14 March 1992

MEMORANDUM FOR THE DIRECTOR OF DEFENSE INFORMATION

From: Robert D. Steele

Subj: CIM AND FUTURE WAR--ACTIONABLE CONSIDERATIONS

Ref: (a) My paper, "Transformation of War and C3I", dtd 11 Mar 92
(b) Yr note rcvd 13 Mar 92

Executive Summary

- A serious underlying problem in defense information management which does not seem to be explicitly addressed by CIM--while CIM improvements will help, they may not be sufficient--is the conceptual foundation for the defense drawdown, i.e. the base force idea which perpetuates our "high tech brute" approach to war while ignoring the other three types of warfare likely to threaten our interests in the future.

- As outlined elsewhere, besides "high tech brutes" like ourselves, there are three other warrior classes that we must deal with in the future, and we are not ready, either in terms of force structure or its accompanying C3I capabilities, to either attack or defend against these powerful emerging warriors: "low tech brutes", "low tech seers", or "high tech seers".

- There are seven specific measures (among others) which could be integrated into the long-term intellectual foundation of CIM in order to expand our effectiveness against these other threats; these measures address:

  -- communications and computer security

  -- continuity of operations

  -- educational "wrap-arounds" (message context)

  -- primacy of unclassified and commercial data

  -- global data entry architecture

  -- global connectivity at the human level

  -- tools for analysts

Subj: CIM AND FUTURE WAR--ACTIONABLE CONSIDERATIONS

1. Purpose. This memorandum builds on the ideas in reference (a) to answer your question as posed in reference (b), paraphrased, as to what specific CIM-related actions might follow from these views of the future of warfare and national competitiveness.

2. Background

a. Reference (a), stimulated by Martin Van Crevald's latest book, The Transformation of War (Free Press, 1991), and by personal discussions with other instructors for the Marine Corps Command & Staff Non-Resident Program as well as Mr. William Lind, a defense reformer of some note, developed the conceptual diagram shown in Figure 1 as a basis for articulating why our future defense doctrine, force structure, and C3I capabilities must be redefined to provide for four substantially distinct families of war-fighting forces.

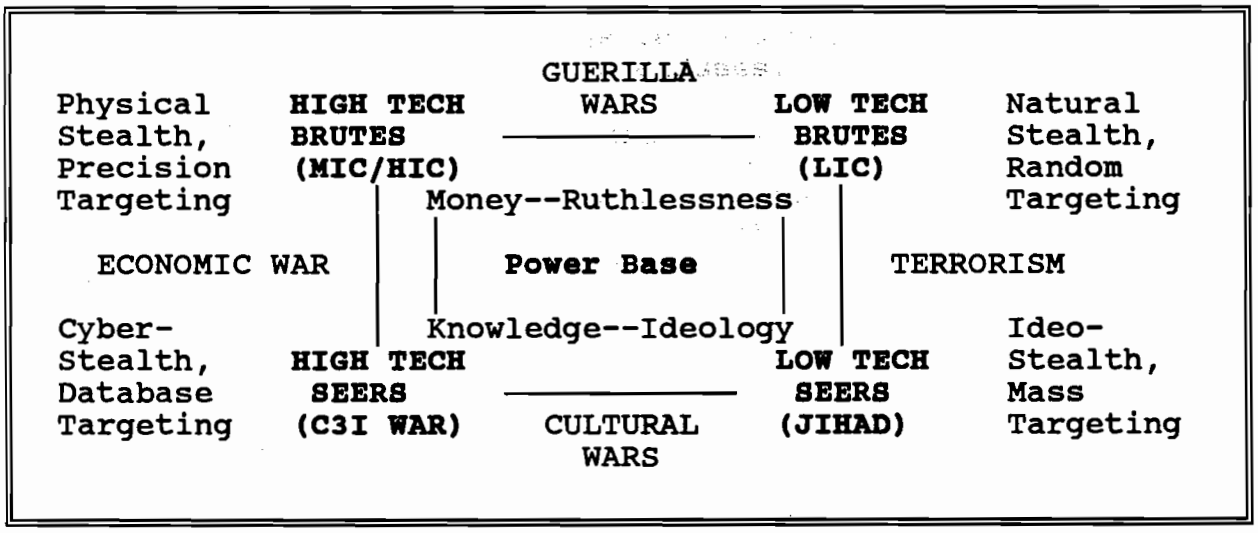

Figure 1. Warrior Classes

b. Reference (a) contains distinctions bearing out the need to address each of these warrior classes as a separate threat category. What is important from the CIM perspective is to also see them as four separate C3I challenges, both in the offense and in the defense.

(1) Even the "high tech brute" challenge, although addressed by CIM, cannot be said to be addressed by our existing capabilities.

