Legal and Practical Constraints on Information Warfare

Maj Karl Kuschner

ABSTRACT OF LEGAL AND PRACTICAL CONSTRAINTS ON INFORMATION WARFARE

Like any new weapon, revolutionary new techniques of information warfare must be reviewed for legal and practical constraints on their use. Because of the unique capabilities and employment methods of these "information weapons," such review will require significantly more attention than other, more evolutionary, types of weapons.

Information warfare weapons must meet the same tests for necessity and proportionality as other weapons under the laws of armed conflict. In addition, commanders must recognize and weigh the possible consequences of weapons that can devastate the information systems of an adversary. Problems such as lack of enemy command and control, post-hostility reconstruction, and retaliation, among others, must be considered by the commander contemplating the use of information weapons.

Because of the extraordinary consequences of these weapons, developers must provide guidance for their employment, and commanders must carefully consider adverse effects from their use.

PREFACE

> The promise of infowar has grown exponentially with the increasing power and pervasiveness of computer microprocessors, high-speed communications and sophisticated sensors.... The potential for low-cost and bloodless resolution of conflicts brings with it other problems.
>
> Douglas Waller in
> ***Onward Cyber Soldiers***

Information Warfare is probably the greatest "fad" for discussion in the U.S. military today. There are, however, some age old questions that need to be asked when "digital solutions" are advanced as a panacea for the problems of declining budgets and increasing global political uncertainty.

The armed forces as an institution has started asking these questions. The first conference on the legal aspects of information warfare was sponsored in November 1995 by the U.S. Air Force. Army chaplains have met to discuss the moral issues. Articles are beginning to appear in the literature that examine the bounds of information warfare instead of extolling its virtues. We are beginning to ask what it can't do and when we shouldn't use it, and those questions are appropriate.

This discussion of constraints on information warfare is not intended to be a checklist for use by the "information warrior." Instead, it is intended as a survey of the types of problems that must be considered as technology provides imaginative new weapons for use against innovative new targets.

INTRODUCTION

The debate continues as to whether technological advances in the past several decades have truly created a "Revolution in Military Affairs.[1]" It would be difficult to dispute, however, that increased dependence on communication and computer systems, combined with long range precision delivery systems and new "non-lethal" methods of electronic warfare, have created previously unforeseen target-weapons matches. The Persian Gulf War has been called the first "Information War" because of the advanced information systems used by the coalition for supply, intelligence, analysis, and weaponry, and the general conclusion that it was this technology that greatly limited coalition casualties.

In this same era, as armed forces became increasingly dependent on advanced technology and information systems, careful planners began to think about protecting them. Simultaneously, others realized that attacking the enemy's systems might yield great advantage. In the 1980s, these ideas gave birth to the concept of Command and Control Countermeasures, and, at the end of that decade, Command and Control Warfare. During that same period, a broad range of technology-much of it highly classified-was evaluated for its ability to directly affect the enemy's information flow and degrade his ability to react. All these technologies are now considered to be a part of the concept of "information warfare."[2]

> The term "information warfare" has thus caught the attention of an entire generation of military thinkers. While the term encompasses both offensive and defensive measures, much of the imaginative thinking has concerned attacks on an enemy's command and control and information systems-using methods as diverse as computer viruses and laser beams. Much of this thought goes into understanding the possibilities-and maximizing the effects-of high technology in information warfare. Here is an example: Let's consider the consequences if the following systems were targeted.... for disablement: financial markets, nuclear power plants, telephone systems, power distribution systems, traffic lights, or air traffic control and airline reservations systems.[3]

The ability to destroy precisely and completely the enemy's command and control system, and the ability to attack his information infrastructure, will bring new questions to the minds of the operational commander. The question of "what can I do" with information weaponry already has a chorus of answers, and will find no shortage of additional ones in the near future. Perhaps a more important question, and one that is only recently receiving the attention it deserves, is: "when shouldn't I use" these high-technology weapons?

