

### Technology and Doctrine in the Information Age

- **Historically, offense often dominates**
    - Long spears of the Macedonians
    - Marriage of gun and sail
    - Cooperation of tank and plane
  - **Defense sometimes comes to the fore**
    - Geometrically designed fortifications
    - Barbed wire and machine guns
    - Patriot and other ballistic missile defenses?
  - **Netwar signals an offense-dominant era**
    - Greater disruptive power in smaller units
    - Wealth of targets, often openly accessible
    - Like LIC or insurgent/partisan warfare
- ⇒ **Emphasize defense to reestablish equilibrium**

In prior eras of military innovation, technological and doctrinal improvements tended to favor either the offense or the defense. For example, nearly doubling the length of the infantry spear (to 16 feet) gave Alexander's Macedonians incomparable advantages in open battle. When wedded to the doctrine of the phalanx, it generated sufficient offensive power to conquer the known world in a very short time. In the late middle ages, the *trace italienne*, a fortification scheme based on advanced construction techniques and a geometry-based doctrine of creating mutually supporting strong points, gave similarly substantial advantages, but this time to the defensive. Later, the combination of gun and sail gave Western Europeans the ability to exert a centuries-long dominance around the world. In the machine age, the internal combustion engine made tanks and planes possible, eventually inspiring the blitzkrieg doctrine that ended the defensive dominance of artillery, barbed wire, and machine guns. The list is as long as history, up through and including recent developments in ballistic missile defenses (BMD).

More recently, mutual nuclear deterrence equated to the superiority of the defensive. However, at the low-intensity end of the spectrum, innovative approaches to revolutionary warfare created tremendous opportunities for the weak to attack the strong, much as North Vietnam challenged American might in the North's campaign of conquest against the South.

In the information age, what will be the case? We anticipate that netwar will resemble low-intensity conflict (LIC) more than nuclear or high-intensity conventional warfare; that it will have many of LIC's offense-dominant attributes. If this is true, there is a pressing need for new doctrinal insights to revivify deterrence and defense. However, it may be that deterrence against netwar will grow problematic, and all that will remain is a choice between either preclusive or depth-oriented defensive schemes. The former implies an ability to provide "leak-proof" defenses, while the latter accepts initial incursions, then aims to expel the intruders or invaders by means of counterattack.

These strategic choices mirror, in many ways, the problems facing the German High Command in the spring of 1944 in Western Europe. Field Marshal Erwin Rommel took a preclusive approach, urging the use of all 60 divisions available to prevent the establishment of an Allied lodgement on the continent. His immediate superior, Field Marshal Gerd von Rundstedt, championed the notion of forming a depth-oriented reaction force that would allow initial landings, then fight a decisive battle of maneuver in the French countryside. After months of fractious debate, Hitler chose a bureaucratic compromise between the two, which made neither approach feasible.

Whatever strategy (or hybrid) is employed to defend against netwar, the age-old cycle of action and reaction between offense and defense appears to be under way again. The path to a new equilibrium is not yet clearly mapped out, and choices made now will have lasting, powerful effects.

The next two charts and their texts begin to address some strategic and doctrinal issues that the U.S. government may face if it has to prepare to defend against netwar actors who may be violently aggressive toward the United States. The supposition is that such actors, by combining aspects of Hamas and the Legion of Doom, would attack through both cyberspace and irregular military (or paramilitary) means. Thus, the text about these two charts does not apply to activist NGOs, though the subsequent charts comparing chess and Go as paradigms of conflict do apply broadly to all varieties of netwar actors.

## Issues for Defensive Netwar

- **Improve intelligence on all levels of adversaries: organizational, doctrinal, technological, and social**
    - Tighten links between warning and response
    - Incorporate alternative images of adversaries
  - **Adapt operational postures to counter adversaries**
    - Detection, protection, and tracking
    - Deterrence, preemption, and prevention
  - **Develop new methods of net assessment**
- Remember: Information warfare is not reducible to computer or cyberspace warfare**

From the American perspective, it seems clear that a key issue will be to move expeditiously toward the development of capabilities for waging defensive netwar. Thankfully, the immediate post-Cold War period has brought a substantially lessened nuclear threat (though it does persist), and U.S. conventional forces enjoy a preeminence seldom seen in world history. The same cannot be said of U.S. preparedness for netwar. Indeed, without sounding unduly alarmist, we feel it necessary to warn of the possibility of a “netwar gap” that sees U.S. adversaries in possession of relatively greater capabilities for waging this lower-intensity form of warfare.

