Naval War College Review

Volume 53
Number 2 *Spring*

Article 11

2000

Review Essay—Don't Techno for an Answer: The False Promise of Information Warfare

Brent Stuart Goodwin

Don't Techno for an Answer

The False Promise of Information Warfare

Brent Stuart Goodwin

Adams, James. *The Next World War: Computers Are the Weapon and the Frontline Is Everywhere*. New York: Simon and Schuster, 1998. 288pp. $25

Arquilla, John, and David Ronfeldt, eds. *In Athena's Camp: Preparing for Conflict in the Information Age*. Santa Monica, Calif.: RAND, 1997. 501pp. $20

Schwartau, Winn. *Information Warfare: Chaos on the Information Superhighway*. New York: Thunder's Mouth Press, 1994. 432pp. $22.95

Shukman, David. *Tomorrow's War: The Threat of High Technology Weapons*. New York: Harcourt Brace, 1996. 272pp. $26

THE U.S. VICTORY IN THE 1991 Persian Gulf War prompted widespread speculation about the future of warfare and the role of technology and information in the conduct of war. This has produced an ever-growing body of literature concerning the future of war and the implications toward U.S. policy. Unfortunately, that literature has gone from explanation to prediction with very little analysis in between.[1] The predictions that have been made need to be studied in light of some of the major works in strategic studies. On the whole, one finds ruminations about information warfare lacking in useful hypotheses toward generating theoretical frameworks for strategic thinking about future events.

By any measure the performance of U.S. weaponry in the Gulf War was impressive, even taking into account some overstatements made at the time. However, there is a profound difference between

Naval War College Review, Spring 2000, Vol. LIII, No. 2

winning the war, on the one hand, and sound strategy and policy being aided by superior technology, on the other. At this point in history, it is important to keep in mind that technology and information are not the automatic solutions to every problem. From a strategic standpoint, we may have reached the point where technology and data complicate more than they clarify. Technology does not fix systemic organizational problems, but it does increase implementation costs in time and money, and thus it should not be seen as a cure-all. Most importantly, technology is a poor offset for unsound strategy and policy.[2]

The volumes reviewed here typify the tone of the literature regarding war in the information age. Taken together, they exhibit a preoccupation with technology and nonstate actors. Those two factors are not without consequence for strategic thinking, but these authors make little attempt to situate their claims in broader strategic thought, which would prove useful in sparking debates that would lead to theory building about information warfare (IW). In none of the works are theoretical frameworks presented for evaluating events, and thus the reader cannot find a basis for the development of sound strategy and policy regarding IW.

This is not to say that authors in this genre are incorrect in suggesting that technological advantages should be exploited or that they present dangers, but rather that their predictions of technological prowess translating into battlefield dominance have not been systematically established. Generally, the literature proceeds from observations to conclusions with insufficient attention to the component parts of society and war, and how they relate to one another.

To varying degrees these four books share two assumptions regarding information warfare.[3] The first is that IW implies the rise of a new political-economic order that privileges nonstate actors because IW allows nonstate actors to threaten the security of Westphalian

---

Mr. Goodwin is a doctoral candidate in the Department of Political Science at Brown University. He teaches courses on international relations and American foreign policy after the Cold War. His research interests are in U.S. national security policy decision making, Pacific Rim security, and the impact of technology on decision making and strategy. In 1996 he worked in the State Department's Office of International Security and Peacekeeping.

states. Second, technological dominance is the key to winning future wars.

Information Warfare (Schwartau) and *Tomorrow's War* (Shukman) present views based largely upon the first assumption. *The Next World War* (Adams) and *In Athena's Camp* (Arquilla and Ronfeldt) accept the first assumption but emphasize the second.

Barbarians at the Gate: Schwartau and Shukman. Winn Schwartau sounds an alarmist note in *Information Warfare,* highlighting the potential "computer Pearl Harbor waiting to happen."[4] His concern is that IW will be part of the formation of a new political and economic order that will have dire consequences for individual, as well as American national, security. In a global information war, technology will combat technology, with widespread chaos the result.[5] According to this view, the vulnerability of individuals and the state lies in the accessibility of computerized data to ill-intentioned, nonstate, information warriors.