If there is something which history teaches about new weapons or methods of warfare, it is that they will often encounter unforeseen limitations in their use. Chemical weapons were so lethal and indiscriminate as to be banned. Nuclear weapons were so powerful that their use became almost unthinkable. Assassination of enemy leaders, even those identified as a "center of gravity," became politically unacceptable as a matter of United States policy.

The weapons of Information Warfare[4] have effects as potentially devastating as those of nuclear weapons, yet there has been relatively little closure in the debates on the implications of the newest technologies and their use in warfare. There are legal and practical limitations that the National Command Authorities and, more specifically, the operational commander, must consider before employing these technologies.

LEGAL LIMITATIONS

The use of technology designed to destroy or incapacitate an enemy's communications or information infrastructure will fall, during hostilities, under the auspices of the Law of Armed Conflict. The two principles by which any act of aggression must be measured under these laws are *necessity* and *proportionality*. An attack must be necessary for a military purpose, and the damage it causes must be worth the advantage that is gained.

It is under these rules that global thermonuclear warfare became (hopefully) obsolete. What military advantage could be proportional to the loss of millions of lives? Thousands of pages have been written on the legality of nuclear war, but current doctrine and literature have little comment on the legal aspects of information or command and control warfare.

These same tests *must* be applied to methods of information warfare. In one of the few references to these principles in joint doctrine, the U.S. Navy explicitly recognizes this requirement, saying

> In formulating and executing [Information Warfare] plans and policies, feasible options may raise difficult legal and ethical questions. When executing any [Information Warfare] mission, U.S. forces must conform to all domestic and international laws, treaties, the Law of Armed Conflict, and all applicable rules of engagement.[5]

Some may argue that non-lethal forms of warfare, such as compromise of an enemy computer system, do not constitute the "use of force," and therefore are not subject to the laws of armed conflict. To advance that contention, proponents must instead show that these actions are legal

under peacetime international laws, a more difficult task. CIA officials, for example, have reportedly rejected intrusion into other countries' computers, considering them to be a "fundamental attack."[6] Clearly, international law would consider such acts illegal in peacetime, hence they must be measured against the principles of the laws of warfare.

The Principle of Necessity

One basic tenet of international law is that attacks against civilians are prohibited. In the passage referred to previously, the author considers attacks on a country's airline reservation system. The operational commander would have a difficult time justifying this action under the test of military necessity. Attacks against a country's financial, transportation, or communications systems *must* be shown to have clear military necessity to be legal.

Even in the more mundane forms of information warfare, such as destruction of an enemy's command and control capability, law of armed conflict questions may restrict the operational commander. In Operation Desert Storm, coalition air forces targeted AM radio stations, telephone exchanges, and microwave stations.[7] From a purely legal standpoint (there are practical elements to be discussed later), intelligence will have to provide evidence that targets like these are being used by the military to be considered as legal targets. Indiscriminate destruction of a nation's communications infrastructure, while possibly good information warfare, will certainly be poor public relations and possibly prove illegal.

The Principle of Proportionality

It is in the attacks on information systems that most of the more imaginative forms of information warfare will run into problems. In a recent best-selling "techno-thriller," rogue elements of the Japanese financial elite insert a computer virus into the computers controlling transactions of the American financial market. While such an act is feasible, and might bring military advantage to the attacker, there are serious questions of proportionality raised by such an attack. It is reasonably clear to the air campaign planner, who must decide whether to destroy a ball-bearing or a baby milk factory, which might be legal. When the attack will indiscriminately affect huge sectors of the enemy's economy for an unknown amount of military advantage, however, the commander must ask hard questions of its legality. As stated in the U.S. Navy's legal handbook, "Weapons that are incapable of being controlled (that is, directed at a military target) are forbidden as being indiscriminate in their effect."[8] If a free-floating contact mine is considered illegal, the theory must raise serious questions about large-scale attacks on a country's information architecture.