(a) The time it took us to obtain digital mapping data and program our precision missiles for the war in Southwest Asia; the emerging data about the number of those precision-

guided munitions which did not detonate (or hit their target); and the fact that Iraq ran a static defense instead of the kind of mobile and audacious offensive-defense the Israelis or Chinese might run, should give us pause.

(b) Looked at from another perspective: the lack of a wide-area imagery capability, our inability to find and destroy mobile tactical missiles, and the major problems we had in tactical imagery dissemination, all suggest we would have significant difficulty against a more aggressive conventional opponent.

(c) Add to this the "sensor to shooter" C3I problem set, and a case could be made that CIM--even if it succeeds beyond our wildest expectations--can do no more than clean the mucus off the dinosaur's eyes; CIM as now envisioned does not contribute to more effective warfighting against other "high tech brutes", nor does it establish a foundation for directing, collecting, analyzing, and disseminating data in ways needed to attack and defend against the more dangerous and more likely threats posed by the other three warrior classes.

3. Discussion

a. This memorandum outlines aspects of defense C3I capabilities which must be established if we are to be fully effective against the four warrior classes which I believe represent a solid foundation for defense planning.

b. One way to approach this task is to create a matrix comprised of the four warrior classes on one axis, and the four basic intelligence/information functions on the other, as shown in Figure 2.

Quick Looks	Direction	Collection	Analysis	Dissemination
High-Tech Brute	From all levels	Sensor to Shooter	New Tools	NRT Multi-Media
Low-Tech Brute	Law Enforce.	Improved HUMINT	New Tools	NRT Multi-Level Secur.
Low-Tech Seer	Long-term In-depth	Improved HUMINT	New Tools	Attention-Getting INT
High-Tech Seer	Automate Global	Constant Global	New Tools	NRT Software Vaccination

Figure 1. Intelligence Evaluation Matrix

c. When looked at in this way, certain strategic priorities and deficiencies are highlighted:

(1) Against the High-Tech Brute we need to do much more in the way of near-real-time (NRT) sensor-to-shooter automated fusion and multi-media dissemination. Weapons systems must be able to "direct" sensor suites (and have such suites available to begin with), while sensor suites must also be able to "direct" weapons systems, including manned weapons systems, where appropriate. Where this whole approach to war breaks down, however, is in dealing with ambiguity or emerging threats which were not programmed into the design of either the sensors or the shooters.

(2) Against the Low-Tech Brute we need to adopt a law enforcement approach to warfare; among other things this implies a much more fluid and tactically distributed force structure, and a requirement for very large increases in our clandestine, covert, and overt human intelligence (HUMINT) capabilities, all of which need related means to communicate and computer what they collect.

(3) Against the Low-Tech Seer, because this threat is not well understood by policymakers unwilling to entertain the concept of cultural warfare, we need, in addition to increased HUMINT capabilities (especially the kind able to penetrate cultural as well as security barriers to understand plans and intentions), but new attention-getting dissemination vehicles which at once explain and educatE--to be blunt: intelligence in some instances must not only be communicated with the intent of informing the policymaker, but will in the future increasingly have to bring with it its own "Basic Education Module" on the topic so the policymaker can learn the import of the intelligence--and all this on less than one page of hard-copy or two minutes of multi-media soft-copy.

(4) Against the High-Tech Seer, a threat now understood but ignored, a whole new concept of operations for C3I must emerge. What "Continuity of Operations" once was in the nuclear era must now be considered in relation to the era of C3I. We must plan for total melt-down of most systems, have "core" C3I capabilities that receive constant security oversight, and develop an in-house "computer security commando" that can--in the magical world of software--go anywhere, do anything. We should seriously consider recruiting our known hackers and building them a golden cage with its own 7-Eleven from which they can explore to their hearts content, the ultimate guinea pigs and--when necessary, available for "Dirty Dozen" special missions run directly from their captive terminals.

(5) Against all of these warrior classes, without exception, we need drastically improved analysis tools. There is no other investment which offers a greater return on investment nor a more significant defense against emerging threats. In many future engagements, it is analysis "cyber-speed" which will "win", not the "force on force" ratios of the past.

d. What specifically does this mean in terms of CIM and related investment strategies for the future? This memorandum is founded on an understanding of problem areas and future threats, not on CIM itself, so rather that being prescriptive, it is intended merely to provoke thought. In that vein, following are seven recommended enhancements of CIM which may merit adoption:

(1) C3 Security Corps. TEMPEST, physical security, and first-generation computer security software are merely starting points. Multi-level security architectures and the compartmented mode workstation may actually be distracting us from routes to a more reliable and encompassing solution. Put someone to work establishing a C3 Security Brigade, with emphasis on integrated approaches to communications and computer security, not either in isolation. We've finally reached the point where we need a C3 security philosophy, organization, and doctrine which is as sophisticated and comprehensive as physical and personnel security once were, before those systems broke down. In addition to wide-ranging efforts integrated into all system design efforts, support to private enterprise (including of course special units in direct support of communications companies), we need a C3 Special Forces capability consisting of teams of hackers supervised by more conventional personnel able to conduct what counterintelligence calls "offensive" operations--penetrating the enemy (or, lacking an enemy, others) is often the best and sometimes the only defense. Example of the kind of question we can begin asking: "in the virtual reality environment provided by cyber-space, how do we validate truth?"