Counternetwar will require intelligence of a type different from that which was most useful during the Cold War. Counting tanks, guns, planes, and other such weaponry must give way to developing information about a potential adversary’s organizational structures, the better to be able to target his key nodes. Threat assessment will naturally involve examining an adversary’s capabilities *and* intentions. However, intelligence may have to shift from the Cold War focus on capabilities to giving primary attention to intentions. During the period of U.S.-Soviet rivalry, it was prudent to hedge, keeping the adversary’s capabilities uppermost in mind, particularly because intentions could not be discerned easily. In the information age, the “intentions side” of the equation has become even less clear, but more important—especially since the societal aspects of netwar revolve more around the less tangible power of ideas and of networked organizational structures. However, since netwar aggression will often be accompanied by an open declaratory policy (e.g., political independence or respect for human rights), there may also be new opportunities for generating insights into intentions.

Improved intelligence may also be needed to help couple warning and response more tightly. As opposed to the Cold War situation in which possession of survivable

second-strike forces enabled the superpowers to eschew doctrines of “launch on warning,” in netwar, by the time warning is received, great damage may already have been done. Thus, it may be incumbent upon decisionmakers to move with dispatch on the basis of warning, and it is vital for intelligence gatherers to provide real-time information as little susceptible to ambiguous interpretation or misconstruction as possible.

In netwar, the attacker may often be difficult to identify. To deal with this ambiguity, defenders may find it useful to use an approach that provides alternative images of the attacker. This analytic framework enables the defender to construct and assess well-hedged defensive strategies, even when uncertainty about the attacker’s identity persists. If, for example, it is unclear whether the attacker is a disgruntled individual (a Unabomber), a small group of malcontents (most likely the case with Sheikh Rahman and his adherents), or a full-blown terrorist organization, perhaps with state sponsorship, then considering the possibility of any of the three being the attacker will usefully inform the search for countermeasures (see Davis and Arquilla 1991a, 1991b). This hedged approach, which relies upon alternate imaging of the adversary, may help to prevent overreaction against minor miscreants. However, this approach may also make it much harder to arrive at decisions to retaliate massively against more serious attackers and/or putative sponsors whose identities have not been established beyond doubt. Indeed, this problem of ultimate identification may be a central security dilemma posed by the advent of netwar.

In tactical, or even operational, terms, defensive netwar will be concerned with three functions: detection, protection, and tracking. Briefly, the ideal in detection would be to gain awareness of an attacker before an incursion is made (either in cyberspace or in terms of some nascent societal-level movement). Practically, however, absent outstanding intelligence about enemy intentions, detection will more likely occur only after an attack has begun. With this in mind, protection will become a key operational task in defensive netwar. Damage limitation will be a primary goal and may be pursued through efforts at preclusive security (e.g., by “firewalls,” or by raising public awareness of the nature of the opponent and its aims), or by allowing the attacker some “running room,” then tracking him down.

Clearly, the greatest operational emphasis in defensive netwar must be protection. Understanding one’s own key institutional nodes is crucial, because defensive robustness will revolve around either the protection of such nodes or the development of redundancies to mitigate their potential loss. Presently, the amorphous nature of the offensive netwar threat makes for an unwillingness to incur the expenditures necessary to provide such protection. Indeed, the situation is not unlike that along the eastern U.S. seaboard during the first months after American entry into World War II. The nature of the U-boat threat was not yet fully understood, and there was an unfortunate practice of allowing port cities to remain illuminated at night. This created something of a “happy time” for German submarine captains, since leaving the harbor lights on allowed them to acquire well-silhouetted targets easily. At present, the netwar threat poses a new “harbor lights” problem, in cyberspace and in the real worlds of government, commerce, and society. For example, there is too little encryption of important military, scientific, and commercial/financial data, and

too much intellectual property readily identifiable and accessible to those who might use such information malevolently.