Nonstate actors receive further treatment in David Shukman's *Tomorrow's War*. Computer hacking on a grand scale will be a facet of future conflict, he believes, along with the use (or at least threats of the use) of weapons in the arsenals of nonstate actors.[6] Shukman adds the threat of nuclear, biological, and chemical (NBC) warfare to the arsenal of nonstate actors. A good part of this book portrays the dangers posed by high-technology weapons, including space-based weaponry. Shukman argues that new weapons systems, from improved missile targeting to complex unmanned vehicles and ant-sized robots, will shape a new geopolitical order. Shukman cites the Aum Shinri Kyo subway attack in Tokyo as a case study to illustrate what nonstate actors can do in "tomorrow's war."[7] One might reply, however, that the subway attack is an example of threats that have been with us for many decades, not those typically associated with information warfare, and that little geopolitical impact has yet been seen from nihilistic or messianic nonstate terrorism.

The concern of Schwartau and Shukman over an implicitly hostile new political and economic order and the rise of nonstate actors as a result of technology arises from a Clausewitzian assumption of trinitarian war. In this formulation, the "Clausewitzian trinity" of the people, army, and government of one state utilizes war as a political instrument against another state's people, army, and government.

Generations of strategic thought have been based upon this assumption, and thus events that appear to be abnormal cause alarm. Strategy, for our purposes here, is regarded as the creation of force and the application of it at a decisive time and place.[8] The specific weapons used are less important than the application of sufficient force at the proper time and place; there is strong historical evidence to suggest that states will remain better at this than nonstate actors.

After the fall of Rome, war was waged by "armies" of Vandals, Huns, and other social entities who have no counterpart in today's world.[9] The early 1500s saw warfare between knights, cities, leagues, popes, and religions, without the presence of anything that could be labeled a well defined state.[10] Niccolò Machiavelli saw war as a tool of the prince, and there was little notion of "the people" or "the state" in his conception of war.[11] It was only after the Treaty of Westphalia that states gained a monopoly on the legitimate waging of war.[12] To this effect, international law since 1648 has excluded nontrinitarian, nonmilitary warfare.[13] The result is that three and a half centuries of the Westphalian state system have left us little experience of nonstate actors waging nontrinitarian war. In a sense, we are now looking forward into the past, and a framework for evaluation is needed.

The threats and problems posed by nonstate actors may be new, then, but nonstate actors are not. The end of the Cold War allowed them to take advantage of new opportunities, some provided by technology. While Aum Shinri Kyo's subway attack could have happened in any decade since 1960, in 1998 computer hackers invaded the websites of China's human rights agency and India's nuclear research center, and posted messages on forty Indonesian servers. Other targets have included Mexican president Ernesto Zedillo and the U.S. Department of Defense. In October 1998 a Serbian group calling itself "Black Hand" crashed the website of a Kosovo Albanian group.[14] Later the same week Black Hand attacked the website of the state-owned Croatian newspaper *Vjesnik*. In retaliation, the next day Croatian hackers attacked the website of the Serbian National Library; Serbian hackers then temporarily disabled the Nato website.[15] Such activities in February 2000 expanded to threaten the computer-based civilian activities of daily life. The vast majority of the literature on IW consists of reviews of these threats and their consequences, but it overstates their strategic significance.

At any rate the future prospects for these nonstate, nontrinitarian, cyber-warriors are not bright. It should be kept in mind why nontrinitarian war went out of fashion in the first place; as Charles Tilly observed, "War made the state and the state made war."[16] Put another way, the state can create and apply decisive force *better* than nonstate actors, and *better* than nontrinitarian methods, such as terrorism and information warfare. Strategic success depends on the control of land, people, and resources (all forms), which means that a technological/information-based approach alone will not prove decisive.[17] Because *resistance* involves resources and will, there is strong reason to believe that the Westphalian state can endure nontrinitarian warfare and outlast nonstate actors—most states being better than the typical nihilist or messianic nonstate group at resisting various forms of IW and at applying decisive force if it becomes necessary.[18]

