The Ethics of Computer Network Attack

WILLIAM J. BAYLES

From *Parameters*, Spring 2001, pp. 44-58.

Go to Spring issue Table of Contents.

Go to Cumulative Article Index.

> "Those who really deserve praise are the people who, while human enough to enjoy power, nonetheless pay more attention to justice than they are compelled to do by the situation." -- Thucydides, Speech of the Athenians[1]
>
> "I have the power, the capability, sitting in my home with my computer and my modem--if I only understood how to do it--to wage war. That is a very different environment than anything that we have experienced in the past." -- James Adams[2]

Today we are on the verge of technological advances that will redefine how we wage war and, in many cases, blur the current line between economic competition and warfare. The technology which holds the most promise, as well as the most unknown danger, is the world of computer networks--cyberspace.

With the proliferation of computers and ever-increasing computing power available to nearly every private citizen in developed countries, microprocessors have changed the lives of countless millions of people. The ubiquity of computing within business, finance, educational, and military institutions has raised concerns about the security of the data and tools upon which we have become increasingly dependent.[3] Many authors have expressed increasing concerns with our computer security. Some have speculated that an attack against the United States could disrupt electricity supplies and telephone service, interfere with air traffic control, cause leaks or explosions at chemical plants or refineries, and cause economic damage ranging into billions of dollars.[4] Likewise, other nations and transnational groups may have similar vulnerabilities the United States could exploit. Therefore, some people reason the United States should develop its own capabilities in the realm of computer network attack.

In many articles and books, authors highlight the supposed elegance of bringing an enemy to his knees without firing a shot, instead rendering him defenseless and harmless by defeating his information infrastructure via surgical attacks.[5] The weapons of computer network attack include "chipping"[6] (inserting malevolent code into hardware during manufacturing), programming "back doors" to allow external control of a computer, and disseminating computer viruses. On the surface, these weapons appear to be nonlethal in nature, but they may have disruptive or deadly higher-order effects.

Technologically capable nations are, perhaps by necessity, contemplating the addition of computer attack to their arsenals. During the Kosovo intervention, the United States attempted limited electronic attacks on Serbian computers containing banking records of Serbian leaders.[7] The United States is not alone, however. In 1995, the National Security Agency and Department of Energy estimated that more than 120 nations already had some sort of computer attack capability.[8] The People's Republic of China reportedly is studying numerous types of "dirty war"--"asymmetric attack" in today's military parlance--which include using computer viruses to pitch China's technologically advanced enemies into "political and economic crisis."[9]

The potential for such a crisis makes the application of computer network attack a very different sort of combat power than the kinetic weapons it may someday supplement or replace. Like kinetic weapons, a computer network attack can destroy both military and civilian targets. Unlike kinetic weapons, however, a computer network attack can reach across the world at the speed of light, invisibly transiting many international borders en route to its target. Like chemical and biological weapons, cyber weapons can target large masses of people in both military and civilian communities. Unlike biological and chemical weapons, however, they affect humans indirectly rather than directly. Cyber weapons thus share some similarities with weapons of yesterday, yet they occupy a completely new niche by their nature. Their uniqueness requires well-considered policy for their use.

To use these weapons ethically and legally, commanders and staffs must weigh their use against classes of targets and in some cases against individual targets, using clearly enunciated interpretations of the doctrines of discrimination and proportionality. The most basic questions were posed clearly by a newspaper reporter: "For now, many sticky questions must be considered: When is a cyber attack justified, what if it affects civilians, and is a cyber attack an act of war?"[10]

Defining Computer Network Attack

Current joint military doctrine includes computer network attack and several more traditional military disciplines in the term "information operations" (IO). Defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems," IO encompasses operations security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare, physical attack, and computer network attack (CNA).[11] Some of these disciplines are as old as warfare itself.

Computer network attack is the newest of these disciplines. While primarily a technical means, successful CNA depends upon clear intelligence, well-defined intent, and clear understanding of the primary and secondary effects of an operation. Thus, while highly technical, CNA relies heavily on the creativity of its practitioner. For a skillful practitioner, CNA becomes an enabler for deception and psychological operations.

There are several technical means of executing a computer network attack. The most straightforward is to physically destroy an adversary's computers or critical network nodes. An example would be to use precision munitions to attack a building containing an important computer to disrupt its functioning or destroy it altogether. There are electronically intrusive means as well. First, one could steal an adversary's data, enabling better decisions for friendly force employment, or one could corrupt the adversary's databases, thereby "helping" the enemy to reach poor decisions. Another means of attack is to deny access to networks or to bring them to a halt by using viruses.[12] This forces the enemy to use less efficient communications and processing means, slowing his logistics and decision cycles. Finally, attackers might surreptitiously reprogram enemy computers to disrupt the processes they control. An example is denying electricity to an area by reprogramming the computers controlling distribution within the power grid.