At the strategic level of analysis, three major concerns of defensive netwar are deterrence, preemption, and prevention. The first relates to the conditions under which an adversary will be dissuaded from launching a netwar offensive. Preemption only comes into play when the defender believes an attack is coming and decides to strike first to avoid or weaken the offensive blow. Finally, prevention seeks to cripple potential netwar adversaries *before* they develop their offensive capabilities. Each of these three strategic perspectives has merits, but also problems, some quite serious.

A deterrent strategy is the most purely defensive in nature. However, a problem with effecting it is that the intelligence requirements for detecting an immediate netwar threat are huge. Even if signs of an impending attack are uncovered, there is a strong possibility that the true identity of the aggressor will be shielded. These problems should lead us to infer that successful deterrence under conditions of uncertainty may rely, ultimately, on the development of protective (i.e., preclusive as well as damage-limiting) measures that serve to convince a potential attacker that the defense can *deny* him the achievement of his aims. This is contrary to Cold War-era deterrence, which relied heavily on *punitive* threats to keep the peace.

Because of the difficulties in correctly identifying a netwar attacker, “denial deterrence” may now have to come to the fore. However, there will no doubt be occasions when the attacker’s identity is clearly established. In these situations, retaliatory punitive action would seem appropriate so as to provide a dissuasive example for other would-be attackers. But what if the attacker strikes at some key aspect of the U.S. information infrastructure and has no similar set of targets of his own that can be held at risk?

An answer to this problem is that retaliation need not be in kind, though proportionality ought, in general, to be the goal (Schelling, 1966). A nuclear response to a state-sponsored attack in cyberspace is wildly disproportionate, but precision bombing of enemy intelligence or other military facilities would likely be appropriate. Depending on the clarity of the evidence identifying the attacker, and the attendant international political costs of a disproportionate punitive response, there may also be occasions on which a kind of “massive conventional retaliation” can be carried out. In such instances, disproportionate responses may have lasting deterrent effects on both the attacker in question, and upon other potential attackers.

Because of the subtle nature of netwar, which makes even deterrence problematic, the prospects for developing a successful preemptive strategic doctrine seem slight at this time. Technical constraints aside, the political costs of preempting, based even on the most compelling indicators, could be enormous. Netwar does not require lengthy mobilization processes common in other forms of warfare. This difference may leave an aggressor in the position of being able to deny plausibly that he ever intended to attack. However, if intelligence indicating an attack is strong enough, decisionmakers will need to weigh the political costs of preemption against the damage likely to be incurred in the netwar attack. There may well be times when preempting, then taking the international “heat,” is the optimal course of action.

Preventive defensive netwar is perhaps the most controversial strategy, because it implies a willingness to keep a potential adversary from developing offensive capabilities. If the political costs of preemption are high, then the price of prevention is likely to be astronomical because, operationally, it will look much like attacking an innocent bystander. However, preventive netwar might also consist of measures scarcely detectable, such as maintaining a “forward presence” inside an information infrastructure, or inside a particular societal or political movement. The implication here is that having preventive netwar as a policy option may require considerable capabilities for intelligence collection and for covert action, an issue that raises political, administrative, and legal questions (see Reisman and Baker, 1992).

## **Will Paradigm Shift Be Required?**

**In a world of netwars, where boundaries are blurred between peace and war, and offense and defense:**

- **How will threats be assessed?**
  - **What will determine and set priorities?**
  - **Will we have to select which netwars to counter?**
- **Will defense or offense predominate?**
- **What will be key new considerations for strategy?**
  - **Linear vs. nonlinear**
  - **Sequential vs. cumulative**
- **Will netwar reflect Sun Tzu more than Clausewitz?**

In the emerging information age, the conduct and context of conflict are undergoing radical transformations. Indeed, the multidimensional nature of netwar makes it ever more difficult to demarcate clearly between peace and war. For example, the rise of a politico-military movement, like the EZLN in Mexico, may signal the opening of a netwar for control of the state, even in the absence of ongoing military operations to seize the state. Or, as in Colombia, state institutions may be compromised or kept under siege by TCOs as part of their day-to-day operations.

Many netwar actions and operations, with regard to offense or defense, are observationally equivalent. Thus, preemptive or preventive actions of a tactically or strategically defensive nature may actually be perceived as offensives. But the reverse may also be true, in that some offensives may not appear as such, weakening the linkage between warning and response. This is quite different from more traditional types of warfare. For example, a conventional blitzkrieg features fast-paced, well-integrated combined-arms operations and is clearly recognizable as offensive. In contrast, netwar actions, such as degrading an opponent's communications structures, may be either offensive or defensive, or both.

