THE TRANSFORMATION OF WAR AND THE FUTURE OF THE CORPS

Major Robert David Steele, USMCR

Cleared for Publication 28 April 1992

The Marine Corps, in combination with supporting Navy elements, is our Nation's "911" force, well-positioned to serve in a variety of joint, combined, and--if necessary--unilateral roles across the spectrum of combat and non-combat operations. The Department of the Navy 1992 Posture Statement, and the Remarks of General Carl E. Mundy, Jr. Before Congress (Gazette, April 1992), clearly outline how far we have come revitalizing our traditional emphasis on littoral operations, and how we are preserving our core capabilities in the face of imposed reductions.

All this is good. Never-the-less, lost in the vortex caused by a changing Unified Command Plan, sharp reductions in manning and resources, and mixed (or absent) signals from national and defense intelligence about the nature of the future threat, is the fundamental fact that war as we know it has been transformed. The future of the Corps depends not just on getting leaner while maintain its traditional expeditionary emphasis, but on our recognizing that we must train, equip, and organize our forces to deal with four completely distinct types of opposing warrior classes.

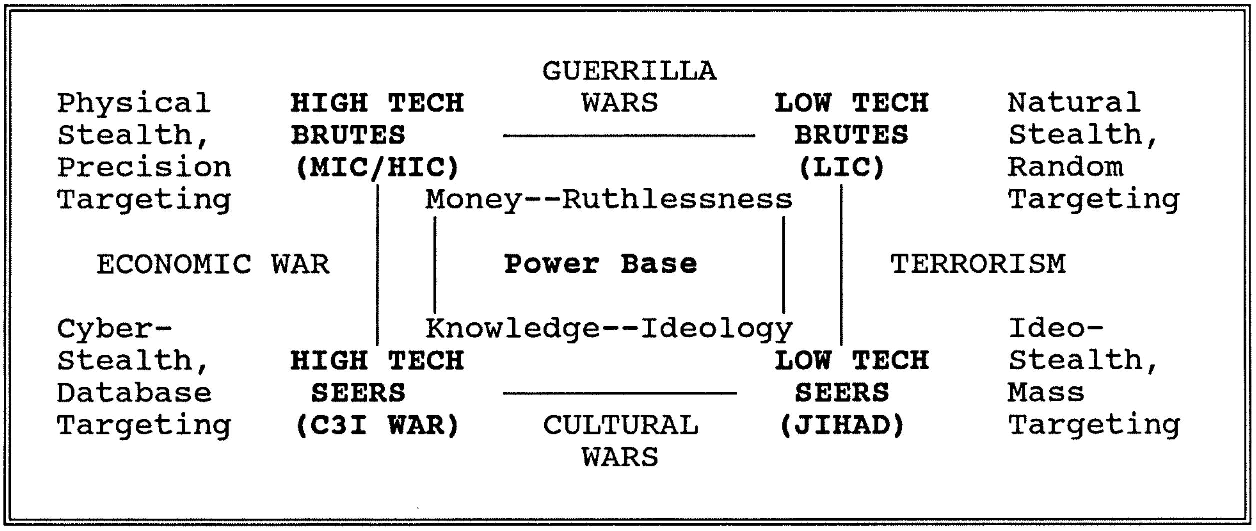
Physical Stealth, Precision Targeting
HIGH TECH BRUTES (MIC/HIC)
GUERRILLA WARS
LOW TECH BRUTES (LIC)
Natural Stealth, Random Targeting
Money--Ruthlessness
ECONOMIC WAR
Power Base
TERRORISM
Knowledge--Ideology
Cyber-Stealth, Database Targeting
HIGH TECH SEERS (C3I WAR)
CULTURAL WARS
LOW TECH SEERS (JIHAD)
Ideo-Stealth, Mass Targeting

Figure 1. Four Warrior Classes Illustrated

Although appearing complex, the above figure simply shows essential distinctions between each warrior class: its power base, its preferred mode of warfare, its stealth mode, and its targeting approach. Additionally, the figure shows the four kinds of war (guerrilla, terrorism, cultural, and economic) which might be encountered between different sets of warrior classes.

I have elected to identify these four classes of warriors as the high-tech brutes, the low-tech brutes, the high-tech seers, and the low-tech seers. Something of their nature is illustrated in Figure 1. Each of these warrior classes has different strategies, capabilities, and vulnerabilities. Each has a different source of power, a different approach to warfare, and a different command and control, communications, computer, and intelligence structure which must be dominated in the attack and the defense.

Below are four summations of each warrior class.

