The US Army War College Quarterly: Parameters

Volume 29
Number 2 *Parameters Summer 1999*

Article 2

5-25-1999

Nuclear Crisis Management and Information Warfare

Stephen J. Cimbala

Recommended Citation
Stephen J. Cimbala, "Nuclear Crisis Management and Information Warfare," *Parameters* 29, no. 2 (1999), doi:10.55540/0031-1723.1927.

Nuclear Crisis Management and Information Warfare

STEPHEN J. CIMBALA

From *Parameters*, Summer 1999, pp. 117-28.

Military analysts and academic experts in security studies have envisioned a post-Cold War world dominated by a "Revolution in Military Affairs" based on high-tech conventional weapons and dominant knowledge of the wartime environment.[1] The same people often have assumed that the evolutionary development of nuclear weapons and their delivery systems is on an entirely different trajectory than that projected for information-based, "Third Wave" warfare and weapons.[2] Nuclear and other weapons of mass destruction are the past; information-based, non-nuclear weapons, in this vision, are the future of war. This assumption of entirely separate gene pools for nuclear weapons of mass destruction and for information warfare may be incorrect for some kinds of situations, however, including crises between nuclear-armed states. The two apparently antithetical kinds of weapons may come together to create a new and potentially terrifying synthesis under the "right" political conditions.

For present purposes, information warfare can be defined as activities by a state or non-state actor to exploit the content or processing of information to its advantage in time of peace, crisis, or war, and to deny potential or actual foes the ability to exploit the same means against itself.[3] This is intended as an expansive, and permissive, definition, although it has an inescapable bias toward military- and security-related issues. Information warfare can include both *cyberwar* and *netwar*. Cyberwar, according to John Arquilla and David Ronfeldt, is a comprehensive, information-based approach to battle, normally discussed in terms of high-intensity or mid-intensity conflicts.[4] Netwar is defined by the same authors as a comprehensive, information-based approach to societal conflict.[5] Cyberwar is more the province of states and conventional wars; netwar, more characteristic of non-state actors and unconventional wars.[6]

This article is organized as follows. First, I explain why the issue of nuclear deterrence remains significant after the Cold War. Second, I discuss what governments must do in order to perform successfully the crisis management function and the complexity inherent in accomplishing these tasks. Third, I identify some of the ways in which information warfare may increase the difficulty of accomplishing those tasks necessary to reduce or eliminate the risks of failed crisis management, with attention to the special character of crises between nuclear-armed states.[7] Fourth, I acknowledge that information warfare cannot be done away with, and is in some cases a desirable option for US policymakers. Therefore, the lion of infowar must be made compatible with the lamb of nuclear deterrence (or is it the reverse?).

Nuclear Weapons Will Not Go Away

Contrary to some expectations, nuclear weapons and arms control issues have not vanished over the horizon in a post-Desert Storm euphoria. There are at least four reasons for this.

The first is that Russia still has many thousands of nuclear weapons, and delivery systems of intercontinental range. US officials await the ratification by the Russian State Duma (lower house of the Russian legislature) of the START II agreement that would reduce permitted strategic nuclear warheads for each side to between 3,000 and 3,500 force loadings.[8] US Department of Defense funds have been authorized by the Nunn-Lugar legislation for the destruction, dismantlement, and secure storage of much of the Cold War Soviet nuclear arsenal. Russia's willingness to ratify START II and to proceed to a Clinton-sought START III is related to two other important security issues: NATO enlargement and continued adherence to the ABM Treaty of 1972.[9]

Somewhat paradoxically, Russia's military and economic weakness for at least the remainder of this century makes

nuclear deterrence a more central element in Russian military strategy. There are two aspects of this weakness that might contribute to a nuclear confrontation resulting from failed crisis management, mistaken preemption, or accidental/inadvertent war. First, Russia's conventional military weakness makes it more reliant on nuclear weapons as weapons of first choice or first use, instead of last resort. Second, Russia's economic problems mean that it will have difficulty maintaining personnel morale and reliability. In addition, Russia's military also will be lacking in funds to modernize and properly equip its early warning and nuclear command, control, and communications systems. Russia's military and economic weaknesses may encourage, at least in the near term, reliance on prompt launch doctrines for nuclear retaliation and emphasis on nuclear first use in situations where conventional forces are in jeopardy.[10] In addition, at least some Russian thinkers have noted the potentially strategic significance of information warfare and have connected the consequences of information attacks to potentially nuclear responses:

