

# **The Ethics of Cyberweapons in Warfare**

**Neil C. Rowe**

*Center for Information Security, U.S. Naval Postgraduate School, United States  
ncrowe@nps.edu*

This appeared in the *International Journal of Cyberethics*, Vol. 1, No. 1, pp. 20-31, January-March 2010.

## **ABSTRACT**

We discuss the ethical issues of using cyberweapons, software that attacks data and other software during warfare. Many people assume these are relatively benign weapons, but we argue they can create serious harms like any weapon. We define cyberweapons and describe them in general terms, and survey their status as per the laws of war. We then discuss the unreliability of cyberweapons, the problem of collateral damage, and the associated problems of damage assessment, maintenance of secrecy, and mounting cyber-counterattacks. We examine some possibilities for creating more ethical cyberweapons and discuss the alternative of cyber-blockades. We conclude that cyberattacks should generally be outlawed by international agreement.

*Keywords:* cyberattack, ethics, weapons, cyberweapons, vulnerability, perfidy, collateral damage, secrecy, damage assessment, attribution

## **INTRODUCTION**

Cyberweapons are software used to attack other software or data within computer systems (Bayles, 2001). We distinguish cyberweapons and cyberattacks (attacks using cyberweapons) from “information warfare”, a more general term that includes propaganda, electronic surveillance, cyber-espionage, and defensive information operations (Jones, Kovacich, and Luzwick, 2002). That is, we will focus on “information attack” and not “information exploitation” or “information defense”.

Like conventional weapons, cyberweapons can be used against a variety of targets in a variety of circumstances with a wide range of lethality (White Wolf Security, 2009). Often cyberweapons exploit flaws or errors in software. Proponents have cited these as “clean” weapons that are safer than conventional weapons since they do not damage physical objects (Libicki, 2007). Furthermore, unlike chemical, biological, and nuclear weapons, people have no visceral fear of cyberweapons for reasons like health consequences. But maybe they should. All weapons can have serious harms by virtue of their being weapons. The public is unaware of the degree to which they depend on computer systems and the information they store, and thus weapons targeting them can have many unforeseen consequences. For instance, targeting a country’s Internet service providers can prevent goods from being delivered and cause people to starve or die from lack of necessary medical supplies.

There are several schools of ethics. In this article we will follow a pragmatic approach derived from utilitarian ethics in which we argue that a technology is unethical if it has a significant net harm to world society ("negative utilitarianism"). We would also like to derive ethical principles of using cyberweapons, so we will follow "rule utilitarianism". Such principles can then be codified in laws of warfare. However, we do not need an elaborate ethical foundation here because most of the ethical issues with cyberattacks seem quite similarly problematic under any ethical framework.

## **THE STATE OF THE ART IN CYBERWEAPONS**

Military organizations have noted the success of amateur attackers ("hackers") in damaging computer systems, and have hoped to use these techniques for military advantage, much as they seek a wide variety of ways to gain advantage in warfare (Denning, 1999). Many of these techniques exploit flaws in software. Certain kinds of errors such as failure to check for buffer overflows in loops or failure to properly embed constants on Web sites can lead to granting of unauthorized special privileges to users of a system. Cyberweapons are programs that package a set of such exploits against a computer system and its data. Cyberweapons can be launched or controlled either externally (from another computer or the Internet) or internally like spies and saboteurs (Knapp & Boulton, 2007).

Cyberattackers can use their access and privileges to destroy the data and software on a computer system or network. But that is pretty obvious and tells the victim they have been attacked. Attacks that modify the data on a victim system to impede military operations are possible, but require a good deal of contextual knowledge about the data. So a better goal for cyberweapons, especially those produced by governments, is to use those special privileges to take control of a system without the knowledge of the system's owner, using it for the attacker's purposes whenever they like. This technology is called "rootkits" (Kuhnhauser, 2004). Controlled computers can be used to create "botnets", or large sets of slave computers under the control of a single user (Bailey et al, 2009). Hacker botnets have been used to earn money by sending spam or phishing email from the slave computers, have been used for denial-of-service attacks against organizations the attacker does not like, have been used for blackmail of organizations by threatening malicious mischief, and have been used for espionage. Botnets developed for military purposes could stop an adversary's military organization from communicating or defending itself.

