Naval War College Review

Volume 37
Number 2 *March-April*

Article 2

1984

The Technology of Command

Eberhardt Rechtin

The Technology of Command

Dr. Eberhardt Rechtin

Who was it who said, "My commander in chief may make me an admiral, but only communications can put me in command"? It could have been an aviator. It certainly could have been a fleet commander. It demonstrably was the thinking of the German Commander-in-Chief, U-Boats, Karl Doenitz in World War II. His story is worth retelling, familiar as it is, because it dramatically illustrates the strengths and dangers of the technology of command.[1]

Admiral Doenitz was recognized within the Allied Command as probably the most dangerous military opponent the Allies faced. As Samuel Eliot Morison stated in his history of the US Navy during World War II, "Let us not forget that the initial successes and surprises effected by the U-boats fell not far short of rendering Germany invincible on the seas while her armies were carrying everything before them on the continent of Europe."[2] Doenitz was a brilliant and aggressive strategist who used coordinated, massed attacks by his submarines to wreak havoc on Allied convoys. In two months in early 1943 he concentrated 40 U-boats against convoys HX 229 and SC 122 to sink 21 ships, with the loss of only one U-boat. Ninety-seven Allied ships were sunk in only 20 days in that period. He had two advantages: he had a good HF radio network to and among the U-boats, and his intelligence service had cracked the Admiralty codes, which gave him the location of the convoys with precision. That part of his story is not unique. The US Navy in the Pacific had the same advantages and produced the same results.[3]

However, there is a second part to the story. The British, picking up work begun by the Poles and the French, had cracked *his* codes. Doenitz was well aware of the risks he was taking in his daily use of the submarine communications network. The dismaying operational turnabout which in two months in the spring of 1943 caused the loss of 56 U-boats led to intensive investigations, which specifically considered the possibility that the codes had been cracked. The people who built and used the Enigma code machines maintained, as one would expect, that their codes were uncrackable in any reasonable period of time. But critically, another group provided a plausible

Dr. Rechtin is past Chairman of the Naval Studies Board of the National Academies of Science and Engineering.

alternative explanation which led to the fatal conclusion that the codes were safe. That group showed that a combination of Allied shore-based HF/DF and airborne radar could produce the observed operational results, and so the codes were absolved.

"Does counter-C^3 work? Ask the Syrians what the Israelis did to them in the Lebanese War. Ask the Czechs what the Soviet bloc countries did to them in the 1968 invasion."

The alternative explanation is interesting for two reasons. First, it was indeed the "cover" for the true situation not only for the period of World War II but also for 30 years thereafter. This is not to discount the value of HF/DF and the radars and the people who operated them so well. They certainly helped. But the long-range HF/DF ashore was not accurate enough and the radar was too limited in range to consistently provide the precision localization necessary for the extraordinary kill rate. The German analysts made an understandable mistake. They assumed that their enemy's equipment was better than it was, and in the process they missed the real danger. But we should not be too critical. The Germans wanted, indeed *had*, to believe that their codes were safe. The implications otherwise were horrendous. Nor should we be too self-satisfied today. We too want to believe our codes are safe. We want to believe that our submarines are quiet and that the ocean is opaque. We want to believe that there are no moles in the CIA and certainly not in the US Navy.

Some historians have disparaged Doenitz by implying that he was foolish to use so much communications to and within his fleet—a perspective that is plausible if one believes that HF/DF on communications from the submarines was the key to the Germans' defeat. By extension one might say, "the less communications, the better." These historians have a point, but they go too far. Doenitz could not have concentrated 40 submarines in just the right place at just the right time without communications, nor could he have used infrequent communications just before a strike without alerting the Allies that something was up. No, simply less communications is not the answer. The right amount of communications is a balance of gains and risks, both of which, unfortunately for the commander, are uncertain.

Now, 40 years after World War II, the commander's decisions are at least as crucial and much more complex. Global surveillance systems coupled with long-range weapons could soon make the decision whether to transmit or to receive messages a matter of life or death within less than an hour anywhere on the globe. And this is true whether one is attacking or defending. Today's commander has far more communications, command, control, and intelligence

(C^3I)* assets at his command than his command than his predecessors. These new assets have built-in opportunities, brilliantly illustrated by recent Israeli successes, and built-in risks, such as were reportedly a concern during the US rescue attempt in Iran. These C^2 assets—the technology of command—are far more important for commanders to understand than ever before.

This essay has four parts. The first is an update on the new technologies of command. Because of their general familiarity, this will be kept brief. My purpose is to reinforce what you already know—that the new technologies are powerful, dramatic, and loaded with command possibilities and risks.

The second part concerns counters to those technologies. It is intended to demonstrate that command and control systems are assets to be commanded, reconfigured, and moved around, just like weapon platforms. C^2 systems fight each other for a supremacy just as real and critical as a battle between ships and planes.

The third part is perhaps the most important. It focuses on the commander and his needs as a decision maker. The final section gives a few suggestions on possible implications of the new technologies to naval strategy. My objective is to leave the reader with the impression that, "I'd better look into this one. If I do, I could win. If I don't, I could lose."

The New Technologies Of Command

The first and most obvious is space communications. Reliable, high-quality communications are now available to fixed and mobile users anywhere on the globe using equipment of reasonable size, weight, and cost. Few, if any, relay stations are required. The risks of enemy direction finding are much reduced. Combined with other communications, space communications today provide the Navy with what Admiral Tom Hayward characterized as the finest crisis management command and control system in the world. His prime example was the 1981 Libyan crisis, in which Libyan fighters fired at American planes, and the latter returned the fire with deadly effect.[4] Within minutes of the action, the Commander of the Sixth Fleet and the Chief of Naval Operations in Washington knew of the incident in detail. The US Government could and did take the diplomatic initiative before the Libyan Government was aware of what had happened.

