Chapter Four

INTERNATIONAL COOPERATION AND CONFLICT

This chapter considers selected policy-relevant implications of the emergence of noopolitik that are likely to influence the development of American information strategy. The analysis first examines various ways in which the traditional political, economic, and military domains of grand strategy may be affected, especially in terms of the prospects for broadening and deepening international cooperation. Next, the role of information strategy in crisis and conflict is examined, both in terms of the importance of new forms of public diplomacy and the need to craft an integrated strategic information doctrine (SID) to guide the management of informational capabilities and resources in wartime.

INFORMATION STRATEGY AND GLOBAL COOPERATION

Because the very notion of a noosphere is global, it should be apparent from the outset that success in actualizing this realm of the mind depends upon the ability to enlist others—from states, to NGOs, to "deep coalitions" of the two—to cooperate in support of it. In thinking about how to build cooperation, we have modified classical notions about grand strategy to reflect the sensibilities implied by the rise of noopolitik.

Thus, economic strategy should be fused with legal structures and norms as the global economy grows ever more reliant upon ideas and knowledge products and practices for its growth and health. In the military realm, it will likewise be increasingly important to move beyond traditional quantitative measures of military effectiveness, in which one party's strength threatens another. Instead, military is-

sues are viewed as tied inextricably to mutual security—placing the need for cooperation in this realm at a premium. Indeed, in a noopolitik world—even one that must coexist with substantial realpolitik elements—militaries that are attractive as partners, rather than feared as hegemons, are more likely to craft robust mutual security arrangements.

With regard to the political means and ends of traditional grand strategy, the realist and neorealist days of state-monopolized "high politics" (see Morgenthau, 1948; Waltz, 1979) are likely numbered, as the rise of nonstate actors and the emergence of a global civil society bring the social dimension of world politics to the fore. Thus, the tight coupling between social and political affairs will feature the active participation—sometimes the predominance—of nonstate civil (and uncivil) society actors.

These modified spheres of grand strategy each afford glimpses into how information strategy may complement the traditional tools of statecraft. But they also show how information strategy might emerge as a distinct dimension of statecraft as well. Note that the following discussion is exemplary rather than exhaustive. Our goal at this point is simply to sketch out the types of policy issues likely to rise in each realm, and the manner in which information strategy may help to foster cooperation and deter conflict.

Finally, it is important to recognize that some blurring and/or blending of the realms is likely to occur. For example, while the diffusion of legal norms and practices will be closely interwoven with economic affairs in a noopolitik world, normative institutions and practices will be visible in the other realms as well. While not likely to take on the same degree of statutory penetration as in economics and trade, military-security and sociopolitical affairs will no doubt be more influenced by ethical considerations in a noopolitik world. This does not change the point that the principal effect of new legal paradigms will be felt in the world economy. It just suggests the permeability of the "membrane" that divides our strategic analytic constructs.

The Economic-Legal Realm

In the economic-legal sphere, the primary concerns are commercial. Given the explosive growth of international trade and finance, especially in cyberspace, ensuring the safety and security of flows of goods and transactions necessarily forms the foundation for cooperation. From an economic-legal perspective, this cooperation may depend upon reaching agreement in several issue areas, beginning with what might be called "substantive law." This notion basically calls for agreement as to what constitutes a "crime," including fraud, forgery, hacking, and sabotage (or, as we have called it, "cybotage").

Cooperation may also hinge upon acceptance of a body of administrative and legal procedure that would establish jurisdiction and allow enforcement of the substantive laws designed to protect property and other assets, both in and out of cyberspace. In the information realm, agreement about such matters as territoriality, extradition, and the notion of "hot pursuit" may form a minimum basis for international cooperation. The challenge will be to harmonize these bases for cooperation—especially in the area of cyberspace-based territoriality—with the noosphere.

Information strategy will likely play a key role in transnational law enforcement, since any information-age "policing paradigm" would rely heavily upon regular flows of information among law enforcement bodies. Although police agencies are indeed showing signs that they recognize the importance of networking, it may be that some sort of clearinghouse will be needed to facilitate cooperation. At a policy level, it might even be useful to build on the Interpol model, adding to it an "Infopol" specializing in dealing with cyberspace-based criminal activities, to help optimize the benefits of already existing police information management operations.