Cyberweapons can be an innocent-looking software module. Running them to see what they do is not easy because many require passwords to run and their effects may be very subtle. Thus it is difficult to identify cyberweapons within a computer system. Cyberweapons are easy to

transport because they are just bit patterns that can be easily copied, or they can even move around autonomously as mobile “agents” (Ceruti, 2001). And when they have served their purpose, they can be deleted. This makes it considerably harder to police cyberweapons than nuclear, chemical, and biological weapons. Nonetheless, traces of a cyberattack will be visible on the victim’s computers and networks, and range of methods of "computer forensics" (Mandia & Prosis, 2003) can help track their effect.

Cyberweapons can attack many kinds of military targets. An obvious one is an adversary's "command-and-control" systems, their communications and electronic mail. Since these are distributed across many machines, there are many potential entry points for an attack. Weapons-controlling and vehicle-controlling software are also preferred targets, but harder to attack because they are carefully protected and often (especially for weapons) do not interact much with networks. Logistics and supply could be targeted, but effects would not be immediate, and surprise is a key element of cyberattack effectiveness. Administrative support for the military could be targeted, because its protections tend to be less detailed, but again the effects would not be immediate, and troops like to think they can fight just fine without administrators. Public relations (like Web sites) might actually be a good target, because public perception is so much a part of winning a war.

Conventional military attacks can enhance their effect by including a simultaneous cyberattack. For instance, China has continued to claim sovereignty over the island of Taiwan, but Taiwan has formidable defenses and the support of the U.S. Navy. If China were to attack, they would need all the resources they could muster, and a simultaneous cyberattack could be very helpful considering the heavy reliance of the U.S. Navy on software and digital data.

Cyberattacks can also target a country's important civilian infrastructure such as its Internet sites, its financial services sector, its power grid, or even the common software it uses. Recent media attention in the United States raises the possibility of this form of terrorism, and the Department of Homeland Security has been studying it. But attacks on nonmilitary targets are generally outlawed by the international warfare conventions, with exceptions for strong military necessity. They are not guaranteed to succeed because there is considerably less centralization in the civilian sector than there is in military organizations, and it is hard to hit a sufficient number of targets to achieve the effect of a conventional military attack. They are also not the first choice of competent military commanders because the commanders' biggest concern is preventing counterattacks, and unless they primarily target a country's military, they will receive counterattacks. Terrorist cyberattacks might be more likely to have civilian targets because terrorist organizations are hard to find and track. Nonetheless, a terrorist organization needs to

do public relations for recruitment, needs to acknowledge attacks to gain a public-relations benefit, and this provides a start in tracking them down.

Cyberweapons development has been reported in several major countries in the last few years. Most reports have focused on China which has ambitious goals for military operations in cyberspace, but other countries with software expertise such as Russia have also been mentioned. The United States military does not like to lag technologically behind anyone; recent announcement of a U.S. Air Force "Cyberspace Command" (24th Air Force Command) suggests the United States is now investigating these weapons in secret work. Cyberweapons need not be confined to advanced countries, however, because the technology for developing them does not require much capital investment. It does require expertise in software, which limits their development in countries with poor educational systems. Cyberweapons could be used by terrorist groups (Verton, 2003), but it seems unlikely in the near future since most groups today are anti-technology or, like Al Qaeda, forced to avoid it to avoid being tracked.

## **LAW FOR CYBERATTACKS**

Cyberattacks using cyberweapons are activities that would be classified as crimes in their victim countries if done by ordinary citizens. Necessarily they involve trespassing; to be effective they must employ fraud and vandalism; and many cases they also involve espionage, sabotage, and virtual assaults. In many cases they violate international war conventions as well (Arquilla, 1999). While enforcement of international laws of war has been inconsistent, enforcement has been increasingly successful in recent years, so they should be taken seriously.

A particularly troubling issue with cyberattacks is their frequent use of identity deceptions of various kinds, such as by the concealed modifications of an operating system done by rootkits, or the masquerading as legitimate users while concealing a malicious intent. This brings cyberattacks often close to perfidy, a war crime outlawed by international law. Perfidy is attackers masquerading as a legitimate civilian activity, such as soldiers pretending to be Red Cross workers. Perfidy is considered unacceptable because it blurs the distinction between combatants and noncombatants, and encourages attacks on civilians. It is certainly fair for combatants to use camouflage. But an operating system is essential to use a computer, so compromising it and turning it into a computer-virus delivery tool is like putting a poison in a community's water system. The argument for perfidy is strongest for the critical parts of an operating system for enforcing access controls, the "kernel", since everyone relies on them and there is no legitimate reason to tamper with them. Other possible candidates for perfidy are tamperings with the key networking software such as routers and as TCP/IP protocols since they are essential for many cyberspace activities.