The far-reaching potential of computer network attack requires thinking about its moral and ethical consequences. There has long been debate about the nature of nuclear, chemical, and biological weapons--whether they differ in kind from kinetic weapons or whether they merely differ in the magnitude of their effects. Similarly, if computer network attack varies only in degree, existing rules are sufficient to examine the morality of its use. Otherwise, mankind should derive new rules or must renounce its use.[13] At first examination, the use of computer network attack against military targets to disrupt clearly military activities appears legal and ethical. However, the legal and ethical issues become more complex if CNA is used to target civil infrastructure or entails attack means that replicate themselves beyond the targeted computer or network.

The Nature of Computer Network Attack

At first glance, the concept of computer network attack appears to be a dream come true for a technologically advanced nation. CNA presents an opportunity for a government to exercise many of the elements of national power without endangering its forces and, if it can do so anonymously, without jeopardizing its honor. Many individuals would not even consider CNA as a weapon at all, or perhaps consider it a nonlethal means of exercising power, one that is unlikely to result in gruesome pictures in the media of dead or maimed soldiers or civilians. First-order effects of an electronic attack will not produce physical destruction, except perhaps to a computer itself. In this light, CNA appears to be an ideal means of exercising national power.

Considering only first-order effects, the nature of CNA places it in a seemingly useful niche in a nation's arsenal. The effects may be of short or long duration--mere harassment or society-wrecking infrastructure shutdown. Attacks may affect either very limited or nearly unlimited populations, including whole classes of noncombatants.[14] The attacker can be very difficult to trace, since an attack may pass through many different computers en route to the target. This feature means that attackers may navigate numerous third-party nations, which may or may not approve of the attack or the means used. Even if the target nation does locate the source of the attack, it will have difficulty distinguishing whether it has been instigated by a sophisticated private hacker, a corporate entity, or another nation. Finally, the worldwide reach of a network attack means that no computer or network is in a sanctuary unless it is completely isolated from outside networks and the telephone system.

The unique nature of computer network attack has several implications for practitioners and policymakers. First, its potentially anonymous nature may result in aggressor nations using CNA widely to accomplish a number of goals in the political and economic arenas. Such use will bring to question which sorts of policy should govern the use of CNA--wartime rules of engagement or civil law. As a political or economic tool, a computer network attack may aim to stress the population at large, which in turn will put pressure on the policymakers of the attacked state. In this way, CNA could take on the nature of economic sanctions, which potentially cause widespread suffering of innocents as a means to achieve political influence.[15] Absent legal precedents to govern the use of technologies such as CNA, we must turn to the just war tradition to examine the ethics of its use.

The Concept of *Jus in Bello*

Mankind has attempted to regulate his conduct of warfare since earliest written history. For example, Sun Tzu, the 5th-century B.C. Chinese military philosopher, wrote, "Treat the captives well, and care for them. . . . Generally in war the best policy is to take a state intact; to ruin it is inferior to this."[16] About a century later, Hindu writings espoused humanitarian rules, including certain prohibitions on poisoned weapons, and described noncombatant status.[17] The point of these examples is twofold. First, throughout the history of organized warfare, rules have existed to lessen its cruelty by imposing regulations on its execution. Second, the cultural and technological contexts determine much about the regulations. Thus, the synthesis of over two thousand years of experience provides the basis for today's just war theory.

The concept of *jus in bello* encompasses two principles, discrimination and proportionality. As noted above, through most of recorded history, the concept of discriminating between the noncombatant and the warrior has been central to the proper exercise of force. Likewise, the ancients sought to decrease the suffering inflicted upon the enemy by encouraging battle with proportional means. Therefore, defining these principles for the sake of analyzing computer network attack is in order.

Discrimination is simply the principle recognizing the difference in treatment accorded the warrior and the innocent bystander. Combatants are legal targets for the application of force and assume the risk of their status since they are present upon the battlefield by their own will. Combatants make themselves recognizable by means of a uniform or carrying arms openly. As combatants, they legally and properly use force to subdue their enemy. Noncombatants, on the other hand, are not proper targets for the application of military force and may not take part in battle unless they assume the role of combatants by taking up arms. Though many notable exceptions exist, armies have generally attempted to discriminate between these two classes of individuals.

