The Revolution in Military Affairs

Martin Libicki, CDR James Hazlett, et al.

CONFERENCE CONCLUSIONS

The most fundamental strategic challenge to the U.S. military is to convert the Military-Technological Revolution (MTR, the impact of information technologies on warfare) into a Revolution in Military Affairs (RMA, the subsequent transformation of operations and organization).

Although the U.S. military's grasp of the MTR is unquestioned, optimism that the U.S. will lead others in converting the MTR to an RMA is premature. Intellectual convergence on the conversion is a long way off.

The core debate at the Conference was over the relative importance of today's small but irksome military tasks compared to potentially more critical but totally unknown tasks that may face the nation two decades from now.

Although information technologies going into military systems have generally been no better, and often less current, than those of commercial systems available for military use, converting data into information remains a highly sophisticated art at which the United States excels.

Other nations with clearer strategic purpose and less sunk capital at risk from an RMA could be the leaders in this new race. The U.S. would be better off if those nations were to waste decades trying to copy what they thought we could do in the 1990s rather than seeking to leapfrog us by grasping the RMA before we do.

Discussion I: Strategic Challenges

Those who assess future strategic challenges tend to look to Asian countries, and to categorize competitors as peer, regional, or niche.

Asia and the Nation-State

Most conference participants believe that, over the next twenty years, the fulcrum of world politics will continue to shift from Europe and its peripheries to the Asia-Pacific region. The period of European dominance produced innumerable wars as various countries challenged each other for power, resources, and sovereignty. With the formation of the European Union and the dissolution of the Warsaw Pact, great power rivalry in particular and the nation-state in general are fading somewhat in importance.

The nation-state remains strong in Asia, however. The last fifty years have seen considerable economic progress as various nations have made themselves richer by grasping the secrets of rapid industrialization. This trend, which started in Japan in the 1950s and 1960s, spread to the Tigers in the 1970s, ASEAN countries in the 1980s, and China and perhaps India in the 1990s, has left no Asian country unaffected. Economic growth, however, has not made the nation-state obsolete. To the contrary, the nation-state has been instrumental in creating the internal and external conditions for economic growth. European history suggests that countries, once they taste wealth, will struggle for power. Will Asian countries follow that pattern or demonstrate new models of what the nation-state is capable of?

China clearly is the country to watch; if its growth rates continue their heady pace and it chooses to funnel such growth into military power, it may become a peer competitor to the United States. With China, well watched indicators of movement such as leadership changes, matter far less than the broader templates of security. For instance, since the late 1970s, China's Army has shifted from its historic commitment to a people's war of defense and liberation, toward a more conventional outward-looking stance. The PLA is steadily building its power projection capabilities.

China's transition may force countries on its periphery to respond in kind. Capitalist growth, which U.S. policy supports and encourages, creates mobilizable surpluses that support the build-up of contesting militaries. In the long run, our role in Asia will be to help tilt competition toward economic rather than military ends, and monitor for indicators and warnings of violent rivalry.

Types of Competitors

One taxonomy of future threats suggested at the conference is to classify potential competitors as peer, regional, or niche. A peer competitor could challenge our military across the board. A niche competitor would be incapable of doing so, but would strive to inhibit or defeat U.S. intervention by developing capabilities such as primitive weapons of mass destruction, sensor blinders, physical terrorism, information system attacks, psychological operations, or hostage maneuvers. A regional competitor would operate primarily against its neighbors and design its forces accordingly. This taxonomy leaves out nations and sub-national groups which, although too powerless to compete directly with the United States, could exact casualties from our forces operating in ambiguous conditions (e.g., peace operations).

The categories of regional and niche competitor are not mutually exclusive -- a nation seeking dominance over its neighbors needs also to ward off U.S. intervention. Nevertheless, the investments required for regional dominance (overt heavy weapons, for instance) and those required to inhibit U.S. involvement (covert light weapons with a high information content) may differ sharply. Even if a nation could afford both, the operational obstacles required to run both concurrently may be complicated. The more they diverge -- and U. S. policy may have ways of forcing them apart -- the more that other nations may have to deliberately choose one or another path to power.

Do Future Competitors Matter?

The defense community appears split between those who would focus on today's threats and those who could concentrate on tomorrow's. These distinctions have more than academic import: the former would spend for readiness, sustainability, force structure, modernization, and R&D in that order; the latter, in the reverse order.

Tomorrow-oriented analysts argue that today's threats cannot put the national security of the United States at risk; but tomorrow's threats might. Preparing for today's threats is precisely the wrong training for tomorrow's.