The current multilateral law enforcement regime (e.g., Interpol) is built on significant information sharing, and a great deal of coordination, both formally (in state-to-state treaties or agreements) and informally (in terms of day-to-day interactions of policing organizations). A policing paradigm should also provide a grassroots basis for broadening the role of international courts of law in the informational domain—a key principle in building a global noosphere. As desirable as this approach seems, it would have difficulty in dealing

with the problem of noncompliance by recalcitrant states asserting their sovereign rights. Thus, this framework would also have to include significant intelligence capabilities to identify and cope with the problem of noncompliance.

The most serious aspect of noncooperation would be that just a few "defectors" from the envisioned international regime, providing "havens" for malefactors, could compromise overall information security, damaging the global economy and weakening nascent international legal cooperation. This difficulty could arise if a state decided that its national interests overrode commitments to some international "public good." Alternately, some nonstate actors (e.g., transnational criminal organizations, or TCOs) might have little reason to cooperate with multilateral agreements. Indeed, these nonstate actors might profit by defying the cooperative regime; and they might then attract some states to align with them, providing "pirate nets" to provide for their information infrastructural requirements.

Also, some states might be motivated to support defiance of an international cooperative regime simply because they fear the growth of transnational, or possibly supranational, authority—or because they feel that the "wiring of the world" might simply make the rich nations richer, widening the gap between the "haves" and "have-nots." Thus, efforts to knit together an information-driven economic-legal regime might engender its own "backlash," which might also affect the military-security realm. Finally, even among states inclined to cooperate, there might be reluctance to agree to a regime in which, say, encryption afforded a great degree of protection to electronic commerce, but only at the price of allowing supranational bodies that would act as "key escrow agents." The other side of this issue is that many states might balk, as the United States has, at the notion of providing unbreakable encryption to individuals and commercial concerns, since this would restrict the surveillance capabilities (and therefore, the power) of the state. If U.S. policymakers are to be persuaded to encourage and nurture the development of the noosphere, the potential constraints that a global noosphere would impose upon American power would have to be carefully analyzed and weighed against the overall benefits.

Concerning advanced hardware, however, there is eagerness, throughout the world, to see the diffusion of high-performance com-

puters (HPCs). The United States has a controlling position in the world market; therefore, the economic gains from wide sales of these machines are substantial. However, HPCs can also be used as a covert means to refine nuclear devices, as well as to aid in the development of other arms, including strategic information warfare weaponry. Thus, the tension in this case between prospects for commercial gain and new worries about weapons diffusion will likely be managed only by an information strategy designed to maintain the equilibrium between competing economic and security values.

Currently, official U.S. policy leans heavily toward openness—in large part because of early assessments that guardedness was infeasible in this area, since the United States is not able to control the diffusion of HPC technology (Goodman, Wolcott, and Burkhart, 1995). This view has been disputed (Arquilla, 1996), and the General Accounting Office, after conducting its own study of the matter, has recently concluded that more-guarded approaches are indeed workable.[1] The key point from this example is that, by adopting a strategy grounded in guarded openness, policymakers might become habituated to seeking out "blended" solutions, and become less susceptible to assessments that rule out from the start either of these aspects of information strategy.

Military-Security Affairs

A major dimension of grand strategy—and of information strategy in particular—is military-security issues. International cooperation in protecting and securing the use of cyberspace and other means of communicating vital information will be necessary for transnational defense. In this realm, it may be necessary to articulate a new vision in which a robust variant of "common defense" will emerge as a top priority to enable both collective security and coalition warfare in the future. Common defense, in terms of information strategy, refers to the notion that all members of a security regime or alliance must have similarly strong remedies against threats to their information infrastructures. Because of the deeply interconnected nature of information security, compromise of one sector could have serious ef-

[1]See Jeff Gerth, "U.S. Agency Faults Study on Exports of Computers," *The New York Times,* September 17, 1998.

fects upon the whole—the chain is only as strong as its weakest link. This implies less "slack" than sometimes existed in Cold War–era collective security regimes, which often had wide disparities in capabilities, and in which deterrence and defense rested on the ability of the strongest partner(s) to defend against aggression. In the future, a compromise in information security of even a smaller member of a coalition might cripple efforts to deal with an attacker. Therefore, information security must be seen of paramount importance to military affairs.