Because netwars are easy to start and wage, there may be many of them going on all of the time. The average number of conventional wars in progress since 1990 has been about 30 (see Brassey's 1991–1994; and Stockholm International Peace Research Institute, 1991–1995). We should expect the number of netwars to increase by an order of magnitude.

This likely profusion of netwars implies a need for prioritization, and for a new calculus of intervention. It is not clear that the public-opinion-oriented criteria of the Weinberger Doctrine (1984) still apply, given that the early stages of intervention,

and perhaps the later ones, will often take place outside the public's knowledge. Also, victory in netwar may not resemble the winning of more conventional conflicts and may defy easy definition or characterization.

Public support and high probabilities of winning aside, some of the Weinberger Doctrine's other guidelines also seem problematic when applied to netwar, particularly its requirement that clear military and political objectives be present from the outset. In counternetwar, clarity may not be achieved for a long time, since attackers will often mask their ultimate objectives as long as possible. To require clarity as a prerequisite for intervention would be to debilitate defensive netwar from the outset.

Perhaps what is needed is a broader, but still practically useful, set of measures for prioritizing interventions. Perhaps Mill's (1857) admonition to limit involvement to countering others' interventions is a good starting point. However, even this limitation to waging counternetwar defensively is likely to leave an overabundance of potential cases for involvement. The best solution to this dilemma may lie in developing a fully articulated methodology for assessing netwar threats, one that would perform a strategic-level *triage*.

One category of triage, the most urgent, would be for cases requiring immediate action, lest some U.S. friend or interest suffer grievous harm or loss. U.S. economic and even military cooperation with Mexico to deal with major, violent instability along the border or to intensify the fight against drug cartels could fall into this category. A second class of cases might contain those in which the victim of netwar may suffer but is likely to ultimately prevail on its own (e.g., Russia's current fight against Chechen guerrillas and criminal elements). Finally, there will always be some set of cases where the costs and risks of intervention in a netwar will outweigh the plausible benefits. Avoidance might be the advisable stance for these (e.g., the ideological, social, and military struggle for control of Algeria).

Despite all the blurring between war and peace, and between offense and defense, the question still stands as to whether offense or defense will predominate in netwar. The advent of netwar is similar to the rise of earlier forms of conflict in that offensive action is initially the easier, and more likely successful, tack (Quester, 1977). This is one reason why U.S. policy faces a challenge in having to emphasize defensive netwar—with the goal of reestablishing an equilibrium between offense and defense.

Strategically, netwar appears to depart from earlier modes of conflict in that it is nonlinear. In the past, warfare and other forms of conflict have tended to follow linear, sequential patterns based on geographically derived aims. Now, in place of linearity and sequential objective-seeking, netwar may be waged anywhere, at any time. Victory will come not so much to those who reach some geographical objective, as to those whose efforts accumulate a set of advantages. Thus, the Mexican military's occupation of Chiapas may have been more than offset by the EZLN's gains in mustering NGO support for its reform agenda. In this case, a territorially oriented counterinsurgency was outflanked by a movement well aware that the netwar "battlespace" extended far beyond the limits of a remote southern state of Mexico.

In the metaphor of board games, the aim in netwar is not for checkmate, as in chess, but rather for control of more of the continuum of conflict, as in Go. Interestingly, Wylie's (1967) visions of cumulative versus sequential strategies offered early, prescient insights into the likely future of conflict. Also, some theorists of nuclear strategy were, because of the nature of the weapons they considered, strategically steeped in both nonlinear and cumulative notions (Kissinger, 1957; Kahn, 1960).

Go, a product of the East, may offer more insights than chess, the favorite of the West. So Western strategic thought, as epitomized by Clausewitz and Jomini, may have to give ground to Sun Tzu, the great Chinese strategic thinker. One key difference between the two is that Clausewitz tended to downplay the importance of informational factors, believing that the problem of "friction" would vitiate any advantages won by means of a "knowledge strategy" (see Handel, 1991). Sun Tzu, however, held that information dominance was crucial to victory, tactical or strategic, and that control of information could create a condition of "entropy" in the opposing camp.