> CIM Implications: What is our concept of operations for integrating and extending computer security to every aspect of every communications and computing activity, not just in DoD, but beyond DoD?

(2) C3 Continuity of Operations

a. Apart from the security cadre which seeks to prevent and resolve cyber-attacks on systems, we need some basic evaluation of what "core" C3I capabilities are required to function as a nation under different scenarios (other than nuclear war), and then make provision for both data backup in both government and industry, as well as either alternate or protected systems, or manual systems. Federal connectivity to

and support of state and local governments, including law enforcement, must be part of this planning effort. In the same way that "strategic minerals" once dominated our thinking on certain aspects of international relations, "strategic data" must now come into vogue and be factored into our calculations.

CIM Implications: Do we have a handle on what our most vulnerable nodes are, and a capability for providing alternate satellite links in lieu of commercial links for specific operations or activities? What data is truly essential and how do we provide for end to end data maintenance in a computer warfare environment?

b. We must also rethink our approach to sensor suites, and endeavor to simplify the over-all architecture while creating protected or redundant capabilities. How do we defend a force from High Energy Radio Frequency (HERF) attack, especially one mounted by just a few individuals creeping stealthily through the rear area? Does this suggest that dogs are the ultimate sensor system for combat against hand-held HERF guns? How do we provide for distributed sensing so that small units are not dependent on parent units for the multi-media battlefield picture?

CIM Implications: How do we transition to distributed sensing and distributed targeting?

(3) C3I as Education. "Intelligence without communications is irrelevant; communications without intelligence is noise". This phrase, coined for recent testimony by the former Commandant of the Marine Corps to the Senate Select Committee on Intelligence, could be joined by two equally powerful but more difficult to understand concepts:

(a) C3I Source Perception. C3I collection and analysis capabilities which permit, encourage, or ignore "mirroring" and other analyst failings are inherently deficient; this is especially true as advanced information technology, if applied, provides the means by which to detect and highlight anomalies and changes in multi-media data. In short, it is not enough for C3I planners to collect and communicate data; they must also make provision for point-of-entry data definition, and for data fusion and data management capabilities which increase the analysts' sensitivity to "meaning" and to knowledge in relation rather than as isolated data fields.

CIM Implications: How do we transition away from a communications strategy that moves bits and toward a communications strategy that conveys multi-media

meaning? How do we build in institutional memory and facilitate data exploitation?

(b) C3I Consumer Perception. C3I dissemination capabilities which permit analysis to reach the consumer in a manner which reduces the ability of the consumer to understand cannot be tolerated in our new approach. Over-loading the consumer with raw intelligence reporting is an example of old forms of consumer abuse--even if the consumer desires to be firehosed, the fact is that consumers ask for raw data largely because they are not satisfied with and do not trust what finished intelligence they do receive...it is either too difficult to deal with (compendiums of compartmented information) or too sterile and equivocating to be useful in reducing ambiguity (National Intelligence Estimates). It is no longer enough to communicate, compute, or intel-ect. If the material which the C3I community delivers to the consumer (whether policy-maker or tactical commander) is not attention-getting and actionable, then we have failed. There are two failings in this area--one of format and media and content, the other of context. We must consider the possibility that--just as corporations are finding they must provide remedial education for new employees who graduate from high school without the basics--we must provide an educational framework, embedded reference service, or some other means of providing policy-makers (and particularly political appointees and politicians) with a user-friendly, discrete personal reference service which "brings them up to speed" on the context so that they can understand the material which we are going to such great lengths to communicate, compute, and intel-ect.

CIM Implications: How do we catalogue what consumers actually read (i.e. outside DoD communications and computing channels), and completely revise our CIM approach to integrate, complement, or counter external sources while also avoiding duplication?

(4) Unclassified Baseline. Over the years both the operators and the intelligence specialists have been allowed to establish families of documentation or data which are classified and then required to have special handling. In effect, data "baggage" has been accumulated, to the point that the knowledge contained within the data is both overwhelmed by the baggage, and diminished because the special handling isolated the data to the point that it cannot be considered in relation to other data. As a strategic objective--and one that most military consumers are quick to establish as their "number one" data priority, we must return to the basics of knowledge management and revise our operational and our acquisition planning and programming processes to "open the books" to the maximum extent possible.