High Tech Brutes Rely on money and capital, physical stealth of equipment, and precision targeting by highly technical munitions. Vulnerabilities include command & control links, and especially commercial communications paths; also financial databases. Capabilities unsuited for combat against low-tech single and mobile targets, mass movements of non-combatants.	Low Tech Brutes Rely on "low slow singleton" invisibility which creates a "needle in the haystack" problem for high-tech brutes; use randomness of route and of objective to frustrate pre-planned physical surveillance. Relatively invulnerable as a class of warriors due to high profit (drugs) and high availability of expendable individuals. Capabilities match goals.
High Tech Seers Reliant on knowledge and cyber-stealth (invisible access to knowledge bases). Vulnerable as a class to electromagnetic terrorism which "melts down" entire communications and computing infrastructures, but single hackers are relatively invulnerable to detection and control. Unable to deal with low-tech seers or low-tech brutes.	Low Tech Seers Reliant on ideological appeal to masses. Impervious to high-tech brute attack if latter pulls punches and fails to take the ideo-cultural high ground; oblivious to terrorism, and insensitive to knowledge or profit pressures. Can only be defeated by a comprehensive ideological and cultural campaign which wins away its grass roots support.

Figure 2. Four Warrior Classes Described

High-tech brutes design systems which can defeat known and predictable opposing capabilities. They cannot handle ambiguity nor can they handle non-conventional defenses or attacks.

Low-tech brutes, in the short-run, will be extremely successful. In the long-run, unless they develop an ideology (or form an alliance with low-tech seers already possessing an ideology), they lack the mental/spiritual energy that religion or ideology can provide, and therefore can be defeated.

Both in the short-run and the long-run, the ability of low-tech to defeat high-tech cannot be underestimated--low-tech, by relying on the human factor, introduces to warfare an unexcelled capability for dealing with ambiguity and creating unanticipated scenarios. The fact that they do not seek political control of a society, and can therefore develop various levels of accommodation and co-existence, also makes it difficult to eradicate this class of warriors.

In considering high-tech seers, it is useful to surface the distinction between "thinkers" and "process" servers. Many of the humans associated with the computer industry are in fact nothing more than unthinking data-entry "slaves". Even the notorious (or illustrious) "hackers" can be considered "unthinking" to the extent that they exercise their pleasure "mindlessly", to no objective end. The most dangerous enemy is that very small group which is morally driven, mentally powerful, and--perhaps through computers--physically endowed. It merits comment that single high-tech seers ("hackers") may exist within low-tech environments (e.g. Colombia, Iran), and place their services at the disposal of criminals or zealots.

Low-tech seers are perhaps the single most dangerous threat to any established community because they represent an alternative or parallel infrastructure which can be used to discreetly undermine any organization. The bottom line is simple: if the existing organization is not providing protection and economic stability for its population--the center of gravity in most nations--then the low tech seer, promising both salvation and comfort, will receive support. The low-tech seer also dominates in the moral arena by having a very powerful ideological construct which can move its members to heroic feats against physically more powerful and mentally more agile opponents.

We as a Nation, with our nuclear and conventional forces and our bureaucratic organization, fall into one of the four categories, that of "high-tech brute". As an aside, one observer has comment that we as a Nation have a tendency to try to fit reality to our force structure, rather than designing our force structure to fit reality. That is the point of this paper--to highlight the four different realities with which we must deal.

We are relatively well prepared to defend ourselves against other high-tech brutes, having just seen the demolition of the Soviet empire. This is however, the least likely form of attack against us in the future.

We are completely vulnerable to attack from the other three kinds of warrior, as illustrated below, and simultaneously ineffective in the attack against those three warrior classes.

Our challenge in the 1990's is two-fold: to significantly reduce our defense expenditures while also developing appropriate capabilities essential to protect our citizens and our property against all four warrior classes. This can only be done by radically changing the way we train, organize, and equip selected elements of our forces.

What is the problem? As high-tech brutes, we are the modern equivalent of dinosaurs sinking into two tar-pits. One is an information tar-pit, overloading our now archaic sensor systems (all of which are designed to deal with "known" threat signatures that can be pre-programmed). The other is a mobility tar-pit, wherein we are frustrated by our heavy logistics train and heavy ground and air mobility systems, constraining our ability to deal with fleet of foot "singleton" threats. Our air power, our artillery, our armor--all of these are marginally effective against the low-intensity opponent, and also remarkably vulnerable to isolated attacks in garrison and rear areas.

Our existing command and control, communications, computer, and intelligence (C3I) infrastructure is only geared for confrontation with other high tech brutes. We are extremely vulnerable to covert attack by emerging high tech seers (hackers), to random attack by low tech brutes (narco-barons), and to broad subversion by low tech seers (fanatics). For example:

-- Our increasing reliance on commercial communications paths, as well as our relative lack of computer security procedures throughout the government, when combined with the pervasiveness of telephone technology, enable a single hacker, from anywhere in the world, to shut down U.S. telephone switching stations, and contaminate with viruses virtually any unclassified system. It merits comment that even if our classified data may be safe, the telephone company operating systems, packet switching networks, and so on, are not encrypted or protected, and the flow of data will simply cease.