Primarily as a result of improvements in space communications, the commander at sea is no longer isolated, a development that, from the standpoint of many commanders, has both pros and cons. But a *new* problem is created: the commander and his staff are deluged with more messages than they can handle. More on that later.

*As with any rapidly developing field, nomenclature can be a problem. C^3I is a generally accepted term and refers to all those systems that support command and control, including the commanders but excluding the command control decisions. Navy usage, as of this writing, uses command and control (C^2) to cover the same things but, to my mind, the general reader might confuse the Navy usage with "commanding and controlling" by the commander.

The technology next in importance is probably space surveillance. Until about 1978 very few people in the US Navy knew about the highly developed capabilities of both the Soviet Union and the United States.[5,6,7] The information was too highly classified for general discussion. As a consequence, its potential impact on naval command and control was obscured. But in January 1978 a Soviet reconnaissance satellite, using a nuclear power supply, reentered the atmosphere and scattered radioactive material across several hundred square miles of Canada. Had there not been a nuclear power supply on board, the story might have been different. But in the public uproar, the mission of that satellite series was revealed. That series, incidentally, had been operational for years. President Carter subsequently announced that there were other satellites that sensed and reported.[8] In the case of that Soviet satellite, the reporting could be directly to military forces, a possibility whose military consequences were much more apparent to military professionals than to the public. In my opinion, Soviet surveillance satellites were and are an integral part of the Soviet force structure and not just peace-time-only intelligence collectors.

It is not necessary to know all the details to appreciate that satellite surveillance systems pose both great opportunities and great threats to naval forces. It is not too much of an overstatement to say that future naval commanders should operate under the assumption that their forces are under continuous surveillance with results available in a timely manner to enemy combat forces. Obviously, it could be critical to the naval commander to have access to similar surveillance and, if possible, to have some way of negating that of his opponent. Gone forever for either side is the protection of being over the horizon, unless, of course, either side can blind, confuse, or deceive the other. In that case, the electronic battle suddenly becomes asymmetric.

The tactical consequences of excellent surveillance are well illustrated by the experience of Admiral Dan Murphy when he was Commander of the Sixth Fleet during a Mideast crisis. The Sixth Fleet was intermixed with a comparably sized Soviet fleet in a period of high tension. Washington, as usual, was concerned. Some retired Navy admirals were advocating taking the Sixth Fleet out of the Mediterranean altogether. Murphy, on the spot, was comparatively calm. He knew that the Soviet ships were not deployed in attack positions. Almost the opposite was true, as a matter of fact. And he knew that if they changed, he would know about it in sufficient time.

Undoubtedly, the Soviet deployment was deliberate. The global positioning of forces these days is often used as a "signal" to the other side about the seriousness with which a situation is viewed. It has reached the point that each side assumes that the other side, through surveillance and analysis, gets the message—an assumption that carries some risk.

Incidentally, to quantify what for Murphy was "sufficient time," a rule of thumb in his tactical situation is that 15 minutes or so would make all the difference. That is, if he had to fight, the outcome would be determined in 15 minutes: the rest would be mop-up. That the critical period is so short is no doubt the result of a combination of wide area surveillance, long-range weapons of high destructiveness per weapon, and the relatively close quarters of the Mediterranean. In the Atlantic or the Pacific the times might be somewhat longer, but they would not extend to hours or days.

Third in a list of new technologies is space weather and space navigation. These assets provide global support and wide area coverage, and they require no emissions from the fleet. Their value for fleet operations is being demonstrated in one naval exercise after another. Perhaps the greatest potential value is in air operations during full emission control (EmCon), during poor weather, and for standoff attack against localized targets. Needless to say, flight vectoring back to the carrier with an accuracy of better than one deck length is extremely useful. These assets, because they require no fleet emissions, thus help defend the fleet against enemy space surveillance—an example of one space system defending the fleet against another.

Fourth in my short list is computerized data bases and the artificial intelligence necessary to use them. Enormons quantities of information can now be inserted, organized, stored, and accessed in very short periods of time. Logisticians were perhaps the first to recognize this capability for cost saving. Using computerized data bases, logisticians could distribute inventories much more efficiently and, in the process, considerably reduce the total inventory.

The Defense Mapping Agency's multiparameter maps are another powerful application. Computers can now make maps showing the locations of all kinds of things, from terrain avoidance profiles to the electronic order of battle.

An early Navy example, and one of the most important developments of the last 30 years, is the Naval Tactical Data System (NTDS), which puts symbols of planes and ships on a map-like display.

In an interesting experiment, a carrier skipper computerized the rules of engagement in a naval exercise, calling out what could or could not be done depending on what the red, blue, and orange forces did. The results were marginal—the computer response time of about a minute was too slow; it had to be seconds! Three problems continue to arise: (1) "garbage in—garbage out"; (2) how to organize the data base so that it is reasonably responsive to nonstandard queries; and (3) how to avoid saturating the commander with more information than he wanted to know about the subject. As one admiral put it, "It used to be tough to find out the location of an aircraft. Now I get not only that but also the aircraft oil pressure, fuel remaining, and other aircraft in the vicinity!"

Of these three problems, the most important in my mind is the problem of operating under saturated conditions, beginning with communications. I

have yet to see a crisis in which all possible communication lines were not tied up for long periods. The priority scheme we now use is primitive. When in difficulty, every user pushes the highest priority button that user controls. The buttons are all too often assigned on the basis of rank, not urgency.

Yet there are techniques, although they have not been evaluated or even studied analytically, that might relieve that situation. They include: mandated limits on message length; computer monitor of message content for key sentences that raise or certify priority, such as *Stop the War*, or *Get the Hell Out of There*; controlled delays for access, such as are used to control freeway traffic, feedback to message senders so they know if and when a message is either transmitted on a link to a user capable of real-time reception or received by such a user; and changes in the modulation systems for increased base band to transmission bandwidth under some circumstances (the signal-to-noise ratio will deteriorate, but that may be acceptable). And, of course, there are procedural possibilities—fewer redundant messages.