Perpetrators of cyberattacks can also be subject to civil legal proceedings for damages in many countries. If someone damages a computer or data, the owner of the computer or data can sue the attacker. If the victims are sufficiently widespread within a country, the entire country may be able to sue an attacker, even if it is another country, using international tort law. Cyberattacks also can be unethical even if legal. Much literature over the years has addressed the ethics of warfare (Walzer, 1977; Nardin, 1998) and many of the ideas extend to cyberweapons. Unethical behavior can be punished by activities like cyber-blockades as discussed below.

A possible analogy to cyberweapons are biological weapons, weapons that cause illness and disease (Lederberg, 1999). These have been banned by international convention because they affect military and civilian personnel equally and are difficult to target exclusively to military personnel. Targeting is difficult because biological agents can spread unpredictably due to wind, contacts, and normal biological processes. Perhaps the best analogy to cyberweapons is that of biological warfare against crops (Whitby, 2002), banned by the Biological and Toxin Weapons Convention of 1972. Crops are necessary resources that everyone in society needs, and are societal infrastructure. Attacking them is akin to terrorism.

Analogously, cyberwarfare does not target military personnel directly but only their software and data. But usually cyberattacks will be effective against any computer with the same type of vulnerable software. Military organizations use mostly software that is also used by civilians. So civilian computers could also suffer from military cyberattacks; in fact, they are usually more vulnerable because their countermeasures are not as good. If an attack on a military target goes astray, or if an attack propagates from a military target, civilian computers can easily be damaged. Or it may be tempting for a nation with cyberweapons to deliberately attack civilian computers and networks to cripple the economy of a target country, even though this violates international law. The Allies in World War II deliberately targeted civilian centers with bombing because they thought it would end the war more quickly.

## **RELIABILITY AND EFFECTIVENESS**

One obvious difference between cyberattacks and conventional military attacks is in reliability and effectiveness of the attack. If you fire a bullet at a target, it is highly likely to arrive there. If you execute cyberattack software against a cyber target, the odds are not good that it will work. For one thing, software-based systems can fail in many more ways than a bullet (Neumann, 1995). For another, the attack design itself may be faulty, the attack may not be able to find the target, or the target may not be vulnerable to the attack because assumptions made about it are no

longer valid. But computers and software can be precise and highly controllable tools, so why cannot cyberweapons be made precise and controllable too?

Some of the problem lies in the nature of warfare. To defend yourself in warfare, you need to hide and harden your assets. Military computers and software are known targets of adversaries, and governments try to limit their use to authorized personnel by passwords, encryption, and other access controls. They also try to conceal them on special networks behind layers of firewalls, or leave them unconnected to networks as in the case of weapons systems. System configurations like IP addresses can be changed periodically to foil overly specific attacks, and decoy machines and "honeypots" (attack-data gathering machines) can confuse an adversary and collect data about them. Network and system logging can track who is using systems and how, so abnormal usage can be caught quickly. So it is easy to see how a cyberattack could fail, how cyberweapons are likely to be quite unreliable, and how "surgical strikes" are unlikely in cyberspace (precise targeting is still rare with conventional bombs, as discussed in (Bissett, 2004)).

Another problem with cyberweapons is just that they are new kinds of weapons and all new weapons have high error rates and low reliability (Dunnigan, 2003). An analogous problem occurs with new conventional weapons like military aircraft, which because of their complexity are often delivered late and overbudget, and often show at first to be ineffective in combat. This is because new technology is complicated and many things can go wrong. Software technology in particular permits implementation of very complex mechanisms. An exacerbating factor is that cyberweapons are poorly understood by military commanders since few have expertise in software. This means that commanders will tend to use cyberweapons, more than regular weapons, against the wrong targets in the wrong circumstances to achieve the wrong goals.

Will cyberweapons improve in reliability and effectiveness with time? It is unlikely, as software in general is not getting any more reliable (Neumann, 1995). More specifically, cyberattacks depend on the novelty of their methods and secrecy to enforce it (as we discuss below). There are a limited number of attack methods and they generally can be used only once. So attackers will chronically suffer from inability to practice their attacks, and the likelihood of success of cyberattacks is not likely to increase.

