Naval War College Review

Volume 51
Number 2 *Spring*

Article 3

1998

Information Operations, Deterrence, and the Use of Force

Roger W. Barnett

Information Operations, Deterrence, and the Use of Force

Roger W. Barnett

"A COUPLE OF YEARS AGO, NO ONE took information warfare seriously. But the more you learn about it, the more concerned you become."[1] Typical of many today on the subject of information warfare, this statement implies the equation: *ignorance* = *complacence*. Yet information warfare has been around since at least the fifth century B.C. IW also was powerfully displayed in the Second World War—it was arguably a key to victory in both the European and Pacific theaters—and it played an important role in the Gulf war of 1991. So why do so many people think the United States (especially the U.S. military) is unfamiliar with IW, and why is there such concern about "taking it seriously"?

Perhaps what is intended is to raise the alarm about some new vulnerabilities to information warfare that have been exposed in the last few years, as societies and economies become more dependent on the free and rapid flow of information. In the United States both the General Accounting Office and the Defense Science Board have released detailed reports on the subject.[2] These reports acknowledge that there are problems to be solved, but neither qualifies as an appeal to urgent action. The jury is still out, however; the President's Commission on Critical Infrastructure Protection is currently in session, studying eight critical domestic infrastructures.[3]

For the U.S. military, the topics of central interest in information operations narrow down to two: deterrence and employment.[4] Deterrence of an information attack against the United States and its friends and allies, and the use of information operations in the affairs of state constitute the dual focus of

Roger Barnett is professor of naval warfare studies at the Naval War College, where he teaches elective courses in information warfare and arms control. Concurrently, he serves as adjunct professor both at Salve Regina University and at Southwest Missouri State University. He retired from the Navy in 1984, having served in cruisers, destroyers, and headquarters staffs in Washington. He has earned a B.A. from Brown University, and M.A. and Ph.D. degrees from the University of Southern California.

Naval War College Review, Spring 1998, Vol. LI, No. 2

attention. This article examines deterrence as it relates to information operations and then offers some insights on employment. It argues first that for the two types of deterrence—general and immediate (or "focused")—the United States has inherent strengths but also identifiable shortcomings that can be rectified. Second, this article contends that there are important and valid arguments against allowing information operations to be characterized as "uses of force" in international law. The more routinely "information operations" can be understood, like "counter-terrorism," as self-defense *not* involving "the use of force," the greater will be its contribution to U.S. national security.

Information Operations

As an instrument of statecraft, information operations can be employed in support of national policy in much the same manner as diplomacy or economic policy. Available in peace, crisis, and at all levels of warfare, information operations have both offensive and defensive aspects. Unlike economic actions to sanction the activities of other states—measures generally considered slow-acting and blunt—information operations can quickly impose severe damage with low levels of violence. This is one of the major characteristics that set information operations apart from other instruments of statecraft.

There are other differences as well. For one, the information environment changes rapidly. An operation that would succeed today might fail tomorrow—or an hour from now—because a computer configuration, a communications channel, a network, or a software protocol has been altered. As in covert and clandestine operations, "agents" ("trojan horses" or "trap doors" for example) can be put in place for later activation.[5] Also different from traditional means is the difficulty of observing and assessing the results of information operations. A virus might be implanted in an adversary's computer; whether or not the virus is effective might well be unassessable by the attacker. Of course, one of the defensive techniques of information operations is actually to deny the adversary the ability to measure his results, rendering the problem even more difficult. Likewise, it often borders on the impossible to know whether one's own defenses are effective. Perhaps our system is being exploited, but we are unaware of our vulnerability. If we are secure, is it because the defenses are working or because no one is testing them? Will we still be secure ten minutes from now? The magnitude of such unknowns is large, and that contributes to the concern that *ignorance = complacence.*