-- The ability of narcotics barons to operate their business with impunity across our borders and within our communities, and the ability of terrorists to strike with relative impunity--they don't play by our "rules"--are well recognized.

-- Our susceptibility to cultural subversion, a susceptibility which stems in part from our national abdication of any cultural standards (e.g. imposing English as a national language in our schools), is less well recognized.

Unfortunately, between our Nation's natural division into nine relatively distinct regions, the deterioration of our schools, and the strong ethnic roots that many of our immigrants choose to nurture long after their migration to our country, we are facing a period of internal cultural warfare which will have a deleterious impact on our ability to wage external cultural warfare.

We exacerbate this situation by imposing an expensive, slow to act and react, hierarchical command & control process on the "brute" force structure on our Nation, at a time when we require a relatively inexpensive, fast-acting, "seer" capability able to act anywhere, anytime, without regard to any national, ethnic, or religious strictures. We persist is having bureaucratic "turf wars" because no one has really come to grips with the fact that we are at war, now, in four different environments!

What does this analysis suggest? It suggests that warfare in the future will be fought at the platoon level, under relatively autonomous circumstances and with limited resource to complex combinations of combined arms.

Brainpower, understanding of local cultures and conditions including operational geography, and highly responsive all-source tactical intelligence will be critical force multipliers under such circumstances. Autonomous decision-making by the commander (or single Marine) on the spot will be the norm.

What is the solution? For selected elements of our national defense organization, we need to revisit our concepts of operation, doctrine, and force structure planning methodology, substantially reduce the base force idea, and think instead of four expanded and significantly improved capabilities:

-- Paramilitary and clandestine/indigenous variants of our Special Forces to attack and destroy selected low tech brute forces on their home ground and without necessarily having the support of local host governments

-- Foreign area experts, ideally with ethnic roots and intuitive understanding necessary to fully appreciate the nuances of religious and other forms of low tech ideology, and to develop global or precision ideological defense and attack campaigns

-- Computer security (defense) and computer attack specialists able, with the selective assistance of tactical and strategic communications specialists to penetrate, monitor, disrupt, deceive, and dominate any computer or any communications system for any length of time, ideally without being detected

-- Expeditionary and sea-based variants of our conventional forces, able to conduct precision raids and guide precision munitions in coordination with covertly-inserted Special Forces or indigenous clandestine assets.

Forces for Future Warfare

Vs. Low-Tech Brute: Paramilitary/Clandestine
Vs. Low-Tech Seer: Foreign Area Specialists
Vs. High-Tech Seer: Computer Specialists
Vs. High-Tech Brute: Expeditionary Forces

Figure 3. Forces for Future Warfare

Each of the above forces will have its own requirements, both for C3I support to its planning, programming, and operations; and for C3I offensive capabilities against its primary warrior class opponent. We are not ready!

Policy-makers, political leaders, and industrial managers need to think through four different kinds of national security capability, each with a different C3I defense/attack problem set, and each with a different concept, doctrine, training, and acquisition problem set.

The private sector, increasingly given to forming its own international security corps and hiring specialists to protect its computers and its people, will have a role to play in the multi-dimensional competition/conflict environment described in this paper.

One of the hardest policy problems--with significant legal ramifications--is that of establishing dividing lines between the public and the private sector.

In a fast-moving global environment, where crime, culture, and knowledge cannot be controlled by any government or group of governments, we are finally going to have to come face to face with the possibility that the private sector can do things that government cannot not, and we may actually have to develop methods of "privatizing" certain security and conflict/competition functions.

Within the Marine Corps, these concepts should translate into a substantially reinforced ability to conduct paramilitary operations (i.e. not necessarily in uniform), augmented by tailored clandestine human intelligence support networks in countries in high interest to the Marine Corps. This should result also in a dramatically expanded investment in our Foreign Area Officer program (both active and reserve); ideally I would like to see every officer, and most non-commissioned officers, required to learn and maintain a second language as a basis for promotion. Truly expeditionary forces should by definition be led if not manned by "foreign area officers". Finally, to deal with the severe threat to our communications and computers, I would create a C4 security occupational specialty, dedicate at least one officer and one non-commissioned officer to computer security matters at each MAGTF or division/wing level, and establish an integrated Marine Corps C4I Security Plan which provides for training, equipping, and organizing our forces to be effective in a fragile C4 environment.

The GOOD NEWS is that these capabilities will cost a fraction of what our high-tech systems have cost and are projected to cost, and, with the exception of the linguistic and cultural warfare capabilities, can be stood up relatively quickly. The money is there, but only if there is a radical reduction in our investments against old technology and old concepts.