The problems of saturation, of preemption of circuits by other authorities, and of general uncertainty of the on-demand availability of communications are some of the major problems limiting the acceptance of shared communication systems by military users. Users, understandably, demand "dedicated" circuits that they can "control," even when it can be shown that such circuits are more vulnerable, less reliable, slower, and more expensive than shared ones. The true need, technically, is for good on-demand communications, yet this need is usually expressed as a demand for circuit control.

With modern communications, the problem of saturation extends beyond the communication circuits. It extends into the control centers where the staffs are inundated with data from sophisticated sensors, consolidated reports from fusion centers, advice and recommendations from subordinate commands, and queries and orders from above—sometimes from *way* above.

Yet it makes little sense to turn off the flow, even if the commander could. Buried in that mass of data is critical information that takes human understanding to find and use. This leads to the problem that there simply are human limits in assimilating and judging information.

Decision aids that store, retrieve, process, and display information are of some help, NTDS again being a good example. But what is now needed is a means to supplement the human ability to reason, to focus attention on what is important, and to manipulate ideas. The technology for this comes from the rapidly developing field of knowledge-based systems, or artificial intelligence.[9] This field has now reached the point of conceptual designs, block diagrams, and reasonably understandable jargon like "situation assessments" and "nondeterministic rule selection."

At the risk of oversimplifying, the essence of artificial intelligence is for computers to process ideas and not just numbers. By ideas are meant

principles, relationships, rules, and logic sequences. The goal is to have a computer act like a cost-effective human consultant, one equipped with an enormous, accurate fund of knowledge and a carefully reasoned way of using it.[10] For that to happen, the computer must make value judgments. It must decide what is important and what is not—just like a human—in order to respond in a timely manner. Like a good consultant, the computer can display its reasoning, but that takes more time. The computer must have a good knowledge base, a good understanding of the situation, a good set of rules, and an effective way of presenting conclusions.

In the vernacular, we want the computer conclusions to make sense. Some researchers call this common sense. I prefer a better-defined term, *contextual sense*, as a statement of the goal of being "sensible" in a defined operational context. Obviously, the computer consultant must be a good match with the commander, just like a human consultant. It must be trusted, reliable, informed, right most of the time, and responsive to the strengths, weaknesses, and reactions of the individual commander.

Two ongoing developments in artificial intelligence for command and control systems will serve as examples. One, at TRW, is for space defense indication and warning.[11] In effect, the computer addresses a surveillance situation by saying, "If the following sensor information is true, and if the following quantitative conditions are met within the stated confidence limits, then by our rules of logic, the conclusions are . . . . " The computer internally decides what is relevant and is prepared to say why.

Another development, at Operating Systems, Inc., approaches an intelligence analysis situation by having information seek the user instead of vice versa.[12] It is an interesting concept, not unlike the human equivalent of advertisers seeking customers instead of customers seeking suppliers. In effect, this approach postulates that it may be easier to describe to the computer the relatively constant interests of the customers than to describe the parameters of the constantly changing information coming into the data base.

Fifth on my list is not a technology, strictly speaking, but a way of thinking. Neither is it really new, but it is as powerful for C^2 as the other new technologies. I call it "architecture."

Architecture is defined as the art and science of planning and building structures or systems. In practice, this means putting things together so that the whole is greater than the sum of the parts, i.e., that things "fit." It is an ancient art. I was introduced to it by my father, a naval architect and engineer who designed and built ships for the Navy. As an architect and engineer my specialty has been space systems. Architectural thinking is much the same whether the system is a ship, an aircraft, a submarine, or a C^2 system.

There are two reasons why architectural thinking is important, whether for ships or C^2: to ensure more reliable and efficient performance, and to help

ensure survivability under attack. Consider the performance advantage first. On the one hand, if individual elements do not work or fit each other, the whole will not work at all. On the other hand, making everything work perfectly costs too much.

For example, one way to improve reliability is through redundancy, but simple duplication of everything is too expensive. Communications engineers learned this years ago and came up with efficient network configurations that provided alternate routes between any two points to be used whenever the regular route was inoperative. Because simultaneous outages of more than a few links were rare, the networks as a whole were very robust but cost no more than the less reliable, specialized, single-route system architectures. The prime example of a highly efficient, very robust network is the Bell Telephone System.

In the space business, there is an architectural principle that calls for dissimilar redundancy. There must be two ways, preferably different, of accomplishing any function. If the primary way is onboard guidance, the alternate is ground tracking and command. Naval architects have a similar specification, one that calls for all ships' spaces to have two accesses, not necessarily alike.

Applying architectural thinking to naval aviation means viewing the battle group as a single integrated weapon system, as a distributed offense/defense tied together by an information network. That thinking, incidentally, affirmed the critical role of the large carriers as the offensive punch of the battle group. It also clarified the role of air-capable ships in company.[13]

Applying architectural thinking to command and control leads to concentrating on connectivity rather than capacity, on interoperability rather than commonality, and on access control as the key to diminished saturation. There has been a major accomplishment in this area recently. A Navy Command and Control System architecture has been drawn up by OP-094 that displays the Navy operational command structure and the connectivities among levels of command required for coordination, exchange of information, and command direction. Top-level C^2 requirements have been laid out. This architecture provides the structure and guidance necessary to exploit the high technologies available to command. Equally important, the architecture provides a framework for discussion and decision on investments to be made by the Navy, the Department of Defense, the White House, and the Congress. This accomplishment is particularly important for command and control systems that in the past have been, or appeared to be, fragmented and unrelated developments.

