Chapter One

WHITHER "INFORMATION STRATEGY"?

Something unsettling is happening to grand strategy. National security experts have long based their calculations on the traditional political, economic, and military dimensions of power. Now they see that a new field is emerging: "information strategy." Although still inchoate, it promises to redefine these three traditional dimensions. Moreover, it promises to seed the creation of a fourth—the "information" dimension, which is broadly understood to include technological conduits and conceptual contents. The world is turning anew into a highly charged battleground of ideas; it is not just a world in which material resources are the objects of protracted, often violent competition. In this emerging world, the key to success will likely lie in managing informational capabilities and resources skillfully—i.e., strategically.

Information strategy remains difficult to define and bound with precision, but the issues and debates shaping its appeal have been clustering around two poles for the past several years. One pole is basically technological: that of cyberspace safety and security. What drives concerns here is a sense of the vulnerability of essential U.S. information infrastructures to various forms of attack, especially by malicious actors who are skilled at launching cyberspace-based threats. Worrying how to defend against attacks by adversarial regimes, terrorists, and criminals, and wondering how to use cyberspace for counteroffensive attacks—that is what this pole is largely about. (See Hundley and Anderson, 1994; Molander, Riddile, and Wilson, 1996; and Campen, Dearth, and Goodden, 1996.)

The other pole is concerned with the politics of ideas—information strategy is seen as a way to harness and express the "soft power" of American ideals, so as to attract, influence, and lead others (Nye, 1990; Nye and Owens, 1996). The debates here are mainly about the benefits to be gained by opening and sharing our information and related information infrastructures with our allies and others, in such areas as intelligence and coalition formation. Moreover, there is a strong, optimistic emphasis on the media's roles in shaping people's views, as well as the Internet's. Broad strategies, involving the media more than cyberspace, are envisaged for using "information power" to promote democracies and constrain authoritarian regimes abroad. Thus, opportunities rather than threats are the motivating concerns.

Of the two poles, the technological one has received far more attention. Numerous conferences and gaming exercises have been held about "information warfare." A growing body of studies—think-tank analyses, congressional hearings, and a presidential commission—are serving to identify the key technological risks and vulnerabilities. Options are emerging, and interagency mechanisms (e.g., the National Infrastructure Protection Center) are taking shape for instituting systemic and nodal defenses to protect America's national and global information infrastructures and strategic subsystems.

Despite this considerable progress, inspection of the debates that are evolving around the more technical issues indicates that the technological pole cannot provide a sole basis for the formulation of information strategy. The debates remain largely about cyberspace-based vulnerabilities, and the ensuing language and scenarios tend to recapitulate old nuclear and terrorist paradigms that place heavy emphasis on potential worst-case threats (e.g., an "electronic Pearl Harbor"). All this is needed—indeed, infrastructure protection must be a priority of the U.S. government and private sector.[1] But this is far from adequate, even for developing the technological dimension as a

[1] For a recent discussion, see Smith, (*Issues in Science and Technology*), and the replies posted in the Forum section of the Winter 1998 issue of that journal by John J. Hamre (Deputy Secretary of Defense), Michael A. Vatis (chief, National Infrastructure Protection Center), and Arthur K. Cebrowski (Vice Admiral, U.S. Navy, and President, Naval War College). All this is available by following links at http://205.130.85.236/issues/index.html/.

basis for information strategy writ large. Analysts must look beyond infrastructure defense; more is at stake in cyberspace than just technological vulnerability. They must look beyond risks, too, to help clarify the opportunities.

Meanwhile, less attention has been given to the development of soft power as a basis for information strategy. Strategists rarely convene to discuss it, and its influence is measured mainly by a small number of publications. True, there have been numerous conferences and studies about the changing roles of the media, public diplomacy, and intelligence in the information age. But a strategist interested in soft power as a basis for information strategy must pull these pieces together—they are rarely presented and analyzed as a coherent whole. The options in this area are not spelled out very well.

More to the point, the communities of experts associated with either the technological or the idea-sharing area do not meet much with those of the other. Both communities are aware of each other and share some common notions. For example, both communities presumably agree (with Nye and Owens, 1996, p. 35) that

> [i]nformation is the new coin of the international realm, and the United States is better positioned than any other country to multiply the potency of its hard and soft power resources through information.

Nevertheless, they remain disparate, insular communities, with few bridges connecting them.

Thus, there is an imbalance in current efforts to frame an American information strategy. Both poles are important. Yet, the concerns encompassing the technological pole have received the bulk of attention and appear to be well on the way to resolution. The sociopolitical dimension of idea sharing is now the one in need of much more work and clarification.

