Command, Control and Communications Countermeasures (C^3CM)

by
Lt. Col. Charles F. Smith

What is C^3CM? Several terms can be applied: concept, strategy, tactic, even philosophy. Whatever term we choose, the major point is the C^3CM is a war-fighting technique — a way of approaching mission accomplishment.

Editor's Note: The following article originally appeared in the January 1983 issue of MILITARY REVIEW.

The middle years of the last decade were turbulent times for the Army and the US military establishment in general. Vietnam disappeared into the Communist orbit despite the United States' years of effort, thousands of lives and billions in treasure. Domestically, conscription came to an end, and a new president was elected amid loud background noises of defense budget cuts and overseas troop withdrawals. As we pulled ourselves psychologically out of the mire of the Southeast Asian debacle, two other points became increasingly apparent:

- Much of our conventional war-fighting capability and expertise had become out-of-date. The emphasis on counterinsurgency had effectively blinded us to developments for the conventional battlefield.
- A renewal of intelligence community interest in the conventional capabilities of our principal antagonists revealed that while we were effectively sitting still for a decade, they had made quantum leaps in both size and quality.

All of these factors, taken together, indicated that we could well be in serious trouble if we had to go to war any time soon on a conventional battlefield. Soldier-philosophers, such as General William E. DePuy, recognized this problem for what it was and gave voice to some serious thoughts about what it meant:

- The first battle of the next war is likely to be the last.
- The next war is likely to be a come-as-you-are affair.
- To win, we will have to fight smarter and get maximum mileage out of our technological advantages to offset the opposition's numerical superiority.

About this time, Army intelligence was discovering and publicizing a Soviet concept known as radio-electronic combat involving the integrated employment of both destructive and jamming systems to attack opposite electronic systems. From what was visible of Soviet training and doctrine, it appeared that Moscow was deadly in

earnest in pursuing a goal of disrupting or destroying the electronic systems which support an enemy's command and control. A guide to fighting smarter had first been offered by the opposition though it would be greatly expanded upon in our version.

Thus were joined perceptions of need (overcome numerical inferiority) and threat (Soviet radio-electronic combat), resulting in immediate recognition of a general concept as a high payoff approach to warfighting. Known as command, control and communications countermeasures (C^3CM), this concept was developed, discussed, defined and refined through the course of several Department of Defense and Air Force studies between 1975 and 1978.

Much confusion exists to this day as to just what C^3CM comprises. So, before discussing its implementation, let us look at what it is and what it is not. First, let us get rid of the one myth which has most inhibited effective planning for C^3CM: that C^3CM equals electronic warfare. While electronic warfare is one significant capability available to the commander for application to C^3CM objectives, total synonymy must not be ascribed to the two terms. There are many other means of executing C^3CM, and its association with electronic warfare tends to result in these other means being ignored. There will be more on this aspect when we discuss implementation.

C^3CM is *not* synonymous with electronic warfare;

C^3CM is for operators.

Second, we cannot define C^3CM in terms of hardware or systems. In today's world of increasing reliance on high technology, any new concept like C^3CM is highly susceptible to the research and development agencies racing off to develop new or modified pieces of equipment to meet the perceived need. That approach is somewhat less than desirable in this case, however. If we fire field artillery at an enemy supply dump, we do not immediately designate the cannon a counterlogistics system. Likewise, we should not dub any other lethal or nonlethal system a C^3CM system.

What, then, is C^3CM? There are several terms which can be applied: a concept, a strategy, a tactic, even a philosophy. Whatever term we choose, the major point is that C^3CM is a warfighting technique — a way of approaching mission accomplishment. Harking back to the cannon and the supply dump, if we face a defending enemy who is vulnerable logistically, we may devote priority of fire, maneuver and combat support resources to make his position logistically untenable, force his withdrawal and allow us to move on to accomplish our mission. The same applies to C^3CM, with the significant exception that command, control and communications (C^3) is almost *always* vulnerable to one form of attack or another: destruction, deception, degradation or denial (of information).

