Security Studies
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/fsst20

The political effects of information warfare: Why new military capabilities cause old political dangers

Bradley A. Thayer [a]
[a] Assistant professor of political science , University of Minnesota , Duluth
Published online: 24 Dec 2007.

To cite this article: Bradley A. Thayer (2000) The political effects of information warfare: Why new military capabilities cause old political dangers, Security Studies, 10:1, 43-85, DOI: 10.1080/09636410008429420

To link to this article: http://dx.doi.org/10.1080/09636410008429420

THE POLITICAL EFFECTS OF INFORMATION WARFARE

WHY NEW MILITARY CAPABILITIES CAUSE OLD POLITICAL DANGERS

BRADLEY A. THAYER

THE OVERWHELMING success of the U.S. military and its coalition partners in the Gulf War has stimulated discussion about information warfare among many military officers, policymakers, and academics.[1] Most envision

Bradley A. Thayer is assistant professor of political science at the University of Minnesota, Duluth.

Thanks to Karen Ballentine, Michael Desch, Christopher Layne, Sean M. Lynn-Jones, Sean Lopez, Thomas Mahnken, Steven Miller, Robert Pape, Brian Taylor, Paul Zimmerman, the *Security Studies* anonymous reviewers, and especially Owen R. Coté Jr., for their helpful comments. I thank Maureen McAleer for research assistance. I am grateful to Antony Sullivan and the Earhart Foundation for their encouragement and generous support of my research.

1. For discussions of information warfare see A. J. Bacevich, "Preserving the Well-Bred Horse," *The National Interest*, no. 37 (fall 1994): 43–49; Stephen Biddle, "Victory Misunderstood: What the Gulf War Tells Us about the Future of Conflict," *International Security* 21, no. 2 (fall 1996): 139–79; Biddle, "Assessing Theories of Future Warfare," *Security Studies* 8, no. 1 (autumn 1998): 1–74; Paul Bracken and Raoul Henri Alcalá, *Whither the RMA: Two Perspectives on Tomorrow's Army* (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1994); Eliot A. Cohen, "A Revolution in Warfare," *Foreign Affairs* 75, no. 2 (March/April 1996): 37–54; Paul Dibb, "The Revolution in Military Affairs and Asian Security," *Survival* 39, no. 4 (winter 1997/98): 93–116; Peter D. Feaver, "Blowback: Information Warfare and the Dynamics of Coercion," *Security Studies* 7, no. 4 (summer 1998): 88–120; Lawrence Freedman, *The Revolution in Strategic Affairs*, Adelphi Paper 318 (London: International Institute for Strategic Studies [IISS], 1998); Dan Gouré, "Is There a Military-Technical Revolution in America's Future?" *Washington Quarterly* 16, no. 4 (autumn 1993): 175–92; Richard J. Harknett, "Information Warfare and Deterrence," *Parameters* 26, no. 3 (autumn 1996): 93–107; Harknett et al., "The Risks of a Networked Military," *Orbis* 44, no. 1 (winter 2000): 127–43; Andrew F. Krepinevich Jr., "Keeping Pace with the Military-Technical Revolution," *Issues in Science and Technology* 10, no. 4 (summer 1994): 43–49; Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest*, no. 37 (fall 1994): 30–42; Martin C. Libicki, *What Is Information Warfare?* (Washington, D.C.: National Defense University Press, 1995); "Symposium on the Gulf War and the Revolution in Military Affairs," *International Security* 22, no. 2 (fall 1997): 137–74; Michael O'Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: Brookings Institution Press, 2000); John Orme, "The Utility of Force in a World of
Scarcity," *International Security* 22, no. 3 (winter 1997/98): 138–67; Thomas G. Mahnken, "War in the Information Age," *Joint Force Quarterly*, no. 10 (winter 1995/96): 39–43; Joseph S. Nye Jr.,

SECURITY STUDIES 10, no. 1 (autumn 2000): 43–85
Published by Frank Cass, London

profound changes in the conduct of war. According to one military analyst, "In any conventional conflict in which the United States or any of the major Western powers is pitted against a Third World adversary, the outcome is preordained."[2] As a result of information warfare, we have now "returned to the military equation of the nineteenth century, when colonial wars pitted small numbers of disciplined, well-trained Western troops with rifles against hordes of tribal warriors armed only with shields and spears."[3] General Ronald Fogleman argued that "in the first quarter of the 21st century it will become possible to find, fix or track, and target anything that moves on the surface of the Earth."[4] Admiral William Owens argues that new technologies, some of which were used in the Gulf War, permit the gathering, processing, and fusion of information over a large geographic area in real time, all the time, and permit the transfer of that information to U.S. forces with accuracy and speed. The result will be "the *system of systems*, namely interactions that will give us dominant battlespace knowledge and the ability to take full military advantage of it."[5]

Policymakers are similarly impressed. Former secretary of defense William Perry, writing in 1991, shares the opinion that information warfare will completely outclass the opponents of the United States. As a result of "a revolutionary advance in military capability," the U.S. military possesses "an overwhelming advantage over an army without it, much as an army equipped with tanks would overwhelm an army with horse cavalry."[6] Just after the Gulf War, Secretary of Defense Richard Cheney argued that the war "demonstrated dramatically the new possibilities of what has been called the 'military-technological revolution in warfare'."[7]

Academics are no less persuaded. David Jablonsky describes the importance of the benefits that increased information provides commanders: "With time compressed over extended space and with that immense space rendered comprehensible by a technological coup d'oeil, an entire theater can become a simultaneous battlefield where events, as in the days of Napoleon, may determine

---

and William A Owens, "America's Information Edge," *Foreign Affairs* 75, no. 2 (March/April 1996): 20–46; and William A. Owens, "The Emerging System of Systems," *U.S. Naval Institute Proceedings* 121, no. 5 (May 1995): 35–39.

2. Wayne K. Maynard, "Spears vs. Rifles: The New Equation of Military Power," *Parameters* 70, no. 4 (spring 1993): 49. Also see Michael J. Mazarr et al., *Military Technical Revolution: A Structural Framework* (Washington, D.C.: Center for Strategic and International Studies, 1993).

3. Maynard, "Spears vs. Rifles," 49.

4. Gen. Ronald R. Fogleman, U.S. Air Force Chief of Staff, "Strategic Vision and Core Competencies," presented at Air Force Association National Symposium, Los Angeles, 18 October 1996, 2.

5. William A. Owens, "The American Revolution in Military Affairs," *Joint Force Quarterly*, no. 10 (winter 1995/96): 37 (emphasis in original).

6. William J. Perry, "Desert Storm and Deterrence," *Foreign Affairs* 70, no. 4 (fall 1991): 66.

7. U.S. Department of Defense, *Conduct of the Persian Gulf War*, Final Report to Congress (Washington, D.C.: U.S. Government Printing Office, 1992), 164.

national destinies."[8] James Blackwell, Michael Mazarr, and Don Snider argue, "Although the revolution in warfare is still underway, its outlines have become clear. The effects of technology—in precision guided weapons, in stealthy delivery systems, in advanced sensor and targeting systems, in battle management platforms—are transforming and in fact already have demonstrably transformed the way in which armed forces conduct their operations."[9]

Despite these accolades, the intention in this article is to determine whether information warfare will have as profound an effect on international politics as many military officers, policymakers, and academics believe. It is argued here that current technological changes and transformations in the acquisition and dissemination of information, known as "information warfare," do mark a significant technological advance in warfare but do not constitute a Revolution in Military Affairs (RMA) because they do not supplant the nuclear revolution.[10]

To accomplish this, information warfare (IW) is first defined, and its origins and the military and political capabilities with which it will provide the United States are discussed. Next, RMA is defined. Third, to determine the effects of information warfare, conflict at three different levels is examined: between the United States and a nuclear armed peer competitor, the United States and a small state, and the United States and an emerging, or threshold, nuclear state. Finally, the article concludes by discussing two unintended consequences of information warfare: first, U.S. information warfare capabilities may increase the perception of the United States as a threat, thus promoting balancing against the United States; and second, it may hinder close and effective military cooperation with U.S. allies, such as that which occurred between the United States and British forces in the Gulf War, because they will lack the ability to fight with U.S. forces.

This argument is important for two reasons. First, having explained what information warfare is one can demonstrate why it will not change the paradigm of warfare but will have important effects on the use of force in international politics.[11] Second, the impact of IW in each of these conflicts is explored. This

8. David Jablonsky, *The Owl of Minerva Flies At Twilight* (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1994), 65.

9. James Blackwell, Michael J. Mazarr, and Don M. Snider, *The Gulf War: Military Lessons Learned* (Washington, D.C.: Center for Strategic and International Studies, 1991), 21.

10. As argued below, a revolution in military affairs is only a revolution if it affects the fundamental relationship in military affairs: the relationship of politics to war. An RMA obviates old concepts about the relationship of politics to war and requires new ones to explain the new synthesis.

11. Indeed, a strong argument may be made that information warfare already has had an important effect on international politics by contributing to the end of the cold war. As discussed below, increased Soviet fear of U.S. capabilities and the concern over the Soviet Union's ability to compete with the United States in the information age served as the impetus for serious economic and political reform, which started under Yuri Andropov and continued with Mikhail Gorbachev, and thus contributed to the end of the cold war. While this issue deserves more research, an excellent study is Manuel Castells and Emma Kiselyova, *The Collapse of Soviet Communism: A View from the Information Society* (Berkeley: International and Area Studies, University of California at Berkeley, 1995).

analysis is not intended to be a comprehensive study. It is rather to frame the study of the effects of IW by detailing some of the major implications of IW in the types of conflicts that the United States almost certainly will face in the future. In general, the three levels of conflict allow for a more nuanced analysis of the political effects of information warfare, and thus provide a better framework for discerning the political effects of information warfare in a world where the United States, at least in the next ten–fifteen years, is the sole possessor of the increased fighting capability provided by information warfare. While here the political effects of information warfare are examined through the three levels of conflict, this article does not claim this to be the only way to analyze the effect of information warfare; employing the offense-defense balance is another.[12]

The argument is put forth that in the first case information warfare will strengthen the conventional attacker, but will not change the fundamental facts of the nuclear revolution. Despite its benefits, information warfare does not change the logic of war in the nuclear era. War between great powers armed with nuclear weapons will continue to be suicidal. Limited wars between such states should be equally unlikely because of the risk of escalation. Information warfare cannot remove either state from the mutual hostage relationship that defines competition between nuclear-armed great powers.

In the second case, information warfare capabilities will increase the ability of the United States to coerce and deter small states, and to intervene in the Third World because it makes such wars and interventions less costly. Information warfare, however, is not a panacea. A significant danger in these conflicts is that the United States will underestimate its opponent and its willingness to pay the costs of war. The U.S. experiences in Vietnam and Somalia show that when the United States fights an enemy more willing to pay a high cost to prosecute the war, it creates the potential for a U.S. defeat.

The impact of information warfare in the third case is more ambiguous. Information warfare increases the capability of the United States to destroy the nuclear forces and command and control systems of small and emerging nuclear states, but does not and cannot eliminate the dangers to the United States and its allies inherent in attacking such a state.

12. In terms of the offense-defense theory, the effect of information warfare is that it will favor the offense as long as three conditions prevail: first, that one state is the sole possessor of the capability; second, that it is able to maintain a technological advantage over competitors; and third, that countermeasures are either not possible or not effective. Under these conditions information warfare will make it easier to take territory rather than to hold it because it permits rapid and seamless target identification and destruction, providing its possessors with a first-strike advantage. On the offense-defense balance see Sean M. Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4, no. 4 (summer 1995): 660–91; Charles L. Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (spring 1998): 44–82; and Stephen Van Evera, "Offense, Defense, and the Causes of War" *International Security* 22, no. 4 (spring 1998): 5–43.

All three cases must be examined in order to ascertain what advantages information warfare provides the United States with. Additionally, this analysis illuminates the risks of information warfare. While the benefits of information warfare are widely discussed, the risks have received almost no attention. This article illuminates two major dangers inherent in information warfare. First, U.S. decisionmakers may so overestimate the military capabilities provided by information warfare that they are seduced into believing that coercion of great nuclear power is possible, that intervention in the Third World will be bloodless, or that it is now safe to attack a threshold nuclear state because the risk of retaliation is acceptable. By increasing U.S. ability to use military force, IW may cause politicians to overlook the question of whether it would be wise to use force. Political leaders must recall Clausewitz's argument that war is conducted for political ends.[13] Despite even significant advances in technology, war is politics. Second, the United States will pose a greater threat to the security of both small and great powers, who will strive to match or counter its capability.

Finally, since this is an article on the political effects of information warfare only minimal analysis is provided of the battlefield effects of information warfare, and its major effects on policy issues such as the need to reformulate U.S. military doctrine, the roles and missions of the military services, or current U.S. defense budget priorities is not studied. These important issues deserve to be addressed by scholars but are beyond the scope of this article.

WHAT IS INFORMATION WARFARE?

SINCE THE time of Alexander, information has been a key factor in warfare. Soldiers have always sought to know what is "on the other side of the hill," where the enemy is and how much threat he poses, as well as the status and deployment of their own forces. What is new is the technology to acquire this information over large areas, in real time, and to process and disseminate it to the forces in the field rapidly and accurately.[14] Information warfare is a new capability, an innovation in warfare comprised of three factors: to know, to deny knowledge, and to manipulate information.[15]

13. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1976), 87.

14. Presently the U.S. military is the leader in developing this ability, although other states, notably China, France, Great Britain, Israel, Japan, and Russia are also developing some if not all capabilities described here. Despite the development of information warfare, we may expect that not all war in the information age is or will be information warfare. War between and among states, and civil wars, will still be fought by states or groups who lack these capabilities.

15. For discussion of the causes and consequences of military innovation see Owen R. Coté Jr., "The Politics of Innovative Military Doctrine: The U.S. Navy and Fleet Ballistic Missiles" (Ph.D. diss., MIT, 1996); Barry R. Posen, *The Sources of Military Doctrine: France, Britain, and Germany between the World*

TO KNOW

The first is knowledge of where U.S. and allied forces are and their status, where enemy forces are and their status, and where noncombatants are, in real time. This is an important aspect of information warfare that its proponents have not recognized. It is important to emphasize that knowledge is not information, and that more information does not necessarily equal more knowledge. Knowledge requires the relevant decisionmaker to be cognizant of the information at hand.[16] A necessary condition is that the information system be able to acquire information and disseminate it reliably in wartime conditions to those who must act upon it. This is done using intelligence collection, surveillance, and reconnaissance (ISR) technologies such as satellites, spy planes like the TR-1, JSTARS (Joint Surveillance and Target Attack Radar System), AWACS (Airborne Warning and Control System), and increasingly unmanned aerial vehicles (UAVs), such as Global Hawk and Predator, that yield information over large areas in all weather conditions.

To be sufficient, however, the decisionmaker must be cognizant of the data so he can act upon it. It is not enough to have information available to him. Therefore, another essential element is a command and control system or infrastructure that can process these large amounts of information and that has a metric to discern quickly what is and is not important for the user's needs and mission. Delivering that information to the relevant decisionmaker is just as important as acquiring the information. IW also demands tight coupling between several systems: intelligence; sensors; command and control; mapping, charting and geodesy (MCG); and weapons.[17]

TO DENY KNOWLEDGE

The second component is knowledge denial—knowledge of U.S. forces is denied to the enemy. In order for information warfare to benefit the United States,

Wars (Ithaca: Cornell University Press, 1984); and Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military* (Ithaca: Cornell University Press, 1991).