Further, the technological and ideational aspects should be linked by strategic analysis. Letting them develop separately along their current trajectories may lead to regrettable omissions of analysis. For example, narrow technical concern about cyber-terrorists who might take "the Net" down misses the strategic possibility that, politically, terrorists might prefer to leave the Net up, so as to spread their own soft-power message or engage in deception or intelligence gathering. On the other hand, enthusiasm about spreading American ideas may cause the United States to overlook the possibility that adversaries may exploit the media, the Internet, and other communications technologies to their own advantage.

However, more is at stake than omissions of analysis. Developing the technological and ideational dimensions of information technology together—rather than allowing them to take separate paths—will garner great opportunities. It is a mistake to think that these two poles represent an unremitting dichotomy rather than two parts of the same whole. Good ideas and options are needed for bridging and uniting them to create a broad, integrated vision of what American information strategy can become. We propose to unfold such a vision.

We begin by reconceptualizing the information realm. First, we argue that existing notions of cyberspace and the infosphere (cyberspace plus the media) should be seen as subsets of a broader "noosphere"—or globe-girdling realm of the mind. Advanced by the French scientist and clergyman Pierre Teilhard de Chardin in the mid-20th century, this concept is being rekindled by visionaries from a variety of quarters and can be of service to information strategists. In addition to recommending adoption of the concept of the noosphere, we suggest the need to shift from the current emphasis on "information processing" (a technology-oriented activity) to thinking also about "information structuring" (which emphasizes issues related to ideas and organization).

Our discussion of the noosphere anticipates the next key proposal: At the highest levels of statecraft, the development of information strategy may foster the emergence of a new paradigm, one based on ideas, values, and ethics transmitted through soft power—as opposed to power politics and its emphasis on the resources and capabilities associated with traditional, material "hard power." Thus, *realpolitik* (politics based on practical and material factors—those of, say, Henry Kissinger) will give some ground to what we call *noopoli-*

tik (nü-oh-poh-li-teek[2]—politics based on ethics and ideas, which we associate with many of those of George Kennan). As noopolitik emerges, the two approaches to statecraft will coexist for some decades. Sometimes they will complement each other, but often they will make for contradictory options. At first, information strategy may well serve in subordinate ways to traditional power politics—but, in our view, this will become ever less the case. Statesmen will always have recourse to traditional forms of power, but they will increasingly see benefits in emphasizing strategies that take advantage of informational means first, with force placed in a complementary role. This will work especially well when ethical notions form a key part of an information strategy approach to conflict, and when the initiative can come from either nonstate or state actors.

Strategy, at its best, knits together ends and means, no matter how various and disparate, into a cohesive pattern. In the case of an American information strategy, this requires balancing the need to guard and secure access to many informational capabilities and resources, with the opportunity to achieve national aims by fostering as much openness as practicable in the international system. Of course, an American strategy that supports a substantial amount of openness is sure to base itself on the assumption that greater interconnectivity leads to more liberal political development—an updated version of Lipset's (1960) "optimistic equation," which saw democracy moving in tandem with prosperity. Even so, it may be prudent to hedge against atavistic tendencies (e.g., an information-age totalitarianism) by means of continuing guardedness. Our term to represent such a strategic balancing act is "guarded openness," which we will discuss further in this report.

Building upon this foundation, we next examine the strategic information dimensions of two key areas that bear closely upon American national security, both in peace and war: strategies for fostering international cooperation with other states and nonstate actors; and a strategic information warfighting doctrine. We examine a variety of approaches to building robust coalition structures and consider the ways in which American influence can be advanced in a manner that

[2] This is the pronunciation we prefer, because it adheres best to the pronunciation of the Greek root *noos.* However, some dictionaries may indicate that other pronunciations are possible (e.g., n ō -uh-poh-li-teek).

will neither threaten nor spark reactions. In the event that diplomatic strategy fails to prevent conflict, our view is that information weapons will have great effects upon the future "face of battle." With this in mind, we advance some doctrinal strategies that strive to reconcile the pragmatic need to strike powerfully with the ethical imperative to wage war justly.

Our study includes recommendations for policy, ranging from high-level emphasis on supporting the emergence of a global noosphere, to institutional recommendations that, for example, the U.S. military should begin to develop its own noosphere (among and between the services, as well as with U.S. friends and allies). In the area of international cooperation, we offer recommendations for strategic approaches to influence—but not alienate—the state and nonstate actors of the noosphere. Finally, we recommend specific doctrine related to information strategy—including the pressing need to deal with such ethical concerns as the first use of information weapons, concepts of proportional response, and the need to maintain, to the greatest extent possible, the immunity of noncombatants.

From these beginnings, we hope that an articulated, integrated, U.S. information strategy will emerge.