Chapter XIV
Ethics of Cyber War Attacks

Neil C. Rowe
U.S. Naval Postgraduate School, USA

ABSTRACT

Offensive cyber warfare raises serious ethical problems for societies, problems that need to be addressed by policies. Since cyber weapons are so different from conventional weapons, the public is poorly informed about their capabilities and may endorse extreme ethical positions in either direction on their use. Cyber weapons are difficult to precisely target given the interdependence of most computer systems, so collateral damage to civilian targets is a major danger, as when a virus aimed at military sites spreads to civilian sites. Damage assessment is difficult for cyber war attacks, since most damage is hidden inside data; this encourages massive attacks in the hopes of guaranteeing some damage. Damage repair may be difficult, especially for technologically primitive victim countries. For these reasons, some cyber war attacks may be prosecutable as war crimes. In addition, cyber-war weapons are expensive and tend to lose effectiveness quickly after use as they lose the element of surprise, so the weapons are not cost effective.

CRITERIA FOR ETHICAL ATTACKS

Ethics starts with laws. International laws of war ("jus in bello") try to regulate how wars can be legally fought (Gutman & Rieff, 1999). The Hague Conventions (1899 and 1907) and Geneva Conventions (1949 and 1977) are the most important. While most cyber war attacks do not appear to fall into the category of "grave breaches" or "war crimes" as per the 1949 Geneva Conventions, they may still be illegal or unethical. Article 51 of the 1977 Additional Protocols of the Geneva Conventions prohibits attacks that employ methods and means of combat whose effects cannot be controlled or whose damage to civilians is disproportionate. Article 57 says "Constant care shall be taken to spare the civilian population, civilians, and civilian objects"; cyber weapons are difficult to target and difficult to assess in their effects. The Hague Conventions prohibit weapons that cause unnecessary suffering; cyber-attack weapons can cause mass destruction to civilian computers that is difficult to repair. Arquilla (1999) generalizes on the laws to suggest three main criteria

for an ethical military attack: noncombatant immunity during the attack, proportionality of the size and scope of the attack to the provocation (i.e., nonoverreaction), and that the attack does more good than harm. All are difficult to guarantee in cyberspace. Nearly all authorities agree that international law does apply to cyber warfare (Schmitt, 2002).

We examine here the application of these concepts to cyber war attacks (or "cyber attacks"), that is, attacks on the computer systems and computer networks of an adversary using "cyber weapons" built of software and data (Bayles, 2001; Lewis, 2002). A first problem is determining whether one is under cyber attack (or is a defender in "information warfare"), since it may not be obvious (Molander & Siang, 1998). Manion and Goodrum (2000) note that legitimate acts of civil disobedience, such as spamming oppressive governments or modifying their Web sites, can look like cyber attacks and need to be distinguished by their lack of violence. Michael, Wingfield, and Wijiksera (2003) proposed criteria for assessing whether one is under "armed attack" in cyberspace by implementing the approach of Schmitt (1998) with a weighted average of seven factors: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. Effective cyber attacks are strong on immediacy and invasiveness (most subvert an adversary's own systems). But they can vary greatly on severity, directness, and measurability, depending on the methods. There is no presumption of legitimacy for cyber attacks; and responsibility is notoriously difficult to assign in cyberspace. These make it hard to justify counterattacks to cyber attacks.

PACIFISM AND CONDITIONAL PACIFISM

A significant number of the world's people believe that military attacks are unjustified regardless of the circumstances—the idea of "pacifism" (Miller, 1991). Pacifism can be duty-based (from the moral unacceptability of violence), pragmatics-based (from the rarity of net positive results from attacks), or some combination of these. Duty-based pacifists are most concerned about the violence and killing of warfare, and cyber attacks could be more acceptable to them than conventional attacks, if only data is damaged. But nonviolence may be hard to guarantee in a cyber attack, since, for instance, the nonviolent disabling of a power plant may result in catastrophic accidents, looting, or health threats. To pragmatics-based pacifists, war represents a waste of resources and ingenuity that could be better spent on constructive activities (Nardin, 1998), and this applies equally to cyber warfare. To them, cyber attacks are just as unethical as other attacks because both are aggressive antisocial behavior. Most psychologists do see types of aggression on a continuous spectrum (Leng, 1994).

More popular than pure pacifism are various kinds of "conditional pacifism," which hold that attacks are permissible under certain circumstances. The most commonly cited is counterattack in response to attack. The United Nations Charter prohibits attacks by nations unless attacked first (Gutman & Rieff, 1999), and the wording is sufficiently general to apply to cyber attacks. Counterattacks are only allowed in international law against nation-states, not groups within countries like "terrorists," however they may be defined. Arquilla 1999) points out, however, that cyber attacks are such a tempting form of first attack that they are likely to be popular for surprise attacks.

COLLATERAL DAMAGE IN CYBER ATTACKS

Cyber attacks exploit vulnerabilities of software, both operating systems and applications. Unfortunately, the increasing standardization of software means that military organizations often use the same software as civilians do, and much of this software has the same vulnerabilities. Many viruses and worms that could cripple a command-and-control network could just as easily cripple a civilian network. And the increasing interconnection of computers through networks means