2007

Ethics of cyberwar attacks / Chapter in Cyber War and Cyber Terrorism

Rowe, Neil C.

Monterey, California. Naval Postgraduate School

This is a chapter in Cyber War and Cyber Terrorism, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.
https://hdl.handle.net/10945/36452

Ethics of cyberwar attacks

Neil C. Rowe

U.S. Naval Postgraduate School

Abstract

Offensive cyberwarfare raises serious ethical problems for societies, problems that need to be addressed by policies. Since cyberweapons 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. Cyberweapons 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 cyberwar 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 cyberwar attacks may be prosecutable as war crimes. In addition, cyberwar weapons are expensive and tend to lose effectiveness quickly after use as they lose their element of surprise, so the weapons are poorly cost-effective.

This is a chapter in *Cyber War and Cyber Terrorism*, ed. A. Colarik and L. Janczewski, Hershey, PA: The Idea Group, 2007.

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 cyberwar 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, and Article 57 says "Constant care shall be taken to spare the civilian population, civilians, and civilian objects"; cyberweapons 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. non-overreaction), 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 cyberwarfare (Schmitt, 2002).

We examine here the application of these concepts to cyberwar attacks (or "cyber-attacks"), attacks on the computer systems and computer networks of an adversary using "cyberweapons" 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 & Goodrum, 2000) notes 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, & Wijesekera, 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 their 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 of 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 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 there are many routes by which an attack could spread from a military organization’s computers to those of civilian "innocent bystanders" (Westwood, 1997; Arquilla, 1999). Military systems try to isolate themselves from civilian systems but are not very successful because access to the Internet simplifies many routine tasks. Furthermore, information flow from civilian to military systems is often less restricted than flow in the other direction, which actually encourages an adversary to first attack civilian sites.

Disproportionate damage to civilians is a key issue in the Geneva Conventions. Incomplete knowledge of an adversary’s computer systems may worsen the spread of the attack to civilians: What may seem a precisely targeted disabling of a software module on a military computer may have profound consequences on civilian computers that happen, unknown to attackers, to use that same module. And even if attackers think they know the addresses of target military computers, the adversary may change their addresses in a crisis situation, or have meanwhile given their old addresses to civilian computers. Another problem is that it is easy to create disproportionately greater damage to civilian computers by a cyber-attack since there are usually more of them than military computers and their security is not as good. Cyber-attacks are more feasible for small organizations like terrorist ones than conventional warfare is feasible for them (Ericsson, 1999), but such organizations may lack the comprehensive intelligence necessary to target their adversary precisely. In addition, it can be tempting to attack civilian systems anyway for strategic reasons. Crippling a few sites in a country’s power grid, telephone system, or banking system can be more damaging to its capacity to wage war than disabling a few command-and-control centers, considering the backup sites and redundancy in most military command-and-control systems.

Another collateral-damage problem is that staging a cyber-attack almost invariably requires manipulating a significant number of intermediate computers between the attacker and the victim since such route-finding has been deliberately made difficult. In fact, a route may even be impossible, since critical computers can be “air-gapped” or disconnected from all external networks. This means attackers need to do considerable exploratory trespassing, perhaps fruitlessly, to find a way to their target. (Himma, 2004) points out that cyber-trespassing is poorly justified on ethical grounds: Even if it were in pursuit of a criminal, which is often not true for cyber-attacks, police do not have to right to invade every house into which a criminal might have fled. Trespassing on computers also steals computation time from those computers without permission, slowing their legitimate activities.