The important point is that C^3CM is a methodical approach to the integrated, balanced and complementary employment of available lethal and

C^3 Countermeasures

What It Is	*What It Is Not*
Concept	*System*
Strategy	*Hardware*
Tactic	*Electronic Warfare*
Philosophy	

C^3CM Studies

US Air Force Net Assessment Task Force, *Soviet Vulnerabilities,* **September 1975**

Department of Defense Office of Net Assessments, *Command, Control, and Communications (C^3) Countermeasures,* **1977**

Defense Science Board, *Approaches to the Countering of Warsaw Pact Command, Control, and Communications Systems (Counter-C^3),* **December 1977**

US Air Force, *Countermeasures Analysis of Warsaw Pact C^3,* **June 1978**

Department of Defense Working Group on C^3 Countermeasures, *Final Report,* **December 1978**

nonlethal means to attack the enemy's C^3, while simultaneously protecting our own C^3 from similar enemy activities. To be more specific, as defined by Department of Defense (DOD) and Joint Chiefs of Staff (JCS) policy guidance, C^3CM is:

The integrated use of operations security, military deception, jamming, and physical destruction, supported by intelligence, to deny information to, influence, degrade, or destroy adversary C^3 capabilities and to protect friendly C^3 against such actions.[1]

It comprises two separate but closely related components:

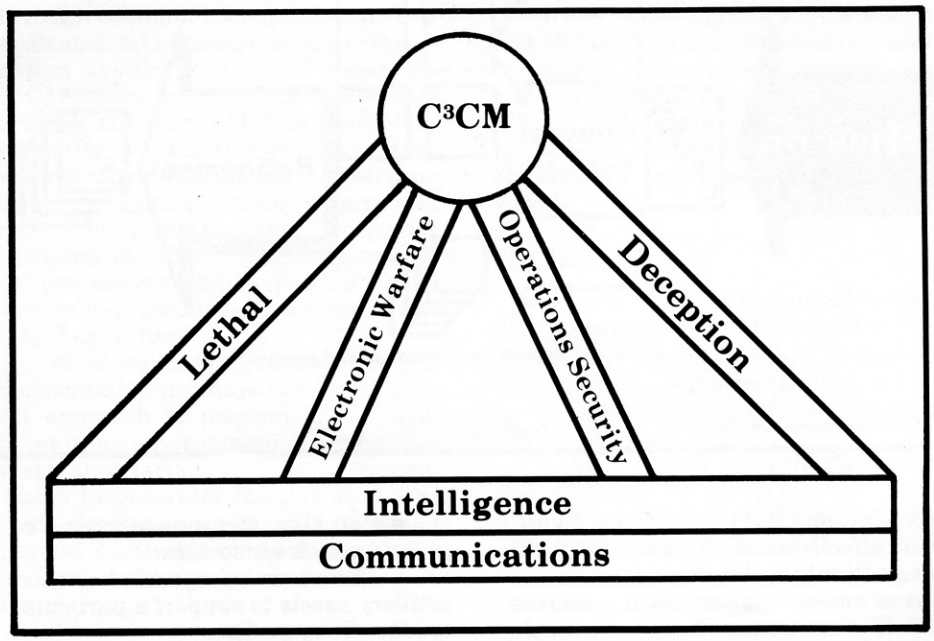
- Counter C^3. *Those measures [from the basic C^3CM definition] taken to deny adversary decisionmakers the ability to effectively command and control their forces.*
- C^3 Protection. *Those measures taken to maintain the effectiveness of friendly C^3 capabilities [in the face of] actual or potential adversary counter-C^3.*[2]

The DOD and JCS policy directives on C^3CM provide extensive lists of objectives and guidance for C^3CM, ranging from the testing of equipment while in development through regular play in joint and combined exercises and tests. Each is deserving, in and of itself, of extensive explication. For our purposes, however, the driving requirement is DOD's directive that "employment of C^3 countermeasures shall be considered in planning . . .,"[3] supplemented by JCS policy that "C^3CM shall be planned and used to maximize . . . operational effectiveness and maintain . . . security."[4]

These directives have been in existence since August 1979 and December 1980 respectively. The problem, of course, is in transition from high-level policy to execution. As with almost any new concept, there is considerable resistance within staff bureaucracies at all levels to revising approved plans just — as the staff officers see it — for the sake of incorporating some new format fad invented back in Washington.

In the case of C^3CM, this problem is compounded by the fact that it is virtually impossible to devise meaningful measures of effectiveness, especially for counter-C^3. Further, the test and evaluation folks have developed extensive programs for joint test and evaluation, a situation which tends to induce a wait-and-see attitude in operators.

On the whole, the net result of all this is that, as a maturing strategy,



C^3CM is moving very slowly. This is unfortunate, for C^3CM is truly a viable concept, even with only the means currently at hand, for improving our force ratio. The time is *now*. We need to get on with it.