In brief, the architectural approach is to look at the overall picture and derive from it fundamental design and operational requirements. Prior approaches had focused on individual systems largely in isolation from the rest.

The second reason for architectural thinking, surviving attack, brings us to the subject of counter-technologies and defending against them.

Counter-Technologies And Defending Against Them

This is an old rule: for every system there is a counter system for which there is a counter-counter system ad infinitum, or, if you depend on something, it becomes a target for your opponent. Or, as expressed by a recent Naval Studies Board report on space: space is both a threat and an opportunity—it depends on which side has how much of what.

Many of our current C^2 systems are vulnerable to electronic and physical attack. Most existing communication links can be jammed. Electronic surveillance can be thwarted and deceived. Low altitude satellites can be attacked with anti-satellites. Data bases can be fed disinformation. Electronic circuits can be disrupted by electromagnetic pulses from nuclear explosions. Fixed ground stations can be targeted.

Of course, to demand full performance of any system under all forms of attack is unrealistic. Survivability is relative. More appropriate survivability criteria would ask, "Survivability under what conditions?" "Compared to what?" and "Does the new system increase or decrease the survivability of the forces it supports?"

In any case, current vulnerabilities are transitory. The counter-counter technologies are known. Spread spectrum and frequency hopping controlled by pseudorandom codes, adaptive positioning of antenna nulls, alternate routing of communications, and low probability of intercept transmissions are effective against jamming. Maneuvering of satellites, mobility of ground stations, and the use of airborne command posts—all coupled with skillful emission control—are effective against physical attack. Concealment, cover, and deception are as useful in the electronic age as they have been for centuries.[14]

The incorporation of these survivability measures into systems is primarily a matter of investment decisions based on national policy. The policy trends tell the story. Before 1972, strategic C^2 was soft as a matter of national policy. The argument seemed to be that if the strategic nuclear deterrent worked, it was not necessary to harden the C^2, and once nuclear war started, who would care? That policy was changed in 1972 to one stating that C^2 should be as survivable as the forces supported, but few if any investments in survivability were made to support the policy. In 1978 President Carter set a policy for space systems stating, in effect, that space was potentially hostile.[15] In 1982 President Reagan set the current policy, which states that space systems *should* survive.[16] This trend in policies reflects the increasing dependency on these systems as they become more capable and more widely used. As the past Commander of the Air Force Space Division put it recently, "Dependency is a given, survivability is a must."

Thus, though current systems, designed between 1968 and 1978, are relatively vulnerable, those now being designed are increasingly survivable. We are at the point now at which future satellites and their links most probably will outsurvive most surface forces. The most vulnerable segments of C^2 will soon be those on the ground. Thus, the more functions that can be put in space, the better.

In technical terms, the trends are toward smarter and smarter satellites depending less and less on the ground elements and performing as many of the conventional ground functions as possible. Surveillance satellites will transmit target location and identification instead of raw data. Communication satellites will become switchboards in the sky instead of simple relays. Navigation satellite systems will keep their high precision with very little ground updating. Satellite radio links will have jamming margins sufficiently large that jammers will have to be large, and hence vulnerable targets, themselves.

Earlier I mentioned alternative routes as an architectural approach to reliable communication performance. The existence of alternative routes also is a powerful deterrent to enemy electronic countermeasures. After all, the best possible antijamming design is the one that convinces the enemy not to jam at all. The alternatives can be different routes, different technologies, different procedures, different channels, or combinations of these approaches. Sometimes it is not even necessary to have an alternative, only to have the enemy believe that you have one.

A classic example of leading the enemy to believe you are better than you really are is the story told by R. V. Jones of British intelligence about the Malta radar in World War II.[17] The British had a search radar installed on Malta that was crucial to the defense of Allied convoys. The Germans, under a Luftwaffe general well versed in electronic warfare, set up powerful jamming stations in Sicily that were extremely effective. Jones was asked what to do, and his response was to keep operating the radar as if the jamming were ineffective. After a few days the jamming stopped. After the war Jones met the German general who was still frustrated by what he perceived as the lack of success of his jammer. Jones told him that the jammer had been effective. "But," the general said in some irritation, "you kept on operating! We must have failed. So we stopped." "Just as we hoped," said Jones—or words to that effect.

There are more sophisticated methods of deception, of course. Many of them are quite fragile to compromise and for that reason are highly classified. By logical extension, the fact that one is *not* practicing cover and deception is also highly classified. Also, in the higher order of systems, for every system there is a countersystem, so for *macrosystems*, there must be macrovulnerabilities. And, indeed, this is true. By destroying or disrupting a macrosystem at critical points, the whole can be put out of action. This mission is usually called counter-C^3 or C^3 countermeasures (C^3CM).

For example, consider the problem of defending our ships against Soviet cruise missiles. The Soviet attack macrosystem probably consists of missiles, aircraft, command and control at the base, a radar ocean surveillance satellite, electronic surveillance systems that tell the radar satellite where to look, and communications to tie the whole together. Unless all these systems work, and work reasonably well, our ships are comparatively safe from that macrosystem. Random and uncoordinated attacks on the Soviet macrosystem might not only be fruitless, but they might also increase our danger by providing the Soviets with more information than they initially had on our forces. Conceptually what is needed is a US countermacrosystem. We are a long way from that, unfortunately. The different elements of such a US countermacrosystem are in different organizations at different places and often committed to other missions. The countermacrosystem is necessarily too dispersed to be organic. The command, or "orchestration," of all transmissions and receptions has no conductor.

