Naval War College Review

Volume 48
Number 3 *Summer*

Article 9

1995

What Is Command and Control Warfare?

Dan Struble

SET AND DRIFT

— I —

What Is Command and Control Warfare?

Lieutenant Commander Dan Struble, U.S. Naval Reserve

COMMAND AND CONTROL WARFARE (C2W) has rapidly become the central idea in the American approach to waging war. C2W reflects a change in the way commanders are to think about, organize for, and conduct combat operations. It affects the actions of combatants at all levels, in that it demands coordination—in the use of information and in precision of action—to a degree never before expected or possible in warfare. In the last two years, a whole new set of terms and concepts have been introduced to the armed

Commander Struble, a graduate of the U.S. Naval Academy, served on board USS *Rentz* (FFG 46) and at the Naval Reserve Officer Training Corps Unit, University of Southern California, before accepting a reserve commission. He earned a master's degree in comparative politics and a doctorate in American politics at the University of Southern California. Dr. Struble has served as a naval reservist at the Naval Postgraduate School in Monterey, California, at the Naval War College, and is at present the Operations Department Head of the Naval Reserve Command and Control Warfare Group Pacific, Detachment 119. He is an administrator and an adjunct assistant professor of diplomacy and world affairs at Occidental College in Los Angeles, California.

Dr. Struble expresses his appreciation to the men and women of Command and Control Warfare Group Pacific for their cooperation and encouragement in the preparation of this essay.

Naval War College Review, Summer 1995, Vol. XLVIII, No. 3

forces. A revolution in warfare is occurring, and today, as is only to be expected, a certain amount of confusion exists. The purpose of this essay is to make sense of, and put into perspective, the bewildering changes that C2W requires of the United States military.

Depending on the context in which one first confronts C2W, one might consider it a policy, a strategy, a doctrine, a subset of Information Warfare, a set of renamed shore commands, a new primary commander within the Navy's Composite Warfare Commander doctrine, or a mish-mash of new terms.[1] Furthermore, one cannot delve far into C2W before confronting security classification obstacles.[2] However, like the proverbial elephant examined by a group of blind men, this confusing array of changes does makes sense when viewed from the proper perspective. Conceptually speaking, C2W is not difficult to understand and does not require access to classified information.

C2W is in fact all of the things listed above, and more. First and foremost, it is the *result of* (not the cause of) a paradigm shift that has had technological, organizational, strategic, and policy significance. A paradigm shift is a change in the way one thinks about things—in this case, the assessment of tools and their employment for waging war.

Much as blitzkrieg altered the world's evaluation of the tank and became the prototype of maneuver warfare, Desert Storm has become the prototype of command and control warfare. Desert Storm changed how tomorrow's commanders must think about warfare. Desert Storm commanders—in addition to simply destroying enemy command facilities, communications nodes, and sensor installations—made good use of operations security, military deception, psychological operations, and electronic warfare in order to prevent Iraqi leaders from effectively employing their own forces. These five tools, mutually supported by intelligence, have become known as the "pillars" of C2W.[3] Their coordinated use to keep an enemy from successfully operating his forces, though it has by no means replaced the option of direct defeat of an enemy's combat elements, has supplanted the primacy of that approach.

"Command and Control Warfare" is the label the Joint Chiefs of Staff have applied to this new way of thinking about the employment of armed force; new policies, doctrines, commands, and terminology are the means by which this paradigm shift is being institutionalized. Institutionalization is necessary if the hundreds of thousands of individuals within the U.S. military are to reorient their behavior and thinking. The message being conveyed to them is that defeating the enemy's ability to employ force is a more effective way to prevail than destroying the force itself.

Technology and C2W

While Desert Storm was a military victory of truly historic proportions, the tools, concepts, and tactics now associated with C2W emerged earlier. Desert Storm was the watershed event, in which tools and procedures that had been developing throughout the armed forces were brought together and employed in a striking new way.