Given the importance of modern computer networks, communication systems, and electronic data banks, information operations should be fully integrated into overall national security policy. In peacetime they can contribute to the prevention of conflict, or they can be used to respond to crises and open

hostilities. They may or may not involve military capabilities or units. In times of crisis, information operations can be employed to resolve disagreements, fortify deterrence, or prepare for the possibility of open conflict. In war they can directly achieve strategic, operational, and tactical objectives or underwrite other means to achieve such objectives. The Joint Staff white paper "Joint Vision 2010" puts down a marker, asserting that military operations in the future will require information *superiority*, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[6]

Offensive actions using information operations include those that move information from one place to another, destroy it, promulgate disinformation, and corrupt, degrade, interrupt, or deny data flows. Defensive actions seek to protect one's own information from similar actions of an adversary. Clearly, a variety of means can be used in both offensive and defensive information operations. These include the well recognized military pillars of command and control warfare (electronic warfare, operations security, deception, psychological operations, and physical destruction);[7] other means are "hacker warfare," "economic information warfare," and "cyberwarfare."[8]

In peacetime a fundamental U.S. security objective is to prevent war. If conflict should ensue, the goal would be to terminate it as quickly and with as little damage as possible without compromise of vital interests or major objectives. Information operations can play important roles both in the prevention and the successful prosecution of war. Their effectiveness pivots on their role in deterrence, and on whether they are to be considered a use of force.

U.S. Readiness for Deterrence of Information Attack

Long considered to be the product of capability and will, deterrence is a subject to which much lip service but insufficient thought has been devoted. The reason is that "general" deterrence is usually relied upon to keep the peace. *General* deterrence stems from maintaining the capability and will to inflict severe damage in retaliation against those who would disturb the peace. Merely by supporting a large, highly capable military, the United States conveys its ability to punish those who would transgress against it. General deterrence does not require the communication of a specific threat against aggressors; its effectiveness relies rather on the presence of an arsenal of tangible capabilities.

Aside from punishment, general deterrence can work through denial. It is made plain to those who would harm the United States or its interests that they will not be permitted to attain their objectives; recognizing that they cannot succeed, they are deterred from making the attempt. To achieve deterrence by denial, one first attempts to make hostile acts as difficult as possible to carry out,

and then, should such an act take place, to thwart its achievement of the attacker's purpose. This is the approach used against terrorists, hostage-takers, and extortionists, for example. The message to prospective perpetrators is this: You cannot prevail, so why make the attempt?

General deterrence through the threat of *punishment* requires maintaining an offensive capability and credibly projecting the will to use it. General deterrence through *denial* requires stout defenses and a history of consistent refusals to yield to coercive threats.

"Focused," or "immediate," deterrence operates at a different level of specificity. It recognizes that sometimes general deterrence does not work—posturing without reference to a particular objective will be viewed as weak or irrelevant—and that a focused, immediate, or specific deterrent *threat* or *statement* is required. Thus, focused deterrence is "stronger" than general deterrence, representing a nation's explicit effort to dissuade an adversary from carrying out an undesirable act (or failing to carry out a desirable one). General deterrence failed between the British and the Argentines over the Falkland Islands in 1982. The British never clearly communicated to the Argentines that they would use force to protect the islands—in fact, the British Foreign and Commonwealth Office signaled much to the contrary. General deterrence failed again in the Persian Gulf in 1990; no specific threat was issued to Saddam Hussein that forcible acts against Kuwait would be redressed with military force. In both of those cases the aggressor concluded that he could discount a general deterrent. Either a specific deterrent statement or a powerful defense was needed to forestall aggression. Neither was provided.

Like general deterrence, focused deterrence can operate through threat of punishment or by denial. Immediate deterrence by threat of punishment requires identifiable targets, and it works best on organized groups that can be located and attacked—governments, for example. Against individuals or organizations that are less formal and more difficult to locate—computer hackers or terrorists, for instance—deterrence by denial is the more appropriate form.

Deterrence of whatever kind or modality requires both *capability* and *will*. Since the end of the Cold War, the United States has enjoyed military superiority over all other states in the world. It maintains the ability to use force up to and including the nuclear devastation of any country or locatable organization. Information operations, although they do not invariably involve the use of force, contribute to the aggregate U.S. deterrent capability. Unquestionably, for deterrence through the threat of punishment, the capability factor in the U.S. equation is virtually overwhelming. As we shall see below, American *will* in this area appears deficient.