Meaconing, or the creation of false navigational signals, has long been a threat to aircraft operating near hostile countries. Should the ability arise to compromise an enemy's airport radar approach system, using computer links to falsify aircraft position, it might provide the commander the ability to destroy enemy aircraft with no threat to his own forces. It will be the commander's responsibility, however, to ascertain that such a technique will not be used to adversely affect civilian traffic in such a way as to cause harm out of proportion with the advantage gained. That the implications of directly affecting an information infrastructure are so astounding should garner equivalently great care in their application.

The leaders who choose to develop these techniques, as well as the commanders who might elect to employ them, must understand that each new weapon brings different questions of legality to the arena.

PRACTICAL LIMITATIONS

Several recent authors have voiced concerns over the eventual utility of the "third wave" weapons.[9] Even under the assumption that these weapons will actually create the desired effects, there are certain situations where their use will adversely affect the outcome of the conflict. The commander must carefully contemplate the consequences of his actions, keeping the strategic objectives of the nation in the forefront. The less "pre-packaged" the weapons are, the more unforeseeable their consequence, the more difficult the task becomes.

Minimum levels of command and control

One can imagine a perfectly executed command and control warfare attack that leaves the enemy leadership with no means to communicate with his forces. There are several reasons, however, why this might not be the ideal situation for the commander.

The first is the most obvious. Should the perfect information warfare campaign leave the enemy command with no means to fight, it is then nonetheless unable to communicate its desire for surrender or truce to its troops. Military units are trained to fight autonomously in the event of lost communications, and, until a reliable and believable command to halt hostilities is received from superiors, they are likely to continue the struggle. While a relatively impotent force, like the retreating Iraqi Republican Guard, might cause few problems, it is easy to imagine a situation like the one in the Pacific theater during World War II where capable Japanese units, isolated by complete destruction of their means of communication, continued to fight. Current techniques of jamming can be simply stopped to allow radio communication, but technology such as EMP[10] could ruin all communications equipment in a large area.

Another consideration is the link between an enemy's information flow and the commander's attempts at military deception. While deception may be aided by degraded communications, severely deteriorated information flow may instead *negate* attempts at military deception. Often the desired end of a deception plan is not simply to prevent the enemy from gaining knowledge of an operation, but in fact to cause him to distribute his forces unwisely, and to his disadvantage. For example, the German insistence that Patton would soon be crossing the Channel made the Normandy invasion a success. Had they not had *any information at all* about the disposition of forces in England, they may have reacted immediately to the D-Day forces by moving reserves down the French coast to oppose it. The commander must ensure that his attempts at deception are not thwarted by successful information warfare.

Economy of Scale

Even in cases where the situation would allow complete destruction of a system, that may not be the ideal form of attack. AFM 1-1 (Basic Aerospace Doctrine) says "Electronic combat is often most useful when it is selective, subtle, and hard to detect."[11] The same can be said of other forms of information warfare. Selective and subtle forms of data manipulation may prove more of an impediment to the adversary in the long run than overt destruction. An enemy intelligence system, for example, is more valuable as a source of misinformation than it would be as a target of distruction. It is the principle of the double agent, and the reason such spies are "turned" rather than exposed. The commander is obligated to assess the possibilities of exploiting an information resource before he authorizes its destruction.

Consider the situation where a belligerent has infiltrated an enemy logistical database. If the database is dual-use (military and civilian), legal questions could prevent widespread destruction of data. But even with a purely military system, complete destruction of a logistical tracking system, while certainly legal, would alert the enemy of the attack, and prompt him to take countermeasures such as "hardening" the system or restoring the data. *Selective* use of data manipulation, however, could divert vital material at a critical time away from the war effort, and still go undetected. In the long run, this technique might not only prove more justifiable but also more effective.

Unsuitability

Even data manipulation may be unsuitable. A Naval War College faculty member writes that information warfare "may be an unsuitable or inappropriate means to deal with prevalent forms of conflict in the new world order."[12] His comment questions the efficacy of information warfare, but should also stimulate some thoughts on the constraints of such weapons.