Technological developments made the shift in emphasis possible. The development of tools to aid in the collection, processing, evaluation, and communication of information—tools that were making possible the so-called "information revolution" in modern society—allowed commanders at all levels to exercise more timely and effective control over their forces. Technology made it possible for them to create a better picture of the "battle space," to understand more clearly where force can be decisive, and to control more precisely the application of that force. Concurrently, the development of precision weapons technology made destruction itself a much more efficient option.

These technological developments have now made a force's command and control (C2) nodes, always vital in battle, even more important.[4] The same technologies also render these nodes more vulnerable than ever before. Improved surveillance capabilities make it more likely that C2 nodes will be identified, evaluated as to importance, and targeted. Furthermore, because effective command and control depends on the information that is received, the performance of a C2 node (or an entire system) can be degraded by way of that input. Thus, one can "target" a system without designating it for destruction; by combining operations security, military deception, psychological operations, and electronic warfare, one may completely nullify an enemy force. The key element these tools have in common is their intended target: the enemy's command and control system. C2W aims at the defeat of that system, whether by physical destruction or effective nullification.

While advances in communications and weapons technology made command and control warfare possible, C2W is not simply a by-product of them. The tank, for instance, was used in World War I, but ineffectually; its potential was fully realized only in World War II, when incorporated in the blitzkrieg. In the same way, highly sophisticated intelligence collection systems, computers, communications, and weapons have been on hand for some time. They were individually developed to improve the ability to gather information, or to analyze it, or to communicate more readily with distant forces, or to penetrate enemy airspace with less risk of detection, or to increase the probability a weapon would hit the intended target, or to counter some new weapon a potential adversary had developed, and so forth, *ad infinitum*. The contribution of Desert Storm was the synergistic employment of tools and tactics for the express purpose of

neutralizing Iraq's command and control capability. The success of that effort has led U.S. military leaders to decide that future battles will be fought with a similar intent in mind—except, of course, when commanders are not empowered to engage the enemy, or against guerrilla-type opponents without sophisticated C2.

Key Concepts

It may be desirable to destroy an enemy's force, but doing so becomes a much simpler and less dangerous proposition if the enemy has been made unable to control that force. C2W, therefore, has the objective of "decapitating the enemy's command structure from its body of combat forces."[5] There are five tools formally associated with this strategy: operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Operations security denies information to an enemy's command and control systems; it prevents key facts about one's own capabilities and intentions from becoming known to enemy forces until it is too late for those facts to be of use to them. Just as the timing of the first strikes on Baghdad was successfully hidden until Tomahawk missiles began hitting their targets, future military operations also must attend closely to operations security.

Through *military deception* one feeds enemy commanders information that is intended and designed to mislead them about present conditions and future activities. In Desert Storm, of course, the best-known military deception was the amphibious feint of the Marine Corps' 4th and 5th Marine Expeditionary Brigades afloat in the Arabian Gulf. To bolster this deception, a widely reported rehearsal landing was staged just weeks before the ground campaign began.

Psychological operations tell the truth in ways that make it difficult for enemy leaders to influence their forces or population as they might desire. The dropping of surrender instructions on front-line Iraqi positions is one example of this component of C2W.

The familiar discipline of *electronic warfare* is now divided into three subsets. Electronic surveillance (ES) aims at acquiring a comprehensive understanding of an enemy's electronic emissions, whether of sensors such as radars or of communications equipment, like radios. Electronic attack (EA) attempts to nullify or mislead enemy systems by such measures as jamming or imitative transmissions. Electronic protection (EP) strives to ensure that one's own electronic sensors and communications equipment are not disrupted or deceived by enemy efforts in electronic warfare. All three forms figured prominently in Desert Storm C2W.

Finally, *physical destruction*, as it pertains to C2W, refers to attacks specifically on enemy command and control assets. Tomahawk missile and laser-guided

bomb strikes on communication buildings in Baghdad, the Apache helicopter attack against early-warning radar sites along Iraq's southern border to "blind" the enemy on the air campaign's opening night, and similar activities illustrate this aspect of C2W.

