous to those of biological weapons or, to pick a more specific analogy, the poisoning of groundwater. While some techniques can make cyberweapons more easily reversible, militaries currently have little incentive to do so.

Since cyberweapons are such ugly weapons, they should be outlawed to whatever extent possible by international agreement. To address the great range of harm possible with cyberweapons, we should seek agreements to forgo use of the most dangerous forms, much as we have done with other weapons. The most dangerous would be computer viruses and worms, which can spread autonomously and thus risk spread to civilian computers; attacks not making their sources clear, which are akin to terrorism; and hiding of "Trojan horses" of malicious code within essential software infrastructure such as operating systems and Web support. Negotiating such agreements is critical for the United States, which is more dependent than its adversaries on cyberinfrastructure.