> From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not. . . . Considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces, . . . Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself.[11]

A second reason why nuclear deterrence remains important in the post-Cold War world is that the other acknowledged nuclear powers, in addition to the United States and Russia, show no inclination to abandon nuclear weapons as ultimate deterrents. China is, by all accounts, engaged in a significant modernization of its military technology base, including the base that supports improved delivery systems for nuclear weapons. France maintains the *force de dissuasion* as its ultima ratio and, despite increased cordiality with NATO of late, continues its Cold War tradition of reserving to itself the decision to launch nuclear weapons in retaliation. British modernization of nuclear strategic delivery systems for ballistic missile submarines continued into the 1990s, with US assistance. With regard to declaratory strategy for nuclear use, while NATO has pushed nuclear weapons into the background as weapons of last resort, Russia's conventional military weakness has propelled its nuclear weapons into the forecourt.

A third reason for the continued importance of nuclear deterrence is the recent spread of nuclear weapons to previously non-nuclear states, and the potential for additional non-nuclear states to acquire these and other weapons of mass destruction. The acknowledged nuclear detonations by India and Pakistan in May 1998 crossed a threshold: previously, the only declared nuclear powers had been the "big five" permanent members of the UN Security Council. In addition, India and Pakistan have been bitter regional rivals and came close to war in 1990 over Kashmir. Intelligence estimates provided to President Bush during the 1990 crisis indicated that Pakistan had assembled from six to ten nuclear warheads by mid-May and might have begun deploying them on F-16 aircraft. Some US officials also believed that then Pakistani Prime Minister Benazir Bhutto had been cut out of the decisionmaking process for nuclear release.[12] In addition to these opaque proliferators, other candidate non-nuclear states thought to be pursuing nuclear capability include Libya, Iran, Iraq, and (until 1994) North Korea. The potential for regional destabilization once any of these currently non-nuclear states acquires nuclear weapons is enhanced given their apparent interest in other weapons of mass destruction and in delivery systems for nuclear, chemical, or biological weapons.[13]

Fourth, nuclear deterrence remains important because non-state actors, including terrorists, interstate criminal organizations, and revolutionary actors of various sorts may acquire nuclear or other weapons of mass destruction. Although for some of their purposes nuclear weapons would be superfluous, for other objectives they would, even in small numbers and puny yields, be quite appropriate. Terrorists who could present a plausible threat to detonate even a small nuclear device within a target state could raise the potential risk of hostage rescue operations--for the hostages and for armed forces of the target state.[14] Terrorists allied with a state actor and equipped with nuclear weapons could gain from their ally valuable intelligence, sanctuary, and diplomatic cover. Criminal cartels could replenish their coffers by trafficking in nuclear weapons or weapons-grade materials as middlemen, even if they were not the end users themselves. Consider the increased degree of freedom for US opponents in Panama (Just Cause) or in Iraq (Desert Shield and Desert Storm) if Noriega's agents in the Canal Zone or Saddam's operatives in Kuwait had had available even a small nuclear device, well timed and strategically located.

Requirements for Crisis Management

Crisis management, including nuclear crisis management, is both a competitive and cooperative endeavor between military adversaries. A crisis is, by definition, a time of great tension and uncertainty.[15] Threats are in the air and time pressure on policymakers seems intense. Each side has objectives that it wants to attain and values that it deems important to protect. During a crisis state behaviors are especially interactive and interdependent with those of another state. It would not be too farfetched to refer to this interdependent stream of interstate crisis behaviors as a system, provided the term "system" is not understood as an entity completely separate from the state or individual behaviors that make it up. The system aspect implies reciprocal causation of the crisis behaviors of "A" by "B," and vice versa.