Adversaries who either discount or do not fear punishment must be deterred by denial. Deterrence by denial rest on very strong defenses, so that aggressors cannot achieve their objectives directly by striking first. Defense against information attack requires effective identification and authentication mechanisms, well trained and disciplined system operators, high assurance firewalls,* and auditing and trace-back methods. For the United States, lack of these protections constitutes soft points that adversaries might successfully exploit. Since no defense is stronger than its weakest point, the ability of the United States and other open societies to deter an information attack by a strategy of denial is, and always will be, suspect.

It should be understood, however, that the complexity of systems constitutes in itself a barrier to attack. Communication systems (particularly governmental command and control networks) are designed to be redundant and to fail gracefully (that is, offering successive "casualty modes") rather than catastrophically. Alternate methods of routing information abound, and complex software routines help ensure the reliability and authenticity of the information carried. While an insider well versed in a system's architecture might assess it as vulnerable, to an outsider it is likely to appear extremely robust and difficult to attack. This helps to explain why a large fraction of successful attacks on information systems originate—or receive assistance—from within.[9]

Will, like capability, extends across both general and focused deterrence, and pertains both to threat of punishment and to denial. While American willingness to deter by threat of punishment generally appears strong, the nation's resolve to retaliate against an information attack is questionable; in this field, readiness to exercise focused deterrence has to date been untested and largely unaddressed. Would the United States, recognizing a particular threat of a planned information attack, issue a deterrent statement specifically addressing it? For the matter of denial, the United States has been quite successful in forestalling terrorists, political extortionists, and others who might contemplate conducting an information attack to further their goals.

Will is communicated in a number of ways, sometimes by the declaration of policy, sometimes by demonstration—by the overt *use* of the capability. If neither of these takes place, then deterrence is general. It is in this situation that the United States finds itself today in information operations. It has great capability to conduct retaliatory information operations; yet no declarations have been made about what would happen if the nation's critical information infrastructure were attacked by hostile agents, nor have demonstrations been forthcoming.

---

* A *firewall* is a means to prevent penetration of an information system by other than authorized users of the system. Firewalls usually require some kind of password or other authentication.

At the same time, its defenses—instrumental for deterrence by denial—are not adequate. Thus at present, for information operations the United States is relying on the weaker form, general deterrence. But even for general deterrence in the information operations arena, the American capability to deny is suspect at best, and its will to punish is questionable.

When it comes to deterrence, U.S. capability to conduct information operations in order to punish is not at issue. The problems for deterrence arise when one considers defenses against information operations by adversaries, or U.S. will—especially for focused deterrence.

The matrix summarizes the current deterrence situation for information operations.

Readiness for Deterrence of Information Operations

		General Deterrence	Focused Deterrence
Capability	*Punish*	Strong	Strong
	Deny	Defenses suspect	Defenses suspect
Will	*Punish*	Questionable	Unaddressed
	Deny	Strong	Unaddressed

Deterrence for Information Operations

The capacity of the United States to conduct information operations, then, is very great, but its vulnerability to the information operations of others is also considerable, because American defenses and will to act are, or might well be perceived as, weak. For deterrence by threat of punishment, then, the outcome pivots on the question of will; for deterrence by denial, it is a question of adequate defenses and of how to demonstrate sufficient will to effect focused deterrence. Issues for resolution therefore have to do first with the capability to deny, which is centrally a question of strengthening information operations defenses; and second, with the will to punish aggressors, which needs to be underwritten by policy statements and other actions that support both general and focused deterrence.

Of the two issues of central interest to the U.S. military, the second, the employment of information operations, is closely related to the first, deterrence. Employment may be direct or indirect, but it reinforces both capability and will. Its objective is either to discourage information attacks against the United States or its friends and allies or to achieve security objectives by offensive action.