One characteristic of modern conflict is a trend toward multi-national coalitions. The United States has developed this trend to include multi-national headquarters, intelligence centers, operations centers, and command structures. Commanders will be required to consider the problems of technology transfer and capability exposure during such operations. Problems of technology transfer may limit the scope of information weapons they can employ.[13]

A similar problem arises for the commander during a conflict against a relatively minor adversary. Some of these technological weapons are so advanced that other possible opponents may be unaware of their existence, and their use may provide future enemies advance warning. Like the ongoing rush to counter stealth technologies due to Persian Gulf War successes, a single use of an information warfare technique could engender countermeasure development that may render it ineffective in future, more critical contingencies.

Another trend in recent conflicts is the involvement of "non-legitimate" adversaries, either because the current government had become corrupt (Panama, Haiti), or because the enemy was working outside the bounds of the legitimate government (drug cartels, for example). In these cases, attack on legitimate military targets may cause serious problems for the legitimate government. The use of information warfare in infiltrating and isolating drug money in Colombian or third country banking systems is a good example. This action would have adverse effects on the credibility and stability of the targeted financial systems. Legitimate investors may

have second thoughts on using systems that have been penetrated, or the damage to those systems could prevent their legal use.

Post-Hostilities

Another issue related to the problem of attacking a nation's economic or civilian information architecture requires the commander to look further ahead-to the end state of the conflict. The history of American warfare is replete with examples of adversaries who later received aid or other support for post-hostility reconstruction. Because information architectures are some of the most expensive to rebuild, the commander must carefully consider the destruction of this infrastructure.

Iraq, for example, will almost certainly spend several decades worth of oil profits to rebuild just the physical structures that were destroyed in the Persian Gulf conflict. If that kind of destruction occurred in a more industrialized nation, and was combined with destruction of their national information infrastructure, the problem of reconstructing that enemy's economy is greatly compounded. Great care is necessary in selecting key communications nodes that serve military as well as economic purposes.

As with the rebuilding of Japan's steel industry following World War II, such reconstruction may have other ramifications. Destroyed information centers may be replaced, at the victor's expense, with advanced technology systems that may eventually give the vanquished country a technological edge in global competition.

Political Considerations

The use of one of the "five pillars of command and control warfare,"[14] psychological operations, can have a profound effect on the popular support on either side of a conflict. New technology, such as digital video editing, that can "put words in the mouth" of enemy leaders, may greatly increase the impact of these operations. Especially when based from a host nation, such operations can have several serious drawbacks that the theater commander must consider.

First, in several theaters of current interest, information concerning United States involvement can adversely affect popular support in the host nation. While "Radio Free Europe" served its purpose well across the iron curtain, blatant American propaganda may not play as well on the ears of Latin American or Islamic audiences. As one example of failed psychological operations, Saddam Hussein's attempts to positively portray his leadership by patting a foreign child on the head only served to increase American resolve. Maintaining a "low profile" has become more important to forward-based forces because of the rise of nationalism around the world. Commanders must consider the impact on the host nation carefully, and fully coordinate any "forced information" with the political structure in the theater.

Second, psychological operations designed to discredit or vilify the adversary's leadership can have two adverse effects. It can cause the enemy's population to "rally around the flag" if popular support is already strong, or it can cause difficulties in a post-hostility environment if the leadership remains in charge. Working with a government discredited by propaganda may prove

difficult, and if the propaganda was effective, civil unrest in the war's aftermath could end up as the theater commander's problem.

A related problem concerns the accepted policy requirement of support from the American public and Congress for military actions. As political and military leaders found during the Persian Gulf War's "Highway of Death" incident, real-time media attention can portray valid military tactics as "unfair," diminishing the United States' position on the "high moral ground." The same backlash might occur, perhaps, should the public be treated with footage of enemy aircraft falling from the sky-due to attacks on flight control systems through "non-lethal" weaponry.