One aspect of crisis management is the deceptively simple question: what defines a crisis as such? When does the latent capacity of the international order for violence or hostile threat assessment cross over into the terrain of actual crisis behavior? It may be useful to separate traffic jams from head-on collisions. A traffic jam creates the potential for collisions but leaves individual drivers with some steering capacity for the avoidance of damage to their particular vehicles. A breakdown of general deterrence in the system raises generalized threat perceptions among various actors, but it does not guarantee that any particular relationship will deteriorate into specific deterrent or compellent threats. Patrick Morgan's concept of "immediate" deterrence failure is useful in defining the onset of a crisis: specific sources of hostile intent have been identified by one state with reference to another, threats have been exchanged, and responses must now be decided upon.[16] The passage into a crisis is equivalent to the shift from Hobbes's world of omnipresent potential for violence to the actual movement of troops and exchanges of diplomatic demarches. The Soviet concept of crisis management during the Cold War years stressed that a "crisis" was an objective situation, corresponding to a period of threat marked by actual preparations for war. As Stephen Shenfield explained:

> Soviet theory legitimizes the deliberate taking of some acceptably low risk of war in the day-to-day conduct of foreign policy. But once "crisis"--the very antechamber of war--has been reached, avoiding war (so long as this is still thought possible) takes overriding priority.[17]

The first requirement of successful crisis management is communications transparency. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send its estimate of the situation to the other. It is not necessary for the two sides to have identical or even initially complementary interests. But a sufficient number of correctly sent and received signals are prerequisite to effective transfer of enemy goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Communications transparency also includes high fidelity communication between adversaries, and within the respective decisionmaking structures of each side. High fidelity communication in a crisis can be distorted by everything that might interfere physically, mechanically, or behaviorally with accurate transmission. Electromagnetic pulses that disrupt communication circuitry or physical destruction of communication networks are obvious examples of impediments to high fidelity communication. Cultural differences that prevent accurate understanding of shared meanings between states can confound deterrence as practiced according to one side's theory. As Keith B. Payne notes, with regard to the potential for deterrence failure in the post-Cold War period:

> Unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them--their individual values, goals, determination, and commitments--in the context of the engagement, and therefore we are surprised when their "unreasonable" behavior differs from our expectations.[18]

A second requirement of successful crisis management is the reduction of time pressure on policymakers and commanders so that no unintended, provocative steps are taken toward escalation mainly or solely as a result of a misperception that "time is up." Policymakers and military planners are capable of inventing fictive worlds of perception and evaluation in which "H hour" becomes more than a useful benchmark for decision closure. In decision pathologies possible under crisis conditions, deadlines may be confused with policy objectives themselves: ends become means, and means, ends. For example: the war plans of the great powers in July 1914 contributed to a shared self-fulfilling prophecy among leaders in Berlin, St. Petersburg, and Vienna that only by prompt mobilization and attack could decisive losses be avoided in war. Plans predicated on the inflexibility of mobilization timetables proved insufficiently flexible for policymakers who wanted to slow down the momentum of late July and early August toward

an irrevocable decision in favor of war.

One result of the compression of decision time in a crisis, compared to typical peacetime patterns, is that the likelihood of Type I (undetected attack) and Type II (falsely detected attack) errors increases. Tactical warning and intelligence networks grow accustomed to the routine behavior of other state forces and may misinterpret nonroutine behavior. Unexpected surges in alert levels or uncharacteristic deployment patterns could trigger misreadings of indicators by tactical operators. As Bruce G. Blair has argued:

> In fact, one distinguishing feature of a crisis is its murkiness. By definition, the Type I and Type II error rates of the intelligence and warning systems rapidly degrade. A crisis not only ushers in the proverbial fog of crisis symptomatic of error-prone strategic warning but also ushers in a fog of battle arising from an analogous deterioration of tactical warning.[19]

A third attribute of successful crisis management is that each side should be able to offer the other a safety valve or a face-saving exit from a predicament that has escalated beyond its original expectations. The search for options should back neither crisis participant into a corner from which there is no graceful retreat. For example, during the Cuban missile crisis of 1962, President Kennedy was able to offer Soviet Premier Khrushchev a face-saving exit from his overextended missile deployments. Kennedy publicly committed the United States to refrain from future military aggression against Cuba and privately agreed to remove and dismantle Jupiter medium-range ballistic missiles previously deployed among US NATO allies.[20] Kennedy and his inner circle recognized, after some days of deliberation and clearer focus on the Soviet view of events, that the United States would lose, not gain, by a public humiliation of Khrushchev that might, in turn, diminish Khrushchev's interest in any mutually agreed solution to the crisis.