Specifically, common defense would need to be able to cope with three types of threats. First, the alliance's information infrastructure would have to feature sufficient robustness to ensure that disruptive actions, in cyberspace and out, could not seriously compromise the deployment or projection of military forces in a timely manner. A second related, and equally nettlesome, concern relates to the need to guard against cyberspace and other attacks that might be used in conjunction with a subversive insurgent or revolutionary movement, either an internal or external one. The risk in this case would be that a key node in a common defense network might be "brought down" by actions that might not ever be identified as those of an external aggressor.

Finally, global cooperation for information security would also have to address the problem of protection against lesser "pinprick" attacks (for example, by cyberterrorists) on members of the alliance or coalition. Such attacks may be aimed at wearing down the will to engage in an intervention, or to continue an ongoing fight, and represent something of an information-age variant of what the early air power theorists, Douhet (1942) and De Seversky (1942), thought could be achieved with the aerial bombardment of civilian targets. The similarity between the air power theory and lesser attacks on cyberspace infrastructure lies in the vulnerability of a civil population to either air (including missile) or cyberspace attacks, despite the fact that its armed forces have not been defeated in the field.

This vision of the complex military-security dimension of information strategy may face problems on two levels. First, establishing a true "common defense" structure would require the sharing of a great deal of sensitive, proprietary information among alliance and coalition members, and perhaps even with informally aligned

"friends." In an era when allies may later become enemies (e.g., Syria during the Gulf Crisis, and subsequently), the need to disseminate information coupled with the possibility of having only conditionally loyal or inconstant allies pose a dilemma. And, if this concern impedes the development of a collaborative security regime, then not sharing sensitive data may spark an information "arms race"—a competition to develop tools for offensive information warfare—even among putative allies. Thus, there must be both guardedness, to avoid undue security risks, but also enough openness and sharing of sensitive information and technologies to provide disincentives to others to commence such an arms race. Clearly, information arms races would be inimical to the goal of building a global noosphere.

A second concern that could cloud global cooperation in the military-security realm involves the rise of nonstate actors. It is possible that the nature of combatants will blur in future wars, with many participants having principal allegiances to ethnic, religious, or revolutionary movements rather than to nation-states. The tendrils of these organizations will reach into, among, and between states, making these malefactors hard to deter or defend against. TCOs also fall into this category, with their potential to engage in "strategic crime" against a state's political, economic, and social institutions (e.g., in Colombia and, to a lesser degree, in Russia).

The Sociopolitical Arena

In the sociopolitical sphere, unlike in the previous realms, there may be a much more robust, global harmony of interests. Indeed, it is possible that, with the rise of a global civil society, a cooperative noosphere might arise and be sustained even in the absence of strong intergovernmental participatory regimes. This prospect can be characterized as a new "optimistic hypothesis," updating Lipset's (1960) idea of prosperity fostering the advance of democracy. In this newer formulation, interconnectivity would have a democratizing influence on all societies. Thus, the ideal future may be one in which free speech is protected as a public good and is disseminated widely to ever freer audiences. However, it is important to underscore the point that this is a hypothesis—one that might be undermined or falsified by the rise of antidemocratic influences that take advantage

of interconnectivity to sow seeds of repression and distrust rather than of transnational harmony.

Thinking strategically regarding the prospect of democratic social evolution via free flows of information through a burgeoning noosphere, we must note that such flows could create permissive conditions for the waging of activist "social netwars" designed to disrupt state stability and control. On one hand, it is possible to argue that such disruption, aimed at an authoritarian state, is ultimately beneficial. On the other hand, both moral and practical dilemmas would be posed by the near-term disruption of friendly, even if authoritarian, states. Lastly, the ethical guidance provided by a noopolitik perspective on statecraft should impel states to ask whether to allow themselves to be used as sanctuaries for those who attack other states.

Building Global Cooperation

The development of American information strategy, especially in support of building a cooperative global noosphere, requires that the major paths ahead be identified. Two stand out. One path consists of a widespread grassroots effort to foster cooperation from the bottom up. This approach would rely heavily upon contributions from and leadership of NGOs and a variety of other civil society actors; it would also presume upon states to relax their hold on sovereignty. The second path would take a top-down approach, relying upon either the hegemonic stability afforded by a leading power (e.g., the United States is seen by many as providing, by virtue of its matchless power, the basis for a liberal international economic order), or the primacy of such international governmental organizations as the United Nations and the Organization for Economic Cooperation & Development.