16. Knowledge does not require that information be true, however. In addition, as some military officers note, more information is not necessarily a good thing but may hinder warfighting capabilities: "More information from more sources, made available more quickly than ever before, equals system overload...we may kill ourselves with silicon unless we learn to get the right information to the right person at the right time in the right place" (General Donn Starry, "Book Review of LTG Frederic J. Brown, 'The U.S. Army in Transition II: Landpower in the Information Age'," *Parameters* 23, no. 3 [autumn 1993]: 117). As William Odom notes, enhanced communication is "an advantage that can just as easily introduce confusion and become a liability" (William E. Odom, *America's Military Revolution: Strategy and Structure After the Cold War* [Washington, D.C.: American University Press, 1993], 48).

17. Command and control is a commander's exercise of authority and direction over his forces to accomplish his mission. Command and control is accomplished by arranging personnel, equipment, facilities, and procedures to execute the mission. It is sometimes called C4I—Command, Control, Communications, Computing and Intelligence, and even C4I/BM (Battle Management), but command and control is used here as this term subsumes the other functions.

knowledge and information about U.S. forces must be protected to minimize the benefit to the enemy.[18] Otherwise, if both the United States and its enemy could use information to an equal extent, or the enemy could take countermeasures to neutralize information warfare, the United States would lose its advantage.[19] The existence and maintenance of an asymmetric information warfare capability is essential. To this end, it is critical to protect the U.S. command-and-control network, and particularly its information processing capability, from destruction or penetration by the enemy in the era of information warfare. The information system is becoming a strategic center of gravity and must be defended as such. Just as the United States worries about its strategic nuclear forces, so too must it protect the integrity of its information system. At present, whether U.S. forces can defend it adequately against either a sophisticated cyber attack or a physical one is questionable.[20]

TO MANIPULATE INFORMATION

Third, the technologies that make it possible "to know" also make possible the manipulation of information and information technology to attack, confuse, and mislead the enemy. The essence of these attacks is to disable enemy weapons systems, such as air defense capabilities, and to prevent or distort communication among elites, or from the political elites to the populace. Such actions are called offensive information operations. As discussed in greater detail below, for example, offensive information operations include attacking enemy computers by introducing viruses into the important computer systems that control communications or air defenses, or inserting false information into a message stream to deceive the enemy. The ability to listen to enemy communications and occasionally introduce false information is "the heart of information operations," according to John Entzminger, deputy for technology with the Defense Airborne

18. Knowledge about military forces and decisionmaking obviously must be protected, but it is also important to protect the economies of modern industrialized states which rely heavily on computer processing and are vulnerable to computer hackers or to physical destruction.

19. An exploration of the measures-countermeasures dynamic in the detail that the subject warrants is beyond the scope of this analysis although this dynamic will be touched upon at times below. Research on this issue will prove to be useful in the future as U.S. capabilities continue to develop and other states attempt to adopt countermeasures.

20. Reportedly the Pentagon experiences about sixty hacker incidents each day and about the same number of intrusions each week. However, Art Money, the Defense Department's chief information officer has stated that no classified network has ever been penetrated successfully. "One on One, Maj. Gen. John Campbell, Commander, Pentagon Computer Network Defense Task Force," *Defense News*, 29 March 1999, 30. Also see Louise Kehoe, "U.S. Squares Up to Cyberterrorists," *Financial Times*, 11 June 1996, 12. In addition, physical systems are vulnerable, especially satellites. Sean Naylor, "U.S. Army War Game Reveals Satellite Vulnerability," *Defense News*, 10–16 March 1997, 50.

Reconnaissance Office.[21] So for the first time in warfare the information systems of the enemy are subject to cyber attack by U.S. information systems. As a result, the enemy will not know or will possess significant doubts about what information is accurate; and second, critical weapons systems or information systems will fail or operate so irregularly that they become unreliable.

As a consequence of these three factors, superiority in information warfare will permit commanders at every level of command to know what is happening "on the other side of the hill," where the enemy is and what he is doing all the time, whether in a jungle or a city, in the Arctic or a desert. This knowledge will enable the military to attack the enemy's center of gravity: the key nodes of its leadership, military forces, or society.[22] Before addressing the effects of information warfare, its causes are discussed: it results from a synthesis of technological developments and the intent of U.S. defense officials. As the Soviets foresaw, advances in weaponry and information processing made the battlefield more lethal and permitted more rapid destruction of the enemy. Intent, however, was equally important: U.S. defense officials like Perry sought to use technology to offset Soviet conventional superiority in Europe.

The Soviets saw the cause of information warfare as the inexorable development of technology. Soviet writers in the 1970s and 1980s, particularly former Chief of the General Staff, Marshal Nikolai Ogarkov, spoke of a "military technical revolution" occurring in the U.S. and Soviet militaries, which would make the European battlefield even more lethal.[23] This increased lethality was caused by

21. Quoted in David A. Fulghum, "Computer Warfare Offense Takes Wing," *Aviation Week and Space Technology*, 19 January 1998, 56.

22. This is precisely what airpower theorist Colonel John Warden wanted in the Gulf War. See John A. Warden III, "Employing Air Power in the Twenty-First Century," in *The Future of Air Power in the Aftermath of the Gulf War*, ed. Richard H. Schultz Jr. and Robert L. Pfaltzgraff Jr. (Maxwell Air Force Base, Ala.: Air University Press, 1992), 57–82.

23. One of the best works that reveals the thought of Ogarkov and other Soviet officers is Notra Trulock III, "Appendix B: Emerging Technologies and Future War: A Soviet View," in *The Future Security Environment*, Report of the Future Security Environment Working Group, submitted to the Commission on Integrated Long-Term Strategy (Washington, D.C.: U.S. Government Printing Office, 1988), 97–163. Trulock's other work is also valuable. See Phillip A. Petersen and Notra Trulock III, "Soviet Views and Policies Toward Theater War in Europe," in *The Dynamics of Soviet Defense Policy*, ed. Bruce Parrott (Washington, D.C.: Wilson Center Press, 1990), 229–56; and Trulock, "A Soviet View of Nonnuclear Strategic Capabilities and Future War," in *Technology and the Future Strategic Environment*, ed. Kenneth B. Moss (Washington, D.C.: Wilson Center Press, 1990), 37–65. Also see Cohen, "A Revolution in Warfare," 39–41; Stephen J. Blank, *The Soviet Military Views Operation Desert Storm: A Preliminary Assessment* (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1991); and Benjamin S. Lambeth, "The Technology Revolution in Air Warfare," *Survival* 39, no. 1 (spring 1997): 74–77. Lambeth sees the origins of the RMA in the writings of Soviet Air Force Lieutenant General N. A. Sbitov in the mid-1960s. The Soviets discussed three modern revolutions in military affairs: the eighteenth century brought the development of gunpowder, muskets, and cannon; the mechanization of warfare came in the early twentieth century with internal combustion engines; and the mid-twentieth century brought electronics and nuclear weapons. See "The Revolution in Military Affairs," *Soviet Military Encyclopedia*, vol. 7 (Moscow: Voyenizdat, 1979), 82 (cited in Gouré, "Is There a

advances in technology that would principally benefit conventional weapons, facilitating what the Soviets termed a "reconnaissance/strike complex"—the combination of sensors, communications, and long-range, highly accurate strike systems that would sharply compress the detection-to-destruction cycle of warfare.[24] In turn, this was caused by advances in computer technology and information processing. Soviet writers who analyzed the revolutionary potential of new military technologies saw several effects: they would increase the tempo of battle, and extend the depths to which sensors and fire systems would operate, permitting the disruption of the enemy's command and control centers, and hindering its ability to reinforce frontline forces.[25] Moreover, Ogarkov argued that integrating new reconnaissance and guidance technologies into future conventional weapons systems would make conventional weapons almost as effective as nuclear weapons; it would also make the system "global in nature" and increase its destructive potential "at a minimum by an order of magnitude."[26]

While the Soviets were the first to identify this issue, thoughts about the effects of advances in technology on the battlefield were mirrored in the U.S. defense community in the 1970s and 1980s. The fundamental idea developed by Carter administration officials like Perry was that technology could be used to offset Soviet conventional superiority in Europe. This came to be known as the "offset strategy." Perry describes the situation he faced at that time: "We had no conceivable way of increasing the size of the U.S. or the NATO forces to deal with?[a Soviet attack], and the 'offset strategy'?was no leap of brilliance. It was simply a necessity."[27] He continued, "the only way we had of dealing with the three-to-one quantity advantage that Soviet forces had was to try to offset that with our superior technology. That was the key to our entire defense strategy in the late '70s and on into the early '80s."[28]

To execute the offset strategy the United States, like the Soviets, created a "reconnaissance strike force" that combined two elements: precision strike

Military-Technical Revolution in America's Future," 177). Ogarkov claimed that the advances in sensors and precision-guided munitions were the fourth revolution.

24. The Soviets identified the promise of an order-of-magnitude increase in accuracy that would facilitate the destruction of any enemy target identified: "[U]p to now, the probability of hitting the target depended on the distance of the shooting: the greater the distance, the less the ability to strike. Precision weapons strike out this dependence....[their] accuracy is not dependent on distance, meteorological conditions, or time of day" (Col. Stanislaw Koziej, "Anticipated Directions for Change in Tactics of Ground Troops," *Przeglad Wojsk Ladowych* [Ground forces review] [September 1986]: 2. Quoted in Trulock, "Appendix B," in *The Future Security Environment*, 107). Also see Phillip A. Karber, *The Impact of New Conventional Technologies on Military Doctrine and Organization in the Warsaw Pact*, Adelphi Paper no. 144 (London: International Institute for Strategic Studies [IISS], 1978).

25. *The Future Security Environment*, 34–42.

26. Ogarkov quoted in Trulock, "Appendix B," in *The Future Security Environment*, 134.

27. Remarks by Secretary of Defense William J. Perry to the Precision Strike Association in Arlington, Va., 15 January 1997. Quoted in "Perry on Precision Strike," *Air Force Magazine* (April 1997): 75.

28. "Perry on Precision Strike," 75.

weapons systems, such as stealth aircraft and cruise missiles that could destroy targets behind Soviet lines; and an intelligence and reconnaissance system that would target for them and conduct battle damage assessment. The goal was to learn where enemy forces were, to kill them, and know that they had been killed. The principal result was increased battlefield lethality and the extension of this lethality to unprecedented depths—far behind the enemy's frontline. Information and new weapons technology make it easier to find and kill the enemy. This force was used for the first time in Desert Storm, and as Perry describes, "when used against an opponent with equal numbers, our technology did not simply offset the other side. It gave us the ability to win quickly, decisively, and with remarkably few casualties."[29]

This article addresses the principal military and political effects of information warfare. The intent here is not a comprehensive analysis—which is not yet possible because the U.S. military has not yet realized the potential of information warfare. Rather, the aim is to suggest what may occur if the U.S. military continues, as is likely, to innovate to become truly a military of the information age rather than the industrial age.

FOUR MAJOR MILITARY EFFECTS: DECENTRALIZATION, MANEUVERABILITY, PRECISION STRIKE, AND INFORMATION WARFARE OPERATIONS

The principal military effects of information warfare are increased decentralization within the military, greater maneuverability of forces, precision strike capability, and cyberwar, or offensive and defensive information operations.[30] Decentralization is

29. Quoted in "Perry on Precision Strike," 76. This strategy was criticized by the military reform community in the early 1980s for placing too great an emphasis on technology. The members of this school wanted simpler, cheaper weapons—in essence, quantity rather than quality. See James Fallows, *National Defense* (New York: Random House, 1981). For replies and analysis see William J. Perry, "Fallows' Fallacies," *International Security* 6, no. 4 (spring 1982): 174–82; Richard K. Betts, "Conventional Strategy: New Critics, Old Choices," *International Security* 7, no. 4 (spring 1983): 140–62; Asa Clark et al., *The Defense Reform Debate* (Baltimore: Johns Hopkins University Press, 1984); and John J. Mearsheimer, "The Military Reform Movement: A Critical Assessment," *Orbis* 27, no. 2 (summer 1983): 285–300.

30. Of course, in order to be realized these effects depend on other factors such as doctrine and improved logistics. Doctrine is important because it informs militaries how to fight—how they will be structured and employed to fight, and how to cooperate with other branches. Making technology serve an armed forces doctrine is difficult: throughout history, the two have rarely been in step. Military doctrine requires that the effects of the technology are known and thus can be distilled to elements that guide officers in conducting operations, but technological ramifications of information warfare are hard to know with certainty. In addition, military organizations historically have adopted new technologies in a way that protects rather than revolutionizes existing doctrine and the platforms that implement them. Thus, implementing information warfare is a problem less of technology than of organization and bureaucracy. Barry Posen and Jack Snyder demonstrate the difficulty of matching technology and doctrine. See Posen, *The Sources of Military Doctrine*; and Jack Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914* (Ithaca: Cornell University Press, 1984). Logistical support is essential as always, but the demands on the logistical system will increase along with the rapid movement of forces over great distances. As Air Force Gen. Ronald R. Fogleman has argued, advances in information technology will make obsolete large stockpiles of parts and equipment, the so-called iron

possible because surveillance and communication capabilities permit all units to know what is occurring with respect to enemy as well as friendly forces. Owens identifies one benefit of decentralization: it will supplant the hierarchy the military had needed to ensure response to orders and to direct soldiers into battle in a coordinated manner. Hierarchy is expensive: it is one of the causes of friction in war.[31] The confusion and lack of coordination among groups leads to disorder and misinterpretation of information, which grow as information is passed up the chain of command. Misinterpretation also passes down the chain of command and confusion delays the execution of orders. As Owens expects, information warfare should minimize this aspect of friction.[32]

Decentralization will have a second benefit: it will remove the existing distinction among strategic, operational, and tactical levels of operation. Information warfare will facilitate the direct communication of units vertically—up and down the chain of command—and horizontally—between units at the same level. Thus, actors at the strategic level may directly control units at the tactical level, and a unit that has information may disseminate it directly to the unit concerned. With the improvement in command and control made possible by information warfare, the spatial, temporal, and hierarchical distinctions among units will no longer be necessary to coordinate battle. The distinctions among the strategic, operational, and tactical elements, and the present hierarchical command structure, should be modified so that the nature and character of the decisions and actions match the fluidity of information warfare.[33]

mountains. See his "Information Revolution: The Changing Nature of Warfare," *Aviation Week and Space Technology*, 16 April 1997, 34. They will be replaced by a smaller, more flexible logistics train, which will allow "total logistics visibility, the ability to know the status of a part at any point in the distribution pipeline, an in-transit visibility to track spare parts between the supplier and user" (Dibb, "The Revolution in Military Affairs and Asian Security," 102). Also see Freedman, *The Revolution in Strategic Affairs*, 13–14. This should enable supply to keep pace with combat forces, and will reduce the logistics footprint by reducing the transport and storage of material and the number of logistics personnel. Fogleman, "Information Revolution," 34.