Documents which in the past have been classified in their entirety solely to protect a few pages of "classified" assumptions are a good example of classification abuse. We could also benefit from an evaluation of the relative return on investment to the consumer of unclassified encyclopedic data as opposed to highly fragmented, incomplete, classified data. A major aspect of their return to an unclassified baseline is that of privatizing basic information production, to include order of battle, transportation, and map information.

> CIM Implications: Should we be accelerating DoD consumer access to external databases, while also reevaluating all "private" and "classified" databases; how do we establish a global integrated multi-level database structure that allows unclassified data to remain unclassified?

(5) Global Data Entry. The single greatest danger facing our defense establishment is ignorance--ignorance of the emerging threat, and ignorance of new sources and methods necessary to collect, analyze, and disseminate knowledge about low-tech brutes, low-tech seers, and high-tech seers. Everyone is familiar with our nuclear/conventional era's emphasis on "throw-weights" and "bean counting"--an emphasis that caused us to overlook the political and economic instability of those building nuclear capabilities (including ourselves), and to overlook the mobility, readiness, and sustainability limitations of large conventional forces. What we need now is a completely revised paradigm for support to decision-makers which is based on what outcome they desire to achieve, and what they need to know in order to be successful. A personal friendship established in one decade with an emerging young leader of a Third World nation could prove to be as valuable if not more valuable (and certainly cheaper) than millions of dollars in foreign aid in a follow-on decade when this is the "price" of a friendship too long deferred. We do not have the paradigm, nor the collection and processing mechanisms in place, to properly integrate political-legal, socio-economic, ideo-cultural, techno-demographic, and natural-geographic information. Our national (global) C3I paradigm is both myopic and color-blind. We need to "hit" our sense of the world, either with a 2 x 4 or a drop of halucigenic, so that our eyes are "opened" to the full color kaleidoscopic spectrum of information, at which point we can then begin to think rationally about what and why we want to collect certain types of predominantly unclassified information, and take steps to establish needed capabilities.

> CIM Implications: Must be extended to include all Departments of the U.S. Government, all Country Teams, and (eventually) State & Local Governments as well as

the Private Sector. Need a national knowledge management (and collection) strategy which integrates private sector capabilities for collection (e.g. digitization) as well as database maintenance.

(6) Global Connectivity At Human Level. This area of concern originally arose as part of a review of our human intelligence (HUMINT) communications infrastructure (lack thereof)--how do we integrate communications to, from, and between overt assets (our people in Embassies), covert assets (individuals on special assignments), and clandestine assets (individuals, including agents, operating under cover). What this really gets down to is how do we develop a global directory, possibly including private sector personnel, which allows any action officer to identify counterparts in other government agencies, international organizations, and the private sector, and to quickly obtain bio-data, clearance data, access to published or appropriate internal records, etcetera. In short, how do we put people in touch with one another?

CIM Implications: At what point do we move away from the hierarchical communication paradigm (vertical communications between organizations) and toward the matrix communications paradigm (functional communications among individuals)?

(7) Tools for Analysts. There is an enormous amount of money being wasted in building tools for analysts, for three reasons: no one is doing good functional analysis and there is no centralized functional analysis office; no one is monitoring the commercial world and ensuring that evolutionary system development is done (i.e. that we avoid investing in development of capabilities that will be on the shelf within a predictable timeframe); and lastly, no one is coordinating the investments in information technology by such diverse organizations as the Defense Advanced Research Projects Agency (DARPA), the Joint National Intelligence Development Staff (JNIDS), the Army Artificial Intelligence Laboratory, the National Security Agency, the four information technology fiefdoms at the Central Intelligence Agency, etcetera. We should approach the analyst workstation as a generic action officer workstation--the same multi-media, multi-window, multi-tasking, multi-level data access requirements which analysts have are also those which the best action officer should share. The best functional requirements document for an analyst workstation is that provided by the Computer Aided Tools for Analysis of Science & Technology (CATALYST), developed under Dr. Gordon Oehler, now National Intelligence Officer for Science & Technology. Two related efforts that could be integrated are those of The MITRE Corporation (the Open Source Processing Research Initiative), and

Subj: CIM AND FUTURE WAR--ACTIONABLE CONSIDERATIONS

Digital Equipment Corporation (a commercial implementation of CATALYST).

> CIM Implications: Data, hardware, and other standards are certainly important starting points, but establishing a powerful workstation suite with standard applications is probably the fastest way of achieving both productivity gains, and opportunities for reducing manpower costs.

4. Conclusion. CIM, however it is defined, could benefit from considering four different global environments within which it might be vulnerable to attack; at the same time, using this multiple environment approach, CIM could begin the process of expanding the definition of its role to include other government agencies and the private sector in conceptualizing data entry and data access architectures for the future.

Very respectfully,

Robert D. Steele