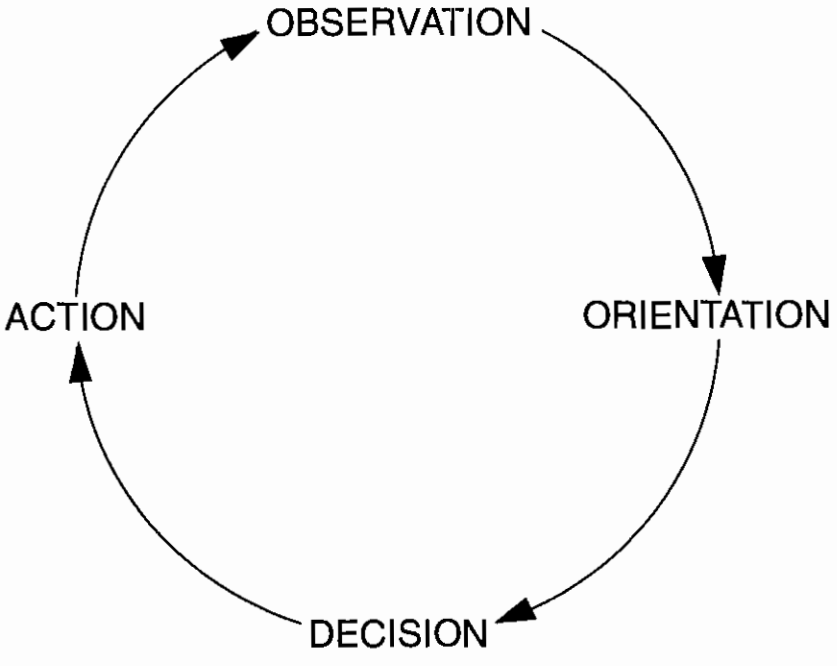
The greatest challenge of C2W is to integrate all five of these tools into a coherent whole to contribute to the commander's overall objective. One must not physically destroy an enemy sensor through which one plans to convey deceptive information, nor should one exercise strict operational security in a group conducting an amphibious demonstration far from one's actual objective. The art of C2W lies in synergistically coordinating all aspects of operations security, military deception, psychological operations, electronic warfare, and physical destruction.

Because one's own command and control systems are as vulnerable as the enemy's, and for the same reasons, C2W has two fundamental aspects: targeting an enemy's command and control ("counter-C2") and protecting one's own ("C2-protect"). The discussion so far has been directed to targeting the enemy's assets, i.e., "counter-C2"; the reciprocal threat will increase as potential adversaries grow more sophisticated, so commanders and their C2W planning staffs will have not only to prevent enemies from successfully degrading "friendly" C2 systems but to use to advantage enemy efforts to target them.[7]

A concept frequently associated with C2W is Air Force Colonel John Boyd's "OODA loop." The OODA loop represents the command and control decision cycle: *O*bservation, *O*rientation, *D*ecision, and *A*ction, arranged in a circle as depicted in figure 1. The OODA loop holds that one must observe the battle space (collect information), properly orient that information (construct a battle-space model), make decisions based on that model, and take actions to implement those decisions. Initiative and agility require that commanders go through the decision cycle quickly and effectively.[8] To prevail, however, a commander must do so more effectively and faster than the enemy. That is, in this connection, one's OODA loop must "get inside" the enemy's.

C2W promotes that end by interfering with the enemy's ability to execute the decision cycle. Operations security, electronic attack, and destruction of surveillance assets prevent enemies from observing activities and discerning real intentions. Deception gives enemy commanders a false picture and thereby degrades their ability to make appropriate command decisions. Psychological operations, physical destruction, and electronic attack and protection prevent enemy forces from taking their preferred courses of action. Each of these tools reduces the speed or degrades the effectiveness with which an opponent can go through the decision cycle.