For the purposes of this analysis, discrimination is the recognition of noncombatants' immunity from deliberate and direct attack against their person or possessions. Simply put, attacking those carrying arms, wearing uniforms, or engaging in war activities normally associated with combatants is a proper (legal) attack. Discrimination applies both to the aim of the weapon--whether the intended target is a proper one; and to the inherent characteristics of the weapon itself--whether it is likely to hit the target. Obviously, a rifle bullet discriminates more than a nuclear weapon.

Sometimes legitimate military operations affect noncombatants by accident. Traditional thought recognizes this possibility. If there is a danger of noncombatant harm, the attacker may prosecute the target only if the "good" to be achieved by the attack outweighs the foreseeable harm that may result. Thus, a commander is not bound to forego a particularly valuable target because there is a remote chance of noncombatant injury or death. Rather he is bound to consider the value of the target, the likelihood of collateral damage, the extent of the damage or injury, and whether such damage or injury is reversible. This concept, referred to by the theorists as the concept of double effect, leads to discussion of the concept of proportionality.

Proportionality refers to the level and extent of force used by combatants in the discharge of their duties. It is important to note that proportionality applies to the effects of the weapons on both noncombatants and combatants alike. In the case of the noncombatant, we return to the concept of double effect. Combatants may not directly attack the noncombatant's life and property, although legal and moral attacks directed against proper targets may affect them. The commander making the attack is bound to use the least amount of force and the most discriminating weapons to achieve his needed target effect. This subjects the noncombatants and their property to the least chance and least amount of destruction commensurate with the attacker's mission. Applying proportionality to the case of the combatant, the attacker is bound to use only weapons that do not unnecessarily prolong suffering after a combatant is injured. The attacker is likewise bound to use the least force that achieves the mission. In practice, this concept makes an expanding bullet an improper weapon, because of its tendency to cause great internal injuries and higher death rates than jacketed bullets. Further, sustained and violent attacks upon a place beyond all possibility of survival for the defenders would be disproportionate violence.

For the purposes of this analysis, proportionality is the concept which commanders use to temper the violence used in their attacks. Proportionality weighs the military goal and the strength of the enemy force against the likelihood of collateral damage and the expected injuries and suffering of the enemy combatants. The result of the balance determines the weapon choices, duration, and moral character of the attack.

The Character of Computer Network Attack

Let us now turn to examining computer network attack in terms of discrimination and proportionality. It is important to attempt a holistic approach, considering not only effects of the "munitions" themselves, but also the higher-order effects of an attack. Three target cases will be examined below: attack on a computer-based military command and control network, attack on an adversary's banking system, and attack on an electrical utility system. In each case, discrimination and proportionality determine the character and propriety of the attack.

These targeting scenarios are germane to the question of computer network attack for three reasons. First, these are plausible and likely scenarios examined in a number of articles and books. Second, these represent attacks on three of the four principal categories of national power--military, economic, and political.[18] Finally, these examine the effect and character of attack on three distinct centers of gravity of an adversary: the military, the adversary's economy, and the will of the people (as reached through disruption of their access to electrical power).

Attacks on Military Computer Networks

The attack of a military computer network presents unique challenges as well as unique potential benefits for the attacker. Attacks in this realm fall under the category of "command and control warfare" (C2W), a category formalized in service and joint doctrine. Joint doctrine defines C2W as measures taken to "prevent effective command and control of adversary forces by denying information, influencing, degrading, or destroying adversary [command and control] systems."[19] Thus, command and control warfare is not a new idea. For example, ground forces have made it a point to locate and destroy command centers with conventional fires since the advent of radio direction finding equipment. Military forces have long practiced radio frequency jamming and imitative deception in adversary radio networks as an accepted means in war. Such measures increase the uncertainty of war for the adversary and slow his decision cycle. In the near future, weapons such as High Energy Radio Frequency (HERF) generators may join viruses and other software means as weapons for computer network attack.

Against command and control systems, most attacks will be proper or moral attacks. Such targets at the tactical level will be single-use systems (i.e., military only) with no connections to civilian networks or civilian functions. Because of this relative isolation, the attacker foresees no effects off the battlefield. Therefore, attacking such a system meets the requirement of discrimination. Because no physical destruction is involved (except perhaps to the computer network hardware itself), proportionality is not an issue vis-à-vis first-order effects. Foreseeable higher-order effects center on the ability of the attacked to control his forces--exactly the effects desired. These may include loss of critical coordination capability and early defeat of the adversary with less loss of life. There is one caveat to the apparently moral targeting in C2W, however. It may be possible through imitative deception to commit perfidious acts. An example would be to broadcast an "all-clear" message just prior to a missile barrage in hopes of catching more people in the open and increasing casualties. Acts such as this increase the casualties and suffering of the enemy soldiers and would be improper using the tenants of *jus in bello*. In summary, command and control warfare appears to be a ripe area for computer network attacks due largely to the discrete and isolated nature of the potential targets.