## THE RISK OF COLLATERAL DAMAGE IN CYBERSPACE

“Collateral damage” or accidental harm to civilians is a key issue in both ethics and laws of warfare. Unfortunately, it is quite possible for cyberattacks aimed at military targets to accidentally hit civilian targets due to their relatively high degree of unreliability and uncontrollability. Firstly, it can be hard to distinguish a military computer from a civilian computer. The localization of the target in physical space and identification from its appearance that help so much in conventional warfare have no counterpart in cyberspace. Cyberspace addresses can be spoofed so a site can masquerade as another. Military organizations often use the same operating systems, bookkeeping, word-processing, and presentation software as businesses because it saves money (Jones, Kovacich, & Luzwick, 2002), so examining the software may not indicate a military system. Most military files and data look just like files and data from any large civilian business, and like them are undecipherable without knowing a good deal of specific jargon. (Some specialized sites can be more easily recognized, such as those controlling power plants, but they should be well protected.) Within a military site, it may be hard to distinguish non-warfare information such as that about hospitals and humanitarian operations like disaster relief from warfare information, so there could be intrasite collateral damage too; on a battlefield, it is easier to distinguish a tank from a Red Cross truck. Although many military computers have military network names and addresses, they could be camouflaged with a civilian name or address to reduce the chances of an adversary finding it (although it is harder in the U.S. where military site names all end in “.mil”). A clever adversary might also camouflage a civilian computer as a military one to provoke an adversary to attack it in the hope of provoking international outrage.

Secondly, because of the difficulty of reaching military targets for a network-based attack or management of an internal attack, it is tempting to use other systems as “stepping stones” which the cyberattack subverts in a chain to reach the target machines. It is appealing to use civilian machines as stepping stones because many (like home computers) have minimal security. Damage to the stepping stones will usually occur in setting up communications, and it is still trespassing and is illegal in most countries (Himma, 2004).

Thirdly, even if a civilian computer is not attacked by mistake or as part of a chain, an attack may spread to it. Some cyberattacks use computer viruses and worms that can propagate from one computer to another. It is desirable that cyberattacks have at least some ability to spread from their original targets because targeting mistakes can be made or defensive surprises may make them impregnable. Then perhaps a secondary target will be sufficient. Also, some attacks like denial-of-service ones require propagation to spread across a network. But propagation abilities also make it easier for attacks to spread from military machines to civilian machines.

The ubiquity of the Windows operating system and other familiar software on both military and civilian machines facilitates attack spread.

Fourthly, technologically developed countries provide the best targets for cyberweapons because they have so many things to attack. But cyberweapons require considerable technical expertise to develop, and such expertise is only readily available in the most technologically developed countries. This means an attack by a less technologically developed country is more likely to go astray and attack civilians, or perhaps be more likely to be deliberately targeted to do so because civilians are easier targets.

## **DAMAGE ASSESSMENT**

An issue exacerbating the collateral damage problem with cyberweapons is the difficulty of determining what they did. When aircraft bomb a target, much damage can be seen from the air. With cyberweapons, the damage is not directly visible, which makes it more persistent and costly. Attacks may also cause much indirect damage because of interdependencies that may not be obvious at first (Borg, 2005). Attacks may also fail for a host of unforeseen reasons; (Libicki, 2007) likens information warfare to introducing noise into a military organization, and the organization may or may not succeed at handling it.

This has important consequences for both the victim and the attacker. It may be hard for the victim to know if they have been attacked. The effects of an attack may be subtle, as when a worm slows down normal operations without changing anything else. Then the harm may persist for a long time because no one realizes anything is wrong. Or the effects may be time-delayed, as when a virus in a defender's weapons system causes it to fail only during combat. Then it may be difficult to find the cause, the harm will also persist until it is found, and repair may be costly. It would be foolish for an attacker to use an attack known to antivirus, antiworm, or antispyware tools, so we can assume such tools will be useless in finding or repairing damage from such attacks. While there are techniques for "system restoration" from backup storage media (Dorf & Johnson, 2007), they are time-consuming and require expertise, and may not be able to restore important data unless backup has been highly diligent. And the original vulnerabilities that enabled the attack need to be found and fixed ("patched") to prevent new attacks of the same kind, something that requires research and knowledgeable systems personnel. Less advanced countries may not have anyone with the necessary skills to do these things, leading to long-persistent damage much like that of landmines and chemical toxins that get into the water supply.

For the attacker, it may be very hard to know if their cyberattack had an effect. They may overcompensate by launching an unnecessarily powerful attack to be sure of an effect. They may attack unnecessarily many kinds of software or data, and they may do unnecessarily drastic modifications to it. Unnecessarily strong attacks that are deep may be unnecessarily difficult to repair, and unnecessarily strong attacks that are broad run a higher risk of collateral damage to civilians. Unnecessarily strong attacks are particularly a danger for cyber-counterattacks, as we will discuss, because an adversary is anticipating them and probably has strong defenses.

