This briefing elucidates a concept—"netwar"—that we mentioned in an earlier article on "cyberwar." Whereas the latter term refers primarily to information-based military operations designed to disrupt an adversary, netwar relates to lower-intensity conflict at the societal end of the spectrum. In our view, netwar is likely to be the more prevalent and challenging form of conflict in the emerging information age and merits careful and sustained study.

In terms of conduct, netwar refers to conflicts in which a combatant is organized along networked lines or employs networks for operational control and other communications. The organizational forms that netwar actors adopt may resemble "stars" that have some centralized elements, or "chains" that are linear, but the major design will tend to be "all-channel" networks in which each principal node of an organization can communicate and interact with every other node. Further, netwar actors may develop hybrid structures that incorporate elements of some or all of the above designs in varied ways. Strong netwar actors will have not only organizational, but also doctrinal, technological, and social layers that emphasize network designs. Netwar actors may make heavy use of cyberspace, but that is not their defining characteristic—they subsist and operate in areas beyond it.

Because of changes in the context for possible conflict, netwar will no doubt prove most attractive, for the near-term future, to nonstate actors. It is likely to become a policy tool of choice for ethnonationalists, terrorists, and transnational criminal and revolutionary organizations. However, nation-states may increasingly find netwar a useful option, especially when the need to pursue limited aims with limited means arises. Additionally, the rise of a global civil society heralds the possibility that nongovernmental organizations associated with militant social activism will become netwar combatants, deliberately or sometimes inadvertently. Overall, the context of netwar may come to be defined by conflicts between state and nonstate actors, nonstate actors that use states as arenas, or states that use nonstate actors as their proxies.

The emergence of netwar implies a need to rethink strategy and doctrine, since traditional notions of war as a sequential process based on massing, maneuvering, and fighting will likely prove inadequate to cope with a nonlinear landscape of conflict in which societal and military elements are closely intermingled. In our view, traditional warfare fits the Western paradigm symbolized by chess, where territory is very

important, units are functionally specialized, and operations proceed sequentially until checkmate. Netwar, however, requires a new analytic paradigm, which, we argue, is provided by the Oriental game of Go, where there are no "fronts," offense and defense are often blurred, and fortifications and massing simply provide targets for implosive attacks. Victory is achieved not by checkmate, as there is no king to decapitate, but by gaining control of a greater amount of the "battlespace."

The equilibrium between offense and defense is another issue of concern. Historically, developments that change the context and/or conduct of war have generally introduced periods of offense- or defense-dominance. On the one hand, the science of fortification long gave the defensive great advantages. On the other hand, mechanization gave the advantage to the offensive. In each case, though, a reaction process occurred, which restored the equilibrium between offense and defense. With regard to netwar, we see an initial period of offense-dominance emerging. This requires the United States to focus on defensive netwar. Briefly, we find that the best chances for successful defense will arise when the defenders move toward more networked structures, emulating the organization, but not necessarily the tactics, of the attackers.

In terms of implications for policy, we argue that forming networks to fight networks and decentralizing operational decisionmaking authority will likely improve the ability of the United States to combat transnational crime and terrorism and to counter the proliferation efforts of rogue states and their nonstate support networks. Further, we urge the establishment of an "information war room" whose purpose would be to provide timely assessments of the netwar capabilities of plausible adversaries, including the preparation of detailed "information orders of battle."

Our concerns about the rapid emergence and likely profusion of netwars in the coming years lead us to call for the creation of a center devoted specifically to developing the means for countering this emergent form of conflict. The institute would serve both as a generator of and clearinghouse for ideas. The scope of activities would include the issue areas of strategy, doctrine, organization, and technology. In addition, an institute for the study of information should also emerge. It would address issues of society and security in the information age that go well beyond the pressing concerns of preparing to wage netwar. Indeed, this institute would help establish a new academic discipline, one that would address key political, economic, social, and military issue areas.

The report that follows addresses and outlines, we believe, the issues that ought to be studied in these two centers, and demonstrates the deductive and comparative methodologies that might be employed.