The use or threat of *force* occupies a central position in deterrence, but deterrence does not rely solely on it. For deterrence to be effective, it suffices that an adversary believe that he will be worse off—perhaps much worse off—for undertaking a particular action than for not attempting it.

Importantly, information operations have tended to be judged by the guidelines governing the use of force: necessity, discrimination, proportionality, and humanity. Clearly, however, some information operations do not by any stretch of language involve the use of force: psychological operations, many applications of deception, and also a variety of computer "code bombs," viruses, and "chipping," for example.[10] In addition, and of note, information operations can be conducted by other than military forces.

The distinction is an important one, not least because to the extent that information operations are considered in the same framework as force, their use will be conditioned by four categories of factors—operational, organizational, legal, and moral. Let us examine how these categories might be misapplied to information operations, bearing in mind that each of these would (and does) constrain the freedom available for information operations, affecting willingness either to use or to threaten their employment. Adversaries or potential adversaries recognize these constraints and how they affect the will of the United States to act or to defend against hostile actions. The overall effect of these constraints on deterrence is not entirely clear, but certainly it is not to strengthen deterrence.

Operational constraints. U.S. decision makers today observe an operational code under which they use force. While they use force only reluctantly, when it is called for they prefer to apply it massively, in order to minimize friendly casualties and terminate hostilities as soon as possible. To this end, objectives should be clearly stated so that progress toward them can be monitored and so that it will be evident when they have been achieved. Targets must be selected carefully. Noncombatants must not be targeted directly, and religious shrines, works of art, monuments, and the like must be preserved. Collateral damage should be minimized. Moreover, unintended consequences are to be, as much as possible, ruled out. Fratricide—"blue-on-blue" engagements—should also be avoided. In fact, it is desirable that casualties on both sides be minimized.

By this code, and generally speaking, while preemptive attack by American armed forces is desirable and workable at the tactical level of warfare, it is problematical at the operational level, and unlikely at the strategic. That is, the

United States goes to war only when forced to do so, but once engaged acts swiftly, aggressively, and decisively. Because of this greater reluctance to preempt at the strategic level, the United States is more vulnerable to strategic surprise and thus to its undesirable effects. Yet if information operations are not considered to involve the use of force, preemption by such means might well be undertaken at any level. That is to say, if information operations can be distinguished from the use of force, the traditional American inhibition about initiating hostile action—especially at the strategic level—will no longer pertain. Moreover, because information operations can take place at very high speeds and without warning, the implications of surprise are potentially serious at all levels of warfare. If this distinction about the operational acceptability of information operations is recognized, U.S. decision makers must assess the possibilities for the adversary to retaliate, and they must determine whether they can defend against or tolerate that retaliation. If they cannot, the United States will probably be dissuaded from attacking.

While these seem an unexceptionable set of operational constraints, they are actually unique as a fighting code. Most of them are clearly of minimal concern to potential U.S. opponents, with respect to their own acts. One that *is* of interest to them, however, is the last one: assessing the potential for the adversary to retaliate. If deterrence by threat of punishment has a pivot, this is it.

Still, by the operational restrictions the United States places on itself, the question of retaliation is made an issue. That is, with regard to punishment, the *certainty* of retaliation is what deters. Deterrence is weakened to the extent that an adversary is uncertain about the level of retaliation or whether it will occur at all. That, of course, is not a matter only of capability but also of will to retaliate. It is an especially difficult task for information operations: to convince a potential foe that one has the will to retaliate with information operations and that he will be much worse off because of that retaliation.

In information operations, as in terrorism, the possibility exists that a devastating attack will be made without the perpetrator being identified. The difficulty of determining the source of computer hacking or the origin of a virus gives rise to concern about catching a culprit or retaliating against an attacker. Even if an attacker can be identified, questions arise about the proper form of retaliatory action. Such questions enervate deterrence by reducing the certainty of retaliation. If one can formulate no appropriate and effective form of retaliation, one is obliged to rely on deterrence by denial.

Organizational constraints. The use of force by the United States is constrained also by the way the country is organized. Democracies are historically more reluctant to use force than are other types of government.[11] That the commander in chief is the president but the power to declare and support war lies with the legislative branch places another layer of constraint on the use of force.