But real progress is being made with Aegis, our naval aircraft and missiles, an Integrated Tactical Surveillance system (ITSS) architecture, and antisatellites being developed to go after the Soviet radar ocean reconnaissance satellite. In addition, EmCon procedures are being worked out to deny electronic surveillance. Meanwhile, on the Soviet side, the idea of countering our C^2 is well developed. The Soviet Army, for example, under what is called a radio electronic combat doctrine, has numerous countermeasure equipments targeted against our Army and Air Force C^2 systems.[18]

We should expect similar C^3CM against our naval C^2. We should expect operational surprises and sophisticated procedures to be used against us. Disinformation has been and will continue to be injected into our links and data bases. We will be induced to make the terrible error of believing our codes are perfect or that our electronic countermeasures are (or are not) effective.

Does counter-C^3 work? Ask the Syrians what the Israelis did to them in the Lebanese War. Ask the Czechs what the Soviet bloc countries did to them in the 1968 invasion. In each case, C^3CM was meticulously planned and executed to the virtual paralysis of the opponent. The shock effect was overwhelming, and it was all over in a matter of hours. A good question is whether a counter-C^3 tactic can work more than once. The next time has to be different. A different plan. A different execution. And perhaps a different opponent.

At this point you, the reader, should be able to visualize a formidable array of C^2 and counter-C^2 systems, both ours and theirs, capable of doing great good or great damage. Wherever you are, in the air, at sea, or under it, these systems watch you, listen to you, transmit to you, direct weapons for or against you, disrupt your command or your enemy's, and affect everything you believe or do. These systems are powerful pieces on your chess board,

capable of acting at great distances across that board, yet vulnerable to similar opposing pieces. They need to be played with skill, with a full knowledge of their strengths and weaknesses, and with an overall strategy in mind.

And now for the third part of this essay—the commander, the center and keystone of command and control.

The Commander

The first lesson learned by a C^2 architect is that command and control is an intensely personal thing. I have known and talked at length with a number of highly successful admirals about command and control. I give you their names so that you can appreciate the strengths of their ideas and personalities—Moorer, Zumwalt, Holloway, Tom Hayward, Murphy, Gayler, Fox Turner, Stan Turner, Harlfinger, and Kidd. No two of them said the same thing or have the same style of effective command. The same applies to the generals and business leaders I have known. And, I repeat, all were highly successful.

Admiral Moorer, emphasizing the highly personal nature of command, specifically included Presidential ideas on command and control. During a discussion in 1972 of the required design characteristics of the World-Wide Military Command and Control System (WWMCCS) and the need to make it responsive and flexible, Moorer said, "I've served five presidents, and the next President will want to exercise command *still* differently." That statement became a design guideline for WWMCCS.

This personal aspect of C^2 has a reverse twist in the design of C^2 systems—one commander's bare essentials are another's gold plating. That means that we C^2 systems architects have two choices—standardize all commanders or design C^2 systems to accommodate considerable variation in style and need. I recommend the second approach.

Not the least of the problems facing an architect attempting to improve any military system is to find the serious deficiencies in the current systems. Military people close to the combat line—and those are the ones who are probably closest to reality—must believe that they can prevail in combat. If they did not, they could not be effective commanding a fighting force. Consequently, their first reaction to a query of whether things are OK is that they will be OK, that they can do the job they were asked to do, that any deficiencies are manageable.

This perspective exists even when the deficiencies are glaring. I remember asking some aviators why they put up with an airborne radar whose mean time between failures was less than a typical mission flight. Their answer: "It's the best we've had, and, anyway, that particular radar controls an air-to-air missile that only works ten percent of the time." Frustrating. The situation in C^2 is, if anything, worse. The military forces put up with

appalling conditions in HF communications, in ad hoc command centers, in nonsecure voice communications and the like because, "We haven't had anything better and we've been OK so far."

The difficulty of designing a naval communications architecture is compounded by the Navy's own traditions of command, an important element of which is the meaning of "special trust and confidence." Every naval officer's commission includes those words, and they have come to mean to him that he is trusted to carry out missions with the minimum possible instruction, i.e., the *less* communications from above the better. The tradition is reinforced by the almost absolute authority vested in ships' captains at sea, an authority originally granted in a time of communication delays of days to months.

"Commanders differ with technologists on a major issue—vulnerability and its risks. Technologists worry about vulnerabilities and try to design them out . . . . Commanders see vulnerabilities as problems in risk taking, not as absolutes."

Commanders at every level, however, insist on knowing what is going on within their commands, i.e., the *more* communications to and from below, the better. Whatever the answer to these conflicting ideas on communications—the less the better or the more the better—it is the latter that is happening in practice. The reason, I believe, is the increasingly precise way in which the Navy is being used as a responsive instrument of national policy.

One would think that there would be agreement on the need for widespread, tactical, secure voice. And yet, up to a few years ago, acquiring such secure voice capability was given low priority. The argument was that voice was used in fast-changing situations and that even if the enemy were listening in, he could not do anything damaging in time. Vietnam showed the fallacies in that argument, but it is still heard, particularly among aviators.

One of the more complicated arguments concerns the use of voice versus messages for command and control. Voice is fast, usually means instant acknowledgment, conveys emotion and nuances in meaning, and is excellent for colorful discussions of what the hell's going on in this damn crisis. By contrast, though they document who said what to whom and when, messages are slow (hours) and are unacknowledged in most Navy transmissions. Messages are preferred by Allied military officers whose ability to read English may be excellent but whose ability to understand accented imperfect English over a poor HF link is minimal. I sympathize with them!

Messages are also preferred, if not mandated, for operational orders. There is, however, a potentially hazardous period—the hiatus between the end of voice discussion and the receipt of written orders. More than a few operations have been jeopardized while awaiting written orders confirming conversations.

Another difficult subject for decision makers is decision theory, with its connotations of automated decision making according to someone else's logic. Certain decisions may be almost automatic, given a set of conditions, but don't tell that to a US President, an admiral, or a chief executive officer. A difficulty inherent in decision theory is that real-world decisions all too often are made under conditions never before considered, much less characterized and quantified. For example, how does the "rational man" theory of decision making apply to irrational events in the Middle East?