## **SECRECY OF CYBERWEAPONS**

As mentioned, most cyberattacks exploit bugs or flaws in software. If the victims knew of these, they would have fixed them. So secrecy of attack methods is essential to the success of most cyberweapons.

This secrecy by itself can be unethical. Secrecy makes it harder for victim countries to figure out what happened to them. Standard attack-intelligence resources like Computer Emergency Response Teams (CERTs) collect information about known vulnerabilities, but cannot provide much help for cyberattacks used in warfare because the vulnerabilities will likely be new. This exacerbates the problem of diagnosis and repair discussed above. Also, misinformation about poorly-understood attacks may spread far in a crisis, creating overreaction and panic in the victim country. Misunderstanding can lead to scapegoating of innocent countries or groups, much as terrorist acts tend to be blamed on a country's known adversaries. It will be essential for information-security experts to provide dispassionate technical analysis of what has occurred, perhaps with neutral experts from an international agency.

Secrecy also has negative consequences for the society that uses it (Bok, 1986). It encourages those who know the secrets to think they are better than those that do not, and permits those responsible for foolish attacks to avoid blame. Secret weapons are harder to test, since testing cannot be done publicly, and without adequate testing it is more likely that they will fail or cause collateral damage when used. An especially important consequence of the necessary secrecy of cyberweapons is that they can only be used effectively once (Ranum, 2004). Once they are used and they create some military effect, computer-forensics methods can usually figure out what happened. Then a solution – turning off a utility, blacklisting a site, or fixing a bug – can often be found in a day or so, and often the solution will prevent similar attacks of the same type as well. This means that cyberweapons provide a poor return on investment, since exploitable flaws in software require work to find. They are like a type of bomb that can only be used once anywhere in the world and never any bomb of that type again. It appears ethically unjustifiable

for a society to spend resources on developing cyberweapons when there are so many other more useful things they could spend money on.

## **CYBER-COUNTERATTACKS**

International law prohibits attacks on other countries unless a country is attacked first (Walzer, 1977). Countries must agree to this in signing the United Nations charter; in the United States, the charter was a treaty approved by the U.S. Senate, and thus has the same force as any other law of the U.S. So unprovoked cyberattacks are clearly illegal and unethical. But what about cyber-counterattacks?

It is more difficult to prove responsibility for a cyberattack than for a conventional attack, since it is hard to trace from where it came because of the possible “spoofing” (illicit changing of source identification data), “stepping-stone” sites as discussed earlier, and inconsistent record-keeping on sites.. Traditional adversaries of a country may be unfairly chosen as scapegoats. Even if we can trace an attack, trace records are highly technical. This makes it hard to justify a counterattack to world public opinion.

In addition, a serious technical problem of cyber-counterattacks is the preparation and experimentation time necessary to set up good ones. If the cyber-counterattacks are from within a system, time is needed to establish a foothold on that system and station attack software on it. It will be unlikely that an attacker will succumb to the same attack they themselves launched – they should have plenty of time to harden their systems against it. In fact, an attacker should take special pains to harden their systems against all attacks, since counterattacks are sanctioned by international law. A smart attacker could even terminate all their network connections to the rest of the world for a time after an attack to markedly reduce the chances of an externally launched counterattack or effective control of an internally launched one. Or they could put all their operating systems into hardware to prevent modification by Trojan horses and other exploits. So it will not be easy to launch a successful counterattack, and some considerable number of tries by the counterattacker with many methods may be necessary to find one that works if one can be found at all.

These issues create problems for the laws of war, because the legitimacy of a counterattack in conventional warfare is established by its immediacy after the attack, its being of the same type as the attack, and its proportionality to the magnitude of the attack (Gardam, 2004). Legitimate counterattacks cannot wait years (such as the claim that the 2001 attack on the New York World Trade Center was a response to the U.S.-Iraq war of 1991), cannot use some quite different

technology (as the introduction of poison gas by the Germans in 1915), and cannot be considerably larger. Counterattacks that violate these criteria must be classified as new attacks and are therefore illegal and unethical (Fotion and Elfstrom, 1986).