Fight Fire with Fire: Adams, Arquilla, and Ronfeldt. In *The Next World War*, James Adams posits a future in which the places we live and work are the battlegrounds for global information war. (This is a common assertion of all four books discussed.) Technology will allow the targeting of communication networks and air traffic control, and support of misinformation campaigns. (The latter is possible due to Adams's definition of information warfare as including perception management.)[19] This in turn leads to the possibility of war by other means, which would seem to imply what are normally referred to as psychological operations.[20] Adams supplies case studies to illustrate what this "war by other means" will look like, before concluding that IW "is no silver bullet."[21] Adams implies that the United States is a Goliath surrounded by nonstate Davids, that unless fire is met with fire, U.S. security will be threatened. By way of example, Adams reports that China once released computer viruses to silence electronically an opposition group.[22] Now this, of course, is an example of a Westphalian state taking action, albeit of an information-warfare nature, and prevailing against a nonstate actor—the reverse of what we are supposed to fear. Yet if China, technologically backward, can wage information warfare against nonstate actors, surely the United States could do so as well.

But for the presence of new technologies in many of Adams's examples, it is unclear how his case studies are different from standard

psychological operations, on the one hand, and terrorism and sabotage on the other. The use of radio stations in Rwanda and Serbia to broadcast hate-filled political messages is just plain propaganda, not information warfare.[23] However, to make his point, Adams categorizes events by the technology used rather than the actors' intentions. Technological capabilities are important, and they are easier to measure than intentions, but the fact that actors possess sophisticated technology need prompt no special distinction. It is their intentions that make them dangerous.

Of the four books discussed, *In Athena's Camp* offers by far the most systematic and sober analysis of IW. Many of its insights regarding network forms of organization come directly from operations research. Editors Arquilla and Ronfeldt describe a "third wave" that empowers nonstate actors; they assert that conflicts will depend on and revolve around information and communication.[24] They suggest that as a result of technology, conflict will become more diffuse and less linear, as well as multidimensional.[25] This notwithstanding, the more parsimonious term "nontrinitarian" is still the operational word here. Arquilla and Ronfeldt go farther, distinguishing between "cyberwar," which they define as an "information-oriented approach to battle," and "netwar," which they call an "information-oriented approach to social conflict."[26] *In Athena's Camp* has chapters titled "Cyberwar Is Coming"; "Preparing for the Next War"; and "Warfare in the Information Age"—subjects that are by now familiar territory.[27] The book as a whole banks heavily on the assumption that information can be translated into power. However, in a world where technology increases information to the point that we may speak of "analysis paralysis" (indecision resulting from forever waiting for the next piece of information to come in), information without any theoretical framework by which to evaluate it may cause as many problems as it solves. A notable exception in this book, and the literature as a whole, is John Rothrock's article, "Information Warfare: Time for Some Constructive Skepticism?" which adds a healthy note of circumspection to *In Athena's Camp*.

The "fire with fire" positions—whether the "fire" is technology, as in *The Next World War,* or information transmitted by technology, as argued in *In Athena's Camp*—places too high a value on technological superiority. The nineteenth-century theorist Antoine Henri de Jomini observed that "the superiority of armament may increase the

chances of success in war: it does not, of itself, gain battles."[28] A more recent observer argues that the Gulf War demonstrated what technology was capable of but did not establish that technology wins wars.[29] Its contribution to winning ground battles is the most important variable for the purposes of strategy; Vietnam, Lebanon, Afghanistan, and Somalia illustrate that the relevance of force is in many ways the inverse of technological modernity.[30]

The example of Somalia shows that no amount of technology could have mitigated the fundamental weaknesses in policy. Means were not provided to achieve the chosen ends, and the ends outstripped political will. While making the debatable claim that Mohammed Farah Aideed was better at perception management than U.S. forces—perception management was not the issue in Somalia—*The Next World War* still asserts that the CIA's high-technology surveillance was evaded by simple walkie-talkies and talking drums.[31] Technological advantages should be explored and exploited at every turn, but without falling down the slippery slope of technological determinism.