Another inherent difficulty in using computers in decision making is that, in a sense, computers are too perfect, too precise. For better or worse, whether computers are operating on simple data or complex algorithms, they will always produce precisely the same answers from the same inputs. If the inputs are incomplete or if unprogrammed events occur, the computers crash. If the context changes, what was the right answer before may be wrong—precisely wrong—in the new context. The computer consultant's results may not "make sense." Human beings confronted with making a decision clearly do not function that way. Rather, they try to be mostly right most of the time. We would rate a commander who was right three quarters of the time as pretty good and one who was right 90 percent of the time as brilliant. But one who demands complete information before making a decision would be judged incompetent. Survival, much less winning, requires prompt but imperfect decisions—they only have to be better than those of the opposition. So far, we don't know how to build computer systems that can operate that way. Research scientists are barely beginning to understand how the human mind operates so well in this mode—the formal term is "heuristically"—and it may be decades before a body of theory is developed that permits computers to emulate it.

So it seems that, no, decision making cannot be automated—but it can be aided. The Navy is making significant progress in this regard. It is comparing and correlating intelligence data to produce a more consolidated product. It is experimenting with computer aids keeping within complex rules of engagement. It is speeding up access to information and making the entry of information into data banks easier. However, such aids understandably make strong commanders nervous, particularly if they do not understand what has been done to the raw information before they see the consolidated result. Several improvements can alleviate their concern. First, any new system must produce more credible and faster results for them than they get now. Second, military officers need to be better informed of the strengths and weaknesses of C^2 systems, just as they are for aircraft, submarines, weapon systems, and the like.

Today's commanders face a rapidly changing C^2 world. In most respects it is a better one than that faced by the admirals I mentioned earlier. To the

extent that there has been a shift in consensus with time, I would expect today's commanders to emphasize these concerns:

- "We need provable answers and information, not an avalanche of data.
- "We want credible, timely, secure, and survivable communications and surveillance.
- "The new technologies are too damned expensive." (A familiar old reaction.)

There are, as always, commanders eager and willing to work with the technologists on new things. They see space systems making possible worldwide, near-real-time coverage of military operations. They have tried out the Global Positioning System (space-based navigation) in Pacific exercises to good effect. They have tried out surveillance fusion centers for support of air, surface, and undersea forces with good results and have learned important lessons. There is growing consensus that the new technologies are essential to winning the outer air battle. There is speculation that space and submarines are natural allies. A new warfare area, counter-ASW, nonexistent in any war to date, would combine the complementary capabilities of space and submarines.

Truly massive exercises have been held in the Pacific, testing and stressing command and control. In 1983 three carrier battle groups were deployed over an ocean region approximately 500 nautical miles in diameter. The fleet was supported by land-based aircraft, submarine forces in direct support of the battle group, and a remarkable array of new command and control systems from underwater to space. It was the largest coordinated exercise and most powerful battle fleet since World War II. All the events were real or near-real time and involved a high degree of innovation. The degree of C^2 asset exercise and dependency was unprecedented, and the exercise was regarded as very successful.

Nonetheless, commanders differ with technologists on a major issue—vulnerability and its risks. Technologists worry about vulnerabilities and try to design them out. Commanders see vulnerabilities as problems in risk taking, not as absolutes. In other words, a commander treats vulnerabilities as things to weigh on the scale of known benefits and possible risks. The vulnerabilities may then be acceptable or prohibitive, depending on the circumstances.

A good example is the story of air-dropped sensors in Vietnam. A group of high-level technologists, including a past science adviser to the President, conceived in the late 1960s the idea of placing sensors all along the border between North and South Vietnam. The sensors were to be variations on sonobuoys, radioing what they heard to commanders who could then direct fire to the vicinity. The question then arose, what would be the response of

the enemy as soon as he found out what the sensors were doing? Would he jam them? Would he systematically home in on their radio signals and destroy the sensors or, worse yet, spoof the sensors? To design and build jam-proof, spoof-proof, tamper-proof sensors would be an expensive time-consuming process. The longer it took to put the system into operation, the greater the chances of the enemy finding out what was intended.

After consultations with high-level commanders, it was decided to deploy as quickly as possible and to take the risk that there would be jamming, spoofing, and destruction of the sensors. As it turned out, the enemy did none of these things, ignoring them or at least not informing their troops. In one reported case, some North Vietnamese soldiers picked up an acoustic sensor, put it in a truck, and took it all the way to Hanoi, the sensor radiating the whole time and broadcasting the events of the trip!

There was for years acrimonious debate among the technologists over whether the North Vietnamese learned of the sensor concept well in advance of deployment. History shows that the North Vietnamese moved across the border in force before the sensors could be deployed. Was that the countermove, or was it a coincidence? Were the troops deliberately kept in ignorance of a psychologically potent danger to them? We may never know. But we do know that the response to our action was not what we would have taken. Subsequently, the sensors were used extensively and well, though in a different way. They provided intelligence information rather than direct targeting information, which, when fused with other information and with military tactics, played a critical role in the US marines' defense of Khe Sanh. The achieved gains, in other words, outweighed the postulated risks.

By contrast, there are commanders who reject the use of secure communications channels—too hard to use or take too long to set up—and talk in the clear, consciously taking what can be great risks for not much gain in the modern world of sophisticated interception techniques. Today's technologies make the targeting of preferred frequencies, preferred channels, known addresses, known telephone numbers, key words, and even certain voices comparatively simple. The commander who thinks that enemy headquarters will not have time to respond to intercepted conversations has not faced modern battle management C^2 systems.