One way around the difficulty of counterattack is to station counterattack software, and channels to communicate with it like those of botnets, on computer systems of adversaries in advance of attack, just in the chance there might be hostilities which could use it. Then they might be invoked quickly. The possibility of such capabilities could function as a deterrent against the adversary attacking in the first place, although deterrence has never worked well as a military strategy. However, developing new attacks that will work when needed is not easy. Just because they worked in the laboratory against easy targets does not provide much confidence they will work during warfare, a problem that occurs in testing much new military technology. Computer systems are installing new protections all the time, so attacks go obsolete without warning. That means that the older an attack is, the less likely it is to work. Counterattack software is identical to attack software, so it is just as criminal to use in most countries, and thus hard to test in realistic warfare conditions. Furthermore, a hasty counterattack may cause more harm to the counterattacker than the attacker because it provides an opportunity for an attacker to learn about the counterattacker's cyberweapons and how they can be defeated, information that they might not be able to obtain otherwise.

A way to reduce counterattack obsolescence is to set up a broader "strategic" counterattack rather than a tactical one. An example would be modifying all the code for a networking protocol used by an adversary by modifying the source for that code in a repository. If all adversary military systems download their code from there, all could be infected from a single source, and the code could function normally until invoked by an external signal from the counterattacker. Such methods would be high on the scale of perfidy. But there are also some difficult practical problems. Adversaries that contemplate attacking other countries will set a high priority on protecting their frequently used software and will use hashes (pseudorandom data reductions) regularly to check for modifications to it. Most software is updated regularly, so the counterattacker would need to repeatedly modify the code with each update. Most updates come directly from software companies and not a military repository, and it would be hard for counterattackers to reach all these sources, and even harder to modify code in transmission. A broad strategic attack is easier to diagnose than a tactical one because there will be many malfunctioning systems simultaneously to provide data for identifying the type of attack and its software locus, so such attacks can be fixed more quickly. Finally, a broad counterattack based in common software risks more collateral damage to noncombat functions of computer systems than a more targeted counterattack.

Not all cyber-counterattacks require preparation. Those launched across the Internet can be mounted more easily at any time. Defending against such attacks is, however, the primary focus of network intrusion-prevention systems, which are kept updated with the latest known attacks. It is difficult, though not impossible, to invent a new attack that will succeed against these defenses. A country could try to “stockpile” new such attacks in the interests of its defense, but the effort to find such attacks might quickly be wasted as countermeasures are independently discovered as discussed above. What attacks that do succeed in circumventing the first level of defenses may succumb to second levels of defenses that note anomalous behavior, so they are unlikely to succeed for long once they start attacking. For instance, systematic search for the computers on a local-area network is necessary for precisely targeted attacks, but is obvious to network packet monitoring since normal usage rarely does it. So network-based attacks are quite unreliable, and military commanders dislike unreliable technology. Thus it appears that cyber-counterattacks are infeasible.

## **DESIGNING ETHICAL CYBERWEAPONS**

Despite the issues raised here, countries will likely continue to develop cyberweapons. Can such weapons be designed to be more ethical? We believe they can, since ethical discriminations can be made today among different kinds of weapons. For instance among nuclear weapons, neutron bombs are arguably less ethical than hydrogen bombs of the same explosive power when civilians are at risk because they harm humans disproportionately (Johnson, 1984).

Since controllability is a serious concern with cyberweapons, ethical weapons should use a variety of methods to ensure focused targeting. Propagation via viruses and worms should be minimized. Attacks should focus on a limited set of important targets which should be clearly identified and confirmed during the attack using more than their Internet address. Important civilian systems such as commercial infrastructure should clearly identify themselves as civilian so attacks can know to avoid them.

At the same time, ethical attacks should also be easily stoppable. If an adversary surrenders, it is unethical as well as against international law to continue attacking and causing damage. This means that all attacks should be under quick control via some mechanism such as an emergency channel so that they can be halted if necessary. This may be difficult because the effects of the attack may impede communication. But it is important.

Identification of the attacker ("attribution") should also be a key feature of ethical attacks, much as how uniforms to identify military personnel in warfare. Acting as a soldier while not wearing

a uniform is outlawed by international law. So some data or code associated with a cyberattack should identify who is responsible for an attack. One way is to add a digital signature to code or data (Mel & Baker, 2000). Several technologies to do this are available, and the best-known is encryption with a private key of a public-private key pair of a hash of the contents being signed. Using a hash means that the contents cannot be modified after they are signed because the public key can confirm it. Responsible attackers will find signatures useful because they prove they are responsible for an attack and prevent scapegoating of others. Unattributed attacks are not very effective anyway since attacks are usually a way to force a country to do something, and the victim cannot know what to do unless they know who has attacked them. Signatures also permit the attacker to recognize already-attacked systems by recognizing their own signature and avoid reattacking them repeatedly. Public keys for attack signatures could be kept with international organizations like the United Nations as a form of "key escrow" like that proposed for backup on encrypted systems.