When it appears that C^3CM is relatively easy to grasp in concept, but extremely complex to execute in detail, the question, then, is: How do we, right now, implement the C^3CM concept? The answer, trite as it may sound, is careful, thorough planning. That may seem too much like a typical school solution, but this is a case where there really is no substitute for prior planning. The smartest commander or G3 in the Army will accomplish little more than harassment of the enemy's C^3 if he leaves counter-C^3 to be handled in an ad hoc mode. He also may find his own C^3 being systematically dismantled around him by a determined and competent enemy if he does not plan carefully for its protection.

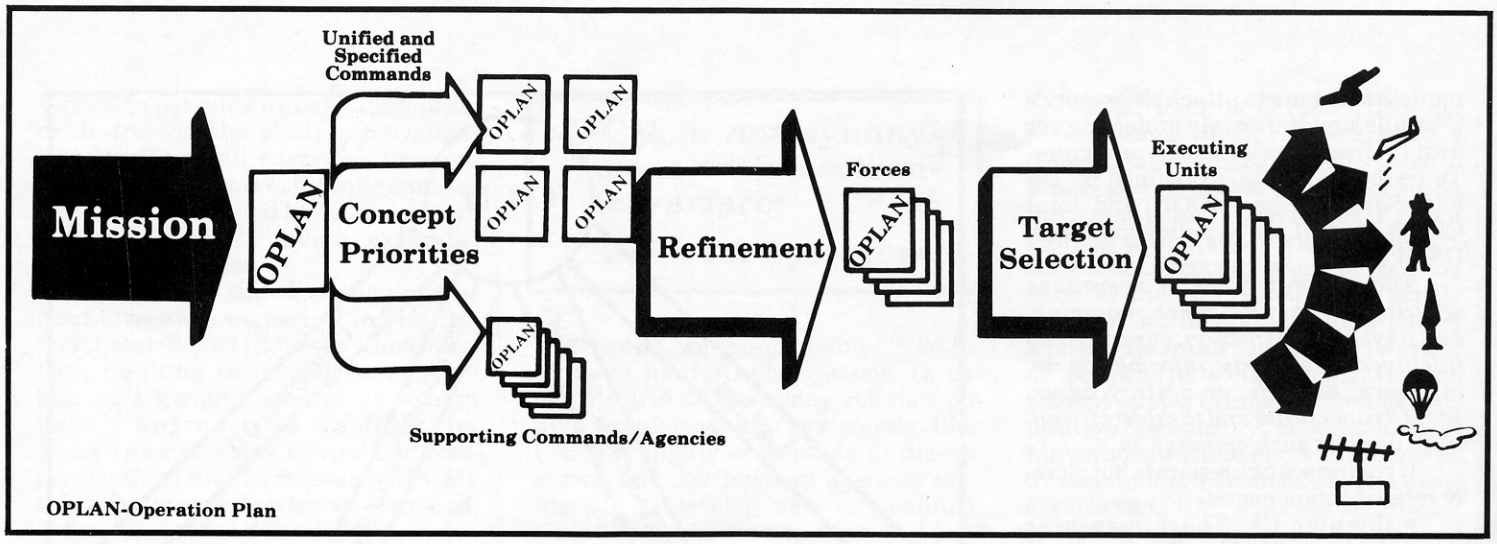
Does that mean there is no value to conducting C^3CM on an ad hoc basis? Of course not! Nuisance jamming, harassing fires, disinformation and many other limited operations against fleeting targets of opportunity will obviously always have a place, provided resources are available.

However, a thoroughly planned and coordinated campaign against the enemy's entire C^3, supporting intelligence and counter-C^3 system will patently produce results several orders of magnitude greater than those to be gained from a haphazard, ad hoc approach. Further, the operations and intelligence staffs, the fire controllers, the jammers, the communicators and the myriad of other participants in an effective C^3CM program will be far better prepared to recognize and react to a C^3 target of opportunity or a friendly C^3 vulnerability if they have routinely planned, trained and exercised for such operations. That should go without saying.