Each approach would seek to create an expanding web of cooperation. We note that similar methods—and goals—can be seen in earlier eras. With regard to the rise of market economies, there was the interplay of top-down and bottom-up forces, particularly from the beginning of the age of oceanic discovery in the 16th century. During this era, great trading states sought to expand global trade, often linking with growing regional trading regimes. However, this created a great deal of tension as the great maritime states soon sought to

bend the market to their parochial interests—leading to the highly competitive, conflictual era of mercantilism. Eventually, bottom-up market forces helped to overturn mercantilist tendencies (see Schumpeter, 1954; von Mises, 1957; North, 1981; Rosecrance, 1984).

A similar pattern existed in the realm of power politics, beginning with the emergence of the modern international system—which also started at the dawn of the 16th century. During this period, great empires strove to bring order from the top down. At the same time, local actors often contrived bottom-up balances of power that created small, but often growing, spheres of peace and order. The Italian city-states of this period, in fact, served as the inspiration for the modern notion of the balance of power. However, as in the economic case, the great powers became imperialist in outlook, causing sharp conflicts. A centuries-long struggle between top-down efforts to impose order and grassroots independence movements ensued, with the empires slowly losing ground, until the last, the Soviet Union, dissolved in 1991 (Dehio, 1961; Kennedy, 1987).

These examples from the past suggest that information strategy will likely develop along multiple paths. There may be incentives to achieve order through a top-down process: (1) American primacy; (2) central institutions, such as the World Court and the United Nations; or (3) alliances of leading states, such as NATO. There will also be grassroots efforts to build a global noosphere from the bottom up, led principally by nonstate actors, especially NGOs. And, just as the market economics and power politics of the past featured tensions between the two approaches to establishing order and cooperation, there will likely be similar frictions in the information age. For example, encouraging a benevolent American hegemony may spark resistance; the United Nations may be hamstrung by the loss of consensus among those with veto power; and NATO's expanding web of security may encourage unruly counterbalancing responses. Indeed, the many constraints on top-down approaches leave room for noosphere-building by nonstate—particularly global civil society—actors.

However, some states, confronted with this challenge to their control of the international system, may act in concert to try to delimit the influence of NGOs. Whether such states succeed in suppressing the rise of the noosphere—or have sufficient motivation even to try—

seems problematic. A far more productive approach would be for states to recognize the comparative advantages of working with, rather than against, NGOs. In this insight lie the beginnings of a true revolution in diplomatic affairs.

To cope with these sorts of problems, a skillful blending of the top-down and bottom-up methods may help in sidestepping the pitfalls of conflict and threat. Such a hybrid strategy would likely feature use of American political, economic, and military capabilities to deliberately empower nonstate actors—including by bringing them into the United Nations (Toffler and Toffler, 1997). In some ways, this strategy is analogous to the Cold War–era strengthening of war-torn Western Europe and Japan against the communist threat—as the United States used its power to build up others, even to the point of creating new economic giants that could rival its own market power.

There are risks in such a strategy. A vibrant, NGO-led global civil society might one day effectively curtail the exercise of American power in some arenas. Yet, if free flows of information do indeed foster democracy and open markets, the benefits of such a strategy are likely to exceed the liabilities. However, even as the United States leads in the creation of what some in (and out of) government are calling an "information commonwealth" (e.g., Cooper, 1997), it must also be remembered that the emerging norms of noopolitik will rise and take hold in a world rife with the conflicts endemic to realpolitik.

INFORMATION STRATEGY IN CRISIS AND CONFLICT

In addition to addressing the uses of information strategy in peacetime, it is also necessary to examine the strategic utility of information in crisis and conflict. With this in mind, this section focuses on two major dimensions of information strategy: public diplomacy and strategic information warfare. The former consists primarily of the use of the "content" aspect of information to influence behavior of an adversary—whether a mass public, a specific leader, or both (on this, see Manheim, 1994). The latter comprises the efforts to strike at an enemy's information conduits (from military command and control to industrial and other infrastructures) by principally electronic means (Molander, Riddile, and Wilson, 1996). Also, we note that although public diplomacy is most useful in crisis, it may also prove effective in wartime. In addition, strategic information

warfare strikes, although clearly intended for use in wartime, might also have great preemptive effect if used during a crisis. For those reasons, it is time now to develop a strategic information doctrine to help guide and govern the use of public diplomacy and information warfare in crisis and conflict.