Not everyone agrees that attacks should be attributable. (Robb, 2009) argues that cyberattacks will be ineffective unless that have deniability, much like "special operations" using commandos. But if he is right, then all effective cyberattacks are forms of terrorism.

A weakness of signatures is that they might make it easier for defenders to recognize they are being attacked, which might matter with the more subtle attacks. But it will not be easy to recognize signatures because, since they are a function of the contents, they will differ when attached to different files or data. Normal code and data can be signed too to prevent unauthorized modification, so existence of a signature does not imply an attack. However, if it is important that a signature be concealed, steganography is useful (Wayner, 2002). This is a class of techniques for concealing data inside innocent-looking other data, like concealing code messages in the least-significant bits of pictures.

Since damage persistence is a key problem with cyberweapons, it would be more ethical to use weapons whose results are easily repairable at the end of hostilities. This is more possible in cyberspace than in conventional warfare. For instance, an attack could encrypt important parts of a victim's system so that they cannot be used until the attacker supplies a key to undo (decrypt) it. Since encryption and decryption do not lose any information, the attack would be completely reversible. This would be an ethical alternative whenever it is impossible for a victim to restore a system from backup. Similarly, an attack could withhold important messages (like orders or email) from a victim. If the attacker saves those messages, they could be supplied to the victim at the cessation of hostilities, thereby reversing the attack. In both cases, there may be some damage from inability to do routine processing at the normal time, but this can be minimized if the target systems are chosen carefully.

## OTHER CYBER-MEASURES

Of course there are many alternatives to the use of cyberweapons such as negotiation and conventional weapons. Even within the cyberspace realm, there are nonviolent alternatives. Publicizing a cyberattack may elicit sympathy and support for a victim country; if it cannot do so, a counterattack is inadvisable. An attack can also be addressed by several kinds of “cyber-blockades”. Much as with methods to impede financing of terrorists (Biersteker & Eckert, 2008), countries can prevent Internet connections (particularly banking transactions) of the offending country. Traditional blockades and sanctions do not always work, but countries depend so much on their Internet connections that cyber-blockades could be more effective. There are alternatives to banks, but there is only one Internet.

## CONCLUSIONS

Most coverage of cyberweapons has been relatively neutral, referring to cyberweapons as interesting new weapons technology that can be employed much like any other technology and is inevitable. Our argument here is that this is not true, and that “cyber-pacifism” should be encouraged. Cyberweapons are less reliable and controllable weapons than conventional ones, much like biological weapons, and thus a poor choice in warfare. They disproportionately threaten civilians and harm the society that develops and uses them. It is hard to figure out what is happening when cyberweapons are used due to secrecy and the inherent difficulty of analyzing cyberspace, and their use in counterattacks seems problematic. While some ways of using cyberweapons are better than others, there are insufficient incentives to use them ethically. Their use should be outlawed.

## 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*, 379-401. Rand Corporation, Santa Monica, CA, USA.
- Bailey, M., Cooke, E., Jahanian, F., Xu, Y., & Karir, M. (2009, March). A survey of botnet technology and defenses. *Proc. Conf. for Homeland Security: Cybersecurity Applications and Technology*.
- Bayles W. (2001). Network attack. *Parameters, US Army War College Quarterly*, 31, 44-58.