Figure 1



The "OODA LOOP"

The obverse is a matter of increasing one's own speed and effectiveness in the cycle both by improving equipment and procedures and by preventing the enemy from interfering. "C2-protect" uses operations security, electronic attack, and physical destruction to safeguard decision processes from the enemy. Electronic protection aims at preventing the effective use of electromagnetic energy against friendly C2 systems. Finally, electronic support helps provide a clear picture of the electromagnetic battle.

The term "battle space" has been used advisedly in this discussion; it is a broader concept than the more common "battlefield," which has traditionally connoted a two-dimensional surface with topographical variations, recently stretched to three dimensions to accommodate air and underwater operations. "Battle space," however, encompasses space-based assets and the electromagnetic spectrum.[9] C2W concepts have as one of their purposes that of directing

commanders' efforts toward the effective use and control of all elements of the battle space.

Intelligence and C2W

Little has been said in this essay about the place of intelligence in C2W, but it is a fundamental element of this approach to warfare. An accurate picture of the battle space would be impossible without data on the weapons of potential adversaries and without surveillance means capable of identifying critical C2 nodes. While intelligence has been a key to winning (and avoiding) wars at least since Sun Tzu aptly identified "foreknowledge" as the fundamental difference between effective and ineffective commanders, modern intelligence systems have earned the discipline a new place in warfare.

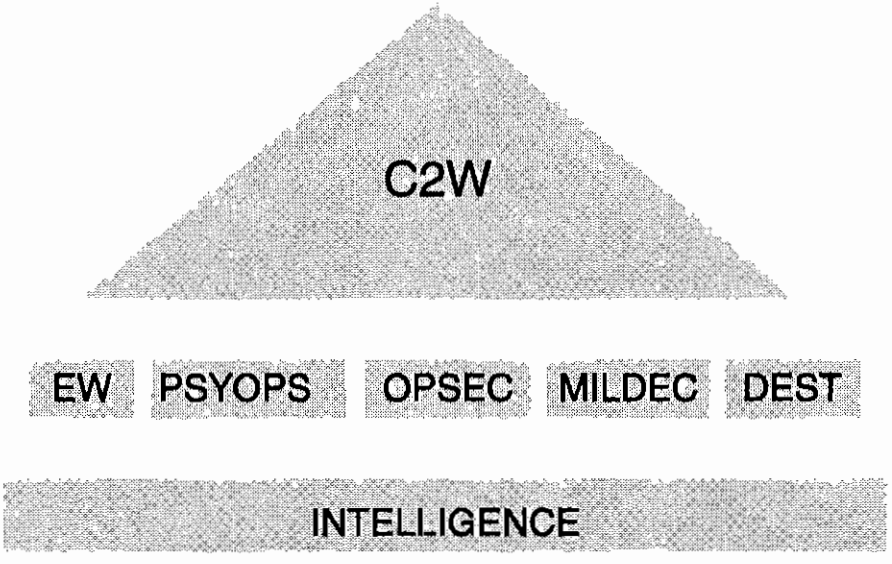
The capability to collect, compile, gain access to, analyze, and communicate intelligence information has increased exponentially with the development of surveillance, computer, and communication technology. Particularly through space-based systems and other national intelligence assets, commanders can now know almost as much about the disposition of hostile forces as enemy leaders, if not more. This information allows one to identify, prioritize, and target enemy command and control nodes (a process called nodal analysis). The five C2W tools, when used in conjunction with intelligence data in real or near-real time, can thereby be extraordinarily effective. (See figure 2.)

In the U.S. Navy, intelligence will be important to all the components of the Composite Warfare Commander organization. The role of the Command and Control Warfare Commander, or C2WC, with respect to intelligence is to sanitize and distribute information more broadly and quickly than has heretofore been the practice.[10] This role is particularly important since equipment and procedures at the national level are being improved to get data to deployed forces rapidly enough to give tactical significance to information and systems previously reserved for strategic uses.