Attacks on Financial Targets

Like military command and control computers, computer networks that run a nation's economy present tempting targets for a well-developed cyber attack. The Clinton Administration recognized the debilitating possibilities of disrupting a stock exchange or central bank in Presidential Decision Directive 63. This document directed study of methods and policies to protect "critical infrastructure," including economic targets. Finance in general is sensitive to perception and hence to misinformation. For example, the prices on a stock exchange and the values of the underlying currency fluctuate with confidence in the currency and banking system. This sensitivity makes a financial system an ideal target for attacks to undermine that confidence. Draining a nation's banks or rendering its currency unstable would produce second- and third-order effects through all segments of the targeted society. A loss in confidence in the national bank or the currency itself would reduce the value of the currency on the international exchange, making imported goods more expensive for the nation's consumers (or military). Rampant inflation and high unemployment might result, bringing disruption and at least minor suffering to innocent and combatant alike. Thus, few would consider an attack on a national finance system discriminating. However, could such an attack have sufficient military worth to be considered a proper attack?

The World War II attempts to disrupt the German economy through strategic bombing provide an example to weigh in considering the justification of targeting financial operations. From 1943 onward, the Allied strategy attempted to isolate essential industries to bring the German economy to a halt and force capitulation. Planning for a campaign of economic paralysis had begun in Great Britain as early as 1937. The plan called for attacks centered on manufacturing resources, the aircraft industry, and communications networks.[20] Analysts subsequently found, however, that during the period after the attacks commenced, the production of aircraft actually increased and the psyche of the German people, far from crumbling, allowed continued operation of the critical industries.[21] Those not driven from their homes or killed suffered from the eventual collapse of the economy. Meanwhile, combat operations continued. This evidence indicates that a population can and may endure great suffering under a government at war, allowing that government's war effort to continue and even tolerating diversion of assets from civilian relief to the war effort. Disruption of the economy failed to disrupt the military potential of the economy as much as the complete physical destruction did in the last months of the war. The pertinent conclusion with regard to the prospect of a computer network attack is that economic attacks cause widespread civilian suffering long before any noticeable effect might occur on the military potential of a warring nation. Thus, such attacks, far from having a proportional effect on military operations, have quite the opposite (disproportional) effect.

Attacks on Electric Power Grids

Since the advent of strategic attacks, the United States has shown much interest in the possibility of denying electricity as a means of disrupting war industry, impeding military operations, and undermining the will of the people. Recognizing this, Nazi Germany housed some generating facilities in buildings that looked like churches.[22] During the 1991 Gulf War, the United States-led coalition devastated Iraq's public power grid.[23] "Proponents [of attacking electrical utilities] assert that attacking electricity results in particularly damaging `second order' impacts on civilian morale, political leadership, military forces, and materiel production."[24]

Power system components fall into four categories:

- Generation equipment, which is centralized, capital intensive, and difficult to repair.
- Control systems, which are less centralized, but which are computerized and thus theoretically vulnerable to a computer network attack.
- Transmission systems, which are distributed and present obvious, but linear, sparse targets.
- Distribution systems, serving localities or specific industrial plants, which are highly distributed.

In general, targeting only the control system disables the entire system.[25]

Since a control system is the portion of the electrical grid most vulnerable to computer network attack, and since it disrupts the transmission and distribution systems serving all consumers, such an attack is indiscriminate except in one isolated, hypothetical case. If it were possible to disrupt only the electricity to those targets which are proper for iron bombs (e.g., military facilities and defense industry targets making only war materiel), then, and only then, would such an attack be discriminate. Until such a capability exists, however, one must assume that an attack on electrical power facilities is an attack on noncombatants, including facilities such as hospitals, specifically excluded from attack by numerous treaties.