Reducing collateral damage

Two factors can mitigate collateral damage from cyber-attacks, targeting precision and repair mechanisms. Cyber-attacks can often be designed to be selective in what systems they attack and what they attack in those systems. Systems can be defined by names and IP addresses, and attacks can be limited to a few mission-critical parts of their software. So an attack might disable “instant messaging” while permitting (slower) email, or insert delays into key radar defense systems; but use of denial-of-service by swamping resources with requests would be too broad in effects to justify ethically. However, naturally an adversary will make it difficult to get accurate information about their computer systems, their “electronic order of battle”. They could deliberately mislead attackers as to the

addresses and natures of their sites, as with “honeynets” or fake computer networks (The Honeynet Project, 2004). Furthermore, (Bissett, 2004) points out that modern warfare rarely achieves its promise of precise “surgical strikes” for many reasons that apply to cyber-attacks: political pressures to use something new whether or not it is appropriate, the inevitable miscalculations in implementing new technology, lack of feeling of responsibility in the attacker due to the technological remoteness of the target, and the inevitable surprises in warfare that were not encountered during testing in controlled environments.

An intriguing possibility for ethical cyber-attacks is to design their damage to be easily repairable. For instance, damage could be in the form of an encryption of critical data or programs using a secret key known only to the attacker, so performing a decryption could repair the damage. Or a virus could store the code it has replaced, enabling substitution of the original code later, but this is hard to do when viruses attack many kinds of software. Repair procedures could be designed to be triggerable by the attacker at a time that they choose, or could be kept in escrow by a neutral party such as the United Nations until the termination of hostilities.

Damage assessment for cyber-attacks

Damage assessment is difficult in cyberspace. When a computer system does not work, it could be due to problems in any number of features; for instance, code destruction caused by a virus can be scattered throughout the software. Unlike with conventional weapons, determining how many places are damaged is difficult since often damage is not apparent except under special tests. This encourages more massive attacks than necessary to be sure they cause sufficient damage. The difficulty of damage assessment also makes repair difficult. Damage may persist for a long time and its cumulative effect may be great even when it is subtle, so noncombatant victims of a cyber-attack could continue to suffer long afterwards from attacks on military computers that accidentally spread to them, as with attacks by chemical weapons. Repair can be accomplished by just reinstalling software after an attack, but this is often unacceptable since it loses data. With "polymorphic" or shape-changing viruses, for instance, it may be hard to tell which software is infected; if the infection spreads to backup copies, then reinstalling just reinfects. Computer forensics (Mandia & Prosise, 2003) provides tools to analyze computer systems after cyber-attacks, but their focus is determining the attack mechanism and constructing a legal case against the perpetrator, not repair of the system.

Determining the perpetrators and victims

Even if an attack minimizes collateral damage, it can be unethical if it cannot be attributed. It can be difficult to determine the perpetrator of a cyber-attack because most attacks must be launched through a long chain of jurisdictions enroute to the victim. Route-tracing information is not available on all sites, and even when it is available, stolen or guessed passwords may mean that users have been impersonated. So a clever attacker can make it appear that someone else has launched the attack, although this violates the prohibition in international law against ruses like combatants wearing the wrong uniforms. In addition, a cyberspace attacker may not be a nation but a small group of individuals or even a single individual acting alone. So just because you have traced an attack to a country does not mean that country is responsible. This makes counterattack difficult to justify in cyberspace, as well as risking escalation even if it correctly guesses the attacker. Legally and ethically, people should be responsible for software agents acting on their behalf (Orwant, 1994) so unjustified indirect attacks and counterattacks are as unethical as direct attacks.

Intended victims of attacks may also be unclear, which also makes it difficult to legitimize counterattacks. Suppose an attack targets a flaw in a Microsoft operating system on a computer used by an international terrorist organization based in Pakistan. Is this an attack on Pakistan, the terrorist organization, or Microsoft? Nations often think that attacks within their borders are attacks on the nation, but if the nation does not support the terrorist group, it would be unfair to interpret it as the target. Multinational corporations like Microsoft have attained the powers of nation-states in their degree of control of societies, so they can certainly be targets too. But chaos can ensue if entities other than nation-states think they can wage war.