31. Jim Blaker, "The Owens Legacy," *Armed Forces Journal International* (July 1996): 20–21; and Owens, "The American Revolution in Military Affairs," 38. For Clausewitz's discussion of the causes and effects of friction in war see *On War*, 119–21.

32. Despite this reduction in one source of friction, the fog of war will remain as a result of potential enemy countermeasures and organizational problems, in addition to the confusion and ignorance always present in battle. The fog of war ensures some confusion, even as advances in communications and information processing permit decentralization and the reduction of hierarchy in command. If a single sensor or individual tasked with surveillance is confused and makes a mistake, it may spread throughout the network. In time that may be corrected, but false as well as true information will be present in the information network. Even if multiple sensors observe an area, there will be some discrepancy in what they observe. Furthermore, the fog of war will ensure some blue-on-blue casualties, those due to "friendly fire," even in the era of information warfare.

33. While the present hierarchies may be eliminated new ones will be created, in shapes which are still unclear. Despite these benefits, as Eliot Cohen has shown, the danger of military micromanagement coexists with the knowledge and communication ability provided by information warfare. Eliot A. Cohen, "The Mystique of U.S. Air Power," *Foreign Affairs* 73, no. 1 (January/February 1994): 109–24. This interference may complicate and impede successful operations because orders are likely to be

The second effect of information warfare, as Jablonsky argues, is increased maneuverability allowed by technological advances in communications.[34] Tacticians envision "smaller, fast moving, more independent units [will] maneuver around a battlefield, coalesce to attack enemy formations, then melt away into smaller component parts less vulnerable to smart weapons. As in war at sea, the focus will be not so much on seizing territory as on destroying enemy combat forces."[35] The elements that Owens identifies as the key elements of information warfare—radically improved situational awareness and agile communications—make such maneuverability possible, and precision weaponry permits targets, once identified, to be rapidly destroyed.[36]

The third effect is precision strike capability. U.S. forces have to have the ability to neutralize the enemy either by destroying, confusing, or avoiding it if they so choose. Again, technology plays a very important part in destroying the enemy by providing the United States with the capability to strike in all weather conditions, at long ranges, and with great accuracy. Targets will not have to be attacked in sequence, in order of priority, because "parallel warfare," attacking targets simultaneously, will be possible. This capability rests on more than the smart bombs which received so much acclaim during the Gulf War; it includes weapons systems, like the Joint Stand Off Weapon (JSOW), or cruise missiles like the Tomahawk, that strike their target accurately from great distances.

The final effect is information operations. Information warfare, like all warfare, may be conducted for either offensive or defensive purposes. Offensive information warfare operations (IW-O) are designed to use information and information processing to coerce an opponent by destroying or manipulating his information without directly engaging his military forces. Offensive information warfare may adversely affect the information available to the enemy, and his information systems and computer networks, in order to gather intelligence and to undermine the leadership, civilian and military infrastructure, weapons systems, and

contradicted, resulting in confusion between units. In addition, units may lose combat effectiveness if soldiers see their commander's order being contradicted or overruled by superior commanders.

34. Jablonsky, *The Owl of Minerva Flies at Twilight*, 32.

35. Blackwell, *The Gulf War*, 11.

36. Owens, "The American Revolution in Military Affairs," 37. Not all military officers and analysts have such a sanguine view of the benefits of information warfare. Charles Krulak, the former U.S. Marine Corps commandant, has argued that future combat will be likely to occur in densely populated urban areas or in impenetrable jungle; the future, he says, "is not son of Desert Storm, but the stepchild of Somalia and Chechnya" (Robert Holzer, "Krulak Warns of Over-Reliance on Technology," *Defense News*, 7–13 October 1996, 4). Retired Marine Lt. Gen. Paul Van Riper, former chief of the Marine Corps Combat Development Command, has stated: "There are a lot of buzzwords floating around associated with the 'revolution in military affairs,' and if they weren't so dangerous, they might be funny." He continues, "With the possible exception of nuclear weapons, technology has never resulted in a fundamental change in how nations go to war. To suggest that such concepts as 'information dominance' will now somehow make all the military doctrine that came before it irrelevant is ludicrous. We had information dominance in Somalia" (quoted in James Kitfield, "The Air Force Wants to Spread Its Wings," *National Journal*, 8 November 1997, 2264–65, quote on 2265).

morale of the state. The enemy may, for example, be deceived by altering or inserting false information into a message, reading communications secretly, or corrupting computer networks.[37] Clearly this capability may be useful in warfighting, as well as covert operations, to undermine a regime for example, or in operations other than war such as peacekeeping operations.[38]

In addition to offensive operations, the United States must possess a strong defensive information warfare (IW-D) capability—to defend against information warfare attacks directed against civilian or military targets.[39] An attack against the commanding heights of a modern economy, such as bank records and market transactions, the elimination of telephone and networked computer communications, or the collapse of air traffic control and railroad traffic, power grids, and key personal information held by the Department of Veterans Affairs or the Social Security Administration, could cause major, albeit temporary, economic disruption.

Military targets are also vulnerable. As then-director of the National Security Agency, U.S. Air Force Lt. Gen. Kenneth Minihan, described, U.S. military computer networks and information systems had so widely proliferated that the Defense Department and the intelligence community could no longer maintain the integrity of key systems. Minihan argues that information technology has created "one of our greatest strategic vulnerabilities. Our ability to network has far outpaced our

37. For a description of these capabilities see David A. Fulghum, "Cyberwar Plans Trigger Intelligence Controversy," in *Aviation Week and Space Technology*, 19 January 1998, 52–54; and also Fulghum, "Computer Warfare Offense Takes Wing," 56–58.

38. Some types of information warfare operations are not new. During the cold war, it is reported that the Pentagon permitted sales of software to Austrian and West German front companies, who would resell it to Soviet Bloc states, so that the United States could enter these computer systems once they had been connected to the state's communication or defense system and probe them for detailed intelligence information using special software. "Attack Software Plays Key Offensive Role," *Aviation Week and Space Technology*, 19 January 1998, 56.

39. Defense against an attack requires that the attack be detected and stopped, and the system restored to its previous condition. The civilian information network, called the National Information Infrastructure (NII), the amalgam of academic, industrial, governmental, and commercial networks, is deemed to be more vulnerable to attack than the military information infrastructure, or Defense Information Infrastructure (DII). DII essentially connects the Pentagon to the rest of the armed services and to the NII. Both infrastructures must be protected against a full range of threats, from pranksters and hackers, to criminals, industrial espionage, and offensive information warfare operations directed by a state. As John Hamre, U.S. deputy secretary of defense, has warned, however, "the internet was never designed with security in mind....The very openness of this technology, which leads to its dynamism, is what creates a risk." Hamre is quoted in Alexander Nicoll and Louise Kehoe, "U.S. Defence Official Warns of Internet Security Risks," *Financial Times*, 20 March 1998, 22. The Pentagon reportedly is developing a cyberwar order of battle by tracking those states that appear to be training to attack computers. David A. Fulghum, "New Weapons Slowed by Secrecy Clampdown," *Aviation Week and Space Technology*, 19 January 1998, 55.

ability to protect ourselves from cyber attack. We have a fundamental new danger in the cyber dimension."[40]

Protecting these systems is difficult: computer networks are designed to interconnect and experience has shown that they are vulnerable to penetration. While they must be protected with stronger defenses, even a worst-case scenario, with markets shut down temporarily, would not have a significant military effect. Indeed, "America Online, the largest service provider, has had a number of outages. The ice storm in the Northeast or the United Parcel Service strike caused more misery than would one day of Internet shutdown."[41] In addition, U.S. deterrent capabilities apply to an information attack, and punishment for an attack, once the attacker is identified, would outweigh any benefit. Why then would an attacker want to launch a militarily insignificant attack on the U.S. economy? Attacks against military computers might have a temporary effect but the force of the U.S. deterrent would still obtain.

Furthermore, military computer systems are viewed as less vulnerable to successful penetration than civilian systems. This is so because "their communications lines are more secure, and they usually have unique programming unfamiliar to most hackers. Viruses are not of much use, experts say, because they probably won't work due to the unfamiliar system, and their course is too undirected to have an assured effect."[42] As one computer security official has said, "If you want to kill a computer system, drop a bomb."[43] Still, strengthening U.S. defenses against offensive operations is certainly prudent.[44]

THE POLITICO-MILITARY RESULTS OF INFORMATION WARFARE: INCREASED U.S. ABILITY TO DETER AND COERCE

Information warfare will increase the capability of the U.S. military to fight wars against enemies not similarly equipped. This capability will give the United States greater ability to coerce and deter opponents.[45] The intent here is only to describe

40. Quoted in Craig Covault, "Cyber Threat Challenges Intelligence Capability," *Aviation Week and Space Technology*, 10 February 1997, 20. Also see Bill Gertz, "Hackers Disable Military in Exercise," *Washington Times*, National Weekly Edition, 20–26 April 1998, 1.

41. Michael A. Dornheim, "Bombs Still Beat Bytes," *Aviation Week and Space Technology*, 19 January 1998, 60.

42. Ibid., 60.

43. In addition, a computer attack "suffers the same drawback as other nonexplosive techniques—it is very difficult to tell whether the target was destroyed" (Dornheim, "Bombs Still Beat Bytes," 60).

44. In one positive step, the defense department is creating a computer security czar. See George I. Seffers, "DoD Recruits Hacker Czar," *Defense News*, 13–19 April 1998, 1.

45. "Coercion" is used here to refer to the same concept that Thomas Schelling terms "compellence." Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966), 69–91.

the capability that the United States will possess, not to evaluate their political feasibility or effect, or to consider in detail countermeasures a foe may take.[46]

With respect to deterrence, information warfare strengthens the conventional ability of the United States to deter great powers or small states in three ways. First, information warfare capabilities will make the U.S. conventional deterrent by denial even more robust than it is presently. Any adversary would be convinced that it could not win a quick and decisive victory over the United States, which is the sine qua non of conventional deterrence.[47] The destruction of the Iraqi forces at Khafji and during the Gulf War itself demonstrates the strength of U.S. capabilities. U.S. battle-management aircraft detected and tracked the Iraqi attack, and coordinated the Coalition response. Iraqi forces were vulnerable the moment they attempted to maneuver and advance; the result was the rapid and total destruction of the Iraqi attack and prevention of its reinforcement.[48]

Second, information warfare will strengthen conventional deterrence by punishment. Information warfare will give the United States the capability to physically destroy the targets it wants to, while minimizing collateral damage. This may allow the United States to threaten state leaders with destruction by conventional weapons, which in turn, may strengthen deterrence.[49] The idea of

46. The enemy that the United States confronts in battle is likely to be dynamic; it will adapt to find the U.S. military's Achilles' heel. It may destroy the sophisticated platforms upon which the U.S. military depends for information warfare, such as those for surveillance and command and control like JSTARS and AWACS, and space-based communications, the GPS satellite constellation, and command and control assets as well. Also it may be simple to deceive the surveillance platforms on which the military would depend to locate and target the enemy through camouflage or to deceive sensors through electronic or visual countermeasures. Of course, the U.S. military is dynamic as well, and will develop active and passive counter-countermeasures. The winner in this action-reaction cycle is the side that possesses an asymmetric threat—a technology that forces the enemy to develop a measure completely out of proportion to the benefit derived. A historical example of technologies that are difficult to counter is the submarine. Britain, Canada, and the United States devoted enormous resources to antisubmarine warfare (ASW) in the First and Second World Wars. The cost to the Allies of countering the German submarine campaign was out of proportion to the cost to the Germans of mounting the submarine campaign. It was, nonetheless, essential for victory in both wars that the allies win the ASW campaign so that Britain could continue to receive the resources needed to fight the war. This example suggests that a technologically less sophisticated opponent will be able to use extant technologies which are difficult to counter or will easily fool sophisticated sensors, for example using dummy tanks to match the optical and infrared signatures of real tanks.

47. John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983), 24, 63–64. For an excellent discussion of conventional deterrence in the post–cold war world see Richard J. Harknett, "The Logic of Conventional Deterrence and the End of the Cold War," *Security Studies* 4, no. 1 (autumn 1994): 86–114.

48. In fact, U.S. capability may make the United States harder to deter because it would be convinced that it has the ability to execute a quick and decisive victory. For accounts of the battle of Khafji see Anthony H. Cordesman and Abraham R. Wagner, *The Lessons of Modern War* vol. IV, *The Gulf War* (Boulder, Colo.: Westview, 1996), 180–83, 507–08; and Michael R. Gordon and General Bernard E. Trainor, *The General's War: The Inside Story of the Conflict in the Gulf* (Boston: Little, Brown, 1995), 267–88.

49. The word *may* is used here because U.S. deterrent capabilities against threshold states are already robust, but whether the United States will use them or not—as explored below—depends on the balance of resolve between both parties and the danger of inadvertent escalation.

counterleadership targeting is not new—it was for much of the cold war a key component of U.S. nuclear deterrent strategy.[50] In the post–cold war era, U.S. officials still believe the logic of counterleadership targeting to be important for deterrence and coercion.[51] U.S. information warfare capabilities suggest that conventional forces will be able to accomplish the same mission.[52]

Third, the United States will have greater ability to extend deterrence credibly to its allies.[53] The United States faced a credibility problem during the cold war: would it risk the destruction of New York for Paris? IW will reduce this problem because increased conventional capability to deter (and to fight if necessary) means that the United States need not rely on its strategic nuclear forces to the extent it did in the past.

Information warfare has great value for nuclear deterrence by denial because very accurate conventional weapons will replace nuclear weapons for destroying large formations of enemy forces—the traditional role of tactical nuclear weapons.[54] As a result of information warfare, tactical nuclear weapons will have even less utility for U.S. forces in the future. On nuclear deterrence by punishment,

50. During the Carter administration, the United States believed effective deterrence required threatening the Soviet leadership itself with destruction. The argument was that the leadership valued itself above Soviet citizens or industry, so the United States had to target Communist Party officials, the KGB, and other manifestations of Soviet power. This was the core component of the Carter administration's countervailing strategy that resulted in Presidential Directive (PD) 59 of 1980 which offered new guidance for U.S. nuclear targeting. See Charles L. Glaser, *Analyzing Strategic Nuclear Policy* (Princeton: Princeton University Press, 1990), 236–38; and Scott D. Sagan, *Moving Targets: Nuclear Strategy and National Security* (Princeton: Princeton University Press, 1989), 48–54. For a good explanation and defense of the countervailing strategy see Walter Slocombe, "The Countervailing Strategy," *International Security* 5, no. 4 (spring 1981): 18–27.

51. Warden's Instant Thunder air war plan, for example, assumed that counterleadership targeting was the only way to coerce Saddam Hussein from Kuwait. For a critique of Warden's plan see Robert A. Pape, *Bombing to Win: Air Power and Coercion in War* (Ithaca: Cornell University Press, 1996), 226–40.

52. Ogarkov recognized "that, in the future, there will be few, if any, missions that would be inappropriate for nonnuclear systems. Consequently, both sides would likely be far less reliant on the use of nuclear weapons to perform tactical, operational and perhaps even some strategic missions" (Trulock, "Appendix B," in *The Future Security Environment*, 134). Nonetheless, there remain some targets that will only be destroyed effectively by nuclear weapons, such as command and control bunkers, which are likely to be deeply buried and hardened.