The widespread effects of electrical grid attacks are so devastating to a modern society that they are neither humane nor proportional to the military effect achieved. Iraq's experience after the Gulf War is an example. Neither water treatment plants nor sewage treatment plants were operational due to the long-term electricity outages. These combined to produce a major health crisis. During the year after the Gulf War, some estimates linked as many as 70,000 to 90,000 Iraqi deaths to the higher-order effects of life without electricity.[26] In Iraq, the outages were long-term in nature because the large, obvious generator halls were a favorite target of allied airmen, and these are more time-consuming and expensive to repair than distribution yards.[27] The efficacy of these attacks also has been called into question because many, if not most, military targets have backup power from dedicated generators, making them independent from the public power utilities. Thus, evidence from past wars suggests that air attack of electricity grids produces only a limited effect on the outcome of a conflict.[28] In such a scenario the military advantage would not outweigh the harm to civilians from reduced hospital capacity, diminished agricultural capacity, and reduced medical refrigeration capability. Indeed, "customary law" protects foodstuffs, crops, and medicines during time of war.[29] Attacking the political stability of an enemy by cutting off his electricity clearly is devastating to the civilian population and thus bears no resemblance to a discriminate attack.

What if the attacker is sophisticated enough to temporarily interrupt power, or can turn it off at random times throughout the day? In these cases too, the military advantage must outweigh civilian suffering. In some societies, power disruptions are a way of life. When the lights go out, life continues. Even in southern California, temporary interruptions have proven to be disruptive but not damaging. Citing widespread power outages in 1996, the *Los Angeles Times* concluded, "People are more adaptable than anyone thought. Critical power users had backup power supplies to get them through short-term outages while maintaining essential emergency services."[30] Although a population may be resilient to short-term power outages, the military may be even more resilient due to backup generation capability, as previously noted. Careful consideration to inflicting temporary outages on a case-by-case basis is clearly in order.

Ethical Implications of Computer Network Attack

Central to the argument is whether computer network attack is a use of force at all. From the foregoing, one might argue that CNA is not an application of force, since there is little or no direct physical damage or suffering. As one current writer points out, it is to the advantage of the United States if CNA is not labeled as "force" because there results much more latitude in its use.[31] Others take a different view, stating that its widespread collateral effects suggest that CNA borders on being a weapon of mass destruction, like chemical or biological weapons.[32]

To attempt a rational adjudication of these widely divergent opinions, let us start by defining a weapon. A weapon is a tool that has utility in causing bodily harm or death to a human being or in damaging or destroying property. Defined as such, a rifle is a weapon, but so is a seemingly benign item such as a broomstick when wielded as a club. Similarly, a computer used to cause damage or bodily harm is also a weapon. To take this a step further, force is the use of weapons to cause bodily harm, death, or destruction of property. Thus, if a soldier uses a computer to create harm or damage, or to do things that result in harm or damage as a foreseeable consequence, then a computer is both a weapon and an instrument of force. It is important to note that the harmful consequences are those which are foreseeable, not merely those which stem directly from the use of force. The only conclusion, then, is that a computer used in a manner that may cause foreseeable injury or destruction is a weapon and such use constitutes force. Like any other weapon, the effects determine whether the computer is a weapon, as well as determine whether it is a legitimate one. Treaties outlawed some weapons, such as barbed spears and expanding bullets, because they had features that only increased the suffering of the warriors without increasing military effectiveness. Today, the United States limits its use of non-guided gravity bombs to those locations where collateral damage is unlikely. Thus, restrictions on weapons stem from the amount of suffering produced as well as whether they have sufficient accuracy in a given situation.

The direct results of a discriminate computer network attack on combatants will not inflict more suffering. Losing command and control of forces may increase casualties locally, but one expects an overall military advantage leading to quicker defeat of the adversary and fewer casualties in the end. Except in the case of feigned surrender, the case of directly targeting computers affecting the care of wounded, or other acts of perfidy as noted earlier, the incidence of combatant suffering will not increase. That said, could CNA be considered discriminate?

The discriminate nature of CNA depends in large measure on the target, its connectivity, and the method of attack. From the above analysis, attacks on civilian electric infrastructures are indiscriminate due to the foreseeable suffering of the affected populations. The target's external connections affect discrimination because the greater the connectivity (defined as both the amount of external communications as well as the number of potential or habitual connections the machine uses), the more likely it is that the attack will reach unintended targets. Finally, the method of attack affects the discrimination of the attack. A simple denial-of-service attack on an e-mail server is likely temporary and only inconvenient to those affected. A pernicious and self-replicating virus implanted to replicate swiftly through both civilian and military networks, on the other hand, is indiscriminate indeed. In sum, like the gravity bomb, computer network attack is not inherently indiscriminate by nature. Only indiscriminate use renders it so.