A fourth attribute of successful crisis management is that each side maintains an accurate perception of the other side's intentions and military capabilities. This becomes difficult during a crisis because, in the heat of a partly competitive relationship and a threat-intensive environment, intentions and capabilities can change. A decade ago Robert Jervis opined that Cold War beliefs in the inevitability of war might have created a self-fulfilling prophecy:

> The superpowers' beliefs about whether or not war between them is inevitable create reality as much as they reflect it. Because preemption could be the only rational reason to launch an all-out war, beliefs about what the other side is about to do are of major importance and depend in large part on an estimate of the other's beliefs about what the first side will do.[21]

Intentions can change during a crisis if policymakers become more optimistic about gains or more pessimistic about potential losses during the crisis. Capabilities can change due to the management of military alerts and the deployment or other movement of military forces. Heightened states of military readiness on each side are intended to send a two-sided signal: of readiness for the worst if the other side attacks, and of a nonthreatening steadiness of purpose in the face of enemy passivity. This mixed message is hard to send under the best of crisis management conditions, since each state's behaviors and communications, as observed by its opponent, may not seem consistent. Under the stress of time pressures and of military threats, different parts of complex security organizations may be making decisions from the perspective of their narrowly defined, bureaucratic interests. These bureaucratically chosen decisions and actions may not coincide with the policymakers' intent, nor with the decisions and actions of other parts of the government. As Alexander L. George has explained:

> It is important to recognize that the ability of top-level political authorities to maintain control over the moves and actions of military forces is made difficult because of the exceedingly large number of often complex standing orders that come into effect at the onset of a crisis and as it intensifies. It is not easy for top-level political authorities to have full and timely knowledge of the multitude of existing standing orders. As a result, they may fail to coordinate some critically important standing orders with their overall crisis management strategy.[22]

As policymakers may be challenged to control numerous and diverse standard operating procedures, political leaders may also be insufficiently sensitive to the costs of sudden changes in standing orders or unaware of the rationale underlying those orders. For example, heads of state or government may not be aware that more permissive rules of

engagement for military forces operating in harm's way come into play once higher levels of alert have been authorized.[23]

Information War and Crisis Management: The Risks

Information warfare has the potential to attack or to disrupt successful crisis management on each of the preceding attributes. First, information warfare can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[24] The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber-victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop.

Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way infowar can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions: only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was. For example, during the Cold War, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew to launch in the absence of contrary instructions.

Second, information warfare during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived time lines within which the policymaking process can make its decisions. Once either side sees parts of its command, control, and communications system being subverted by phony information or extraneous cyber-noise, its sense of panic at the possible loss of military options will be enormous. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the SIOP (the strategic nuclear war plan). The SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.

A third potentially disruptive effect of infowar on nuclear crisis management is that infowar may reduce the search for available alternatives to the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem-solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives:

> A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.[25]

The propensity to search for the first available alternative that meets minimum satisfactory conditions of goal attainment is strong enough under normal conditions in nonmilitary bureaucratic organizations.[26] In civil-military command and control systems under the stress of nuclear crisis decisionmaking, the first available alternative may

quite literally be the last. Or, so policymakers and their military advisors may persuade themselves. Accordingly, the bias toward prompt and adequate solutions is strong. During the Cuban missile crisis, for example, a number of members of the presidential advisory group continued to propound an air strike and invasion of Cuba during the entire 13 days of crisis deliberation. Had less time been available for debate and had President Kennedy not deliberately structured the discussion in a way that forced alternatives to the surface, the air strike and invasion might well have been the chosen alternative.[27]

Fourth and finally on the issue of crisis management, infowar can cause flawed images of each side's intentions and capabilities to be conveyed to the other, with potentially disastrous results. Another example from the Cuban missile crisis demonstrates the possible side effects of simple misunderstanding and noncommunication on US crisis management. At the most tense period of the crisis, a U-2 reconnaissance aircraft got off course and strayed into Soviet airspace. US and Soviet fighters scrambled, and a possible Arctic confrontation of air forces loomed. Khrushchev later told Kennedy that Soviet air defenses might have interpreted the U-2 flight as a prestrike reconnaissance mission or as a bomber, calling for a compensatory response by Moscow.[28] Fortunately Moscow chose to give the United States the benefit of the doubt in this instance and to permit US fighters to escort the wayward U-2 back to Alaska. Why this scheduled U-2 mission was not scrubbed once the crisis began has never been fully revealed; the answer may be as simple as bureaucratic inertia compounded by noncommunication down the chain of command by policymakers who failed to appreciate the risk of "normal" reconnaissance under these extraordinary conditions.