Sun Tzu also held that the key to victory lay more in position than maneuver, arguing that the possession of key points (not "fronts" but points) could lead to victory even in the absence of battle. This idea runs counter to Clausewitz's view that victory could only be won through an unflinching willingness to engage in bloody fighting for territorial dominance.

In the information age, Sun Tzu may thus provide a more appropriate foundation for the development of a new strategic paradigm. Just as in many areas of activity, a "Pacific Century" is emerging, so key advice for strategic thinkers may be, "go East" (as opposed to Horace Greeley's advice to go West).

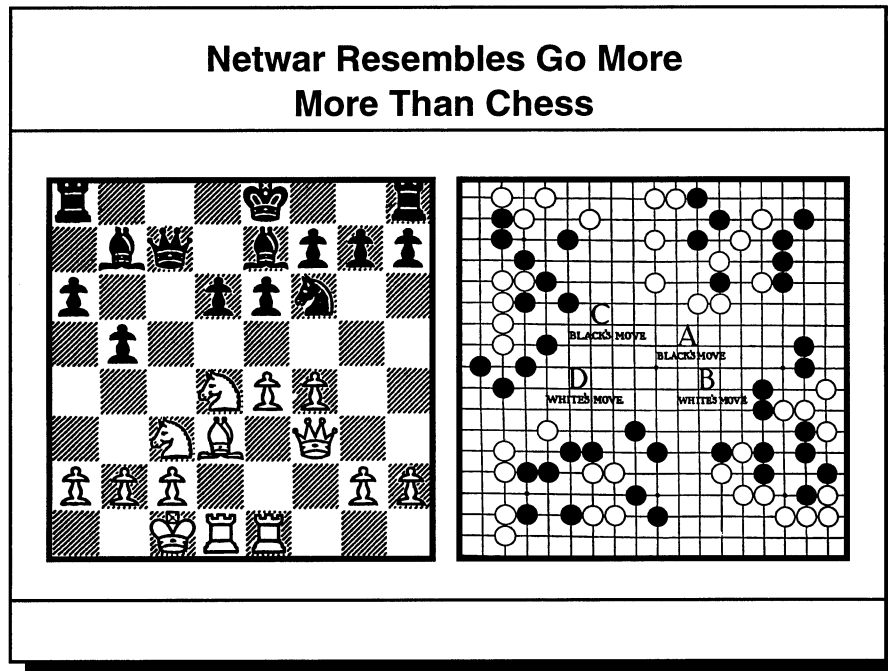
Previous views of history have inclined toward a view of conflict as dual in nature. For most, warfare is either positional or maneuver-oriented (Liddell Hart, 1954). Hans Delbrück (1900) also adopted a dual definition, contending that conflict was of two types, either "exhaustion" or "annihilation." He noted the Periclean strategy at the outset of the Peloponnesian War as a key example of attritional warfare; he saw the campaigns of Napoleon as the apex of "decisive battle."

More-modern examples of these two types of war abound. World War I was certainly fought to exhaustion, and the major limited conflicts of the Cold War-era (Korea and Vietnam) and numerous civil wars (from Guatemala to Angola) were clearly attritional in nature. World War II, however, was decided by great annihilational battles (Stalingrad and Normandy, in particular); and many internal wars have aimed at the utter destruction of one side, as can be seen in recent societal conflicts, from Bosnia's "ethnic cleansing" to the outright genocide that took place in Rwanda.

In our view, a new paradigm for conflict is needed that incorporates the various implications of the information age. Broadly put, conflict may be moving beyond attrition and/or annihilation to a new phase in which "information dominance" (Arquilla, 1994) may allow for victory through *disruption*. In the future, it may be likely that forces disrupted cannot fight with any degree of effectiveness. Certainly the Persian Gulf War provides an example of a very large, well-armed military that was almost completely disrupted because of strikes at its key communications nodes.

Victory was achieved at very modest cost, relative to the comparative historical experience of other wars.

Next, using our game metaphors, we explore further these notions of the blurring of offense and defense, nonlinearity, cumulative strategy, and disruption as a new “third face” of conflict. The following discussion of chess and Go is drawn from Arquilla and Ronfeldt (1996).