Information warfare will also facilitate conventional deterrence by allowing the United States to threaten destruction of the enemy's computer networks, holding hostage—electronically—its financial, communications, and electrical centers. While the military utility of such targets is questionable, the ability to threaten to disrupt them is another arrow in the U.S. quiver.

53. Although credible extended deterrence is the product of multiple factors, including the balance of resolve, and the value of the future for the deterred state in relation to the status quo. For a thoughtful analysis of extended conventional deterrence see Charles T. Allan, "Extended Conventional Deterrence: In from the Cold and Out of the Nuclear Fire?" *Washington Quarterly* 17, no. 3 (summer 1994): 203–33.

54. Deterrence of premeditated aggression requires the ability to deter an attack either by denying the opponent its objective—deterrence by denial—or by being able to punish the opponent so severely that no gain would be worth the cost of aggression—deterrence by punishment. On the distinction between deterrence by denial and deterrence by punishment see Glenn H. Snyder, *Deterrence and Defense: Towards a Theory of National Security* (Princeton: Princeton University Press, 1961), 14–16.

however, information warfare will have less of an effect. Information warfare raises the nuclear threshold for the United States because IW provides it with conventional superiority, the United States has no reason to threaten escalation to the nuclear level. Strategic nuclear forces may be further reduced, such as in a potential START III treaty, without jeopardizing U.S. security.[55]

Like deterrence, coercion must be analyzed in both its conventional and nuclear contexts. Information warfare will make conventional coercion against states (non-great powers) more effective. IW will allow the United States to use both coercion by punishment and coercion by denial more effectively. In his analysis of the utility of airpower for coercion, Robert Pape has shown that conventional coercion by punishment is rarely effective; conventional coercion by denial succeeds more frequently.[56] Coercion using conventional weapons "is most likely to succeed when directed at military, not civilian, vulnerabilities."[57] This explains why strategies of coercion by punishment, such as the decapitation strategy advocated by U.S. Air Force planners like John Warden during the Gulf War, are not effective.

Information warfare has the potential to change this situation, to make coercion by denial and punishment more effective. It will make conventional denial easier by marrying the ability to identify, target, and destroy a target with the ability to collect, process, distribute, and act upon information. Again, the destruction of the Iraqi attackers on Khafji during the Gulf War demonstrated this ability. Iraqi forces were vulnerable the moment they attempted to maneuver and advance; they were quickly and totally destroyed.

Information warfare will affect conventional coercion by punishment because it makes decapitation increasingly possible. The ability to destroy the enemy leadership is always hindered by ignorance of where key decisionmakers are in real time.[58] This problem was especially acute in the Gulf War when the U.S. effort to kill Saddam Hussein was thwarted by the real time limitation. The synthesis of

55. In fact, in a world where the United States has overwhelming conventional superiority, nuclear weapons are a great hindrance to the exercise of U.S. power. In October 1996, Gen. Lee Butler, and two months later, Gen. Andrew Goodpaster, advocated the elimination of all nuclear weapons. This struck many observers as odd, especially because Lee Butler is a former commander-in-chief of the Strategic Air Command. It could not have escaped these generals that, by abolishing nuclear weapons, information warfare would provide the United States with great advantages in the use of force. Not only would the United States be the dominant military, but other great powers would have no immediate way to check its power.

56. Denial strategies target the opponent's military ability to achieve its territorial or other political objectives. See Pape, *Bombing to Win*, 12–54.

57. Pape, *Bombing to Win*, 19.

58. Occasionally in the past, U.S. officials knew where an individual was early enough to permit an attack; for example, in 1943 communications intercepts allowed U.S. fighter planes to shoot down Japanese Admiral Isoroku Yamamoto's plane over Bougainville.

technology and information will help the United States identify and destroy the enemy leadership and command and control nodes.[59]

It is clear that information warfare will increase the military capabilities of the United States. As we have seen, many authors claim that information warfare will be so effective as to cause a revolution in military affairs. This may be so, but the definition of an RMA is not clear. I now turn to defining the concept of a revolution in military affairs, and argue that, while information warfare has significant benefits for the United States, it has not supplanted the nuclear revolution.

WHAT IS A REVOLUTION IN MILITARY AFFAIRS?

A REVOLUTION IS radical change. This is true of all revolutions whether they are social, like the French Revolution, or a revolution of the natural sciences, such as the change from a geocentric universe to a heliocentric one as discovered by Copernicus. The intellectual, or ideational, element of a revolution is a fundamental conceptual change: a revolution invalidates old conceptual frameworks or paradigms and identifies and requires new concepts or paradigms to comprehend the new order.[60] Liberalism, for example, was the new political concept necessary to understand the political order in Europe after the French Revolution.

A revolution in military affairs is only a revolution if it affects the fundamental relationship in military affairs: the relationship of politics to war. An RMA obviates old concepts about the relationship of politics to war and requires new ones to explain the new synthesis. The rise of the state and nationalism, for example, were political changes that affected the fundamental relationship between politics and war. The rise of the state made professional military forces possible, and nationalism, spawned by the French Revolution, united nation and state and made total war possible. Changes in technology may also affect this relationship; the nuclear revolution made war so costly that it no longer had any political benefit beyond the defense of the state itself. Military developments which do not affect this fundamental relationship may be important, but they will not produce RMAs.

59. The effect of information warfare on nuclear coercion is likely to be very modest. Information warfare adds very little to the U.S. ability to use nuclear weapons to coerce by denial. With respect to coercion by punishment, information warfare will allow the United States to rapidly identify targets and destroy an opponent's nuclear forces. The opponent's nuclear forces, however, would probably be numerous enough and its command and control system sufficiently robust to make any U.S. attack not worth the risk to the United States. Thus, as discussed below, any attempt at coercion would be both incredible and imprudent.

60. Thomas Kuhn's conceptions of paradigm and paradigm shift are relevant here. A revolution like the Copernican or the French may be thought of as a change in paradigm. Thomas S. Kuhn, *The Structure of Scientific Revolutions*, 2nd ed. (Chicago: The University of Chicago Press, 1970).

For information warfare to be an RMA, it has to supplant the nuclear revolution as the dominant paradigm of warfare.[61] That is, it has to change the relationship between war and politics that the nuclear revolution created.[62] The essence of the nuclear revolution is that nuclear weapons have made war so costly that the only political end justifying their use is defense of the state. This is revolutionary because force is no longer ultima ratio in the settlement of major disputes for states armed with assured destruction capabilities. For these states, Clausewitz's dictum that "war is an act of force, and there is no logical limit to the application of that force," is no longer true. There is a logical limit to the application of force in the nuclear age because, clearly, to engage in a total war with nuclear weapons would result in the annihilation of the states concerned. This is incomprehensible in a political sense because it violates Clausewitz's fundamental recognition of the relationship between politics and war: such a catastrophe defeats the political rationale for war as a continuation of politics by other means.

Before the nuclear revolution, the goal of war as a theoretical concept that Clausewitz identified was "*always* and *solely* to be to overcome the enemy and disarm him."[63] To accomplish this end the "fighting forces must be destroyed: that is, they must be *put in such a condition that they can no longer carry on the fight.*"[64] Once this is accomplished, then the country may be subdued and the enemy brought to the peace table.

The nuclear revolution changed the validity of Clausewitz's reasoning. Nuclear weapons, coupled with delivery systems against which there was no defense, meant that it was no longer necessary to defeat the enemy's forces in order to subdue or punish him.[65] It also meant that nuclear states must rely on their ability to deter a nuclear war rather than to fight one.[66]

During the cold war, the central argument of deterrence theorists was that a state must have a secure second-strike capability for a stable deterrent relationship to obtain. That is, it must have sufficient nuclear forces to retaliate even in the face of

61. A dominant paradigm of warfare determines the highest level of conflict possible. As the Napoleonic wars introduced total war, the nuclear revolution introduced societal annihilation. Of course, in any paradigm of warfare, wars below the highest level are still possible, such as those between great powers and small powers, those between two or more small powers, and civil wars. For a thoughtful discussion on the relationship of nuclear weapons to the RMA see Colin S. Gray, "Nuclear Weapons and the Revolution in Military Affairs," in *The Absolute Weapon Revisited: Nuclear Arms and the Emerging International Order*, ed. T. V. Paul, Richard J. Harknett, and James J. Wirtz (Ann Arbor: University of Michigan Press, 1998), 99–134.

62. As Clausewitz most famously has described it: "War is not merely an act of policy but a true political instrument, a continuation of political intercourse, carried on with other means" (Clausewitz, *On War*, 87).

63. Ibid., 90 (emphasis in original).

64. Ibid. 90 (emphasis in original).

65. Schelling, *Arms and Influence*, 26–34.

66. As Robert Jervis notes, it is the possibility of fighting a war with a nuclear opponent, rather than the possibility of losing it, that causes restraint. Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon* (Ithaca: Cornell University Press, 1989), 9.

a first strike by an adversary.[67] The ability to retaliate produces the mutual vulnerability of the states' societies; because no defense is possible to protect a state's society from unacceptable damage, all are vulnerable. It is this result of mutual vulnerability, produced by mutual secure second-strike capabilities, that causes the nuclear revolution.[68] Three factors make deterrence robust: the inability of states to defend effectively against rapid delivery systems; the enormous destruction that even a few nuclear weapons may cause to a society; and states leaders' knowledge of these facts.[69]

In addition, two other factors contribute to stability. Escalation dominance—moving to a higher level of conflict where one side has superiority—is not possible between two states that have mutually assured destruction capabilities. Second, the risk of inadvertent escalation is present. As Barry Posen has shown, there is little chance that the United States could prevent a conventional war with the Soviets (or Russians) from escalating to the nuclear level.[70] This is largely because a conventional war affects the victim's confidence in its assured destruction capability.[71] Posen's analysis demonstrates that wherever the conventional forces of nuclear powers interact, there is the risk of inadvertent escalation. Thus, while the nuclear revolution does not make war between nuclear-armed states impossible—there are significant risks—it does, in general, make war so costly that it is not worth the cost of aggression. It has changed fundamentally the relationship between war and politics.

Accepting this definition and assuming that the claims of information warfare advocates quoted above are true, we can ask whether U.S. information warfare capabilities are leading to a fundamental change in the relationship between war and politics. Is it a sea change in warfare—a revolution in military affairs? In order to determine this, I examine three different levels of combat: conflict between nuclear armed peer-competitors, conflict between a great power and a smaller nonnuclear state, and conflicts between a great power and a nuclear threshold state. Because

67. For authors who most forcefully made the argument that nuclear weapons have revolutionized warfare see Bernard Brodie et al., eds., *The Absolute Weapon: Atomic Power and World Order* (New York: Harcourt, Brace, 1946), 21–69 and 70–107; Jervis, *The Meaning of the Nuclear Revolution*, 14–45; and Michael Mandelbaum, *The Nuclear Revolution: International Politics Before and After Hiroshima* (Cambridge: Cambridge University Press, 1981).

68. Jervis, *The Meaning of the Nuclear Revolution*, 5–16. The development of nuclear weapons has made one type of deterrence, deterrence by punishment, much easier to obtain.

69. Although deterrence by punishment may be robust, it is not perfect. It requires survivable forces, a robust command and control system, and sufficient safeguards against nuclear inadvertence. For an analysis of these components of stable deterrence see Bradley A. Thayer, "The Risks of Nuclear Inadvertence: A Review Essay," *Security Studies* 4, no. 3 (spring 1994): 431–42; and Thayer, "Nuclear Weapons as a Faustian Bargain," *Security Studies* 5, no. 1 (autumn 1995): 149–63.

70. Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca: Cornell University Press, 1991).

71. Ibid., 2. Posen notes that the riskiest types of attacks are those that threaten the assured destruction capability of the enemy or the early warning system.

these conflicts involve different dynamics, they permit us to see that the benefits of information warfare to the United States vary in each, and that the risks inherent in the nuclear era cannot be removed.

Conflict Between Nuclear-Armed Great Powers: The Nuclear Revolution Remains

To determine the effect of information warfare on the relations among established nuclear states I examine its influence on the U.S.-Russian nuclear relationship. Information warfare will have an effect on this relationship because imbalances in information warfare capability greatly favor the conventional attacker, but this effect will be mitigated by the nuclear revolution.

Information warfare benefits the United States in its relationship with Russia in three ways. First, it increases the U.S. ability to destroy Russian strategic nuclear forces; second, it improves its damage limitation capability; and third, it greatly strengthens U.S. conventional deterrence capabilities so that as NATO expands to the east, the conventional balance, measured in terms of capabilities, will favor NATO rather than Russia as it did in aggregate terms during the cold war. I examine each benefit in turn and critique each one. My conclusions are, first, that information warfare will result in increased U.S. conventional deterrence capabilities; and second, the nuclear revolution, specifically the danger of inadvertent escalation, mitigates the advantages that the U.S. gains in its increased ability to destroy Russian nuclear forces with conventional weapons.

Splendid First Strike and Limited Strikes with Conventional Weapons

As a result of the capabilities described above, information warfare should allow the United States to identify and destroy, with either conventional weapons, nuclear weapons, or a combination of both, Russian nuclear forces and command and control centers with greater efficiency. In addition, the reduced number of nuclear forces required by the START II Treaty (no more than 3,500 warheads), and the possibility of deploying an effective U.S. national missile defense (20–100 launchers at a single site), maximize the ability of the United States to consider two options that it was denied for much of the cold war. The first is the execution of a splendid first strike: to destroy the Russian nuclear force completely in a first strike.[72] Second, it allows the United States to execute limited strikes with conventional

72. It is not clear for what political benefit the United States would want to incur even the greatly reduced risk of retaliation by executing a splendid first strike option even were it to have one. For the origins and discussion of splendid first-strike capability see Herman Kahn, *On Thermonuclear War* (Princeton: Princeton University Press, 1960), 3–4, 36–37.

weapons against Russian nuclear or other military targets.[73] Information warfare is valuable because it allows forces to strike in circumstances where both sides feel compelled to limit the collateral damage—such as those against transportation networks, power grids, and port facilities—without the risk of widespread collateral damage inherent in a nuclear attack against such targets, which are usually located in populated areas.[74]

Despite information warfare capabilities, reductions in the Russian nuclear arsenal, and the possibility of limited U.S. deployment of strategic missile defenses, information warfare will not give the United States a splendid first strike capability, nor will it permit limited strikes with conventional weapons against Russian targets. This is so for three reasons: first, the plan is difficult to execute, especially given a predictable Russian response to redress its vulnerability; second, the United States still would not possess escalation dominance; and, third, the risk of inadvertent escalation is too great.

The United States cannot destroy with sufficient certainty the nuclear forces or command and control systems of established nuclear states. There is always the risk that U.S. intelligence is incomplete or wrong and is unaware of Russian military assets that could retaliate against the United States. While this would be less likely in an era of information warfare, the cost in American lives if U.S. decisionmakers are wrong is unlikely to be worth any benefit gained in attacking Russia. The possibility of mistakes can never be discounted entirely, even considering the importance of the issue to U.S. national security. Iraq's suspended effort to acquire nuclear weapons is an important example. Before the Gulf War, the United States reportedly knew of only two sites of Iraq's nuclear weapons program and suspected two more; now we know that its nuclear weapons program used more than 25 major facilities.[75]

73. For a discussion of Russian concern over this possibility see Sumner Benson, "Deep-Strike Weapons and Strategic Stability," *Orbis* 40, no. 4 (fall 1996): 499–515.