The prophets of technological determinism have been with us for some time. Several significant studies have concluded that though technology is important, it may have only marginal impact upon battlefield outcomes.[32] A closer look at these works reveals that more often than not, victory comes to the side with an advantage in morale, leadership, skill, and discipline—not necessarily the side with a technological advantage.[33] In Europe, the spread of technological advances brought multinational similarity, which led to a stalemate.[34] Even where one side had clear advantages in technology (such as when European powers faced indigenous forces in the New World, Africa, and Asia), that side also often had military strengths beyond technology. For instance, the institutional superiority that allowed the maximization of firepower goes a long way toward explaining outcomes in the colonial era.[35] Similarly, in comparison to the indigenous forces they faced, European militaries were more professional, standardized, and concentrated, which allowed greater projection of force irrespective of technology.

The "center of gravity"—the "hub of all power and movement," the "decisive strategic point," the point "exercising a marked influence on the result of the campaign"—is unlikely to be destroyed by information warfare in and of itself. [36] It may be hindered and

inconvenienced, but it seems inconceivable that the United States, or any state, would surrender in war because cell phones, satellites, or computers were no longer functional. To the authors, it is as if states never went to war before the microchip.

The "techno-centric" view also downplays the centrality of vital interests in a state's grand strategy. Technology is a dependent variable, not an intervening or independent one, which means that states can get by with a little or a lot of technology but that the technology needs a strong state in which to develop. This type of state is not likely to become wholly vulnerable to information warfare.

Taken as a whole, these four books place too high an emphasis on the role of technology and its impact on the international system. It has always been the case that "readiness to suffer, die, and kill are the most important factor in war."[37] Technological prowess does not obviate this fact.

Much of the aura surrounding the concept of information warfare is a direct descendant of the "arsenal of democracy" thinking of World War II. According to this view, American industry and technology would be used to limit the loss of American lives in global conflicts. This approach has practical and political utility, and it remains a worthwhile goal. However, the desire for low-risk, low-commitment responses to foreign threats lures policy makers into the false promise of IW. As recent events have shown, there are no easy ways out of post–Cold War conflicts. Technological changes will come and go, and it is in our interest to master them; but technological changes should not obscure stark realities—bloodless victories are seldom of strategic utility.

In the nearly ten years since the end of the Gulf War, a relatively large body of literature has been produced on information warfare. All of it suffers from lack of a strategic theory for evaluating events and technological developments. Absent such a political framework, amateur speculations and armchair quarterbacking about present and future events and technological developments replace sound strategic thinking.

Ideally, books of the kind discussed here (studies of possible futures) can clarify, define, name, expound upon, and argue the major issues of future scenarios.[38] The goal, of course, is to identify possible futures and how to work toward what is desirable and to prevent or minimize the impact of what is undesirable. Another worthwhile

goal is to understand better whether the trends observed are smooth, cyclical, dialectic, or alternating. This leads to insight regarding mechanisms of change and assumptions regarding the operating environment.[39] The result would be an increase in understanding our environment and, one hopes, an increase in our control of it.

This essay is not an attempt to sketch a strategic theoretical framework or to survey what is desirable or possible in the future of information warfare. Rather, it suggests that technology—a means of waging war—cannot supersede the classical theorists' examinations of the ends or purposes of war. The nature of society remains more central to understanding war than the technology employed in its conduct.

Notes

1. A good start for analysis of the Persian Gulf War from an information-warfare perspective is Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (Washington, D.C.: AFCEA International, 1992).

2. These points are discussed further in David Shenk, *Data Smog: Surviving the Information Glut* (San Francisco: HarperEdge, 1997).

3. This term is used to describe what has also been referred to as "techno-war." Information warfare is at present an ill-defined concept, but it may be thought of as assets and processes that are information based. These include command and control, psychological operations, and other information sources. As these assets and processes become automated they become susceptible to viruses and hackers.

4. Winn Schwartau, *Information Warfare: Chaos on the Information Superhighway* (New York: Thunder's Mouth Press, 1994), p. 13.

5. Ibid., p. 291.

6. David Shukman, *Tomorrow's War: The Threat of High Technology Weapons* (New York: Harcourt and Brace, 1996), p. 205. See also Schwartau, p. 215.