Response from Moscow, or Washington, brings us to one of the most contentious subjects among commanders—command afloat or from the beach. In an era in which all assets were organic to the fleet, command afloat, particularly of the battle, was logical. As early as World War II the picture began to change, as other assets, generally located ashore, came into play. The use of intercepted and decoded messages to direct our Pacific submarine fleet against Japanese shipping is now a well-known story. Today, with over-the-horizon weapons, long-range ASW and space surveillance, a battle group is at a serious disadvantage without outside assistance. It is not

uncommon for a station ashore to know more about the battle situation than the commander afloat. Hence the unavoidable question, "Should the shore station be in command?" It would be presumptuous for me, as a technologist, to answer that question, but let me suggest that the answer may lie in some form of distributed command. If so, there is a close cousin, technically, in the field of distributed information systems. Unhappily, that field is plagued with the same problems. What computer is in charge? How do you know? Which computer has what information? Which computer should preempt, and when, and why?

As if the question of command afloat or ashore is not difficult enough, let me extend the command question one step further. Who commands information flow? In other words, who decides who gets what? Two things are apparent:

- Information is going to be so important in future conflicts that it may well determine their outcomes.
- If so, command of information flow becomes a critical command function.

But who is the information flow commander? Should there *be* a C^2 systems commander comparable to commanders of platforms? This question, these days, is not trivial. There is more information available than can be absorbed by a battle commander; someone must filter and condense it. To do that, decisions have to be made as to what is important and what is not. Who decides, how, when, and why? The current solution seems to be a "deputy commander," probably ashore, judging from the operations I have seen of the Sixth and Seventh Fleets. In any case, without answers to the questions of command of information flow, a C^2 architecture will satisfy no one.

These questions of command are not easy to answer. They imply changes in the command structure itself. But organizational changes due to new technologies occur all the time.

For example, consider the question now being addressed by Captain Fogarty of the USS *New Jersey*, a battleship now equipped with long-range antiship missiles in addition to its 16-inch guns. The question is, which is the main battery, the missiles or the guns? The gunnery officers among you will know that is not a simple question. The answer will significantly affect the power structure aboard that ship. A more complicated question is, should the *New Jersey*, which is as fast and as survivable as they come, be the command and control ship of the battle or action group? (Currently, she is not.)

In this discussion of the commander, I have posed more questions than I have answered. If my assessment of naval commanders is correct, you will not agree among yourselves on the answers. There is also likely to be a strong minority view, which, under the right circumstances, could be right. As

Admiral Moorer indicated, the right answer may even depend on who is President!

The architects of command and control systems are therefore confronted with both technological opportunities and controversial perceptions of what is needed. Whatever is designed and built will take years to implement, by which time the original advocates of the selected approach will have left the scene. To some extent, this has led to redirection or paralysis of programs. Proponents of top-down architecture and proponents of fleet-generated requirements have each held the field for a while before giving way to the other. I doubt that this will change, even with the new emphasis on survivable command and control.[19]

On Strategy

The resurgence of strategic thinking in the Navy challenges a writer to offer at least a few thoughts on the possible impact of his specialty on naval strategy.[20] In my mind, two factors stand out: the increase in combat radius and the emergence of new dimensions of warfare.

It was not very long ago that combat radius was measured in tens of miles, with each combatant performing most of the combat functions of surveillance, fire control, weapon launching, and battle damage assessment. The combat radius is now thousands of miles, with dispersal of the functions to different, widely separated platforms. This change, at the very least, raises questions about such long-held concepts as command afloat, independent action, organic assets, and withdrawal to comparative sanctuaries. The extended combat radius inherently calls for very-large-scale, coordinated, real-time command and control. Clearly, combat is now more complex—yet some of the past constraints and limitations have been opened up. Forward combatants need not be limited by the ammunition they can carry; they can call up long-range weapons and guide them to their targets. Submarines no longer need be limited by the range of their own sensors. Fleet commanders can command more assets than those organic to their fleet.

The extended combat radius does raise difficult questions of roles and missions. Fleet commanders necessarily will be concerned with events hundreds of miles inland that critically and immediately threaten the fleet, a situation already confronting the commander of the Sixth Fleet in the Mediterranean. In effect, the oceans of the world have become seas, the seas have become lakes and even narrow waterways. The Red Sea, with its narrow channel, is even narrower than it looks on the map, and the Caribbean is not as far from the Soviet Union as some might think. The Navy thus finds itself both confined and dispersed by the extended combat radius.

Mahan wrote 94 years ago, "Commerce-destroying by independent cruisers depends upon wide dissemination of force. Commerce-destroying through control of a strategic center by a great fleet depends upon

concentration of force. Regarded as a primary, not as a secondary operation, the former is condemned, the latter justified, by the experience of centuries."[21] Mahan advocated concentration rather than dispersal of force, a line of strategic thinking followed by the navies of the world for almost a century.

What might Mahan say today? I believe he would be one of the first to recognize that the new technologies of command make possible coordinated operations over vast distances. He would recognize that his concentration of force now means coordination and integration of force, not necessarily close proximity, especially in the age of nuclear weapons. He would, as before, discount small, isolated independent forces as a foundation of a strategy. He would, I would hope, recognize as in the tradition of his great fleet the 1982 Frosch Report on Naval Aviation[13] and the concept of a battle group tied together by an integrated information network.

On the other hand, and here I tread as carefully as I can, he would probably discount, at least as primary, the concept of independent submarine actions isolated from global sensors and disconnected from timely command and control. He would have endorsed Doenitz' close coordination of his submarine fleet and condemned sending the *Bismarck* out as an independent cruiser against a coordinated air and sea force.

Mahan's study of history through 1783 could not, of course, include submarines or aircraft, much less modern command and control technologies. He was looking for underlying principles, not projecting future forms of combat. His purpose was to bring into the foreground a dimension of warfare—seapower—that land-oriented historians had slighted.

In that tradition, let us look at the second impact of the new technologies of command on naval strategy, the emergence of new dimensions of warfare.