74. As retired Russian Gen. Vladimir Belous said in the wake of Operation Allied Force, "Russia must take into consideration that high-precision weapons can be used against us, including against strategic installations, missile silos and submarine bases" (quoted in David Hoffman, "Russia Laments Lost Power," *Washington Post*, 12 June 1999, A1).

75. See Thomas A. Keaney and Eliot A. Cohen, *The Gulf War Air Power Survey Summary Report* (Washington, D.C.: U.S. Government Printing Office, 1993), 123; and David M. Kay, "Denial and Deception Practices of WMD Proliferators: Iraq and Beyond," *Washington Quarterly* 18, no. 1 (winter 1995): 88. The United States was also unaware of the size of Iraq's biological and chemical weapons capability. While U.S. and Israeli intelligence officials underestimated the scope of the Iraqi program, the issue of how to prevent such a failure is a useful one on which to focus. As John Deutsch wrote: "The point is not how wrong the United States was about Iraq's timetable for acquiring a bomb, but rather how greatly the United States underestimated the magnitude of the Iraqi covert effort. As it stands, such a massive miscalculation of a nation's capability...can surely happen again" (John M. Deutsch, "The New Nuclear Threat," *Foreign Affairs* 71, no. 4 [fall 1992]: 128).

In addition, the Russians will likely take steps to redress their vulnerability.[76] They can do so in three ways: by alternating their strategic nuclear posture, by developing countermeasures to information warfare technologies, and possibly by violating the limitations of the START treaties. Russia has already revised its nuclear doctrine, abandoning the defensive doctrine Gorbachev announced in 1987, to permit first use of nuclear weapons, and is becoming more dependent on nuclear forces as its conventional forces deteriorate.[77] Three trends are making Russia vulnerable: U.S. conventional capabilities are increasing as a result of information warfare; the disparity between NATO and Russian conventional forces continues as NATO expands; and Russia cannot match U.S. strength as its economic hardship continues and its military decays. Given these trends, Russia can be expected to depend more on its nuclear capability for its defense, while its leaders lay the economic foundation to match U.S. military capabilities in the long run.[78] Though hardships are affecting all of the Russian military, the nuclear forces are relatively well off because they are supported by military and political leaders.[79]

Second, the United States would not possess escalation dominance because it could not reasonably be certain of its ability to destroy all of the Russian strategic nuclear force. The Russians would have an incentive to escalate because their nuclear capability would be threatened.[80] During the cold war, many scholars argued that it was impossible to keep nuclear war limited, principally because the losing side has an incentive to escalate; this logic still obtains.[81] Escalation to nuclear war ensures that the United States will suffer horribly and Russia will incur even greater losses. While the United States will not possess escalation dominance, U.S. possession of information warfare capability threatens crisis stability. In a crisis,

76. One insight of the realist theory of international politics is that great powers will strive to match the capabilities of their rivals. This will be discussed in more detail below. For seminal neorealist arguments see John J. Mearsheimer, "The False Promise of International Institutions," *International Security* 19, no. 3 (winter 1994/95): 11–12; and Kenneth N. Waltz, *Theory of International Politics* (Reading, Mass.: Addison-Wesley, 1979), 161–93.

77. On the importance of nuclear weapons for Russia's defense and the deterioration of its conventional forces see "Nuclear Weapons First in Russia's Defence Policy," *IISS Strategic Comments* 4, no. 1 (January 1998). On the change in Russian military doctrine see Charles J. Dick, "The Military Doctrine of the Russian Federation," *Journal of Slavic Military Studies* 7, no. 3 (September 1994): 481–506; and Mary C. FitzGerald, "The Russian Military's Strategy For 'Sixth Generation' Warfare," *Orbis* 38, no. 3 (summer 1994): 457–76.

78. See Sumner Benson, "Will Modern Technology Remilitarize Russia?" *Orbis* 39, no. 3 (summer 1995): 403–15.

79. Alexei G. Arbatov, "Military Reform in Russia: Dilemmas, Obstacles, and Prospects," *International Security* 22, no. 4 (spring 1998): 83–133.

80. On the motivations of states to escalate see Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).

81. Desmond Ball, *Can Nuclear War Be Controlled?* Adelphi Paper 169 (London: IISS, 1981); Klaus Knorr, "Controlling Nuclear War," *International Security* 9, no. 4 (spring 1985): 79–98.

the Russians would have greater incentives to attack first.[82] The danger may be greater now than at any time since the 1960s when the Soviet Union acquired a secure second-strike capability. As the shrinking Russian arsenal becomes more vulnerable, especially in the face of increased U.S. conventional capabilities, the incentive increases for Russia to maintain its launch-on-warning retaliatory policy.[83] Any crisis with the United States increases the pressure for Russia to use its nuclear forces rather than jeopardize their destruction by superior U.S. capability.

Third, the risk of inadvertent escalation prevents the United States from making limited conventional strikes against Russian military targets, and specifically its strategic nuclear forces. As Posen's analysis shows, a conventional war affects the victim's confidence in its assured destruction capability.[84] He argues: "Direct conventional attacks on critical nuclear forces, attacks that degrade strategic early warning or command and control systems, or even attacks on general-purpose forces that protect strategic nuclear forces, could all produce strong reactions from the party on the receiving end."[85] Posen's scholarship demonstrates that whenever the conventional forces of the United States and Russia interact, the risk of inadvertent escalation is present. Thus, the United States may execute limited strikes at Russian military targets without intending to provoke a nuclear war, but that could still be the result.

DAMAGE LIMITATION

The second effect of information warfare on the U.S.-Russian nuclear relationship is damage limitation. While information warfare will not give the United States a splendid first-strike capability, it does increase the U.S. ability to limit damage by striking first. The United States would be able to destroy much of the Russian nuclear force before it could launch, and with its defenses, have a good probability of destroying some of the Russian retaliatory force.[86] Thus, the United States would have greater damage limitation capabilities than it did during much of the cold war.

This provides three capabilities. First, U.S. extended deterrence commitments, such as those to Europe, Japan, and South Korea, would be more credible because Russia and China, the principal threats to these states, are less able to retaliate

82. For discussions of crisis stability see Glaser, *Analyzing Strategic Nuclear Policy*, 44–49; and Richard Ned Lebow, *Nuclear Crisis Management: A Dangerous Illusion* (Ithaca: Cornell University Press, 1987), 157–85.

83. The best analysis of the link between conventional and nuclear forces is Posen, *Inadvertent Escalation*. On Russian retaliatory doctrine see Bruce G. Blair, *The Logic of Accidental Nuclear War* (Washington, D.C.: Brookings, 1993), 28–29. Russian missiles are not presently targeted on the United States but most Russian ICBMs may be retargeted so rapidly as to make this fact meaningless.

84. Posen, *Inadvertent Escalation*, 2.

85. Ibid., 3.

86. This argument applies equally well to the U.S. deterrent relationship with China.

against the United States.[87] Second, fewer Americans would die in a nuclear war because many of the nuclear weapons targeting U.S. cities would be destroyed. Third, the principal political effect of this might be that the United States would be better able to coerce the Russians in a crisis—the reverse of the "Nitze scenario" that greatly concerned U.S. decisionmakers in the 1970s and 1980s.[88] U.S. superiority in counterforce weaponry would allow it to destroy Russian counterforce capability, leaving Russian decisionmakers with the choice of either accepting defeat or retaliating against U.S. cities and thus inviting U.S. destruction of Russia's as well.[89]

A reverse Nitze scenario, however, is unlikely. As it did with splendid first-strike, the fundamental fact of the nuclear age resurfaces: very few political goals are worth incurring the risk of nuclear war, and this risk is always present as long as the opponent has an assured destruction capability. The Russians recognize this fact. They know that there is always the risk that U.S. intelligence is so incomplete as to be misleading or wrong, and will strive to redress this imbalance in capabilities by altering its strategic nuclear posture and by taking countermeasures. These factors alone are likely to defeat any attempt at coercion.

Attempts at coercion, however, may also be dangerous. The danger arises out of the risk described above in Posen's arguments on inadvertent escalation. As he has shown, a conventional war with the Russians will quite likely escalate to the nuclear level.[90] There is, however, also the risk of nuclear inadvertence: nuclear weapons may be used by accident, by third parties, or without authorization.[91]

The risk of nuclear inadvertence makes conventional war and nuclear coercion dangerous because it becomes more likely as military forces increase readiness, such as going on alert status, in order to send a coercive signal to the enemy. While nuclear inadvertence is always possible, it becomes more likely as the alert increases the operational tempo of nuclear forces.[92] In addition, the inherent nature of

87. The credibility of extended deterrence is also strengthened by the conventional superiority of the United States. On the relationship between force size and credibility see Earl C. Ravenal, "Counterforce and Alliance: The Ultimate Connection," *International Security* 6, no. 4 (spring 1982): 26–43. Thus, in the post–cold war world the U.S. ability to maintain an extended deterrent is much greater. For the argument in support of maintaining our commitment see Robert J. Art, "Geopolitics Updated: The Strategy of Selective Engagement," *International Security* 23, no. 3 (winter 1998/99): 79–113. For the argument against see Eugene Gholz, Darryl G. Press, and Harvey M. Sapolsky, "Come Home, America: The Strategy of Restraint in the Face of Temptation," *International Security* 21, no. 4 (spring 1997): 5–48; and Christopher Layne, "From Preponderance to Offshore Balancing: America's Future Grand Strategy," *International Security* 22, no. 1 (summer 1997): 86–124.

88. In the mid-1970s Paul Nitze argued that Soviet nuclear superiority would allow them to coerce the United States in a crisis. See Paul Nitze, "Deterring Our Deterrent," *Foreign Policy,* no. 25 (winter 1976/77): 195–210.

89. On nuclear coercion and its utility see Richard K. Betts, *Nuclear Blackmail and Nuclear Balance* (Washington, D.C.: Brookings, 1987); and Robert Jervis, *The Illogic of American Nuclear Strategy* (Ithaca: Cornell University Press, 1984).

90. Posen, *Inadvertent Escalation.*

91. Thayer, "The Risks of Nuclear Inadvertence," 439–45.

92. On the likelihood of nuclear inadvertence in peacetime see Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton: Princeton University Press, 1993).

military organizations makes nuclear inadvertence possible: these systems are complex, they face great uncertainty, and nuclear forces are tightly coupled with warning systems.[93] While the risk of nuclear inadvertence may be low, it remains a risk that complicates a decision to use nuclear forces to coerce an enemy.

For these reasons, information warfare will not give the United States the ability to coerce Russia in a crisis. The probable result for U.S. foreign policy is that the United States would be unlikely to take actions that would risk initiating, either directly or inadvertently, a nuclear war because the costs of such a war remain too great to justify any gain.

CONVENTIONAL DETERRENCE

Information warfare will have an important effect on the conventional deterrence capabilities of the United States. This is relevant for the United States in the post–cold war world in two instances: the inter-Korean border and, as NATO expands, a new central front which now exists on the Polish-Russian border.[94] During the cold war the debate on the conventional balance on the Central Front between NATO and Warsaw Pact forces revolved around the issue of how unfavorable the balance was.[95] This debate is less important because information warfare capabilities will provide the United States with the ability to defeat all three available strategies. As John Mearsheimer explains, "Basically, decision makers are faced with three distinct and narrowly defined strategies: the attrition, the blitzkrieg, and the limited aims

93. This danger is recognized by Schelling, *Arms and Influence*, 92–125; John Steinbruner, "Beyond Rational Deterrence: The Struggle for New Conceptions," *World Politics* 28, no. 2 (January 1976): 223–45; and Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven: Yale University Press, 1983), 129–78.

94. The precise contours of the new NATO-Russian central front cannot be ascertained at this time because additional states may join NATO and because at least some of the states excluded from NATO expansion, such as Slovakia, are likely to align with Russia. The ability of the United States and South Korean militaries to conventionally deter a North Korean attack is robust; I will not address it further. See Nick Beldecos and Eric Heginbotham, "The Conventional Military Balance in Korea," *Breakthroughs* 4, no. 1 (spring 1995): 1–8; Michael O'Hanlon, "Stopping a North Korean Invasion: Why Defending South Korea Is Easier than the Pentagon Thinks," *International Security* 22, no. 4 (spring 1998): 135–70; and Stuart K. Masaki, "The Korean Question: Assessing the Military Balance," *Security Studies* 4, no. 2 (winter 1994/95): 365–425.

95. The conventional balance on the Central Front between NATO and Warsaw Pact forces in Europe was a very important topic during the cold war, especially in the middle and late 1980s. Advocates of a favorable balance include John J. Mearsheimer, "Numbers, Strategy, and the European Balance," *International Security* 12, no. 4 (spring 1988): 174–85; and Barry R. Posen, "Is NATO Decisively Outnumbered?" *International Security* 12, no. 4 (spring 1988): 186–202. For a pessimistic assessment see Eliot A. Cohen, "Toward Better Net Assessment: Rethinking the European Conventional Balance," *International Security* 13, no. 1 (summer 1988): 50–89. A second debate occurred over the proper metric to measure the balance. On this see John J. Mearsheimer, "Assessing the Conventional Balance: The 3:1 Rule and Its Critics," *International Security* 13, no. 4 (spring 1989): 54–89; and Joshua M. Epstein, "The 3:1 Rule, the Adaptive Dynamic Model, and the Future of Security Studies," *International Security* 13, no. 4 (spring 1989): 90–127.

strategies."[96] As long as only the United States has information warfare capabilities, it can defeat enemies quickly and decisively using all three strategies. The United States will be able to defeat a limited-aims attack which requires that the attacker seize a portion of the defender's territory. This will be difficult when the defender's battlefield transparency allows it to detect mobilization for the attack, and break up the attack as it occurs.[97]

An attrition strategy will not be a viable option for an attacker facing the United States. This strategy requires concentration in order to advance, like a steamroller, over the defender. "Rout and retreat alternate, eventually wearing down the defense. Little emphasis is placed on achieving the battlefield equivalent of a knockout punch. Instead, victory follows from a series of set-piece battles and is not expected to be quick."[98] An attrition strategy will be defeated because, again, IW can detect and defeat attacks in detail, quickly and rapidly.

The ability of a defender armed with information warfare capabilities to defeat a blitzkrieg is robust. A blitzkrieg requires that the attacker concentrate his forces in depth, then fight the breakthrough battle, and finally effect a strategic penetration that severs the defender's lines of communication and command and control network.[99] Again, with IW capabilities, the United States can detect concentration and the attacker will be very vulnerable to interdiction that likely will destroy the attacking forces. As a result, the expansion of NATO may or may not be sound diplomacy or in the grand strategic interests of the United States, but its information warfare capabilities make the conventional deterrent of NATO credible and relatively easy to obtain.[100]

My analysis has shown that information warfare technology will not make the world safe for nuclear or conventional war between great powers. The fundamental political logic that obtains among nuclear states is still present and so the incentives for restraint in order to prevent escalation still exist. Thus, the paradigm of war has not changed for nuclear-armed great powers, and it still takes place within the context and limitations of a nuclear world.