The Navy, Space and Electronic Warfare, and C2W

C2W did not simply "appear," as if from a vacuum. In the U.S. Navy, its precursor was called Space and Electronic Warfare, or SEW. In 1988 the Chief of Naval Operations established a Radio Electronic Battle Management Review to integrate intelligence, surveillance, communications, signature management, electronic warfare, targeting, and command and control; one result was the Space and Electronic Warfare concept. Approved in 1989, it was implemented in 1990 as a primary warfare area, complete with its own commander within the Composite Warfare Commander doctrine—the

Figure 2



Space and Electronic Warfare Commander, or SEWC. The first battle group to deploy with a SEWC sailed shortly before Iraq's invasion of Kuwait; needless to say, the concept was by no means fully developed at that time, nor was the fleet practiced in its use.

The Navy continued to develop SEW concepts and tactics during and after the Persian Gulf War. In May 1992 the commanders of the Second and Third fleets issued a joint tactical memorandum on the subject, and in July 1992 the Chief of Naval Operations issued the "Navy SEW White Paper," marking "the end of the beginning." The white paper's purpose was to capture as an integral part of naval warfare the revolutionary new opportunities that had been offered by Space and Electronic Warfare. Work was progressing on an SEW "tactical notice" from the commanders in chief of the Atlantic and Pacific fleets when, in March 1993, the Chairman of the Joint Chiefs of Staff established Command and Control Warfare as a joint policy.

The Navy's prior development of SEW now placed the service, in some respects, in the vanguard of the general movement toward new approaches to warfare. Full utilization of the battle space and a target set comprising command and control

assets are key elements of both the C2W and SEW concepts. But they are in fact very different approaches, and their differences have created problems. First, C2W and SEW use different vocabularies. Also, where C2W has five "tools," SEW is divided into eight "disciplines."[11] C2W is primarily, in itself, a paradigm shift; SEW incorporates that shift but emphasizes systems and technology more specifically.

In October 1993 the Navy decided to move from SEW to the C2W focus and attendant terminology. While this shift was necessary if the Navy was to continue to strengthen its embrace of joint warfare, and was likely inevitable anyway, the specific manner in which it was carried out resulted in difficulties: the Chief of Naval Operations simply directed that the SEWC be renamed the C2WC. It was done in a manner that implied that SEW and C2W were effectively interchangeable, which contributed to the subsequent confusion associated with the adoption of C2W concepts, terminology, and tactics.

Changes of this sort and magnitude always result in problems to be worked through. The Navy has had lately to make several strategic and organizational adjustments, e.g., from a focus on war at sea to littoral warfare; from the traditional bureau system to a general staff organization; and the adoption and development of Space and Electronic Warfare and, in turn, its supersession by Command and Control Warfare. Each change has been accompanied by new ideas, terminology, and organizations, all of them during a period of such radically reduced budgets that it is not always obvious whether rationales have to do more with strategy or down-sizing. It is no wonder that a time lag exists between implementation, understanding, acceptance, and effective utilization.

That lag is clearly in evidence in the fleet today. SEW terminology and concepts, themselves still not fully understood, remain in use and are confused with those of C2W. Inevitably, Navywide understanding of the latter will take quite some time. Acceptance and effective utilization, on the other hand, while requiring understanding, depend more on the decisions of service leaders. If this new approach to warfare is truly to affect operations, the structures created toward that end must be enabled to make a place for themselves among established organizations, especially in staffs afloat.

The fleet, which was asked to make two fundamental, successive, and not quite congruent conceptual leaps, now has to accomplish a highly significant paradigm shift with respect to its internal procedures before it can properly accommodate this revolutionary new approach to war, C2W.