As in the past, war and other modes of conflict in the information age will continue to bear resemblances to the game of chess. But such conflicts will increasingly take on characteristics of the “double-blind” chess variant *kriegsspiel* and of the very different Japanese game Go. If chess or *kriegsspiel* were played so that one’s own side has sight of both his and his opponent’s pieces, but the opponent can see only his own pieces, then we would have an analogy for military “cyberwar.” For an analogy for social and other types of “netwar,” we would play Go so that, again, one’s own side sees all pieces but the opponent sees only his own pieces.

In chess, each side has a king and five other types of specialized pieces. Each piece, including the king, has a different “value” and a different ability to move. Each side lines up its pieces in assigned positions on opposite sides of the game board. Thus the two sides face off across a “front line.” Then, each side maneuvers in ways that are generally designed to fight for control of the board’s center, to shield one’s valuable pieces from being taken, to use combinations of pieces selectively to threaten and capture the opponent’s pieces, and ultimately to achieve checkmate (decapitation) of the one-and-only king. Warfare before World War II was often like this and, indeed, frequently continued to retain this linear flavor up through the Persian Gulf War.

For the age of cyberwar, a modified *kriegsspiel* analogy is more apt. *Kriegsspiel* is based on chess—the board, the pieces, and the rules are similar—but the game is operationally distinct. Each player has his own board and arrays his pieces as in chess. A screen to block vision stands between the two boards, manned by a monitor (referee). Thus, once the game starts, each player knows where he has moved his pieces but cannot see, and must guess based on limited information, where the other player moves. The monitor signals when contact is made. Then, whoever’s turn is

next gets to choose whether to take the contacted piece or make another move. He does not see what piece he may take until he has taken it, and it is handed to him by the monitor.

Throughout the game, each player speculates but rarely knows which of the opponent's pieces are where. The game revolves around information vacuums and uncertainties. A premium is placed on deception. Indeed, a player who opens with classic chess moves and strategies—e.g., controlling the center—is likely to lose. (The edges of the board may become more important for maneuver than the center.)

The aim of cyberwar is for its side (the United States) to play chess—i.e., to have full sight of its own and the opponent's pieces—while blinding the opponent so that it has to play *kriegsspiel*, at best knowing the location only of its own pieces, and maybe not even that. In this analogy, both sides start with similar mass and energy—the same set of pieces—at their disposal. But the U.S. side has an enormous informational advantage—what David Gelernter (1991) calls “topside”—and because of this, each of the U.S. pieces is well informed. This advantage means that the United States should not require as many pieces to win; it might even be able to achieve checkmate without taking many of the opponent's pieces. The Persian Gulf War was, in some respects, rather like this and marks a watershed in the transition from traditional attritional warfare to a new generation of information-age warfare.

## Strategic Characteristics of Go Differ from Chess

- Go starts with empty board
- All pieces (“stones”) are identical—unlike specialization in chess
- No preassigned starting positions; multilinear opening moves
- Primary aim is to surround territory—taking pieces is secondary
- Decapitation not possible—no “king” in Go
- Control of corners and edges precedes control of center
- Presence is more important than maneuver—distributing pieces is more important than massing them
- Defense and offense blurred
- Success depends on lines of communication to link pieces
- Go ends with full board; winner has largest secure territories

The game of Go provides a better analogy for netwar, i.e., for networked types of conflict and crime at the opposite end of the spectrum from high-intensity conventional warfare. Whereas chess starts with all pieces on the board, this game starts with an empty board. It resembles a vast, grid-like chessboard with lots of tiny squares. Each side takes turns placing pieces called “stones” anywhere on the board, one by one. But the stones are placed not in the squares as in chess, but on the points where the grid lines intersect. All stones are alike—there is no king to decapitate, and no queen or other specialization.

Once placed, a piece cannot move; it can only be removed, if surrounded and captured according to the rules. But in this game, taking pieces has secondary importance. The goal is to surround and hold more territory than one’s opponent. Once emplaced, a piece exerts a presence in that part of the board, making it easier for the player to place additional pieces on nearby points in the process of surrounding territory. As a result, there is almost never a front line, and the major battles are less for control of the center than for the corners and sides (since they are easier to box off). And whereas in chess no piece is ever totally secure, in Go a piece of territory can be made totally secure if it is surrounded in a particular way (in Go parlance, given two “eyes”).