96. Mearsheimer, *Conventional Deterrence*, 29.

97. In such a circumstance, the defender would also have the option of preempting an attack.

98. Mearsheimer, *Conventional Deterrence*, 34.

99. Ibid., 36.

100. Simply because the United States has the ability to defeat these strategies, however, does not mean that new strategies cannot be developed to offset U.S. capabilities. As Jonathan Shimshoni has shown, a military entrepreneur can almost always create a relative advantage over an opponent. Shimshoni, "Technology, Military Advantage, and World War I: A Case for Military Entrepreneurship," *International Security* 15, no. 3 (winter 1990/91): 187–215.

CONFLICT BETWEEN A GREAT POWER AND A NONNUCLEAR SMALL STATE: INCREASING ALREADY CONSIDERABLE U.S. MILITARY ADVANTAGES

Information warfare provides the United States with two advantages in its relations with the small, nonnuclear states of the Third World: it makes winning a conflict with such a state easier, and increases the capabilities of the United States to intervene in the Third World.[101]

U.S. advantages in information warfare capability simply amplify the already prodigious advantages that accrue to the United States when it fights an adversary like Iraq or Libya whose Gross Domestic Product (GDP) is approximately one-tenth the size of the U.S. defense budget.[102] Such overwhelming U.S. superiority makes it difficult to determine the added value of information warfare to U.S. military capabilities in these circumstances. Clearly, in such conflicts the United States possesses escalation dominance with conventional weaponry, and it alone possesses nuclear weapons so there is almost no risk of inadvertent escalation. The principal effect of information warfare is that it will lower the cost of war for the United States and increase the rapidity with which the United States is able to win.

While IW capabilities may enhance U.S. ability to win a war with such a state, they do not guarantee such a result. Even a state as powerful as the United States, armed with information warfare capabilities, can lose a war with a small power. As the United States learned in the Vietnam War, when it is faced with an enemy willing to pay much higher costs to prosecute the war, the potential exists for a U.S. defeat. Napoleon's adage still applies in the age of information warfare: the morale is to the matériel as three is to one.

Nevertheless, the ability of the United States to intervene in the Third World is augmented by information warfare. U.S. interventions in the Third World have greatly increased in the wake of the cold war.[103] It helped suppress an attempted coup d'etat in the Philippines in December 1989, then immediately intervened in Panama, maintained "no-fly" zones in northern and southern Iraq, and intervened

101. The assumption here is that these states do not have biological weapons capabilities, which can be as deadly to an unprotected population as nuclear weapons.

102. The U.S. defense budget was about $267 billion in 1998. Iraq's GDP in 1997 is estimated to be $17 billion, Libya's $27 billion, and North Korea's $18 billion. IISS, *The Military Balance 1998/99* (London: Oxford University Press, 1998), 15, 128, 134, 185.

103. For recent publications on this debate see Richard K. Betts, "The Delusion of Impartial Intervention," *Foreign Affairs,* 73, no. 6 (November/December 1994): 20–33; David Fisher, "The Ethics of Intervention," *Survival,* 36, no. 1 (spring 1994): 51–59; Richard N. Haass, *Intervention: The Use of American Military Force in the Post–Cold War World* (New York: Carnegie Endowment, 1994); Stanley Hoffman, "The Politics and Ethics of Military Intervention," *Survival,* 37, no. 4 (winter 1995/96): 29–51; Samuel P. Huntington, "Playing to Win," *The National Interest,* no. 3 (spring 1986): 8–16; Michael Mandelbaum, "The Reluctance to Intervene," *Foreign Policy,* no. 95 (summer 1994): 3–18; Charles William Maynes, "Containing Ethnic Conflict," *Foreign Policy,* no. 90 (spring 1993): 3–21; Barry R. Posen, "Military Responses to Refugee Disasters," *International Security,* 21, no. 1 (summer 1996): 72–111; and Tony Smith, "In Defense of Intervention," *Foreign Affairs,* 73, no. 6 (November/December 1994): 34–46. An excellent examination of this problem remains Hans J. Morgenthau, "To Intervene or Not to Intervene," *Foreign Affairs* 45, no. 3 (April 1967): 425–36.

in Somalia, Haiti, Liberia, Bosnia, and Kosovo. Information warfare will increase U.S. ability to intervene abroad.[104] It will not, however, necessarily affect Washington's willingness to do so, because that consideration is influenced by more than military capability. Clearly, political considerations should be central in such a decision.[105] In order to determine how information warfare will augment intervention, the criteria of successful intervention must be defined.

Samuel Huntington sees five criteria for intervention. First, it should be as brief as possible; second, the operational plans of the intervention should emphasize the offensive; third, high technology should be exploited to serve these ends; fourth, overwhelming force should be used; and fifth, military force should be used to achieve goals for which it is suited.[106]

If intervention is governed by these criteria, information warfare will improve U.S. ability to intervene. Used against an opponent not similarly equipped, information warfare will meet all the military requirements of Huntington's criteria: it will emphasize the offensive, obviously use high technology, and permit the use of overwhelming force. Furthermore, information warfare capabilities should, first, reduce the number of casualties incurred by the United States in an intervention. The war of NATO against Yugoslavia in 1999 was strongly influenced by the Clinton administration's desire to minimize U.S. casualties.[107] It is probable that U.S. decisionmakers will possess a similar desire in interventions where less than vital interests of the United States are threatened. Information warfare capabilities should, ceteris paribus, reduce U.S. casualties due to the knowledge of where the enemy is and the ability to confuse and destroy him.

Second, information warfare will be a force multiplier for U.S. forces enabling—again, the ceteris paribus caveat is necessary—a smaller sized U.S. force to accomplish the mission which, at present, would require a larger size force. This should also contribute to reducing the number of U.S. casualties as well since there will be fewer U.S. soldiers, sailors, and airmen put at risk. More importantly, those put at risk, particularly in the opening days of an intervention, will have sufficient firepower to address the threats faced. IW reduces the danger that the United States will have insufficient firepower, as in Somalia when the death of eighteen U.S.

104. As long as the United States is the world's sole superpower, the international system will pose few constraints on U.S. intervention. This is unlike the cold war, when the United States could not intervene at will due to Soviet power.

105. Even domestic political considerations are important. Clearly, a major reason the United States intervened in Haiti was to stop the flow of Haitian immigrants into Florida, an important state in U.S. domestic politics.

106. Huntington, "Playing to Win," 15. Haass develops similar criteria: intervention is better done sooner than later; too much force is better than too little; and decisive early use of force is better than gradual escalation. Haass, *Intervention*, 87–100.

107. See "The Victors of Kosovo," *Economist,* 12 June 1999, 23–24; Bradley Graham, "War without 'Sacrifice' Worries Warriors," *Washington Post,* 29 June 1999, A12; and Craig R. Whitney, "Air Wars Won't Stay Risk Free, General Says," *New York Times,* 18 June 1999, A16.

soldiers and the wounding of seventy-seven in a firefight led to the decision to withdraw.[108]

Third, although sophisticated weaponry has proliferated in the Third World, information warfare should allow the U.S. military to offset any relative advantage in weaponry. Third World arsenals have grown to include many sophisticated air-, ground-, and naval-combat weapon systems that these states have purchased, largely from China, Russia, and Ukraine, or developed indigenously. Were it not for increased U.S. military capabilities provided by IW, the United States would face greater resistance in intervention and very likely greater casualties. Thus, information warfare should increase the chance of successful interventions as judged by military criteria.[109]

It cannot guarantee successful intervention, however, because military capabilities do not inform Huntington's fifth criterion. The objective of the intervention must be one that is appropriate for the military and not one that would be better accomplished using diplomatic or economic means. It is the responsibility of political decisionmakers to ensure that this is so, and not something that information warfare can influence.

Information warfare does make such wars and interventions more likely by making them less costly, but it is difficult to disentangle the effects of information warfare advantages from the effects of sheer military superiority in a world where the United States is at least temporarily hegemonic. One result of such power, when augmented by IW capabilities, is that states which perceive themselves threatened by the United States, could choose to pursue nuclear weapons. This adds to the likelihood of the third type of conflict.

108. For an analysis of U.S. involvement in Somalia see Chester A. Crocker, "The Lessons of Somalia," *Foreign Affairs* 74, no. 3 (May/June 1995): 2–8; Jonathan T. Howe, "The United States and United Nations in Somalia: The Limits of Involvement," *Washington Quarterly* 18, no. 3 (summer 1995): 49–62; Terrence Lyons and Ahmed I. Samatar, *Somalia: State Collapse, Multilateral Intervention, and Strategies for Political Reconstruction* (Washington, D.C.: Brookings, 1995); and Jonathan Stevenson, *Losing Mogadishu: Testing U.S. Policy in Somalia* (Annapolis, Md.: Naval Institute Press, 1995).

109. Information warfare is not a panacea, however. It cannot compensate for underestimating the enemy, as in Vietnam or Somalia when the use of the same tactics, quickly identified by the Somalis, contributed to the 3 October 1993 disaster. As one Somali commander, Colonel Ali Aden, who fought U.S. forces at that battle said, "If you use one tactic once, you should not use it a third time. And the Americans had already done basically the same thing six times" (quoted in Stevenson, *Losing Mogadishu*, 94). A detailed account of the raid is found in Mark Bowden, *Black Hawk Down: A Story of Modern War* (New York: Atlantic Monthly Press, 1999).

CONFLICT BETWEEN THE UNITED STATES AND A NUCLEAR THRESHOLD STATE: THE DANGERS OF INFORMATION WARFARE

The third type of potential conflict would be between the United States and a nuclear threshold state such as Iraq, North Korea, or Iran in the near future.[110] In this type of conflict we again see both the benefits and the dangers of information warfare. IW undeniably increases the technical ability of the United States to counter small nuclear forces, but does not increase the willingness of U.S. leaders to run the risk of a nuclear or biological attack against the United States in a conflict over less than vital interests with a threshold nuclear power.[111] An analysis of this problem will explain why the military balance favors the United States, but U.S. advantages are offset by the balance of resolve that is likely to favor the emerging nuclear state, as well as the risk of nuclear inadvertence. As a result, the United States is likely to take steps to avoid a crisis or conflict by deterring these states. If deterrence were to fail, the United States should limit its aims in the conflict in order to avoid a situation where the nuclear state faces annihilation, thus removing any restraint on the use of nuclear or biological weapons.

The military balance between the United States and a nuclear threshold state overwhelmingly supports the U.S. IW capabilities make the U.S. military even stronger and were the conflict solely conventional it could expect to prevail just as in the case of nonnuclear small states. This is because in a confrontation with the United States, threshold nuclear states are vulnerable to U.S. attack. Such states do not have a secure second-strike capability because they have vulnerable nuclear forces, as defined by the number of weapons and survivable delivery vehicles, and vulnerable command and control systems.

110. As the tests in May 1998 reveal, India and Pakistan have small nuclear arsenals and Israel does as well. North Korea may have a few nuclear weapons. Iraq would likely have acquired nuclear weapons had the Gulf War not occurred. Iran is widely believed to be seeking nuclear capability. At the end of 1995 India had 315–45 kilograms (kgs.) of weapon-grade plutonium. Assuming that each weapon would use 5 kgs. of this plutonium, it has enough for as many as 69 nuclear weapons. India clearly has both fission and fusion nuclear weapons, as the tests of May 1998 revealed. By early 1995, it is estimated that Iraq would have had 34 kgs. of Highly Enriched Uranium (HEU). This is enough for a simple fission weapon assuming that about 20 kgs. of HEU is needed. It could have had two by 1996, and enough for almost twenty by 2000. By 1994, Israel is estimated to have anywhere from 190 kgs. to 880 kgs. of weapon-grade plutonium and 38 to 176 warheads. In addition, Israel may have tritium-boosted fissile weapons. As of the end of 1991, Pakistan is estimated to have 157–263 kgs. of HEU, and as many as 12 nuclear weapons. It probably does not have fusion weapons, or it would have tested the design, as India did in the 1998 tests. North Korea has 25–30 kgs. of weapon-grade plutonium, so it may have as many as five or six nuclear weapons. See David Albright, Frans Berkhout, and William Walker, *Plutonium and Highly Enriched Uranium, 1996: World Inventories, Capabilities and Policies* (New York: Oxford University Press, 1997), for India, 268–69; Iraq, 341–42; Israel, 262; Pakistan, 276–77; North Korea, 306–7.

111. Biological weapons are potent weapons particularly in an era of genetic engineering. They can kill as many people as nuclear weapons. For an analysis of the increasing threat from biological weapons see Richard A. Falkenrath, Robert Newman, and Bradley A. Thayer, *America's Achilles' Heel: Nuclear, Biological, and Chemical Weapons and Covert Attack* (Cambridge, Mass.: MIT Press, 1998), 97–165.

Iraq's delivery systems, aircraft and missiles, for example, were severely damaged by the Gulf War and subsequent United Nations Special Commission (UNSCOM) inspections.[112] As a result, it will be some time before Iraq completely rebuilds its military forces and nuclear and biological programs, although we can be sure it will happen. Iraqi scientists, engineers, and military officers retain their knowledge, and nothing so far has stopped Saddam Hussein in his effort to acquire Weapons of Mass Destruction (WMD)—nuclear, biological, and chemical weapons. Iran possesses many missiles and aircraft capable of delivering nuclear or biological weapons, including Su-24s, F-14s, and MiG-29s.[113] In addition, it is suspected of seeking to develop a missile capability including intermediate-range ballistic missiles.[114] North Korea also has many bombers, attack aircraft, and missiles that would be able to deliver a nuclear or biological weapon.

These delivery systems are vulnerable to attack and destruction by the U.S. Aircraft and missiles launched from a fixed platform are targets that the United States can destroy relatively easily, as the Gulf War demonstrated. Threshold states have found and used one solution to the problem of force vulnerability to offset U.S. advantages: mobile launchers. The United States had great difficulty during the Gulf War destroying Iraq's mobile SCUD launchers.[115] It is very difficult to find few mobile targets in a large area, especially when the enemy's employment tactics include the use of high-fidelity decoys. This problem will be reduced but probably will not disappear with the greater surveillance capabilities provided by information warfare: while U.S. capabilities will evolve, so too will the fidelity of the decoys.[116] Notwithstanding the advantages of mobility, the missiles and aircraft of a threshold

112. Iraq has an estimated six bombers and about 130 attack aircraft (some may be able to carry nuclear or biological weapons) that survived the war in addition to twenty-seven missiles. IISS, *The Military Balance 1998/99*, 128–29.

113. IISS, *The Military Balance 1998/99*, 128.

114. Steven Erlanger, "U.S. Gets Russia's Firm Vow to Halt Missile Aid to Iran," *New York Times*, 16 January 1998, A8. The missiles reportedly have a range of 700 to 1,200 miles enabling them to hit targets in Western Europe, North Africa, and South Asia. Thomas W. Lippman, "Israel Presses U.S. to Sanction Russian Missile Firms Aiding Iran," *Washington Post*, 25 September 1997, A31.