Today-oriented analysts respond that small unsophisticated actors, many not even nation-states, could nonetheless constrain U.S. freedom of action, particularly if weapons of mass destruction proliferate. For example, they assert that (1) even if the outcome of a conflict such as that in Bosnia has little direct impact on the United States, the resultant chaos could give rise to a much larger conflict tomorrow, and (2) a military that cannot prove its effectiveness against small foes could lose the institutional prerogatives necessary to prepare against large foes.

Discussion II: Operational Challenges

Considerable evidence suggests that commercial access to information -- GPS readings, space-based imagery, and Internet data -- could be transformed into military advantage thereby levelling the playing field between ourselves and our potential opponents. Other dual-use technologies, for instance, those that would permit remote piloting of aerial vehicles, permit commercial technologies such as electronic video photography to act as powerful military tools accessible to all (RPVs are made in more than thirty countries).

Technologies That Level the Field

Does the proliferation in information technologies necessarily negate our current military lead? Information-based warfare creates new vulnerabilities for industrial-age institutions slow to adapt. Because most U.S. logistics facilities and command nodes are not well hidden, they are vulnerable to precision strike. The widespread availability of overhead imagery coupled with GPS integration into weapon systems-- no more than a few years away for countries such as India--poses a serious threat to which our improving defensive measures (e.g., anti-tactical ballistic missiles) will provide only a partial solution.

Our own counter-C2 operations are complicated by the rapidly falling cost of bandwidth and redundancy. Even if 90 percent of a bit flow can be interdicted, the remaining 10 percent may suffice for operational uses. Rapid expansion of cellular nodes, particularly through exploitation of commercial space assets, may make targeting and communications denial difficult or impossible. Multiple channels of electronic access will also complicate psychological operations and countermeasures.

With the advent of the global information infrastructure, a clever adversary could take advantage of open information systems to enhance its own communications, information, navigation, intelligence, and operational support: examples include GPS, one-meter imagery, weather data, and even CNN. Every year more information with potential military use can be gleaned by anyone from the Internet without leaving fingerprints. How easily can a country's access to the global satellite communications networks be blocked? The coming global information infrastructure will have many points of entry. It will also be difficult to curtail certain services (e.g., global navigation) without denying them to U.S. users or even our own national security establishment.

Technologies that Keep Us Ahead

The United States, nevertheless, retains an edge in two important areas: space and systems integration. Space systems are relatively difficult to build and although many potential middle-income adversaries can borrow space services from third parties, fewer can own satellites, and far fewer can launch them. Thus the United States will retain a clear edge in the size and sophistication (timeliness and interpretation) of space capabilities, in their adoption and adaptation for military uses, in their augmentation or adaptation for the particulars of future contingencies, and in the assurance of their continuity.

The distinctions between data and information, and between information and knowing could also favor U.S. forces. There are vast differences between, for instance, access to meteorological imagery and determining, for instance, that a locus of operations is likely to be fogged in 24 hours hence (a distinction relevant to the Falklands campaign). The art of operational planning is not acquired automatically with the acquisition of computers. Similarly, as sensors proliferate in type as well as numbers, data fusion is likely to become more decisive in future conflicts.

Tomorrow's warfighting organizations will be increasingly fed by surveillance grids fusing all-source data from national to regional and platform sensors. Articulation of that information will enable every Joint Task Force commander to employ a Joint Intelligence Center responsible for information needs ranging from broad situational awareness to targeting and battle damage assessment.

The need for continual institutional adaptation cannot be overstressed. Business reacted to the information revolution by replacing traditional function-oriented vertical structures with process-oriented horizontal structures; fundamental notions of hierarchy, span of control, response time, and centralization were reevaluated. Yet, DOD has seen little parallel change; the old stovepipes still smoke. Information flow and processing no longer traces the hierarchy of command lines, but occurs in grid networks of people and subsystems that collect, transport, process, disseminate, and protect information as well as support counter-C2 warfare. Instantaneous flexibility is needed for a common, clear image of the situation integrated with commanders intent and execution data that is relevant to each echelon throughout the force.

POLICY RECOMMENDATIONS

Two conference threads merit further examination:

- U.S. defense policies that make it more difficult for potential competitors to threaten their neighbors and hold off the United States at the same time may be worth pursuing for that fact alone.

- If militarily relevant information technologies are everywhere, sophistication at using them may be a better predictor of how challenging a competitor may become for the United States. Therefore, in addition to worrying about how large future foes are (and sizing our own forces accordingly), we should also focus on the potential sophistication of our foes (and develop doctrine accordingly).