One also needs to consider the distinction between lethal and nonlethal weapons. Though regulated in a number of treaties, nonlethal weapons are not by nature either illegal or immoral. Returning momentarily to the analysis of the computer as a weapon, we see that the effects of a weapon determine its nature, not the weapon itself. Nonlethal weapons are legal with respect to *jus in bello* if the effects of the weapon are not long-term, debilitating, or irreversible. Conversely, attacks with permanent collateral effects are illegal.[33] Nevertheless, the above argument showed that even nonlethal weapons may cause unintended but foreseeable lethal effects. Even absent these higher-order effects, there are several implications that govern the consideration to employ nonlethal weapons in general and CNA in particular.

The first of these considerations deals with the potential for increased use of nonlethal weapons. If the political cost of an attack is less with a nonlethal (or easily denied) attack, policymakers may use such means more frequently, and sometimes without considering the ethical consequences. Preemptive strikes might become more politically palatable, thus increasing the chances for intervention without thorough debate of the consequences.[34] Employing CNA may blur the distinction between peace and war, as some in the media have suggested.[35] Accordingly, lacking the protective rubric of the just war convention, a computer network attack, like other interventions, would boil down to a simple criminal intrusion or act of terrorism.

Conclusions

Examining computer network attack leads to four major conclusions. These suggest a way ahead for those concerned with its employment and its policy. These are:

- CNA is an act of force.
- CNA is not, by itself, morally wrong. Its moral implication derives from its context, particularly the method of attack and its target.
- While parallels exist with both conventional weapons and weapons of mass destruction, CNA occupies a unique niche as an "Electronic Means of Mass Disruption" (EMMD).
- There is a need for new conventions of international law to deal with EMMD.

First, computer network attack is clearly an act of force. The examples of attacks on the relatively isolated military command system and the attack on the electrical power grid illustrate this assertion. In both cases, physical destruction and bodily harm are foreseeable results. Whether employing computer network attack at the operational or strategic levels, combatants must consider their actions as carefully as if they were employing a cruise missile.

Second, the context of the computer attack determines its moral or ethical quality. The weapon itself is morally neutral. The three-step test used by US Navy Judge Advocates in evaluating the legality (morality) of nonlethal weapons demonstrates this. These are: "(1) Would the weapon cause suffering that is needless, superfluous, or disproportionate to military advantage? (2) Can it be controlled to strike only a lawful target and be discriminate? (3) Do rules or laws exist that prohibit its use?"[36] When applied to computer network attacks, clearly the context rather than the weapon determines the answers to these questions. Importantly, depending upon that context, the answer to all three questions may be no. Accordingly, CNA is morally neutral.

Third, the effects of a computer network attack are potentially so varied with respect to bodily harm, permanence, and extent that there are no parallels in conventional weapons or in weapons of mass destruction (WMD). Computers as a weapon are "nonlethal," yet their higher-order effects may potentially cause widespread suffering and deaths. The duration of their effects may be transient and have only nuisance effect; conversely, their effects are potentially as permanent as that expected from explosive weapons. If a weapon of mass destruction is defined as a weapon that has widespread effects from a relatively small device, then a self-replicating virus is a weapon of mass destruction. However, if one requires those effects to include bodily harm, then an entirely new debate must ensue, depending upon the targets and the effects of the virus. Because they defy categorization, computer network attacks are best considered as Electronic Means of Mass Disruption.

Finally, because of the above conclusion, nations need to undertake continued dialogue to regulate both computer crime and computer warfare, and to differentiate between the two. Such dialogue should advance on two fronts: First, what target effects should be outlawed because they represent suffering of noncombatants? (Attack on electric power grids comes immediately to mind.) Second, what targets should be outlawed because the effects are unknown, unpredictable, but foreseeably will result in suffering? Perhaps, as some have suggested, mankind must redefine its definition of a "hostile act,"[37] and even attempt a redefinition of war itself.

Proposed Computer Network Attack Policies for the United States

The main points of a US computer network attack policy should serve the national interests of the United States as well as ethical considerations. The mainstays of such a policy are deterrence and right of first use. For use within the military, considerations of *jus in bello* are required in operational concepts and joint doctrine.

To promote deterrence, national policy must be flexible enough to allow the United States to respond to computer attacks by criminals working for monetary gain, terrorists striving for political gain, and nation-states conducting information warfare. Sufficient technology overmatch to determine the source of attacks, and intelligence collection capabilities robust enough to determine the actors, should back up this policy. Like many terrorist or criminal acts today, attacks will be difficult to trace, and perpetrators will be difficult to bring to justice unless international cooperation improves with increasing concern about the computer attack events. In the case of nation-state actors, the United States should clearly state its position concerning retaliation. In practice, retaliation may be actions in kind or conventional retaliation, marked by a consideration of consequences proportional to the original attack. Only by clearly stating these policies can the United States justify its retaliation. Thus, a clearly stated policy is key to deterrence.