Notes

1. "Command and Control Warfare," Chairman of the Joint Chiefs of Staff, Memorandum of Policy no. 30 (first revision) [hereafter MOP 30], 8 March 1993, was issued to "provide joint policy and guidance for command and control warfare (C2W)." The Student Text for the Joint Command and Control Warfare

Staff Officer Course at the Armed Forces Staff College calls (page 1-6) C2W an "integrated" and "supporting" strategy. Joint Pub 3-13, *Joint Command and Control Warfare*, provides C2W doctrine for joint operations and was in draft form at this writing. MOP 30 declares that "C2W is the military strategy that implements Information Warfare (DOD Directive TS-3600.1, 21 December 1992, 'Information Warfare') on the battlefield and integrates physical destruction." The Navy operates Command and Control Warfare commands in Coronado, California, and Little Creek, Virginia. Now called C2WGRUPAC and C2WGRULANT, prior to 1 March 1994 these commands were known as Fleet Tactical Deception Groups. At the joint level, the Joint Electronic Warfare Center in San Antonio, Texas, has been renamed the Joint Command and Control Warfare Center (JC2WC). It now appears that these entities will again change names, this time to "Information Warfare" commands.

The U.S. Navy's Composite Warfare Commander (CWC) doctrine structures the operational staffs of battle and amphibious ready groups, and the like, for combat: "commanders" (e.g., the Antisubmarine Warfare Commander, known as the ASWC) direct the operations of all assigned ships, aircraft, etc., in a particular warfare area; and "coordinators" allocate critical but scarce assets (such as helicopters) needed by more than one warfare commander. The function of Command and Control Warfare Commander, C2WC, was established on 17 October 1993, replacing the Space and Electronic Warfare Commander, SEWC—of which more below.

Finally, C2W replaced the use of C3CM (Command, Control, Communications, and Countermeasures) in revision 1 of MOP 30. At about the same time, MOP 6, "Electronic Warfare," was revised to rename concepts long associated with EW; see note 6, below.

2. Security classification is an obstacle to understanding C2W only when one begins to look at the specific equipment involved or goes beyond concepts to doctrine concerning intended tactics.

3. The term "tool" is more descriptive of the five elements of C2W than "pillar" and will therefore be used throughout this essay. "Pillar" is used here because readers may encounter it in other reading on this topic.

4. A "C2 node" is a physical entity within a command and control system at which are concentrated personnel, procedures, and equipment. "Nodal analysis" is the process through which commanders determine which nodes are most critical and vulnerable.

5. MOP 30, p. 3.

6. MOP 6 and MOP 30 both use new terminology for what was formerly electronic surveillance measures, or ESM (now ES), electronic countermeasures, or ECM, (now EA), and electronic counter-countermeasures, or ECCM (now EP). The revised MOP 6 also broadens electronic warfare to include directed-energy weapons.

7. This is a common practice in espionage, where the doubling of agents and the manipulation of unwitting agents are time-honored traditions. The parallel to intelligence craft is no accident, as discussed further below.

8. Initiative and agility are familiar Army terms. The U.S. Army operates on the basis of four key battlefield tenets: initiative, agility, depth, and synchronization. Success in the battle space, according to this philosophy, requires seizing the initiative and retaining it through operations that move faster than the threat, are not limited to frontal confrontation (i.e., that take advantage of the full depth of the battle space), and focus combat power at decisive points. This philosophy is consistent with and complemented by C2W strategy.

9. The "Navy SEW White Paper" (p. 2) refers to "the fourth and fifth dimensions of battle space: the geography of space and the physics of the electromagnetic spectra."

10. "Sanitization" is the process of removing highly sensitive elements (often related to the information's source) in order to render intelligence usable at a lower level of classification.

11. SEW disciplines are divided into two categories, "warfare" and "warfare support." SEW warfare disciplines include operational deception, counter-surveillance, counter-C4I, and electronic combat. The SEW warfare support disciplines are operational security, surveillance, C4I, and signals management. "C4I," in turn, is "command, control, communications, computers, and intelligence."

Ψ