Retaliation

A final problem for the commander to consider, especially with new, highly destructive technology, is the problem of retaliation. The United States is the most information-dependent country in the world, and, even if military systems are hardened, has the greatest vulnerability to information attack. As ***Time*** magazine says, "An infowar arms race could be one the U.S. would lose because it is already vulnerable to such attacks."[15] These attacks could take the form of escalation, or simple desperation. Just as Iraq slung Scud missiles in frustration during the Persian Gulf War, an adversary that found its information weapons ineffective against U.S. armed forces may direct them against civilian targets- the Internet, communication satellites, or undersea fiber optic cables, for example. While these targets may not be militarily significant during actual hostilities, they could prove politically sensitive or at least disruptive. Intelligence should be tasked to determine possible enemy responses to information attack, and the impact of possible retaliation considered in the selection or rejection of information weapons.

CONCLUSION

There are two stages in any major technological advance. The first stage, the one the military is currently in regarding information warfare, is exploratory and imaginative. This is the period where new doors are opened, new possibilities glimpsed, and the "explorers" of the era gather their expeditions in search of new vistas. In the second stage, the technological limits inevitably are found, and their practical use becomes constrained. So it must be with information warfare.

Unfortunately, the great responsibility that lies on the shoulders of the armed forces will not allow its leaders to walk blindly down the information armory, choosing and employing new weapons without regard to consequences. For them, exploration must be tempered by solicitude. They should, and must, consider with great care the possible consequences of "third wave" weapons and the targets selected for compromise or destruction. The greater capacity those weapons have, the greater temperance they demand. Military leaders cannot afford to wait until the enemy is at hand before regarding their own arms.

The rule of international law requires that new weapons be reviewed for problems of legality. The United States has fully embraced this principle and established detailed methodology to

facilitate its accomplishment. The difficulty that creates a higher level of concern for advanced technology weapons is that the weapon, and the legality and practicality of its use, cannot be easily separated. A technique for invading an information system is like a guided bomb, in that it can be either legal or illegal in its application. The problem is that the range of possibilities of the former is more difficult for today's commander to comprehend. With *any* new weapon the commander is given, he will need explicit guidance in its use, and a discussion of the possible adverse effects-this is even more critical to this new arena of warfare.

Organizations responsible for developing weapons technology must concern themselves with its use, and provide operators with guidelines that will ensure the effective and legitimate use of new weapons. Nothing about that statement is revolutionary, but the non-traditional sources of these weapons make it more imperative. A pilot dropping a laser-guided bomb has been trained on the Law of Armed Conflict and the weapon's effects. Commanders must give the same guidance to the computer hacker loading a virus into the financial network of an enemy-or suffer the consequences.

NOTES

---

1. Warren Caldwell, Jr., "Promises, Promises," *Proceedings*, January 1996, 54.

2. For an excellent survey of the types of offensive weapons that are being considered or developed, see Douglas Waller, "Onward Cyber Soldiers," *Time*, August 21, 1995, 38-46.

3. Joanne Sexton, "A Combatant Commander's View of Information Warfare and Command and Control Warfare," Unpublished research paper, U.S. Naval War College, Newport, RI: 16 June 1995, 3.

4. Command and Control Warfare is generally considered to be the military's contribution to the national strategy of Information Warfare. Recent sources have referred to the military use of IW as "information operations."

5. Department of the Navy, *Policy Planning and Guidance for Naval Information Warfare/Command and Control Warfare*. (Washington DC: 16 Feb 1995), 3.

6. Waller, 44.

7. Department of Defense, "Appendix O: The Role of the Law of War," *Conduct of the Persian Gulf War: Final Report to Congress*. (Washington DC: April 1992), O-11.

8. Department of the Navy, *The Commander's Handbook on the Law of Naval Operations* (NWP 1-14M), Draft ed. (Washington DC: May 1995). 9-1.

9. Caldwell, 54-57 and R.L. DiNardo and Daniel Hughes, "Some Cautionary Thoughts on Information Warfare," *Airpower Journal*, Winter 1995, 69-69.

10. Electromagnetic Pulse

11. Department of the Air Force, *Basic Aerospace Doctrine of the United States Air Force* (AFM 1-1, vol. I) (Washington DC: March 1992), 14.