7. Shukman, p. 243.

8. Martin van Creveld, *On the Future of War* (London: Brassey's, 1991), p. 48.

9. Ibid., p. 52.

10. Ibid., p. 126.

11. See Niccolò Machiavelli, *The Art of War*, ed. Neal Wood (Indianapolis: Bobbs-Merrill, 1965).

12. Van Creveld, p. 57.

13. Ibid., p. 193.

14. "Serb Hackers Declare Computer War," *Los Angeles Times*, 22 October 1998.

15. Amy Harmon, "'Hacktivists' of All Persuasions Take Their Struggle to the Web," *New York Times*, 31 October 1998. Also see Amy Harmon, "Serbs' Revenge: NATO Web Site Zapped," *New York Times*, 1 April 1999.

16. Charles Tilly, ed., *The Formation of National States in Western Europe* (Princeton, N.J.: Princeton Univ. Press, 1975), p. 42.

17. Paul Van Riper and Robert H. Scales, Jr., "Preparing for War in the 21st Century," *Parameters*, Autumn 1997, p. 8. I shall address this point later in this essay.

18. Michael Handel, *Masters of War: Classical Strategic Thought* (London: Frank Cass, 1996), p. 14.

19. James Adams, *The Next World War: Computers Are the Weapon and the Frontline Is Everywhere* (New York: Simon and Schuster, 1998), p.17.

20. Ibid., p. 39.

21. Ibid., p. 313.

22. Ibid., p. 250.

23. Ibid., pp. 90, 273. At a basic level, these are examples of controlling perception and information. This type of activity is not representative of a new phenomenon, however. Julius Caesar wrote his works from the battlefield in part to serve the same function, spreading political messages.

24. John Arquilla and David Ronfeldt, eds., *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica, Calif.: RAND, 1997), p. 4.

25. Ibid.

26. Ibid., p. 6.

27. John Arquilla and David Ronfeldt, "Cyberwar Is Coming!"; Stephen J. Blank, "Preparing for the Next War"; and Bruce Berkowitz, "Warfare in the Information Age," can be found in *In Athena's Camp*, edited by Arquilla and Ronfeldt.

28. Antoine Henri de Jomini, *The Art of War* (Novato, Calif.: Presidio Press, 1992), p. 47.

29. Handel, p. 8.

30. Van Creveld, p. 32.

31. Adams, p. 67.

32. See William H. McNeill, *The Pursuit of Power: Technology, Armed Force and Society since A.D. 1000* (Chicago: Univ. of Chicago Press, 1984); Timothy Travers, *The Killing Ground: The British Army, the Western Front, and the Emergence of Modern Warfare, 1900–1918* (London: Allen and Unwin, 1987); George Raudzens, "Blitzkrieg Ambiguities: Doubtful Usage of a Famous Word," *War and Society*, September 1989, pp. 77–94; and George Raudzens, "War-Winning Weapons: The Measurement of Technological Determinism in Military History," *Journal of Military History*, October 1990, pp. 403–33.

33. Raudzens, "War-Winning Weapons," p. 404.

34. Paul M. Kennedy, *The Rise and Fall of Great Powers: Economic Change and Military Conflict from 1500 to 2000* (New York: Vintage Books, 1989), pp. 23–72.

35. McNeill, pp. 128–35. The author notes that the development of close-order drill was a significant force enhancer.

36. Carl von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton, N.J.: Princeton Univ. Press, 1976), pp. 595–6. See also Jomini, pp. 85–92. An excellent treatment of the concepts of "center of gravity" and "decisive strategic point," respectively, is given by Handel, p. 40.

37. Van Creveld, p. 160.

38. Herman Kahn and Anthony J. Wiener, *The Year 2000: A Framework for Speculation on the Next Thirty-three Years* (London: Macmillan, 1967). See also Brita Schwartz, Uno Svedin, and Björn Wittrock, *Methods in Future Studies: Problems and Applications* (Boulder, Colo.: Westview Press, 1982).

39. Schwartz et al., p. 20.

Ψ