- Berman P. (2002). The globalization of jurisdiction. *University of Pennsylvania Law Review*, 151 (2), 311-545.
- Biersteker, T., & Eckert, S. (2008). *Countering the financing of terrorism*. London: Routledge.
- Bissett A. (2004). High technology war and 'surgical strikes'. *Computers and Society (ACM SIGCAS)*, 32 (7), 4.
- Bok S. (1986). *Secrets*. Oxford, UK: Oxford University Press.
- Borg, S. (2005, November-December). Economically complex cyberattacks. *IEEE Security and Privacy*, 3 (6), 64-67.
- Ceruti, M. (2001, March). Mobile agents in network-centric warfare. *Proc. 5th International Symposium on Autonomous Decentralized Systems*, 243-246.
- Denning, D. (1999). *Information Warfare and Security*. Boston, MA: Addison-Wesley.
- Denning, D. (2007). The ethics of cyber conflict. In Himma, K., & Tavani, H. (Eds.), *Information and computer ethics*, New York: Wiley.
- Dorf, J., & Johnson, M. (2007). Restoration component of business continuity planning. In Tipton, H., & Krause, M. (Eds.), *Information security management handbook*, Sixth Edition, CRC Press, 645-1654.
- Dunnigan, J. (2003). *How to make war, fourth edition*. New York: Quill.
- Fotion, N., & Elfstrom, G. (1986). *Military ethics: guidelines for peace and war*. Boston: Routledge and Kegan Paul.
- Gardam, J. (2004). *Necessity, proportionality, and the use of force by states*. Cambridge, UK: Cambridge University Press.
- Gutman, R., & Rieff, D. (1999). *Crimes of war: what the public should know*. New York: Norton
- Himma, K. (2004). The ethics of tracing hacker attacks through the machines of innocent persons. *International Journal of Information Ethics*, 2 (11), 1-13.
- Hollis, D. (2007). New tools, new rules: international law and information operations. In David, G., & McKeldin, T. (Eds.), *The message of war: information, influence, and perception in armed conflict*. Temple University Legal Studies Research Paper No. 2007-15, Philadelphia, PA, USA.
- ICRC (International Committee of the Red Cross) (2007). International humanitarian law – treaties and documents. Retrieved December 1, 2007 from [www.icrc.org/ihl.nsf](http://www.icrc.org/ihl.nsf).
- Jensen, E. (2003). Unexpected consequences from knock-on effects: a different standard for computer network operations? *American University International Law Review*, 18, 1145-1188.
- Johnson, J. (1984). *Can modern war be just?* New Haven: Yale University Press.

- Jones, A., Kovacich, G., & Luzwick, P. (2002). *Global information warfare*. Boca Raton, FL: CRC Press.
- Knapp, K. & Boulton, W. (2007). Ten information warfare trends. In Janczewski L. & Colarik, A. (Eds.), *Cyber Warfare and Cyber Terrorism*, 17-25. IDG Global, Hershey, PA, USA.
- Kuhnhauser, W. (2004, January). Root kits: an operating systems viewpoint. *ACM SIGOPS Operating Systems Review*, 38 (1), 12-23.
- Lederberg, J. (Ed.) (1999). *Biological weapons: limiting the threat*. Cambridge, MA: MIT Press.
- Libicki, M. (2007). *Conquest in cyberspace: national security and information warfare*. New York: Cambridge University Press.
- Mandia, K. & Proise, C. (2003). *Incident response and computer forensics*. New York: McGraw-Hill / Osborne.
- Mel, H., & Baker, D. (2000). *Cryptography decrypted, 5th edition*. Boston, MA: Addison-Wesley Professional.
- 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/sfsl/sfsl.htm](http://www.aaas.org/spp/sfsl/sfsl.htm).
- Nardin, T. (Ed.) (1998). *The ethics of war and peace*. Princeton, NJ: Princeton University Press.
- Neumann, P. (1995). *Computer related risks*. Reading, MA: ACM Press.
- Ranum, M. (2004). *The myth of homeland security*. Indianapolis, IN: Wiley.
- Robb, J., The U.S. and cyberwarfare. Retrieved February 6, 2009 from [globalguerrillas.typepad.com/globalguerrillas/2007/12/the-us-and-cyber.html](http://globalguerrillas.typepad.com/globalguerrillas/2007/12/the-us-and-cyber.html).
- Schmitt, M. (2002). Wired warfare: computer network attack and *jus in bello*. *International Review of the Red Cross*, 84 (846), 365-399.
- Verton, D. (2003). *Black ice: the invisible threat of cyber-terrorism*. New York: McGraw-Hill Osborne Media.
- Walzer, D. (1977). *Just and unjust wars: a moral argument with historical illustrations*. New York: Basic Books.
- Wayner, P. (2002). *Disappearing cryptography: information hiding: steganography and watermarking*. San Francisco, CA: Morgan Kaufmann.
- Westwood, C. (1997). *The future is not what it used to be: conflict in the information age*. Fairbairn, ACT, Australia: Air Power Studies Center.
- Whitby, S. (2002). *Biological warfare against crops*. Houndmills, UK: Palgrave.

White Wolf Security, Offensive operations in cyberspace. Retrieved February 6, 2009 from [www.whitewolfsecurity.com/publications/offensive\\_ops.php](http://www.whitewolfsecurity.com/publications/offensive_ops.php).

The views expressed are those of the author and do not represent those of any part of the U.S. Government.