Thus Go, in contrast to chess, is more about distributing one’s pieces than about massing them. It is more about proactive insertion and presence than about maneuver. It is more about deciding where to stand than whether to advance or retreat. It is more about developing web-like links among nearby stationary pieces than about

moving specialized pieces in combined operations.<sup>1</sup> It is more about creating networks of pieces than about protecting hierarchies of pieces. It is more about fighting to create secure territories than about fighting to the death of one's pieces. It is also less linear than chess.

Go analogies appear at times in high-intensity, conventional conflicts. For example, the World War II Battle of the Atlantic had many of the game's characteristics. Moves—attacks—were made all over the board (the seas) from day to day, and secure areas in the battlespace were developed first around the edges (the European and American coastal seas), and later extended to protect convoys throughout their voyages. Victory in this campaign depended upon the cumulative results of the fighting (merchant ship production less losses versus U-boat production less losses), rather than upon the achievement of some sequential, territorial objective.

Yet, Go is far more like social, criminal, and revolutionary forms of low-intensity conflict than like full-scale military war. It might even be said that the forces of North Vietnam and the Viet Cong played Go while U.S. forces tried to play chess (Boorman, 1969). In line with this analogy of Go with irregular warfare, the game's tactics are very unforgiving of efforts either to build fortifications or to seize unclaimed territory. Bastions or redoubts are subject to implosive attacks that bring them down from within, while "ground taking Go" is quite predictable, allowing a smart adversary to ambush these interspersed forces, defeating them in detail.

Finally, we note that the comparison of chess and Go speaks to another distinction that may prove increasingly significant in the information age: the distinction between "vital" and "strategic" interests. Chess is mainly about vital interests, particularly in the opening—notably, the security of the king, and control of the center. As the game progresses, the interaction of black and white pieces (forces) creates additional, strategic interests, which may or may not concern the center or the immediate vicinity of the kings. Go, on the other hand, *begins* with only strategic interests—a player has yet to determine where to stand, attack, or disconnect. Only later, as the board fills with black and white forces, do vital interests emerge, often according to which portions of the board seem to develop greater or lesser degrees of importance to the outcome of the contest. As the world grows more interconnected, it is incumbent upon the United States to attend to the distinction between vital and strategic interests, and to the possibility that the strategic ones will grow in significance relative to the vital ones.

---

<sup>1</sup>The extension of a piece into a line (a chain network?) might be a form of maneuver.

### **Game Is Even More Like Netwar If One Side Has to Play Blind**

- **Information warfare is about who knows what and when**
  - **In *kriegsspiel*, both sides are blinded**
  - **What if one side gets to play chess, while other side has to play *kriegsspiel*?**
  - **And what if this is applied to Go?**
- **If one side is kept blind, then side with “top-sight” has the best-informed pieces**
  - **The side with top-sight will surely win**
  - **It can do so even if it starts with fewer pieces**

The metaphoric possibilities for netwar deepen if one imagines combining Go with the key characteristic of *kriegsspiel*: the screen that obstructs sight. Again, presume that one side has full knowledge of its own and the opponent's array, but the opponent can see only its own pieces until contact is made with an opposing piece. The dynamics of Go differ from those of chess/*kriegsspiel*, but the point still stands: Both sides start play with virtually equivalent mass and energy at their disposal. But the side with top-sight has far more information. Thus, it should win handily over a blinded player and require (or need to risk) far fewer pieces to do so.

It might be illuminating to run experiments about this point, not only to test its validity, but also to see whether a minimum essential force size can be defined that invariably wins at chess/*kriegsspiel* or Go so long as its side has top-sight and the other side is blinded. The experiment could vary the amount of information available to either side to see what types and thresholds of information may make the most difference.

To refer to the well-known “information pyramid,” which features wisdom at its narrow top and raw data at its broad base, it might be found that a game will turn in favor of whoever has better knowledge and wisdom, so long as both sides have full view of the board. But the more one side is blinded, the more the game may turn simply on who has the most data and information in the narrow senses.

In addition, it might be illuminating to identify for study a series of cases in which apparently small, weak military forces effectively defeated or defended against what appeared to be much larger, stronger forces. The offensive skill of the Mongol “hordes” of Genghis Khan (which were anything but hordes) comes to mind, as do the strategically defensive campaigns waged by the Royal Air Force and related ele-

ments in the Battle of Britain, and by hard-pressed U.S. Navy forces up through the Battle of Midway during the Pacific War.