The planning process for C^3CM really is not new. It begins, as with almost all other planning, with a mission statement to, or developed by, a unified or specified command commander-in-chief or joint task force commander. At this level, it is mandatory, under the Joint Operations Planning System format for deliberate planning, that the operations annex (Annex C) address C^3CM to "Establish procedures necessary to effect the integration of supporting disciplines to insure maximum effectiveness of C^3CM operations. . . ."[5]

Unless we are talking about a very small joint task force, it is highly unlikely that the operation plan developed at this level will specifically target enemy C^3 nodes, except the very most important, for attack. Nor is it likely to address real details of C^3 protection.

Instead, the really critical event is the very initiation of the planning process itself. For C^3CM must be incorporated into top-down planning in concert with the commander's overall concept



of operations if it is to achieve significant effectiveness. Fragmented planning will only lead to redundant, ineffective or missed application of resources. For C^3 countermeasures to be implemented in a fully coordinated manner designed to truly disable the enemy's C^3 and to protect our own, the very first consideration must be at the theater's highest levels. Thus, the theater commander's plan should address:

- A C^3CM concept in the operations annex.
- Implementing instructions in the various appendixes to the operations annex and in other annexes — for example, logistics, public affairs and civil affairs. Of particular criticality to C^3 protection will be communications-electronics and operations security annexes although they both will also be vital to the success of the counter-C^3 attack.
- Intelligence requirements and operations to support execution of the C^3CM concept.
- Communications arrangements.

The term "detailed implementing instructions" is, of course, relative to the echelon under discussion — that is, the theater. Hence, as indicated earlier, we are unlikely to be talking about such levels of detail as specific target selection or specific means of protection. Rather, what we will see is command establishment of priorities and resource allocations. For example:

- Priority of jamming effort to a given type target and/or reallocation of jamming resources to critical areas.
- Priorities for protection of critical C^3 nodal points (command posts, communication centers, early warning sites, and so forth) and allocation of materiel and engineer forces for hasty construction.
- Priority for employment of ground attack air sorties.
- Allocation of specified theater artillery assets to support a particular counter-C^3 operation.

As assignments, tasks, priorities and resource allocations pass downward through the planning chain, there will obviously be much refinement of both concept and the details of execution. In this, C^3CM is patently no different from any other specialized type of planning. Nor does this mean that subordinates can plan C^3CM operations only to the extent that they implement C^3CM concepts and tasks handed down from above. First priority for resources probably would have to be placed on the execution of the higher headquarters plan to ensure it remains a coordinated, cohesive whole, but every unit should be planning for localized action against the enemy's C^3 and to protect its own C^3 in furtherance of its own mission accomplishment.

I would offer a word of caution, however. Commanders developing C^3CM plans outside the overall framework of the "big C^3CM picture" must exercise extreme care to ensure they do not inadvertently compromise or otherwise disrupt wider scale C^3CM plans or operations.

As this refinement and expansion work progressively downward from theater to corps to division, the tasking will become more and more explicit as it becomes increasingly possible to identify specific units and their assets for the execution of the C^3CM operation. Following are some, but by no means all, of the potential candidates for C^3CM employment. Keep in mind, however, that this is not only a partial index of measures we can use against the enemy's C^3, but also actions from which we must be prepared to protect our own C^3.

Destruction. This is the classical approach. There are all sorts of ways to go about it: artillery, close-air or high-level bombing support, or naval gunfire. Nothing quite so disrupts a command post or communications center as spreading it noncoherently over several acres of real estate.

Maneuver. Maneuver can likewise result in destruction, but also offers the extra added attraction of possible capture. Would you like to see your local G2 salivate? Mention the idea of capturing a command post or communications center. This may not be an easy task, but it is not impossible either. If we can identify and locate a command post accurately enough to destroy it, we can also maneuver against it given today's battlefield mobility.

Deception. This is a difficult area to treat in an unclassified way, even in the abstract. It is enough to say that deception on the battlefield is designed to mislead enemy decision makers, usually through their intelligence systems. Therefore, it is inherently interrelated with C^3CM. Neither can function out of context with the other. During World War II, we had some real professionals at the decption game. Have we locked all those ideas and notions away forever? We need to resurface and reevaluate this significant capability.

Psychological warfare. This type of warfare can be waged against the enemy both directly and indirectly — for example, through third parties such as the indigenous population. However it is done, the C^3CM objective is still somehow to destroy, degrade or deceive the enemy's C^3

Communications jamming. This is an extremely limited resource in the

Army, especially in light of the redundancy most modern military forces build into their communications systems. Jamming must, therefore, be carefully orchestrated and massed at the critical time against the critical target. It will not help significantly if we blank a critical unit's receivers — say a counterattack force — for an hour if it can still accomplish its mission if notified within two hours to commence operations.