The United States also should enunciate a policy preserving the right of first use of computer attacks. In addition to stating that such weapons are part of the US arsenal in wartime, the policy should include the considerations for their use and these considerations must rest firmly on *jus in bello*. Outside of use in wartime, such a policy would require a presidential "finding" and congressional approval for CNA use in national security covert and clandestine operations.[38] Clearly stating such a policy may quell debate following a first use. More important, it may convince other nations that any collateral damages were unintended side effects, rather than brutish, illegal violence. A convincing argument backed by a previously stated policy may limit escalation of a crisis. Finally, such a policy will open debate with the Russian government, whose representatives have classified computer network attack as a weapon of mass destruction, and which they promise to answer with unspecified WMD countermeasures.[39]

Like national policy, the concepts of employment must clearly rest upon the principles of just war theory. Current technology, while sophisticated, should not constrain these concepts; rather the concepts should drive research and development to meet conceptual needs. Such research should be directed toward bettering intelligence collection capabilities and, importantly, making CNA weapons ever more precise and discriminate. While computer network attack may someday have the capability for stand-alone employment, that day may be well in the future; therefore, operational concepts using CNA as an adjunct or supporting capability are in order. The laws of warfare still apply, however. Even in the context of supporting a psychological operation, larger information campaign, or conventional strike, using a computer network attack in a treacherous or perfidious manner is morally wrong. Joint doctrine must make the considerations of *jus in bello* clear to planners and commanders who will use these potentially powerful weapons.

Just as the increasing dependence upon sea trade brought pirates and navies to the oceans, increasing reliance on the microchip and communications networks will attract criminals, terrorists, and the military interest of nations. As the Royal Navy's prominence on the high seas drove the prosperity and expansion of Great Britain in earlier centuries, prominence in the computer dimension holds great promise for the United States. The US government must carefully craft its policies relating to this new dimension. Such policies will determine whether cyberspace becomes a lawless, crime-ridden highway where no one is safe, or an orderly and productive tool of economic expansion. These policies will drive the development of US capabilities to police this dimension, as well as the ability to defend US national interests there. The success of these policies will rest to a large measure on the extent to which they incorporate considerations of the just war tradition.

NOTES

[1] Thucydides, *History of the Peloponnesian War*, trans. Rex Warner (Harmondsworth, U.K.: Penguin Books, 1972), p. 80.

[2] James Adams, "Information Warfare: Challenge and Opportunity," *USIA Foreign Policy Agenda*, November 1998, internet, http://www.usia.gov/journal/itps/1198/ijpe/jp48adam.htm, accessed 4 October 1999.

[3] This has been expressed in a Presidential Decision Directive, PDD-63, forming a Critical Information Assurance Organization within the federal government. See William J. Clinton, *White Paper: Presidential Decision Directive 63, Critical Infrastructure Protection* (Washington: White House, May 1998), internet, http://www.fas.org/irp/offdocs/pdd-63.htm, accessed 10 October 1999.

[4] John Arquilla, "The Great Cyberwar of 2002," *Wired*, February 1998, p. 160. See also Robert T. March et al., *Critical Foundations: Protecting America's Infrastructures* (Washington: US President's Commission on Critical Infrastructure Protection, October 1997), p. 8.

[5] James Adams, *The Next World War* (New York: Simon and Schuster, 1998), p. 1. Chapter one is a fictional account of an "elegant" information campaign against a peer competitor in the year 2010.

[6] Doug Richardson, "Hacker Warfare: Threat of the Future?" *Armada International*, August-September 1997, p. 64.

[7] Elizabeth Becker, "Pentagon Sets Up New Center for Waging Cyberwarfare," *The New York Times*, 8 October 1999, p. A16. See also John Markoff, "Military Breaks the Rules of Military Engagement," *The New York Times*, 17 October 1999, p. L5.

[8] Richardson, p. 72.

[9] David Harrison and Damien McElroy, "China's Military Plots `Dirty War' Against the West," *London Sunday Telegraph*, 17 October 1999, p. 1.

[10] John Diedrich, "Star Wars in Cyberspace," Colorado Springs Gazette, 15 January 2000, internet, http://ebird.dtic.mil/Jan2000/s20000124cyberspace.htm, accessed 24 January 2000.