115. Keaney and Cohen report that Iraq had about thirty mobile launchers at the start of the war, none of which were destroyed. They conclude that "Coalition air power does not appear to have been very effective against this militarily insignificant target category" (Keaney and Cohen, *The Gulf War Air Power Survey Summary Report*, 78–90, quote on 90). For a thoughtful illumination of how to execute a successful "Scud hunt," see James J. Wirtz, *Counterforce and Theater Missile Defense: Can the Army Use an ASW Approach to the Scud Hunt?* (Carlisle Barracks, Pa.: Strategic Studies Institute, U.S. Army War College, 1995).

116. Where such a race ends ultimately is difficult to foresee. Decoys may have to improve in their mimicry of actual launchers across a variety of conditions and spectra, for example matching the optical, infrared, and radar signatures, but this is relatively easy to accomplish. The preliminary data on Operation Allied Force indicate that decoys are still a great problem. It appears that NATO forces dropped 3,000 guided weapons that resulted in the destruction of 500 decoys but only fifty Yugoslav tanks. See David A. Fulghum, "Pentagon Dissecting Kosovo Combat Data," *Aviation Week and Space Technology*, 26 July 1999, 68–69.

state are vulnerable, and the threshold state cannot be certain how much of the force would survive U.S. attack.

The command and control systems of threshold states are vulnerable, given U.S. capabilities, to detection, manipulation, and destruction. The United States has considerable ability to detect command and control nodes through its ground-, air-, and space-based electronic and signals intelligence sensors.[117] Threshold states have an early warning network of radars, but some offer only incomplete coverage and cannot currently counter the stealth technology of the B-2. Nor can they reliably detect low-flying cruise missiles like the Tomahawk or the stealthy advanced cruise missile. The command and control may also be manipulated by offensive information operations. Yugoslavia's computer systems, for example, were attacked during the war in 1999. False radar images were introduced into the system to protect attacking NATO aircraft.[118] Manipulation of the enemy's command and control system through offense information operations could contribute to the immobilization or destruction of the state's command and control network. In sum, the United States can hit the known command and control centers of these states almost simultaneously; this capability will only grow as information warfare capabilities continue to develop, perhaps even to the point where physical destruction is not necessary.

Nonetheless, complete decapitation—separation of a state's national command authority from the forces tasked with executing nuclear or biological retaliation against the United States or an ally—is very difficult to accomplish even with information warfare capabilities. This is because these states may take relatively simple countermeasures to minimize the chances of a successful attack. A prudent assumption is that threshold states will plan to execute an attack against a U.S. ally such as Saudi Arabia, Israel, Japan, or South Korea, as well as against U.S. cities, in order to deter the United States. It is also reasonable to expect that threshold states know, given U.S. superiority, that their aircraft and missiles are vulnerable and so are not reliable delivery systems for either a nuclear or a biological weapon. Even under these conditions, however, they can deliver a nuclear or biological weapon against the United States or a U.S. ally.

117. Examples are Rivet Joint aircraft which monitor communications and locate radars and command and control centers; Compass Call and Commando Solo aircraft which can monitor, jam, and alter communications by inserting false messages; and electronic and signals intelligence satellites like Orion and Trumpet. Robert Wall, "EC-130Hs Blanket Serb Communications," *Aviation Week and Space Technology*, 3 May 1999, 30.

118. David A. Fulghum, "Yugoslavia Successfully Attacked by Computers," *Aviation Week and Space Technology*, 23 August 1999, 31, 34. Fulghum notes that there are restrictions on offensive information operations governed, in part, by concern that attacks may spill over and affect communications and banking in countries other than the one attacked. Fulghum, "Yugoslavia Successfully Attacked by Computers," 34. William Arkin argues that "cyberwar" did not aid the campaign in any significant manner. William M. Arkin, "A Mouse That Roars?" *Washington Post*, 7 June 1999, http://www.washingtonpost.com/wp-srv/national/dotmil/ arkin.htm.

To execute such a plan they would have to rely on small groups of dedicated and trusted agents, probably isolated from any known military base and possessing one or more nuclear or biological weapons.[119] The plan of the threshold state would include delineating the exact conditions under which a group of agents would undertake such a mission, including the conditions under which an attack is to be called off. Such a plan to reduce the risk of decapitation entails other risks and dangers for the threshold state but it would probably incur these risks to ensure the ability to retaliate.[120]

It is easy to imagine a crisis or war scenario where a nuclear or biological weapon could be used against the United States or a U.S. ally. On the eve of a future conflict with North Korea, for example, the North Koreans might deem it prudent to move some or all of their small nuclear arsenal, or biological weapons, out to sea on a trawler. The trawler would be insignificant against the volume of the sea and other maritime traffic. It might be instructed to sail under a false flag to Japan or China, where the nuclear or biological weapons could be transferred to a plane or ship bound for the United States, where in the event of war, or during a war, the nuclear weapon(s) could be detonated, or the biological weapons disseminated. In addition, especially if the timing seemed urgent, it would not be implausible for the North Koreans to decide to ship biological weapons from China or Japan to agents in the United States via an overnight delivery company.

The increased U.S. capability provided by information warfare would allow the United States to use conventional weapons to destroy quickly and with great certainty more of the state's nuclear forces and to weaken its nuclear command and control system. In a narrow, military sense, then the United States has escalation dominance—it would prevail at any level of conflict from a conventional to a nuclear exchange. U.S. information warfare capabilities are formidable, yet cannot guarantee the decapitation of the command and control system or the complete destruction of the arsenal. So, despite great military advantage, in a political sense the United States does not possess escalation dominance because escalation invites

119. Of course, no such group may exist, but the United States could never be sure and U.S. decisionmakers would always be aware of the possibility.

120. The steps threshold states may take to reduce the risk of decapitation are not perfect. In general, however, such steps may be the least bad alternative that these states face. In their nuclear command and control, all states must balance between concerning the tradeoffs between positive and negative control, the so-called always/never dilemma. That is, nuclear weapons must always work when directed by a state's decisionmakers and never when they are not. States must worry about unauthorized use ("never") but also about decapitation ("always"). A threshold state may run the risk of unauthorized use to ensure its ability to retaliate. Peter D. Feaver describes the "always/never" dilemma and many characteristics of the command and control systems of threshold states: "The Command and Control of Emerging Nuclear Nations," *International Security* 17, no. 2 (winter 1992/93): 160–87. For a thoughtful analysis of the advantages and risks for stability that the command and control systems of minor nuclear states may have, see Jordan Seng, "Command and Control Advantages of Minor Nuclear States," *Security Studies* 6, no. 4 (summer 1997): 50–92; and Peter D. Feaver, "Neooptimists and Proliferation's Enduring Problems," *Security Studies* 6, no. 4 (summer 1997): 93–125.

retaliation against the United States itself, incurring a cost to the United States that would not be worth the benefit.

Moreover, the threshold state would probably possess the balance of resolve and thus have the incentive to escalate. In a crisis or war the balance of resolve—the willingness to absorb punishment in pursuit of a political objective—is more likely to favor the small nuclear state than the United States.[121] The actual circumstances of a crisis will determine this balance, but, in general, the will of the threshold nuclear state defending its sovereignty and survival is greater than the will of the United States to conquer or punish that state. As a result, a threshold state will be able to threaten, credibly, the United States or a U.S. ally because both sides in the deterrent relationship know that the issue is of greater concern to the threshold state, and that it is willing to pay a higher price and incur greater risks for the political goal. This fundamental political logic of deterrence will not be overturned by information warfare because the U.S. military will not be able to guarantee the destruction of the other state's nuclear or biological weapons capability. The United States underestimates the will of a threshold state in a crisis or war only at its peril.

The balance of resolve is not the only factor at work in a confrontation between the United States and a threshold state. The possibility of inadvertent escalation makes a successful limited strike very risky for the United States. The logic demonstrated above with respect to the U.S.-Russian relationship also applies here. The United States is not likely to prevent a conventional war from escalating to the nuclear or biological level because a conventional war with the United States would make a threshold state less confident about its modest assured destruction capability.[122] The United States would direct its conventional attacks at whatever nuclear forces, delivery systems, command and control, and early warning systems exist in these states—which risks provoking a strong reaction from the threshold state.[123] As discussed above, Posen demonstrates that wherever the conventional forces of two nuclear states interact, they risk inadvertent escalation. Thus, the United States may not intend to provoke the use of nuclear or biological weapons, but it could be the result.

Thus, in this third scenario we see a lack of escalation dominance, asymmetry in the balance of resolve, and the risk of inadvertent escalation. Considering these factors, the fundamental question again arises: Will the increased capabilities provide sufficient assurance to U.S. political leaders that the political goal is worth the risk of retaliation against the United States itself? This stubborn fact of the nuclear age will hinder the United States in its interactions with emerging nuclear states as it does with nuclear great powers. This prospect alone might deter the

121. On the importance of the balance of resolve in deterrent relationships see Shai Feldman, *Israeli Nuclear Deterrence: A Strategy for the 1980s* (New York: Columbia University Press, 1982), 30–31.

122. Posen, *Inadvertent Escalation*, 2.

123. Ibid., 3.

United States from engaging in any conflict with such a state, thus rendering moot any advantage it gains from IW capabilities.[124]

The United States is unlikely to attack these states because the risk of retaliation against the United States, or a U.S. ally, is too great to warrant an attack. If a conflict were inevitable with one of these states, however, then the advantages provided by information warfare would benefit the United States, giving it potent damage limitation capabilities. By striking first at the state's nuclear forces or command and control centers, the United States would greatly reduce the state's nuclear forces.[125] In fact, these capabilities may make U.S. involvement more likely: they would permit a dangerous but strong argument to be made that the nuclear capabilities of the state may be destroyed in a first strike, and thus would pose no, or an acceptable, danger to the United States or its allies. This is not the only factor that weakens crisis stability. In the event of a crisis, the emerging nuclear state will have an incentive to use its small nuclear force quickly or risk its destruction. This logic augments the danger of inadvertent escalation described above.

In sum, these crises have the potential to be very dangerous and unstable due to the vulnerable forces and command and control forces of threshold states which yield no escalation dominance, an incongruence in the balance of resolve, and the risk of both inadvertent escalation and crisis instability. The best solution for the United States, obviously, is to accomplish its foreign policy objective while avoiding a crisis or war. This may be done by a conventional buildup of U.S. and allied forces, creating what Posen terms "little NATOs," to permit a robust conventional deterrent backed by U.S. nuclear forces.[126] A second solution would be to change U.S. grand strategy. The United States would declare that it is no longer willing to defend the Gulf, or South Korea and disengage from the world to minimize its chances of becoming the object of an attack.[127]

For the purposes of this analysis, the assumption will be made that the United States does become involved in a crisis or war with a threshold state. To prevent an attack on itself or an ally, the United States should strive to keep such conflicts conventional by limiting its war aims, and through deterrence.[128] Neither of these

124. Barry Posen makes this argument in "U.S. Security Policy in a Nuclear-Armed World (Or What If Iraq Had Had Nuclear Weapons?)," *Security Studies* 6, no. 3 (spring 1997): 1–31.

125. Of course, the very vulnerability of a nonestablished nuclear state's capability in the face of U.S. capabilities may threaten crisis stability. Given its weakness, it has strong incentive to strike first: to use its nuclear weapons or lose them.

126. Posen, "U.S. Security Policy in a Nuclear Armed World," 11.

127. Posen also suggests this possibility in "U.S. Security Policy in a Nuclear-Armed World," 12–13. For the argument that the United States should disengage from the world see Gholz, Press, and Sapolsky, "Come Home, America."

128. A third option would be to pursue strategic and tactical missile defenses. Such defenses make sense to defend our allies like Saudi Arabia and South Korea, but it is currently unlikely that a threshold state would use a ballistic missile in an attack on the United States: they lack the capability and covert delivery would be easier.

policies is a perfect solution, but individually or in combination, they minimize the risk of a nuclear or biological attack on the United States or its allies.

To prevent a crisis from escalating to war, or a conventional war from escalating to the use of nuclear or biological weapons, the United States should be explicit about its aims in crisis or war and state that its aims are limited. That is, the United States does not seek the overthrow of the regime in the threshold state. Clearly, the United States has the capability to remove any regime in a threshold state from power. A lesson of deterrence theory, however, reinforced by prospect theory in psychology, is that for deterrence to obtain the leadership on both sides must value the future.[129] So, if the United States were to try to remove a regime from power, that regime might believe that it had no future and would attack the United States or an allied state with nuclear or biological weapons.[130] Declaration of a limited aims policy is not a panacea, but it can help reduce this risk.

In addition, the United States does have a robust conventional and nuclear deterrent capability that should not be underestimated, and the U.S. victory in the Gulf War demonstrated how effective the U.S. military can be. It is reasonable to expect that threshold states recognize this reality and would avoid conflicts of interest with U.S. regional interests that might result in crisis or war, since they have no interest in risking their state's survival. It is incumbent upon the United States, however, to be explicit about its strategic interests around the world so that all states, both friend and foe, know what they are.[131]

Despite significant U.S. capabilities, a crisis or war with a threshold nuclear state is dangerous for all states concerned. U.S. information warfare capabilities do not lower the risk to the United States or its allies because such a confrontation is inherently risky and unpredictable: the United States will not have escalation dominance, the balance of resolve will favor the threshold state, and the risk of inadvertent escalation will be present. As a result, the United States must proceed with caution. The capabilities that information warfare provides the U.S. military are, in these circumstances, no substitute for skilled and judicious statecraft.

129. For discussions of prospect theory see Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica* 47, no. 2 (March 1979): 263–91; and Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982). Also see Jack S. Levy, "Prospect Theory and International Relations: Theoretical Applications and Analytical Problems," in *Avoiding Losses/Taking Risks: Prospect Theory and International Conflict*, ed. Barbara Farnham (Ann Arbor: University of Michigan Press, 1994), 119–46.

130. The logic of this condition is analyzed in Barbara Farnham, *Roosevelt and the Munich Crisis: A Study of Political Decision-Making* (Princeton: Princeton University Press, 1997); and Kenneth Watman, Dean Wilkening, with John Arquilla, Brian Nichiporuk, *U.S. Regional Deterrence Strategies* (Santa Monica, Calif.: RAND, 1995).

131. The United States does its utmost to avoid the situation that arose in July 1990, when U.S. actions intended to deter Saddam Hussein were confused and contradictory. See Janice Gross Stein, "Deterrence and Compellence in the Gulf, 1990–91: A Failed or Impossible Task?" *International Security* 17, no. 2 (fall 1992): 147–79.

CONCLUSION: UNINTENDED CONSEQUENCES AND OLD DANGERS

THE CAPABILITIES that information warfare will provide the United States are impressive. Being more maneuverable and decentralized, knowing what is happening on the other side of the hill, using information systems to spy upon or deceive the enemy, and being able to manipulate through offensive information operations or destroy the enemy with precision strikes in any weather, are clearly powerful advantages. Information warfare promises to increase the U.S. military's ability to deter attacks with conventional weapons, to fight conventional wars, especially against nonnuclear small states, and to intervene successfully in the Third World. Information warfare, however, is a double-edged sword. While it introduces new capabilities, it may produce some unintended consequences, and it does not redress the dangers inherent in a nuclear world.