Operations security. This is absolutely vital to success of the counter-C^3 effort as well as to C^3 protection. This is especially true with deception activities where operations security not only will have to advise on protection of deception plans and operations, but also will have to figure out how to "leak" the misleading information to the enemy.

The foregoing represent selected capabilities which are available to Army commanders at various levels for coordinated execution of C^3CM operations. The reader can undoubtedly visualize many others.

What about support? It should be intuitively obvious that none of these capabilities can be exercised effectively without the complete support of those vital functions: intelligence and communications. The commander who cannot see the enemy will patently do naught but flail at him, much less conduct the kind of surgically precise, resource-saving operations envisioned in C^3CM.

Intelligence information from all available sources will have to be gathered, analyzed, evaluated and disseminated on the entirety of the enemy's C^3 system and on the enemy's capabilities and intentions for attacking our C^3. Where are his command posts and communications hubs? Where are the key points in his battlefield surveillance system? How well is his C^3 protected, and what are its vulnerabilities? What are his critical C^3 nodes?

Finally, based on the mission and the commander's C^3CM concept in support of the mission, intelligence will have to assist the commander and operations officer to select and prioritize targets. (This also has the side benefit in peacetime of providing "real-world" work for intelligence personnel assigned to tactical units.)

Communications is the *sine qua non* of C^3CM. The requirement ranges from a network of staff action officers who know each other as points of contact, and how to reach each other through common-user systems, up to a dedicated, ad hoc-assembled communication system to support a specific C^3CM operation. Despite all of this article's advocacy of C^3CM prior planning, the fact is that it will never work without timely dissemination of information, intelligence, orders, reports and coordination instructions. Thus, prior planning and effective, timely communications are mutually supporting, indispensable ingredients of any successful C^3CM operation.

What we have discussed here is a conceptual, coordinated and high-payoff approach to mission accomplishment in an environment of serious numerical inferiority. It is a concept which incorporates the Soviet idea of radio-electronic combat, but goes well beyond it in that it addresses the attack and protection of more than just electronics.

While joint, sophisticated C^3CM tests and evaluations are in the offing, it is a concept which can be implemented right now through careful operation planning. Future hardware evolutions and revolutions will undoubtedly bring change to the details of how we approach C^3CM, in varying circumstances, in varying theaters.

The principles, however, are unlikely to change significantly. If we can disrupt or destroy the enemy's command and control system, or its suporting communications, or deceive him as to our true intentions and capabilities, we can produce major changes in force ratios at minimal cost. And if, at the same time, we can also preserve the effectiveness of our own C^3 in the face of what we know will be a determined enemy attack, we can enhance that favorable adjustment of force ratios.

We have the basic concept. We have the mechanism — an operation planning system with which all Army officers should be familiar. We have the hardware means in the executing units. We have the intelligence and communications capabilities to support the effort.

All that we lack is getting the planners energized from the top down to make it happen. What we need are a few dedicated planners to orchestrate this multifaceted concept — intelligence, communications and operations as a minimum — and get underway. Especially critical, we need to get operations planners — not just some electronic warfare "crows" talking to each other — directly involved in this planning.

We need not wait for sophisticated test and evaluations. We need not wait for studies and analyses. We need not wait for doctrinal or training changes. With a little common sense, a lot of cooperation and hard work, we can get started. The time is now. Let us get on with it.

NOTES

[1] *Department of Defense Directive 4600.4, 27 August 1979, Enclosure.*

[2] *Joint Chiefs of Staff Memorandum of Policy, 9 December 1980, p 5.*

[3] *Department of Defense Directive 4600.4, op. cit., p 2.*

[4] *Joint Chiefs of Staff Memorandum of Policy, op. cit., p 7.*

[5] *Joint Qperations Planning System, Volume I, p V-42.*

Lt. Col. Charles F. Smith is an action officer with the Operations Directorate, Organization of the Joint Chiefs of Staff, Washington, D.C. He received a B.A. from Ohio State University, an M.A. from Boston University, and is a graduate of the US Army Command and General Staff College. He has served with the US Army Security Agency in the Continental United States, Germany and Vietnam; with the 2d Infantry Division in Korea; and with the US Army Intelligence and Security Command and the US Army Western Command in Hawaii.