Caveat: Two Hardy Perennials

Neither the next Army nor the Army After Next can be imagined in the absence of offensive and defensive information operations. Nor can a truly post-nuclear world be expected even well into the next century; the trend is not in favor of denuclearization, and some states presently seeking to acquire nuclear weapons are among the most visible rogues in the international system. So if interest in infowar can only grow, and interest in nuclear deterrence will be forced on policymakers and planners by the exigent circumstances, why worry about a possibly malign mating of the two? Could both nuclear deterrence and infowar not proceed smoothly on separate tracks, with a stable balance of terror in one dimension and a competitive international environment for conventional, high-technology warfare, including information warfare, in another? This possibility of a benign future in which the evolutionary trees of nukes and *infomacht* never cross cannot be ruled out among future scenarios.

But the assumption of separate evolution may be wrong. If, instead, the paths of the ultimate weapons of mass destruction--nuclear weapons--and of the supreme weapons of soft power--information warfare--should ever cross, the product of the two may be an entirely unforeseen and unwelcome hybrid. Crises by definition are exceptional events. No interstate crisis may ever take place between states armed both with perfervid infowarriors and with nuclear weapons. But given the durability of the two trends, interest in infowar and in nuclear weapons, it would be prudent to consider the possibility of a crisis-born genetic accident.

All crises are characterized to some extent by a high degree of threat, short time for decision, and a "fog of crisis" reminiscent of Clausewitz's "fog of war" that confuses crisis participants about what is happening. Before the discipline of crisis management was ever invented by modern scholarship, historians had captured the rush-to-judgment character of much crisis decisionmaking among great powers.[29] The influence of nuclear weapons on crisis decisionmaking is therefore not so dramatic as has been sometimes supposed. The presence of nuclear forces obviously influences the degree of destruction that can be done should crisis management fail. Short of that catastrophe, the greater interest of scholars is in how the presence of nuclear weapons might affect the decisionmaking process itself in a crisis. The problem is conceptually elusive: there are so many potentially important causal factors relevant to a decision with regard to war or peace.

The firebreak between crises under the shadow of potential nuclear destruction and those not so overshadowed remains important. Infowar can be unleashed like a pit bull against the command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structures of a potential opponent in conventional conflicts with fewer risks compared to the case of a nuclear-armed foe. The objective of infowar in conventional warfare is to deny enemy forces battlespace awareness and to obtain dominant awareness for oneself, as the United States largely was able to do in the Gulf War of 1991.[30] In a crisis with nuclear weapons available to the side against which infowar is

used, crippling the foe's intelligence and command and control systems is at best a necessary, and certainly far from a sufficient, condition for successful crisis management or deterrence. And under some conditions of nuclear crisis management, crippling the C4ISR of the foe may be simply unwise. What do we think the Russians will do when their bunkers go bonkers? The answer lies only partly in hardware: the mind-sets of people, their training, and their military-strategic culture must also be factored in.[31]

Conclusion

The possible combination of information warfare with continuing nuclear deterrence after the Cold War could have unintended by-products, and these may be dangerous for stability. Optimistic expectations about the use of information warfare to defeat or disrupt opponents on the conventional, high-technology battlefield--in cases where nuclear complications do not figure--may be justified. On the other hand, where the nuclear specter overhangs the decisionmaking process between or among states in conflict, the infowarriors' efforts to obtain dominant battlespace knowledge may provoke the opponent instead of deterring it.

One cannot overstate the case that nuclear weapons even after the Cold War remain different in kind, not just in degree, from other forces. Thus interactions between nuclear forces and templates for superiority in battle must always be carefully controlled, and especially so in time of crisis.

NOTES

I am grateful to John Arquilla, Peter Feaver, and Timothy Thomas for suggesting pertinent sources and sharing their work and ideas. They bear no responsibility for arguments here.