UNINTENDED CONSEQUENCES

Two consequences of information have received too little attention. First, as predicted by neorealist theory, the greater the U.S. military capability produced by information warfare, the greater the perception, held by many great powers and small states, of the United States as a threat. Second, IW will increase the gap in fighting capabilities between the United States and its allies, making them less effective military partners and thus reducing their influence on U.S. policies.[132]

Why IW increases the perception of the United States as greater threat. The neorealist theory of international politics expects that states, in an anarchic international system, will balance against threats.[133] What causes threat? Neorealists differ over this question. Kenneth Waltz sees threat as principally a function of military capability, while Stephen Walt says it results from aggregate power, geographic proximity, offensive power, capabilities, and aggressive intentions. As I have shown above, information warfare increases U.S. offensive military capabilities. So by either standard, information warfare makes the United States a greater threat.

In addition to neorealist theory, history also demonstrates that states are particularly threatened when one greatly increases its military capability relatively quickly because such sharp changes in relative power have important implications for security. States will take action to counter the military capability of rival powers:

132. Another potential unintended consequence is hubris among U.S. political and military leaders generated by undue optimism in the benefits of information warfare. Too much emphasis on technological solutions was a major reason the United States lost the war in Vietnam. At root, warfare remains an interactive contest of will. Information warfare will improve the capabilities of the United States, but cannot redeem flawed strategies. Nor can it substitute for careful strategic thinking by U.S. decisionmakers. Information warfare cannot save U.S. decisionmakers from themselves.

133. Christopher Layne, "The Unipolar Illusion: Why New Great Powers Will Rise," *International Security* 17, no. 4 (spring 1993): 5–51; Waltz, *Theory of International Politics*, 125–27; and Stephen M. Walt, *The Origins of Alliances* (Ithaca: Cornell University Press, 1987), 17–33.

consider, for example, the transformation of the Prussian army from a Frederickian to a mass army after its defeat by Napoleon, the naval arms race before the First World War spawned by Britain's *Dreadnought*, and the Soviet race to acquire atomic weapons after 1945.

Using neorealist theory and history as guides, I expect that great powers such as Russia and China will seek to balance against the United States. A Sino-Russian alliance is one possibility, and was widely discussed during and shortly after Operation Allied Force, but will more likely strive to match U.S. capabilities, given their divergent interests and the many disputes that each has with the other.[134] As they cannot surpass the information warfare capability of the United States in the near future, I expect them to balance the United States in the only way they can, through their nuclear forces, because information warfare does not trump the nuclear revolution.[135] I expect these states will jealously guard their nuclear capability in the short run, while striving to match the information warfare capabilities of the United States in the future.[136] In fact, this is occurring. The Joint

134. Since Chinese president Jiang Zemin visited Russia in April 1996, Sino-Russian relations have warmed. The joint statement released at a Jiang–Yeltsin meeting in April 1997 stated that "no country should seek hegemony, practice power politics or monopolize international affairs," and both agreed on the need for a "multipolar world." Michael Gordon, "Russia-China Theme: Contain the West," *New York Times*, 24 April 1997, A3. Russian president Boris Yeltsin was quoted as saying "Someone is longing for a single-polar world. He wants to decide things himself" (Chrystia Freeland, "Jiang and Yeltsin Warn on U.S. Hegemony," *Financial Times*, 24 April 1997, 6). Also see Lee Hockstader, "Russia, China Sign New Friendship Pact," *Washington Post*, 24 April 1997, A1. The war with Yugoslavia caused such statements to be made with a certain regularity. Jiang has accused the United States of conducting "gunboat diplomacy and economic neo-colonialism". See Ted Bardacke and James Kynge, "China: Beijing Lashes Out at U.S. 'Gunboat Diplomacy,'" *Financial Times*, 4 September 1999, http://www.ft.com/hippocamus/q14d766.htm; and John Pomfret, "China Ponders New Rules of 'Unrestricted War'," *Washington Post*, 8 August 1999, A1. Yeltsin said at a Sino-Russian summit in Bishkek, Kyrgyzstan that he was "in fighting form, ready for battle, especially with westerners" (Charles Clover, "Yeltsin and Jiang Attack U.S. Hegemony," *Financial Times*, 26 August 1999, 6). Despite such rhetoric for an insightful analysis of Sino-Russian relations that recognizes the significant difficulties in Sino-Russian relations see Jennifer Anderson, *The Limits of Sino Russian Strategic Partnership*, Adelphi Paper no. 315 (London: IISS, 1997). Nor is a Sino-Russian alliance the only possibility. France, Germany, and Russia will meet in the first half of 1998 in Yekaterinburg to create a relationship that Moscow hopes will counterbalance the United States. See "Russia, Germany and France to Meet in '98," *New York Times*, 1 December 1997, A8; and Susanne Hoell, "Russia Bolsters European Ties with Plans for 3-Power Summit," *Washington Times*, 1 December 1997, 15.

135. At this time, it is impossible to tell if these states will be able to leapfrog the United States in the future, to use information warfare to offset U.S. military advantage. An appropriate example is the British development of the tank in the First World War; shortly thereafter J. F. C. Fuller conceived many of the fundamental ideas of armored warfare, but it was the Germans who used the ideas most effectively in the Blitzkrieg.

136. With the United States the world leader in computer technology, computer software, and information processing technology, it may seem odd to see information warfare as a genie, released by the United States and creating new dangers for it. In the future, other states may be better able than the United States to use the military capabilities IW provides, as late industrialization permitted Germany to surpass Britain, and to use those capabilities against U.S. interests. On the advantages of being in a subsequent wave of a technological change see Alexander Gerschenkron, *Economic Backwardness in Historical Perspective* (Cambridge, Mass.: Belknap Press of Harvard University, 1962). How quickly states will acquire information warfare capabilities is a complex question, beyond the scope of this article, but

Intelligence Committee, a forum comprised of intelligence officials from the United States, Britain, Canada, and Australia wrote in an October 1997 report which was leaked to the *Washington Times*, that the Russians are relying more heavily on nuclear weapons as they cut their conventional forces.[137]

Neorealists expect that great powers will react this way, but small states will react too. They may voice their displeasure with the United States as former South African president Nelson Mandela did when he denounced U.S. efforts to isolate Libya: "How can [the United States] have the arrogance to dictate to us where we should go or which countries should be our friends?We cannot accept that a state assumes the role of world policeman."[138] Small states have a second way to react: acquire WMD to offset U.S. power and interference. As a retired chief of staff of the Indian Army is reported to have argued, the lesson of the Gulf War is that if you want to fight the Americans you must have nuclear weapons.[139]

This is not to claim that the tendency of great powers or small states to balance power cannot be offset by clever U.S. diplomacy, or by the necessity of aligning with the United States to offset other, greater threats. It is only to recognize that the United States may be perceived as a greater threat due to its increased military capabilities. U.S. political leaders in particular must be sensitive to this perception, so that U.S. diplomacy can counteract it as it does arise.

Information warfare and U.S. allies. Information warfare will affect alliance politics as well. To be effective, U.S. allies need to be able to "plug in" to U.S. forces. In the past, even as recently as the Gulf War, close U.S. allies like Britain could equal U.S. capabilities, as the British First Armored Division "plugged in" almost seamlessly with the U.S. Seventh Corps, and by all accounts fought well.[140] In the future, this

---

the answer is informed by the increasing dependence of advanced weapons systems on "spin-on" rather than "spin-off" technology—technological diffusion from the commercial to the defense sector. Advanced industrial states like Britain, Germany, and Japan may acquire most such technologies readily because many are "spin-ons." China and Russia may lag because the high-technology sectors of their economies are currently underdeveloped. For a discussion of "spin-on" and new defense technologies see Wayne Sandholtz, Michael Borrus, John Zysman et al., *The Highest Stakes: The Economic Foundations of the Next Security System* (New York: Oxford University Press, 1992), 29–35, 60–71, 137–40.

137. Bill Gertz, "Russia to Slash Ground Forces, Rely on Nukes," *Washington Times*, 17 October 1997, 1; and Walter Pincus, "Russia Considering Increased Nuclear Dependence," *Washington Post*, 7 December 1997, A11. Russia's dependence on nuclear weapons has only grown since 1997. See David Hoffman, "Russia's Nuclear Future Is Uncertain," *Washington Post*, 31 August 1999, A1.

138. William Drozdiak, "Even U.S. Allies Resent U.S. Dominance," *Washington Post*, 4 November 1997, A1.

139. Patrick J. Garrity, *Does the Gulf War Still Matter? Foreign Perspectives on the War and the Future of International Security*, CNSS Report no. 16 (Los Alamos, N.M.: Center for National Security Studies, Los Alamos National Laboratory, July 1993), 32. This remark was purportedly made by General K. Sundarji.

140. For an account of the British forces see General Sir Peter de la Billière, *Storm Command: A Personal Account of the Gulf War* (London: HarperCollins, 1992), 89–101; and Gordon and Trainor, *The General's War*, 165–67, 382–83. De la Billière describes the reason he argued for and received an armored division (the 1st Armored) from British leaders: "the level of influence enjoyed in theatre so far would be much reduced if we did not reinforce what the Americans did: We would have to do what we were told to a greater degree." Moreover, in the future, "we could not expect to enjoy the same

ability will have to change as U.S. abilities do. U.S. allies will need to be able to exploit information, to move, and to destroy the enemy as well as U.S. forces can. Operation Allied Force demonstrated a profound gap between the capabilities of the United States and its NATO allies. American and European officials expressed concern publicly about the implications of this for the alliance itself.[141]

One fear is that the division of labor in the alliance between the United States and European states only grows leading to a situation of complete dependence on the United States. As Dietrich von Kyaw, former German ambassador to the European Union, warned: "What Kosovo has shown is that we—the French, the Brits and the Germans...are all, at maximum, second rate. Not as far as numerical strength is concerned. Not as far as courage is concerned. But if we are not careful, we Europeans will become the Hessians of the Americans."[142] A European military capability is therefore necessary, von Kyaw argued, in case "the Americans are not interested to fight a European war. We never have a guarantee against neoisolationist developments. Nobody knows how Congress will decide. Nobody knows what sort of U.S. president we might have."[143]

A second, more likely, fear is that European militaries can no longer fight with the American military seamlessly—having similar doctrine, equipment, and ability. As information warfare progresses, U.S. allies like Britain will be less likely to have forces compatible with those of the United States. German Gen. Klaus Naumann, former chairman of the military committee of NATO, said that Allied Force showed the day is coming when the United States and its European allies "will not even be able to fight on the same battlefield."[144] If this situation is not reversed by European states, then Naumann's fear may be realized. This situation might be reversed by European states spending more on defense, particularly increasing their research and development budgets, or by increasing U.S.-European cooperation in key areas of military technology.[145] If it is not reversed then it is likely the United

credibility...in the United States if we had not matched America in raising our force levels at a critical moment" (de la Billière, *Storm Command*, 99–100).

141. William Drozdiak, "Air War Exposed Arms Gap Within NATO," *Washington Post*, 28 June 1999, A1; and Colin Clark, "Campaign in Kosovo Highlights Allied Interoperability Shortfalls," *Defense News* 16 August 1999, 6.

142. "Von Kyaw: EU 'Must Embrace the Whole Continent'," *Financial Times*, 5 August 1999, http://www.ft.com/hippocampus/q12caf2.htm.

143. Quoted in "Von Kyaw: EU 'Must Embrace the Whole Continent'."

144. Quoted in Drozdiak, "Air War Exposed Arms Gap Within NATO," A1. Retired Royal Air Force Air Vice Marshal R. A. Mason has warned that "There is concern in Europe that unless we get our act together, we're going to end up as spear carriers for the U.S" (quoted in David A. Fulghum, "Kosovo Conflict Spurred New Airborne Technology Use," *Aviation Week and Space Technology*, 23 August 1999, 31).

145. At present, European nations spend half of what the United States does on procurement and a third of the American research and development budget. John D. Morrocco, "Kosovo Reveals NATO Interoperability Woes," *Aviation Week and Space Technology*, 9 August 1999, 32. The creation of NATO in April 1999 of the Defense Capabilities Initiative to help bridge the technological and operational gaps

States will be less considerate of allied interests; the United States is likely to pay less heed to allies who cannot fight with U.S. forces.[146]

OLD DANGERS

Though it provides the U.S. military with significant advantages, information warfare will not provide it with a splendid first-strike capability or escalation dominance in a conflict with another great power. To be sure, the U.S. conventional deterrent will be more effective and this bodes well for the U.S. ability to extend deterrence to an expanded NATO. The danger of inadvertent escalation, however, will make efforts to coerce or fight a limited conventional war too risky for the political goal. In sum, information warfare will not make the world safe for conventional or nuclear war between nuclear-armed great powers.

Information warfare cannot remove the dangers present when the U.S. confronts a threshold nuclear state in crisis or war. The military is never likely to be able to guarantee that it can destroy all of another state's nuclear or biological weapons. An attempt to coerce these states may fail, or succeed too well and threaten the existence of the leadership itself, leading it to use a nuclear weapon against a U.S. ally or the United States itself.

Very few political goals are worth such a risk. The defense of the United States clearly is, as may be the protection of vital interests, but in other circumstances the risks may be too great to run. Decisionmakers must remember that what is militarily possible is not necessarily politically prudent. To President Kennedy's credit, he chose a blockade over an airstrike and invasion in response to the Cuban Missile Crisis. The most effective military solution was an airstrike to destroy the missiles, but the ultimate political goal was to avoid a nuclear war, and the blockade better served this end. Decisionmakers must be certain that they choose the right military instrument when they threaten or use force. Neither they nor information warfare can undo the nuclear revolution. One danger is that military capabilities may overwhelm prudent political judgment. The use of force against nuclear states carries great risks that may not be worth the death of U.S. citizens in a retaliatory attack. As the dominant military power in the world today, it may be unpleasant for the United States to recognize that information warfare does not change the extent

between the United States and its NATO allies is a welcome step. Luke Hill, "Kosovo Spurs Review of U.S.-Allied Capabilities Gap," *Defense News*, 2 August 1999, 9.

146. This is not to argue that the United States has ever paid great heed to its allies since becoming a superpower, but only that it will have less reason to do so in the future. Also, my argument is not that information warfare marks the end of multilateralism. For political reasons, U.S. diplomacy will need the figleaf of multilateral operations, as the participation of Egypt and Syria in the Gulf War enabled the United States to claim that the coalition arrayed against Iraq was precisely that—a coalition that included Arab states—and not an effort wholly created and dominated by the United States. Although it is likely that U.S. military leaders will increasingly tend to view multilateral actions as unnecessarily obstructing U.S. freedom of action as its technological capabilities increase.

to which military and political leaders must still design their military and foreign policies according to the constraints imposed by the nuclear revolution.

Nuclear and biological weapons are enormously destructive and relatively easy to deliver. This is why information warfare cannot change the paradigm with respect to the use of force in international politics. The relationship among states armed with nuclear or biological weapons is such that even if the United States could use information warfare perfectly, it still could not escape unacceptable destruction of its population for the political goal at issue. Military technology changes, but the logic of the nuclear age still remains the same.