[11] Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Information Operations*, Joint Publication 3-13 (Washington: US Department of Defense, 9 October 1998), p. I-9.

[12] RAND Corporation, "Information War and the Air Force: Wave of the Future? Current Fad?" March

1996, internet, http://www.rand.org/publications/IP/IP149/, accessed 28 September 1999.

13. Paul Christopher, *The Ethics of War & Peace: An Introduction to Legal and Moral Issues* (Englewood Cliffs, N.J.: Prentice Hall, 1994), p. 201.

14. Bruce Bigelow, "Cyberwarriors: Pentagon's New Priority: Train Troops to Cripple Computers--and Enemy Forces they Control," *San Diego Union-Tribune*, 13 August 1995, p. A-1.

15. Joy Gordon, "A Peaceful, Silent, Deadly Remedy: The Ethics of Economic Sanctions," *Ethics and International Affairs*, 13 (1999), 124-25.

16. Samuel B. Griffith, *Sun Tzu: The Art of War* (London: Oxford Univ. Press, 1963), p. 76.

17. Christopher, p. 9.

18. Charles L. Cornwall, ed. *The Joint Staff Officer's Guide*, Armed Forces Staff College Publication 1 (Norfolk, Va.: National Defense University, 1997), p. 6-15.

19. Chairman of the Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare (C2W)*, Joint Publication 3-13.1 (Washington: US Department of Defense, 7 February 1996), p. I-4.

20. Christina J. M. Goulter, "The Ministry of Economic Warfare and Royal Air Force Strategy During the Second World War" (Carlisle, Pa.: US Army War College, 1991), p. 7.

21. US Army Air Corps, *Summary Report: The United States Strategic Bombing Survey (European War)* (rpt.; Maxwell AFB, Ala.: Air Univ. Press, 1987), p. 19.

22. One such structure is located on the north end of Wuerzburg on the Main River.

23. Eliot A. Cohen, *Gulf War Air Power Survey* (Washington: Dept. of the Air Force, 1993), pp. 297-98, 302.

24. J. W. Crawford III, "The Law of Noncombatant Immunity and the Targeting of National Electric Power Systems," *Fletcher Forum of World Affairs*, 21 (Summer-Fall 1997), 101.

25. Ibid., p. 103.

26. "Tactical Bombing of Iraqi Forces Outstripped Values of Strategic Hits, Analyst Contends," *Aviation Week and Space Technology*, 17 January 1992, pp. 62-63.

27. Ibid.

28. Crawford, p. 105.

29. Ibid., p. 110.

30. Hector Tobar and Miles Corwin, "Outage Shows Technology's Fragile Links," *Los Angeles Times*, 13 August 1996, p. A1.

31. Roger W. Barnett, "Information Operations, Deterrence and the Use of Force," *Naval War College Review*, 51 (Spring 1998), 17.

32. Byard Q. Clemmons and Gary D. Brown, "Cyberwarfare: Ways, Warriors and Weapons of Mass Destruction," *Military Review*, 79 (September-October 1999), 42.

33. Margaret-Anne Coppernoll, "The Nonlethal Weapons Debate," *Naval War College Review*, 52 (Spring 1999), 123.

34. Douglas C. Lovelace, Jr., and Steven Metz, "Nonlethality and American Land Power: Strategic Context and Operational Concepts" (Carlisle, Pa.: US Army War College, Strategic Studies Institute, 1998), p. 12.

35. John Markoff, "Cyberwarfare Breaks the Rules of Military Engagement," *The New York Times*, 17 October 1999, p. L5.

36. Coppernoll, p. 118.

37. Frederick W. Kagan, "Star Wars in Real Life: Political Limitations on Space Warfare," *Parameters*, 28 (Autumn 1998), 116.

38. Barnett, p. 16. Also, Clemmons and Brown, p. 44.

39. Clemmons and Brown, p. 40.

Colonel William J. Bayles commands the Rock Island District, Corps of Engineers. Previous assignments include Chief of Theater Operations Branch, US Space Command; Commander, 4th Engineer Battalion; and numerous combat engineer assignments in Germany and the United States. He is a 2000 graduate of the Army War College and a 1990 graduate of the School of Advanced Military Studies. He has published several previous articles in *Engineer* magazine.

Go to Spring issue Table of Contents.

Go to Cumulative Article Index.

Go to Parameters home page.

Reviewed 12 February 2001. Please send comments or corrections to Parameters@carlisle.army.mil