1. Information has, of course, always been an important part of war and crisis management. But as Steven Metz and James Kievit have explained, the informational aspect of RMA may "alter the traditional relationship between operational complexity and effective control" as new means of acquiring, analyzing, and distributing information allow for added complexity in military action without sacrificing control or timing. See Metz and Kievit, *Strategy and the Revolution in Military Affairs: From Theory to Policy* (Carlisle Barracks, Pa.: USAWC, 27 June 1995), p. 4 and passim.

2. Alvin Toffler and Heidi Toffler, *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner Books, 1993), passim.

3. For an introduction to this topic, see John Arquilla and David Ronfeldt, "A New Epoch--and Spectrum--of Conflict," in *In Athena's Camp: Preparing for Conflict in the Information Age*, ed. Arquilla and Ronfeldt (Santa Monica, Calif.: RAND, 1997), pp. 1-22. See also, on definitions and concepts of information warfare: Martin Libicki, *What Is Information Warfare*? (Washington: National Defense Univ., ACIS Paper 3, August 1995); Libicki, *Defending Cyberspace and other Metaphors* (Washington: National Defense Univ., Directorate of Advanced Concepts, Technologies, and Information Strategies, February 1997); Toffler and Toffler, pp. 163-207; Arquilla and Ronfeldt, *Cyberwar Is Coming*! (Santa Monica, Calif.: RAND, 1992); David S. Alberts, *The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative* (Washington: National Defense Univ., Institute for National Strategic Studies, Center for Advanced Concepts and Technology, April 1996); and Gordon R. Sullivan and Anthony M. Coroalles, *Seeing the Elephant: Leading America's Army into the Twenty-First Century* (Cambridge, Mass.: Institute for Foreign Policy Analysis, 1995). A roadmap to information resources related to strategy and other military topics appears in James Kievit and Steven Metz, *The Strategist and the Web Revisited: An Updated Guide to Internet Resources* (Carlisle Barracks, Pa.: USAWC, Strategic Studies Institute, Army After Next Project, 17 October 1996).

4. Arquilla and Ronfeldt, "A New Epoch--and Spectrum--of Conflict," p. 6.

5. Arquilla and Ronfeldt, "The Advent of Netwar," in *In Athena's Camp*, pp. 275-94.

6. Ibid., passim.

7. See Alexander L. George, "A Provisional Theory of Crisis Management," in *Avoiding War: Problems of Crisis Management*, ed. Alexander L. George (Boulder, Colo.: Westview Press, 1991), pp. 22-27, for the political and operational requirements of crisis management; and George, "Strategies for Crisis Management," ibid., pp. 377-94, for descriptions of offensive and defensive crisis management strategies.

8. The White House, *Joint Statement on Parameters on Future Reductions in Nuclear Forces*, Office of the Press Secretary, Helsinki, Finland, 21 March 1997.

9. Jack Mendelsohn, "START II and Beyond," *Arms Control Today*, 26 (October 1996), 3-9.

10. Separate studies on these aspects of Russia's nuclear dependency are under way by the author.

11. V. I. Tsymbal, "Kontseptsiya `Informatsionnoy voiny'" (Concept of Information Warfare), speech given at the Russian-US conference on "Evolving Post-Cold War National Security Issues," Moscow, 12-14 September 1995, p. 7, cited in Timothy L. Thomas, "Deterring Information Warfare: A New Strategic Challenge," *Parameters*, 26 (Winter 1996-1997), 82.

12. Christopher Andrew, *For the President's Eyes Only: Secret Intelligence and the American Presidency from Washington to Bush* (New York: Harper Collins, 1995), p. 516.

13. William C. Martel and William T. Pendley, *Nuclear Coexistence: Rethinking U.S. Policy to Promote Stability in an Era of Proliferation* (Montgomery, Ala.: Air War College, April 1994), pp. 3-5, 10-11, and passim.

14. General Aleksandr Lebed, former national security advisor to Russian President Boris Yeltsin, claimed in a US network television "60 Minutes" interview on 6 September 1997 that many portable "suitcase" nuclear weapons (atomic demolition munitions, or ADMs) created during the Cold War for use with Soviet special operations forces could not be accounted for by the Russian military now. The program raised the possibility that missing weapons could have been sold to terrorists or states like Iraq with nuclear ambitions. Russian defense officials denied that any nuclear weapons were unaccounted for.