The Role of Public Diplomacy

In the area of public diplomacy, we consider several key issues. First, to have truly strategic (i.e., lasting) effect, initiatives in this area should be based on the truth. This is already a fundamental tenet of the American practice of psychological operations, as can be seen in Joint Publication 3-53, *Doctrine for Psychological Operations*. But it must be noted that others have, in the past, found great value in the use of falsehoods—seeking strategic leverage through deception. During the Cold War, the Soviet Union adopted this approach for psychological operations, which were often effective for long periods of time (see Radvanyi, 1990). In our view, an approach based on falsehoods will more likely have only short-term, or tactical effects—not enduring strategic ones. Therefore, truth must be the polestar of American strategic public diplomacy, and uses of information as "propaganda" should be eschewed.

The effective use of public diplomacy will likely hinge upon the ability of nation-states to reach out to and form "deep coalitions" (term from Toffler and Toffler, 1997) with NGOs. In this way U.S. public diplomacy would be complemented by the actions of countless supporters operating on behalf of an emerging global civil society steeped in American-oriented values: democracy, human rights, and social, political, and economic liberalism. A key doctrinal question is, What should be done when global civil society differs in its aims from what are thought to be key American interests? The answer to this question is two-part.

First, U.S. information strategy could determine whether civil society actors are divided or largely united in their views. If divided, then the clear strategy is to reach out to those most congenial to the American position and to ally with them to help shape the world perceptual environment. Second, if there were widespread opposition to an American policy position, there may be a need to reconsider the policy itself. The goal would be to amend it so as to bring policy

more into line with the preferences of civil society. Failure to do so would greatly hamper the ability to continue using public diplomacy in the given issue area.

An example of this sort of problem is the U.S. policy in response to the global civil society effort to ban land mines. U.S. leaders, keenly aware of the broad international consensus on the ban, and the unanimity among the NGOs, strove to soften the American position by seeking a phaseout over a 10-year period, with an exception made for the Korean peninsula. These marginal adjustments to U.S. policy had little effect on the activities of the movement to ban land mines—which have led to the signing of a multilateral treaty by over 100 countries. The United States has refused to sign it, mainly for military reasons. Yet, if the United States were to reconsider its position on this issue it could focus on rethinking the military's reliance on land mines, either in the form of shifting to new maneuver doctrines that have little utility for land mines or in the form of developing mobile mines that will move along with ground troops. Either solution would resolve the issue, and both may lead to better military doctrines.

The key point is that when faced with serious and sustained opposition from global civil society (and by many nation-states also) to a particular policy, America will not find that public diplomacy alone will prevail in the arena of international discourse. It will be necessary, in cases like these, to reconsider the policy in question very carefully and to let the world know that reassessment is under way.

Strategic Information Doctrine (SID)

From the 1997 report of the President's Commission on Critical Infrastructure Protection and the emerging spate of government, military, and academic studies, it seems clear that most analysts accept the argument that strategic information warfare (SIW)—electronic attack against communications, transport, and other key nodes—has emerged as a threat to U.S. national security. While there is some concern about threats from other nations, the basic American view is that this type of war, or cyberterror, will be commonly wielded by nonstate adversaries. Abroad, we also see that there is international consensus about this threat to foreign assets as well—however, foreign (especially Russian and Chinese) views of SIW generally see

the United States as the serious threat (Thomas, 1997; Arquilla and Karmel, 1997).

Against this backdrop, incentives are growing for the United States to move toward the development of a "wartime" strategic information doctrine (SID) to complement its peacetime approaches to perception management and public diplomacy. To date, strategic thinking in this issue area is redolent with nuclear-era concepts. With regard to defense, it has been argued by the President's Commission on Critical Infrastructure Protection and others (e.g., see Molander, Riddile, and Wilson, 1996) that a "minimum essential information infrastructure" (MEII) be created. This notion has clear roots in the nuclear-era minimum essential emergency communication network (MEECN). On the offensive side, SIW is seen as consisting of strikes that aim at countervalue or counterforce targets—either in massive or proportionate retaliatory fashion.