Most of this discussion has been devoted to one new dimension in particular, the information war. It is a war between sensors and signature control, between codes and cryptanalysis, between military security and intelligence. Unfortunately for strategic thinkers and historians, the information war, with its closely held intelligence secrets, is largely hidden from view. The result, all too often, is that conclusions about strategy are reached that can be far from reality. Ronald Lewin, in *Ultra Goes to War*, the most objective evaluation of the operational consequences of code cracking I have ever read, shows dramatically how history must be rewritten when the actualities of the information war are made public. J. A. Carr shows how an even earlier battle, the battle of Virginia Capes and the subsequent surrender of Yorktown, was won by the French and Americans more by superior command and control than by firepower.[22]

As with seapower in the late 1800s, command and control is today treated by many strategists as incidental, uncontrolled, and even uncontrollable. Communications is mentioned when it fails. Intelligence appears as a matter

of sheer cloak-and-dagger luck instead of as an often deadly battle over information.

Military exercises treat information flow in much the same way historians do. Information is treated as if it were perfect, as if no disinformation were in the command and control system, and as if time lates did not exist. When communications breakdowns occur, they are ignored—the scenario is played out according to a script. In the days when intelligence and communications were unreliable or at least erratic, this treatment of information might have been understandable. Today's information flow is drastically different—voluminous, checkable, controllable, and vulnerable. The Soviet Services know this and, being a part of a society whose government makes pervasive use of information control, they have readily developed a military doctrine for it. For the Soviets, information is a weapon. Distortion and destruction of information available to the enemy is as valuable as destruction of firepower. Clearly it is time for us to include the information war as an element of our own strategy and to develop modern doctrines for its use.

As for the future, we have all heard of star wars and the science fiction visualization of them as combat between battle stations in the ocean of space. Well, perhaps. For the present, the most immediate and probable impact on naval operations will be the effects on the information war. Put another way, the objectives of star wars in the immediate future will be the protection and denial of information generated and relayed by satellite systems. Much of star wars will be electronic combat. Heavy weapons operating in and from space will come much later. Nonetheless, it is not too soon for Navy strategists to be thinking about the impact of space war on naval operations.

For years the Navy has described itself as a three-dimensional Navy, one that fights under, on, and above the sea. It may be time to add more dimensions. Space systems certainly have arrived as elements of combat. Modern command and control systems are engaged in a combat every bit as real as that between submarines, ships, and aircraft and with comparable impact on the outcome of the overall battle. Perhaps we should talk about a four, a five, or a multidimensional Navy, lest these new dimensions be slighted the way nineteenth-century historians slighted seapower. All these dimensions are essential to the Navy, regardless of how furnished or managed. Take away one and naval strategy is in trouble. Add to any one and naval strategy improves. Together they make the Navy the powerful and uniquely effective instrument of national policy that it is.

Notes

1. Ronald Lewin, *Ultra Goes to War* (New York: McGraw Hill, 1978).
2. Samuel E. Morison, *The Two Ocean War* (New York: Ballantine, 1963).
3. Ronald Lewin, *The American Magic* (New York: Farrar Strauss Giroux, 1982).
4. Thomas B. Hayward, "'Technology Push' Opportunities in Space," *Signal*, March 1982, pp. 19-24.
5. James E. Oberg, *Red Star in Orbit* (New York: Random House, 1981).

6. Department of the Air Force, *Soviet Aerospace Handbook (Pamphlet 200-21)* (Washington: US Govt. Print. Off., May 1978).
7. Robert B. Berman and John C. Baker, *Soviet Strategic Forces: Requirements and Responses* (Washington: Brookings Institution, 1983).
8. Weekly Compilation of Presidential Documents, 9 October 1978, *Administration of Jimmy Carter*, 1978 (Washington: US Office of the Federal Register, National Archives and Record Service), p. 1684.
9. A.J. Baciocoo, Jr., "Artificial Intelligence and C^3I," *Signal*, September 1981, pp. 23-30.
10. S.J. Andriole and G.W. Hopple, "They're Only Human: Decision Makers in Command and Control," *Signal*, March 1982, pp. 45-50.
11. D.A. Brown and H.S. Goodman, "Artificial Intelligence Applied to C^3I," *Signal*, September 1981, pp. 23-30.
12. C.A. Montgomery, "An Active Information System for Intelligence Analysis," *Signal*, October 1981, pp. 20-27.
13. Naval Studies Board, *The Implications of Advancing Technology for Naval Aviation* (Washington: National Academy Press, 1982).
14. Cave Brown, Anthony, *Bodyguard of Lies* (London: W.H. Allen, 1976).
15. The White House, *U.S. Civil Space Policy* (Office of the White House Secretary, 11 October 1978).
16. The White House, *National Space Policy* (Office of the White House Press Secretary, 4 July 1982).
17. R.V. Jones, *Wizard War, British Scientific Intelligence* (London: Coward, McCann and Geoghegan, 1978).
18. G. Guy Thomas, "Soviets' Fight-to-Win Doctrine Incorporates Radio Electronic Combat," *Military Electronics/Countermeasures*, December 1982, pp. 36-41.
19. Norman Waks, "Inherent Conflicts in C^2 Systems Acquisition," *Signal*, May 1983, pp. 83-86.
20. F.D. Kennedy, Jr., "Naval Strategy for the Next Century Resurgence of the Naval War College as the Center of Strategic Naval Thought," *National Defense*, April 1983, pp. 27-30.
21. Alfred T. Mahan, *The Influence of Seapower on History, 1660-1783*, American Century Series (New York: Hill and Wang, 1975), original copyright 1890.
22. J.A. Carr, "Virginia Capes: The Unknown Battle," *National Defense*, April 1983, pp. 32-39.

Communications dominate war; broadly considered, they are the most important single element in strategy, political or military.

A.T. Mahan