If information operations are regarded as the use of force—and especially if those operations are preemptive or a first use—consideration must be given to how to address these problems.

Similarly, many forms of freedom and rights to privacy, including of personal information, are considered to be fundamental in the United States. These have great import for the conduct of information operations, in particular when attempting to track or trace the source of attacks on the nation's infrastructure. Strong legal and societal forces are highly resistant to governmental monitoring of, or interference in, the unfettered flow of information, plain or encrypted.

There are other organizational hindrances as well. The free, neutral press in the United States represents another source of restrictions. The power of the media to raise difficult questions and issues would have to be considered before information operations were undertaken. Then there are the constraints posed by external organizations of which the United States is a member—most notably the United Nations and Nato. Mere membership in these organizations means acceptance of additional layers of constraint. Ad hoc coalitions have a similar restrictive effect.

Legal constraints. A significant body of legal restrictions on the use of force has been formalized. It resides in international law—in particular in the law of armed conflict—and in arms control agreements, which are legally binding documents.

The law differentiates between initiating the use of force—*jus ad bellum*—and how force is used in war—*jus in bello*. To satisfy the law governing the former, the use of force must stem from a cause that is just, be motivated by right intentions, and be authorized by competent authority. In addition, four tests must also be passed: the use of force must have a reasonable chance of success, be expected to produce a net balance of good over evil, and be a last resort; peace, finally, must be the expected outcome. The Charter of the United Nations, moreover, takes *jus ad bellum* another step, requiring that the use of force always and exclusively be in self-defense.

Once warfare has commenced, whether or not the requirements of *jus ad bellum* have been satisfied, different criteria must be met: the *jus in bello* stipulations mentioned earlier—necessity, proportionality, discrimination, and humanity. The law of armed conflict, codified in the Hague and Geneva conventions and in other legal documents, has provided specificity to the requirements of *jus in bello*. These deal, inter alia, with the rights and responsibilities of belligerents and neutrals and with the protection of noncombatants in time of war. For their part, arms control constraints limit quantitatively and qualitatively the inventories and deployment of armament. There have been no specific arms control agreements directed at limiting information operations. In fact, however, with its emphasis on confidence-building measures and

operational transparency, arms control has acted to hobble effective information operations.

Other treaties and executive agreements have a potential effect on information operations as well. The International Telecommunications Satellite Organization (INTELSAT) Agreement of 1973, for example, seeks to ensure that satellites are used only for peaceful purposes. While the agreement does recognize satellite systems with military purposes and exempts them, the Department of Defense uses civilian systems heavily.[12] Whether information operations that involve such systems (including, for instance, portions of the Internet) are always to be regarded as "non-peaceful" is a fundamental issue that has not yet been settled.

Likewise, covert and clandestine acts under the mantle of national security are governed by federal law. A presidential finding and congressional approval are required. A variety of peacetime information operations might fall within this category, especially those involving emplacement of information operation "agents," but this too has not been determined.

Moral constraints. Over and above operational, organizational, and legal constraints, there are moral considerations. U.S. foreign policy has always had a moral element; it asks whether the nation may undertake a particular act or follow a certain policy line that is legally permitted and prudentially attractive. U.S. decision makers are often torn by competing requirements, for example the need for humanitarian intervention and the principle of noninterference with internal affairs of other states. It is difficult even to articulate a moral code in such circumstances, let alone to follow one consistently.

Among the vexing issues is separating intellectually the use of force or information operations among nation-states from that in the context of interpersonal relations. International actions often are judged indiscriminately under the same set of rules and with the same moral template as are interpersonal situations. Yet the actions a state may morally and legally do are very different from those that individuals may do. Dean Acheson articulated the difference over thirty years ago: "A good deal of trouble comes from the anthropomorphic urge to regard nations as individuals.... The fact is that nations are not individuals; the cause and effect of their actions are wholly different."[13]

U.S. decision makers believe it is important for the nation to act as a moral leader in interstate relations. One consequence of this view is that policies or actions should not cause unnecessary suffering on the part of noncombatants in a target state. Moreover, Americans tend to be uncomfortable with the notion of superiority, believing strongly in egalitarianism. This makes it somewhat awkward for the United States to deliver a deterrent threat based on superior capabilities. Public justification of the use of information operations will be important, for the moral aspects of U.S. policy will demand it. How the use of

information operations is morally justified will go a long way toward either identifying it with, or divorcing it from, the use of force.