The nuclear analogy will likely prove to be an insufficient basis for developing a clear strategic framework for waging information warfare. The differences between nuclear war and SIW are too great, beginning with the overwhelming destructive power of nuclear weapons, whose very lethality has made deterrence strong for over 50 years. By comparison, SIW is basically disruptive rather than destructive. Furthermore, the nuclear "club" remains small and is still composed of states only, while SIW does not require the wherewithal of a state. Moreover, it is extremely unlikely that a nuclear attack could be undertaken anonymously, or deniably. SIW is characterized by the inherent ease with which perpetrators may maintain their anonymity.

A final difference between the two is that even today, over half a century into the nuclear age, defenses remain minimal and problematic (partly a result of political decisions not to develop robust defenses during the Cold War).[2] In the area of information security, however, good—although certainly not leakproof—defenses have been identifiable from the outset. As to the current state of defenses of the information infrastructure, Willis Ware has put it succinctly, "There is no evidence that 'the sky is falling'" (1998, p. vii).

---

[2]This point is highlighted by the recent (May 1998) failures in field experiments held to test the efficacy of a theater high-altitude area defense (THAAD).

In the case of SIW, the effort to look ahead, doctrinally, is not likely to be well rewarded by looking back to the nuclear paradigm—save perhaps for the exception provided by the nuclear "no first use" concept, as discussed below. Instead, there must be fresh theorizing about the nature and scope of SIW, which must then be related to American national security needs. What are these needs? On the defensive, or guarded side, the United States must develop a robust information security regime that protects both the ability to project military force abroad and the key nodes that sustain the American way of life at home.

The MEII, as originally conceptualized, is not likely to achieve a secure infosphere for either of these needs. The MEII allows much of the United States to remain wide open to disruption; it also misses the point that present military reliance upon civilian communications means that an insecure civilian sector imperils American military capabilities. However, broad use of strong encryption will substantially improve the defenses of both the civilian and military sectors from the threat posed by SIW.[3] An important recent development has been the effort to rethink the very notions of what constitutes a "minimum" information infrastructure, and what indeed is "essential." This line of discussion holds out the promise that it will be possible to create layers of information security that vary across those areas where there is either a substantial or a poor ability to control access and use (Anderson et al., forthcoming).

On the more proactive side, the United States should develop a SID that eschews first use of information attacks on others. In this regard, SIW features many of the moral dilemmas that were part of the emergence of strategic air power (e.g., see Arquilla, forthcoming).

Generally speaking, an ethical imperative to avoid first use of SIW could actually have practical benefits. This is the case because the United States has the largest set of information targets in the world—and will continue to do so for the foreseeable future. In this regard,

---

[3]It must be recognized that the price of diffusing strong encryption throughout cyberspace will decrease government ability to gain access to private communications. FBI director Louis Freeh has been the most articulate opponent of widespread diffusion of strong encryption tools, citing the limiting effect it would have on criminal investigations. However, examination of all federal prosecutions in 1996 indicates that less than one one-hundredth of a percent of these cases employed cybertaps.

an American information strategy aimed at mounting normative prohibitions on the use of SIW could form a powerful step in the direction of fostering noopolitik. But, as desirable as this might be, a convention on no first use (one of the few nuclear-age concepts that does have information-age relevance) would also hinder the United States from using SIW as a preemptive tool in a crisis or conflict situation.

The solution to this moral dilemma may lie in the medieval Thomist "just-war" formulation about the need to balance the benefits of an act against the harm done. Seen in this light, the United States might then introduce doctrinal nuances, such as reserving the right to use information attack first only if the adversary has already begun to use other forms of force—and if the initiator of SIW has the clear intent to engage in information operations as a means to foreshorten military operations.

In sum, a strategic information doctrine for crisis and conflict should be built around two doctrines. First, to defend and protect against information attacks, emphasis should be placed on a regime where the most advanced encryption is disseminated widely. Second, regarding offensive SIW, doctrine must be driven by the constraints of an ethical noopolitik—with the benefit that placing constraints on first use will likely have practical positive effects. These are key strategic issues for information doctrine in crisis and war that can and should form the core of thinking about defense against, as well as use of, SIW.