There are always many explanations why a smaller, weaker force wins. But a crucial constant may be superior intelligence and communications, be that because of fast scouts on horseback (the Mongol “Arrow Riders”), breakthroughs in radar and cryptography (the British and American cases), or other technological and organizational innovations.

Indeed, an historical study could help illuminate not only the importance of the information factor, but also the extent to which it depends on correctly combining the technological and organizational dimensions of innovation. Such a study, along with the gaming experiment proposed above, might offer lessons for whether and how the United States could move to develop military and other forces that will be lighter and leaner yet more effective than those of any potential rival in the information age.

## Next Moves for Our Research

- **Finalize elaboration of netwar theory**
- **Commence research on improving interagency efforts**
- **Perform case studies of key conflicts**

The next phase in our research agenda will emphasize three strands. First, the theory behind netwar must receive additional attention. In particular, the issues of offense dominance, weakened deterrence, and proactive defensive measures require analysis. At the level of applications, research will likely focus on improving interagency effectiveness. Finally, a third aspect of our research program calls for a series of in-depth case studies to test key hypotheses (e.g., the need for networks to fight networks) and to generate new insights about information-age dilemmas.

Further research will also enable us to deal in more detail with concepts that bear upon operational concerns. For example, we have hypothesized earlier in this briefing that, if networked and hierarchical forms are mixed in a netwar actor, an optimal course is to attack the hierarchical structures first. Such a targeting strategy presumes that the destruction or disruption of hierarchical elements will have resonant effects, particularly if the opponent network is of the “star” or “chain” variety. Another issue is the need to develop a methodology for assessing which targets possess the most valuable “information packages”—and whether it is indeed better to attack them than other targets.

An applied policy recommendation that may be advanced in this next phase is the creation of an “information war room,” a facility that would support defensive netwar strategies, inform operational planners, and raise the probability of success by optimizing joint interagency and inter-organizational efforts. Those assigned to this facility would provide net assessments of the informational capabilities of likely netwar adversaries. They would also “map” the key nodes of opponents, identify the “high information” targets, and develop detailed “information orders of battle.” It is crucial to note that both the war room and its outputs, from orders of battle to maps of an adversary’s key nodes, should not be limited to, or even primarily focused

upon, cyberspace factors and components. An information order of battle will also have to consider the adversary's public media and private diplomatic resources and capabilities.

When an opponent is a state, mapping key nodes includes, but should not be limited to, its power grid, financial market structures, and other forms of electronic interconnectivity. The notion of key nodes should include some sense of an opponent's societal structures and its strong and weak points, because some, perhaps many, adversaries will have little by way of information infrastructure to hold at risk. Thus, a broader view of the mapping function may enable proportionate, if asymmetric, damage to be done if retaliation is needed against low-tech opponents who can nevertheless attack the inviting, rich targets of the U.S. "infosphere." Of course, when an opponent is a nonstate actor, different approaches to mapping and other assessments will have to be designed than is the case with states.

These are the sorts of broad issues that could be raised in an information war room, leading to the creation of lucid, usable information orders of battle. If this approach can be initiated and sustained, then the prospects for waging defensive netwar successfully will grow considerably.

Finally, in the area of comparative analyses, attention should be given to cases that combine social, political, and military factors. Mexico and Haiti come to mind as recent cases. Yet, we feel that historical analysis should not be entirely retrospective. For example, there may be significant analytic benefits to be derived from designing a hypothetical information-age netwar, one with links to a military cyberwar. The goal is an heuristic exercise that can inform and influence policy and strategy.

A classic example of this type of study can be found in the work of Hector Bywater, who wrote his visionary *The Great Pacific War* in the 1920s. Bywater speculated about a U.S.–Japan conflict and anticipated carrier-based, island-hopping amphibious warfare and even developed insights into such innovations as kamikaze attacks. At the policy level, his views had a profound effect on War Plan Orange, which, until that time, had planned to have the U.S. battle fleet traverse the breadth of the Pacific to engage the Imperial Japanese Navy in one climactic battle for naval supremacy. Perhaps a similar intellectual exercise, along the lines of a "Great Netwar," would generate equally insightful results. We hope to achieve this in a prospective book, *Society and Security in the Information Age*.