12. Caldwell, 54.

13. Caldwell, 56.

14. Lt. Col. Norman B. Hutcherson, *Command and Control Warfare*, Research Fellow., Air University, 1994 (Maxwell AFB, Alabama: Air University Press, 1994) 21. The other pillars are operations security, military deception, electronic warfare, and physical destruction.

15. Waller, 43.

BIBLIOGRAPHY

Barlow, W. J., et al. *Implementation of a Command and Control Countermeasures Strategy in Korea*. Alexandria, VA: Institute for Defense Analysis, June 1990.

_____. *Command, Control, and Communications Countermeasures During Desert Storm/Desert Shield*. Alexandria, VA: Institute for Defense Analysis, June 1992.

Caldwell, Warren Jr. "Promises, Promises." *Proceedings*, January 1996.

Chairman of the Joint Chiefs of Staff *Command and Control Warfare*, Memorandum of Policy #30. Washington DC: 8 Mar 1993.

Cook, Wyatt C. "Information Warfare: A New Dimension in the Application of Air and Space Power." *Selected Essays- Air War College Class of 1994*, Maxwell AFB, AL: June 1994.

van Creveld, Martin *Command in War*. Cambridge, MA: Harvard University Press, 1985.

Department of the Air Force. *Basic Aerospace Doctrine of the United States Air Force* AFM 1-1. Washington: March 1992.

Department of Defense, "Appendix O: The Role of the Law of War," *Conduct of the Persian Gulf War: Final Report to Congress*. Washington DC: April 1992.

Department of the Navy. *The Commander's Handbook on the Law of Naval Operations* NWP 1-14M, draft ed. Washington DC: May 1995.

Department of the Navy, *Policy Planning and Guidance for Naval Information Warfare/Command and Control Warfare*. Washington DC: 16 Feb 1995.

DiNardo, R.L. and Hughes, Daniel. "Some Cautionary Thoughts on Information Warfare," *Airpower Journal*, Winter 1995.

Department of Defense. *Information Warfare*, DOD Directive TS3600.1. Washington DC: 21 December 1992.

Hopper, William Frank. *Command and Control Countermeasures Doctrine in the Naval Environment*. Monterey, CA: Naval post-graduate School, June 1983.

Hutcherson, Norman B. *Command and Control Warfare*. Maxwell AFB, Alabama: Air University Press, 1994.

"Non lethal Weapons Give Peacekeepers Flexibility." *Aviation Week & Space Technology*, December 7, 1992, p 50-52.

Orr, George E. *Combat Operations C3I: Fundamentals and Interactions*, Maxwell AFB AL: Air University Press, 1983.

Rorke, Steven C. "Command and Control Warfare: Panacea or Pandora's Box?" Unpublished Research Paper, U.S. Naval War College, Newport, RI: 16 June 1995

Schultz, Richard H. Jr. and Robert L Pfaltzgraff, Jr. *The Future of Air Power in the Aftermath of the Gulf War* Maxwell AFB, AL: Air University Press, July 1992.

Sexton, Joanne. "A Combatant Commander's View of Information Warfare and Command and Control Warfare," Unpublished research paper, U.S. Naval War College, Newport, RI: 16 June 1995.

Toffler, Alvin and Heidi Toffler. *War and Anti-war: Survival at the Dawn of the 21st Century.* Boston: Little, Brown, and Co., 1993.

U.S. Navy. *Policy Planning Guidance for Naval Information Warfare/ Command and Control Warfare*. Washington, DC: Office of the Secretary of the Navy. 16 Feb 1995.

Ward, Robert W., et al. "C3/Space and Electronic Warfare," *Desert Storm Reconstruction Report* vol. VIII, Alexandria, VA: Center for Naval Analysis. June 1992.

Warden, Col. John A. *The Air Campaign: Planning For Combat*. Washington, DC: National Defense University Press, 1988.

Waller, Douglas. "Onward Cyber Soldiers," *Time*, August 21, 1995.

Disclaimer