As a result of the interplay of these factors, the ability of the United States to deter an information attack can be assessed as no better than problematical. The capability of this nation to respond to an information attack by a state or an organized, locatable group cannot be doubted; its *will* to do so is another question. If the attacker is amorphous and hidden, the United States will have to rely on deterrence by denial, precluding the harms that a determined and competent information attacker may seek to cause, or acting in such a manner that even successful attacks prove to be of no benefit to their perpetrator. Unfortunately, self-protection is a key aspect of deterrence by denial, and that is another weak point in U.S. information operations.

Deterrence by both punishment and denial would be bolstered by articulation of a deterrent policy and other actions that communicate the willingness of the United States to play an active role in information operations across the board. As the Defense Science Board concluded, "Deterrence must include an expression of national will as expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack."[14]

In the foregoing, information operations have figured much as armed attack or physical defense might in more traditional deterrence calculations. It might seem implicit, then—especially from the matrix—that an information operation is in essence a new kind of force. But is it? Should it be? The extent to which any or all of the myriad restrictions on the use of force apply to information operations can be a matter of choice. The default, "fail-safe" position would seem to be to treat information operations as if they were in fact a use of force, subject to all the constraints and tests mentioned. On the other hand, a deliberate policy decision might establish the separate nature of some kinds of information operations and seek to put distance between those information operations and the use of force. Such a statement would first of all have to differentiate the effects of certain information operations from those of the use of force, and then establish principles for the creation of those particular effects, to which many of the force-analogues would then no longer be applicable. For instance, the distinction between combatants and noncombatants—a central requirement in the law of armed conflict—would now be seen quite differently. Likewise, the policy statement might stipulate, for example, that proportionality is not an issue for the information operations that are identified as not being matters of force. Some forms of information operations would also be exempt from scrutiny on questions of necessity or on their effects on noncombatants. In some situations of retaliation against hacker warfare, it could be argued, standard

judicial rules of evidence would not apply; a new code would have to be developed.

If the case can be made and sustained that particular forms of information operations do not constitute uses of force, they could be very valuable assets for national security. Careful, controlled use of these particular information operations could fortify deterrence in peacetime—both general and focused. Employment in peace, crisis, and war, unencumbered by the baggage that attends the use of force, would render the information operation an integral, high-leverage instrument of statecraft. If, on the other hand, no sort of information operations can be brought out from under the "use of force" mantle, all will be hamstrung. For the country with the greatest capability to conduct information operations, this would forfeit what could be a decisive advantage in peace, crisis, and war.

Notes

1. Howard Frank, director of the Information Technology Office of the Defense Advanced Research Project Agency, quoted in Steve Lohr, "Ready, Aim, Zap," *New York Times*, 30 September 1996, p. D-1. See also Winn Schwartau's World Wide Web site, <http://www.infowar.com>, a focal point for the subject of information warfare.

2. U.S. General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD 96-84 (Washington, D.C.: General Accounting Office, May 1996); and Defense Science Board, *Report of the Defense Science Board Task Force on Information Warfare—Defense (IW-D)* (Washington, D.C.: Office of the Secretary of Defense, November 1996).

3. The Commission was formed by Executive Order 13010 of 15 July 1996. Its report is expected in mid-October 1997. The "critical domestic infrastructures" identified in the executive order are: telecommunications, electrical power systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government.

4. This article employs the U.S. Department of Defense definitions of information operations: "Actions taken to affect adversary information and information systems while defending one's own information and information systems," and of information warfare: "Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries."