Reusability of cyber-attacks

Cyber-attacks have a peculiar problem not shared by traditional attacks: They can generally be highly effective only once (Ranum, 2004). Analysis of an attack by the victim usually reveals the software that was exploited and the vulnerabilities in it. This software can be immediately disabled, and then fixed (“patched”) to prevent a repeat of the attack (Lewis, 2002). News of the attack can be quickly disseminated through vulnerability-clearinghouse Web sites like www.kb.cert.org, cve.mitre.org, and www.securityfocus.com so that other potential victims can be quickly protected, and automatic downloading of a security update for all installations can be

initiated by the vendor. This can be accomplished nowadays within a few days. So if an attacker tries the same attack later, it is likely to much less effective. Countermeasures can also be found, independently of attacks, by security professionals in testing and analyzing software, so a new attack may be foiled before it can ever be used.

On the other hand, cyber-attacks are costly to develop. "Zero-day" or new attacks are the most effective ones, but new weaknesses in software that no one has found are rare and difficult to find. Software engineers are getting better at analyzing and testing their software for security holes. Another problem is that at least part of a new attack ought to be pretested against an adversary to see if the adversary is vulnerable to it, since there are many variables (like the version of software that the adversary is running) that may prevent the success of an attack; such initial testing can warn the adversary of the type of full attack to come. Thus, generally speaking, research and development of cyber-attacks appears highly cost-ineffective and a waste of resources, and thus ethically questionable.

Secrecy and cyber-attacks

A related problem with cyber-attacks is the greater need for secrecy than with traditional attacks. With bombs one does not need to conceal the technology of the explosives from the adversary, because most of it is well known and bigger surprises are possible with the time and place for attacks. But knowledge about the nature of cyber-attacks and their delivery mechanisms usually entails ability to stop them (Denning, 1999). Time and place do not provide much surprise since everyone knows attacks can occur anytime at any place. Thus cyber-attacks require secrecy of methods for a significant period of time from the discovery of the attack to its employment. Since many adversaries have intelligence resources determined to ferret out secrets, this secrecy can be very difficult to achieve. (Bok, 1983) points out other disadvantages of secrecy, including the encouragement of an elite out of touch with the changing needs of their society. Secrecy also promotes organizational inefficiency since organizations easily may duplicate the same secret research and development. Thus cyber-attack secrecy can be argued to be questionable on ethical grounds.

Policy for ethical cyber-attacks

(Hauptman, 1996) argues that computer technology is sufficiently advanced that we should have a full ethics for it, not just a set of guidelines. So cyberwarfare should have ethics policies with associated justifications. (Arquilla, 1999) proposes some possible policies. One is a “no first use” pledge for cyber-attacks analogous to pledges on other kinds of dangerous weapons. Another is that cyber-attacks should only be in response to cyber-attacks, and should be proportionate to the attack. Another is a pledge simply to never use cyberweapons since they can be weapons of mass destruction. When cyberweapons are used, additional policies could require that the attacks have distinctive non-repudiable signatures that identify who is responsible and their intended target, or that attacks be easily reversible. Policy is also needed on the status of participants in cyberwar, as to whether they are soldiers, spies, civilians, or something else (Nitzberg, 1998).

Conclusion

Cyber-attacks raise many serious ethical questions for societies since they can cause mass destruction. They raise so many questions that it is hard for a responsible country to consider them as a military option, so they are somewhat like chemical or biological weapons although not as bad. Although cyberweapons can be less lethal than other weapons and can sometimes be designed to have reversible effects, their great expense, their lack of reusability, and the difficulty of targeting them precisely usually makes them a poor choice of weapon. International law should prohibit them and institute serious punishments for their use.

References

Arquilla, J. (1999). Ethics and information warfare. In Khalilzad, Z., White, J., & Marsall, A., (Eds.), *Strategic appraisal: the changing role of information in warfare* (pp. 379-401). Santa Monica, California: Rand Corporation.
Bayles, W. (2001, Spring). Network attack. *Parameters, US Army War College Quarterly, 31,* 44-58.
Bissett, A. (2004, January). High technology war and "surgical strikes". *Computers and Society (ACM SIGCAS), 32* (7), 4.
Bok, S. (1986). *Secrets.* Oxford, UK: Oxford University Press.
Denning, D. (1999). *Information warfare and security.* Boston: Addison-Wesley.
Ericsson, E. (1999, Spring/Summer). Information warfare: hype or reality? *The Nonproliferation Review, 6* (3), 57-64.

