## **SUMMARY**

Information and communications have always been important to strategy. But they are changing from subsidiary to singular concerns—"information" matters more than ever for reasons that did not exist even 20 years ago. One reason is technological innovation: the growth of a vast new information infrastructure—including not only the Internet, but also cable systems, direct broadcast satellites, cellular phones, etc.—in which the balance is shifting away from one-to-many broadcast media (e.g., traditional radio and television) toward many-to-many interactive media. In many nations a growing, though varied, population is enjoying an ease of entry and access to the new infrastructure for commercial, social, diplomatic, military, and other interactions. This easy access is resulting in a huge increase in global interconnectivity.

A second reason is the proliferation of new organizations: Vast arrays of state and nonstate organizations are emerging that directly concern information and communications issues. A third reason why information and communications have become more important is that "information" and "power" are becoming increasingly intertwined. Across many political, economic, and military areas, informational "soft power" is taking precedence over traditional, material "hard power."

The new field known as "information strategy" is emerging around two poles, which define opposite ends of a spectrum of security concerns. One is an essentially technological pole, that of cyberspace safety and security. The other pole is essentially political and ideational—information strategy is seen as a way to harness and ex-

X

press the "soft power" of American democratic and market ideals, to attract, influence, and lead others.

Of the two poles, the technological one has received far more attention. Thus, there is an imbalance in current efforts to frame an American information strategy. Both poles are important. Yet, the concerns that encompass the technological pole have received the bulk of attention and appear to be well on the way to being figured out. The ideational pole is now the one more in need of work and clarification. Moreover, the technological and ideational poles should be linked together by strategic analysis that bridges the gap between them.

Such strategic thinking should impel a shift in American grand strategy, a shift growing out of and led by the rising importance of information strategy. In our view, a new paradigm is needed—in fact, it is already emerging—which we call *noopolitik* (nü-oh-poh-li-teek). This is the form of statecraft that we argue will come to be associated with the noosphere, the broadest informational realm of the mind (from the Greek *noos*) under which cyberspace (i.e., the Net) and the infosphere (cyberspace plus the media) are subsumed.

Noopolitik is foreign-policy behavior for the information age that emphasizes the primacy of ideas, values, norms, laws, and ethics—it would work through "soft power" rather than "hard power." Noopolitik is guided more by a conviction that right makes for might, than by the obverse. Both state and nonstate actors may be guided by noopolitik; but rather than being state-centric, its strength may likely stem from enabling state and nonstate actors to work coniointly. The driving motivation of noopolitik cannot be national interests defined in statist terms. National interests will still play a role, but they may be defined more in societywide than state-centric terms and be fused with broader, even global, interests in enhancing the transnationally networked "fabric" in which the players are embedded. While realpolitik tends to empower states, noopolitik will likely empower networks of state and nonstate actors. Realpolitik pits one state against another, but noopolitik encourages states to cooperate in coalitions and other mutual frameworks.

Noopolitik will not likely supplant the existing realpolitik paradigm of power politics in the near future. Rather the two forms will coexist, in an often rough, edgy balance that will vary regionally—because patterns of development remain uneven around the world. Some areas are already quite steeped in the dynamics of the information age, while others still seem more medieval than modern. Thus, noopolitik will be more pertinent in some parts of the world than in others, and in regard to some issues more than others.

We surmise that noopolitik will be most pertinent where technologically advanced societies predominate: e.g., parts of Western Europe and North America. It will be less so where conditions remain traditionally state-centric, and thus ripe for the continuation of realpolitik (e.g., much of Asia). Moreover, noopolitik will be most effective where all manner of media are prevalent, nongovernmental organizations (NGOs)<sup>1</sup> have an edge in generating attention to issues, the issues are complex rather than strictly economic or political or military, and where government-NGO relations are good.

The following measures could encourage construction of a global noosphere that would be of interest to all realms of society. They also embody a mix of measures to favor openness, on one hand, and protection, on the other. In this regard, they capture the essence of our preferred strategy for the United States—"guarded openness."

- Continue to support worldwide access to cyberspace. Support the access of NGOs as well as state and market actors to it, including where this runs counter to the preferences of authoritarian regimes.
- Move away from realpolitik-oriented designs to control encryption, and move toward freedom of encryption.
- To assure cyberspace safety and security at the international level, develop multitiered information systems for conditional information sharing, creating a shared—but still secure—infosphere.

<sup>&</sup>lt;sup>1</sup>A word of clarification: NGOs are, for the most part, civil-society organizations. The point has been made to us several times by devotees of economic power that private, for-profit, commercial corporations are powerful NGOs. But this is incorrect usage. Such corporations are nonstate actors but not NGOs—that term (and acronym) apparently dates from the early years of the United Nations and was not meant to include commercial corporations. Neither was a related term, international nongovernmental organization (INGO), which we do not use here.

- Promote freedom of information and communications as a right (and responsibility) around the world.
- Encourage the creation of "special media forces," modeled along the lines of special forces units but armed with the weapons of the media rather than those of the military. These squads could be dispatched into conflict zones to help settle disputes through the discovery and dissemination of accurate information.
- Open up diplomacy to greater coordination between state and nonstate actors, especially NGOs, by undertaking a "revolution in diplomatic affairs" that matches the revolutions under way in business and military affairs.

In addition to building a global noosphere, it might also be advisable for the U.S. government to work on constructing a military noosphere that, emphasizing jointness and sharing, would span the U.S. services and allied and other friendly forces around the world. However, the balance between openness and guardedness might have to be different in a military noosphere from what it should be in a general global noosphere.

In the immediate future, to deal with a world in which noopolitik is emerging but strong elements of realpolitik persist, there is a need to prepare for information-age conflict by developing a strategic information doctrine (SID) to guide policy in crisis and conflict. Composed of "depth defenses" (i.e., layered electronic defenses against hackers), but also of proactive elements (electronic measures for going on the offensive), a SID should emphasize the guidance of the moral dimensions of noopolitik. This emphasis implies a policy of "no first use" of information weapons, which would allow the United States to "do good" in terms of decreasing the likelihood of information-age conflict—but also to "do well" by mitigating its own vulnerabilities to attack in cyberspace, where it has more information targets than almost any other entity.

Finally, we urge a shift from focusing on an "electronic Pearl Harbor" to aspiring to the benefits of an American-inspired information-age "Manifest Destiny."