15. For pertinent concepts, see: Ole R. Holsti, "Crisis Decision Making," in *Behavior, Society and Nuclear War*, ed. Philip E. Tetlock, et al. (New York: Oxford Univ. Press, l989), I, 8-84; and Phil Williams, *Crisis Management* (New York: John Wiley and Sons, l976). See also Alexander L. George, "Coercive Diplomacy: Definition and Characteristics," in *The Limits of Coercive Diplomacy*, ed. Alexander L. George and William E. Simons (2d ed.; Boulder, Colo.: Westview Press, 1994), esp. pp. 8-9, and in the same volume, Alexander L. George, "The Cuban Missile Crisis: Peaceful Resolution Through Coercive Diplomacy," pp. 111-32.

16. See Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, Calif.: Sage Publications, 1983); and Richard Ned Lebow and Janice Gross Stein, *We All Lost the Cold War* (Princeton, N.J.: Princeton Univ. Press, 1994), pp. 351-55.

17. Stephen Shenfield, "Crisis Management: the Soviet Approach," in *Strategic Power: USA/USSR*, ed. Carl Jacobsen (New York: Macmillan, 1990), pp. 198-205, citation p. 200.

18. Keith B. Payne, *Deterrence in the Second Nuclear Age* (Lexington: Univ. Press of Kentucky, 1996), p. 57. See also David Jablonsky, *Strategic Rationality Is Not Enough: Hitler and the Concept of Crazy States* (Carlisle Barracks, Pa.: USAWC, Strategic Studies Institute, 8 August 1991), esp. pp. 5-8 and pp. 31-37.

19. Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington: Brookings Institution, 1993), p. 237.

20. Lebow and Stein, pp. 122-23.

21. Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca, N.Y.: Cornell Univ. Press, 1989), p. 183.

22. Alexander L. George, "The Tension Between "Military Logic" and Requirements of Diplomacy in Crisis Management," in *Avoiding War: Problems of Crisis Management*, pp. 13-21, citation p. 18.

23. Ibid.

24. A virus is a self-replicating program intended to destroy or alter the contents of other files stored on floppy disks or hard drives. Worms corrupt the integrity of software and information systems from the "inside out" in ways that create weaknesses exploitable by an enemy.

25. Blair, p. 252.

26. James G. March and Herbert A. Simon, *Organizations* (New York: John Wiley and Sons, 1958), pp. 140, 146.

27. Lebow and Stein, pp. 335-36.

28. Graham T. Allison, *Essence of Decision: Explaining the Cuban Missile Crisis* (Boston: Little, Brown, 1971), p. 141. See also Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton, N.J.: Princeton Univ. Press, 1989), p. 147; and Lebow and Stein, p. 342.

29. For example, see Richard Ned Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins Univ. Press, 1981); Michael Howard, *Studies in War and Peace* (New York: Viking Press, 1971), pp. 99-109; Gerhard Ritter, *The Schlieffen Plan: Critique of a Myth* (London: Oswald Wolff, 1958); and D. C. B. Lieven, *Russia and the Origins of the First World War* (New York: St. Martin's Press, 1983).

30. As David Alberts notes, "Information dominance would be of only academic interest, if we could not turn this information dominance into battlefield dominance." See Alberts, "The Future of Command and Control with DBK," in *Dominant Battlespace Knowledge*, ed. Stuart E. Johnson and Martin C. Libicki (Washington: National Defense Univ., 1996), pp. 77-102, citation p. 80.

31. As Colin S. Gray has noted, "Because deterrence flows from a relationship, it cannot reside in unilateral capabilities, behavior or intentions. Anyone who refers to *the* deterrent policy plainly does not understand the subject." Gray, *Explorations in Strategy* (Westport, Conn.: Greenwood Press, 1996), p. 33.

Dr. Stephen J. Cimbala is a professor of political science at Penn State University (Delaware County), and has contributed to the literature of defense and security studies for more than two decades. He received the Ph.D. from the University of Wisconsin, Madison. His recent books include *Coercive Military Strategy* (Texas A&M University Press, 1998).

Reviewed 25 May 1999. Please send comments or corrections to carl_Parameters@conus.army.mil