5. Some useful definitions: "*Computer virus:* malicious computer code that attaches itself to another block of code in order to propagate. . . [;] *malicious computer code:* any computer code on a system without the consent of the owner . . . ; *trap door:* a hidden software mechanism triggered to circumvent system security measures[;] *trojan horse:* malicious computer code located within a desirable block of code (i.e., an application program, operating system software, etc.). To be a trojan horse, the presence of the code must be unknown and it must perform an act that is not expected by the owner of the system . . . [;] *logic bomb:* a type of trojan horse that may or may not be a virus. Its mission component is triggered by a true/false condition. Logic bombs do not propagate; they just sit and wait . . . [;] *time bomb:* a subset of the logic bomb; its trigger is the date and/or time . . . [;] *worm:* malicious computer code, similar to a virus, that can replicate itself. Worms are independent operating programs that can mail replicas of themselves outside the host system. Worms may or may not have a mission component or a trigger." Lawrence G. Downs, Jr., "Digital Data Warfare: Using Malicious Computer Code As a Weapon," in Mary A. Sommerville, ed., *Essays on Strategy XIII* (Washington, D.C.: National Defense Univ. Press, 1996), p. 45.

6. Chairman, Joint Chiefs of Staff, "Joint Vision 2010" (Washington, D.C.: 1996), p. 16.

7. Chairman, U.S. Joint Chiefs of Staff, *Command and Control Warfare*, CJCS Memorandum of Policy (MOP) 30 (Washington, D.C.: The Joint Staff, 8 March 1993).

8. Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, August 1995).

9. "The USSS [U.S. Secret Service] commented that over the last year there has been a rise in the percentage of ontsider attacks on industry versus iusider. The proportion is now approximately 40 percent

outsider versus 60 percent insider attacks." U.S. Joint Chiefs of Staff, *Information Warfare: Legal, Regulatory, Policy, and Organizational Considerations for Assurance*, 2d ed. (Washington, D.C.: 4 July 1996), p. A-146.

10. "Chipping" is the practice of making electronics chips vulnerable to destruction by designing in weaknesses. For example, certain chips may be manufactured to fail upon receiving a specific signal. Daniel E. Magsig, *Information Warfare in the Information Age;* electronic version, <http://www.seas.gwu.edu/student/dmagsig/index.html> (7 December 1995).

11. Alexis de Tocqueville argued, "Democratic nations naturally desire peace." Quoted in Josef Joffe, "Democracy and Deterrence: What Have They Done to Each Other?" in Linda B. Miller and Michael Joseph Smith, *Ideas & Ideals: Essays on Politics in Honor of Stanley Hoffman* (Boulder, Colo.: Westview Press, 1993), p. 114. Walter Laqueur put a fine point on it: "Democracies, with rare exceptions, always incline to pacifism, and they find it difficult to understand those who do not share this predisposition: how can anyone be so unreasonable as to consider war an instrument for the solution of conflicts?" Walter Laqueur, *The Political Psychology of Appeasement: Finlandization and Other Unpopular Essays* (New Brunswick, N.J.: Transaction Books, 1980), p. 135.

12. General Accounting Office, passim.

13. Dean Acheson, "Ethics in International Relations Today," *Amherst Alumni News*, Winter, 1965, pp. 2–3, quoted by James Finn, "Morality and Foreign Policy," in Michael Cromartie, ed., *Might and Right after the Cold War: Can Foreign Policy Be Moral?* (Washington, D.C.: Ethics and Public Policy Center, 1993), p. 38.

14. Defense Science Board, executive summary, p. 4.

Ψ

The Naval War College Press is pleased to note that . . .

Dr. Leslie C. Green

Charles H. Stockton Professor of International Law at the Naval War College, and a contributor to this journal, has been awarded

The John Read Medal

by the Canadian Council on International Law.

The medal, whose namesake was the dean of the University of Toronto and a judge on the International Court of Justice, is awarded to "persons of distinction" who have made significant contributions to international law in Canada. Its recipients—Dr. Green is the twelfth—include some of the world's most renowned legal theorists.