Gutman, R., & Rieff, D. (1999). *Crimes of war: what the public should know.* New York: Norton.
Hauptman, R. (1996). Cyberethics and social stability. *Ethics and Behavior, 6* (2), 161-163.
Himma, K. (2004). The ethics of tracing hacker attacks through the machines of innocent persons. *International Journal of Information Ethics, 2* (11), 1-13.
The Honeynet Project, *Know Your Enemy, 2nd Ed*. Boston: Addison-Wesley, 2004.
Leng, R. (1994). Interstate crisis escalation and war. In Portegal, M., & Knutson, J., *The Dynamics of Aggression* (pp. 307-332). Hillsdale, NJ: Lawrence Erlbaum.
Lewis, J. (2002, December). Assessing the risks of cyber-terrorism, cyber war, and other cyber threats. Center for Strategic and International Studies, Washington, DC. Retrieved November 23, 2005 from www.csis.org.
Mandia, K., & Prosise, C. (2003). *Incident response and computer forensics.* New York: McGraw-Hill / Osborne.
Manion, M., & Goodrum, A. (2000, June). Terrorism or civil disobedience: toward a hacktivist ethic. *Computers and Society (ACM SIGCAS), 30* (2), 14-19.
Michael, J., Wingfield, T., & Wijiksera, D. (2003, November). Measured responses to cyber attacks using Schmitt analysis: a case study of attack scenarios for a software-intensive system. *Proc.27th IEEE Computer Software and Applications Conference*, Dallas, Texas.
Miller, R. (1991). *Interpretations of conflict: ethics, pacifism, and the just-war tradition*. Chicago, IL, USA: University of Chicago Press.
Molander, R., & Siang, S. (1998, Fall). The legitimization of strategic information warfare: ethical considerations. *AAAS Professional Ethics Report, 11* (4). Retrieved November 23, 2005, from www.aaas.org/spp/sfrl/sfrl.htm.
Nardin, T. (Ed.) (1998). *The ethics of war and peace*. Princeton, NJ, USA: Princeton University Press.
Nitzberg, S. (1998, October). Conflict and the computer: information warfare and related ethical issues. *Proc. 21st National Information Systems Security Conference*, Arlington, VA, D7.
Orwant, C. (1994, November). EPER ethics. *Proc. of the Conference on Ethics in the Computer Age*, Gatlinburg, Tennessee, 105-108.
Ranum, M. (2004). *The myth of homeland security.* Indianapolis: Wiley.
Schmitt, M. (1998). Bellum Americanum: the U.S. view of twenty-first century war and its possible implications for the law of armed conflict. *Michigan Journal of International Law, 19*(4), 1051-1090.
Schmitt, M. (2002, June). Wired warfare: computer network attack and jus in bello. *International Review of the Red Cross, 84* (846), 365-399.
Westwood, C. (1997). *The future is not what it used to be: conflict in the information age.* Fairbairn, ACT, Australia: Air Power Studies Center.

Key terms

Collateral damage: Damage from an attack to other than the intended targets.
Computer forensics: Methods for analyzing computers and networks to determine what happened to them during a cyber-attack, with the hope of repairing the damage and preventing future similar attacks.
Cyber-attack: Offensive acts against computer systems or networks.
Cyberwar: Attacks on computer systems and networks by means of software and data.
Cyberweapon: Software designed to attack computers and data.
Jus in bello: International laws for conducting warfare.
Pacifism: An ethical position opposed to warfare and violence.
Patch: Modification of software to fix vulnerabilities that a cyber-attack could exploit.
Zero-day attack: A cyber-attack that has not been used before.