INCIDENTAL PAPER

Seminar on Command, Control, Communications, and Intelligence

Getting in Front of C^4I^2 Problems
Frank J. Breth

Guest Presentations, Spring 1988
Rae M. Huffstutler; Richar L. Thornburgh; James R. Locher, III; Robert T. Herres; John F. McLaughlin; Jerry O. Tuttle; Earl F. Lockwood; Robert C. Kingston; Frank J. Breth; Ruth M. Davis

March 1989

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

Chairman
Anthony G. Oettinger

Managing Director
John C. B. LeGates

E-mail: pirp@deas.harvard.edu URL: http://www.pirp.harvard.edu
I-89-1

Getting in Front of C^4I^2 Problems

Frank J. Breth

Brigadier General Frank J. Breth has been Director of Intelligence, Headquarters, Marine Corps, since 1985, and became Director of the C^4I^2 (Command, Control, Computers, Communications, Intelligence, and Interoperability) Department in 1988. Since joining the Marines in 1959, he has held positions of increasing responsibility both in the United States and abroad. He served as a rifle company commander and operations officer in the 3rd Marine Division in Vietnam and as the Division's liaison officer to the 1st ARVN Division; and Naval Forces Korea Liaison Officer to the 1st Marine Division, Republic of Korea Marine Corps. From 1976 to 1978, he commanded the 2nd Battalion, 1st Marines, 1st Marine Division and later served as Assistant Chief of Staff, G-1. He served as Chief, Contingency Plans Branch (C-5), of the newly formed Combined Forces Command (ROK/US) in Seoul from 1979 to 1981; became Deputy Director, 9th Marine Corps District, in 1981, and assumed command of the district in 1982. In 1984 he became Assistant Chief of Staff, G-3, I Marine Amphibious Force, and was promoted to his present rank in 1985.

Oettinger: Our guest today, as you all know, is Brigadier General Breth. He is Director of Intelligence for the Marine Corps, and you know his history from the biography that you have. What you do not know is that he has acquired, in addition to the title I just mentioned, some more titles, and I'll let him describe that and his functions as he speaks. He would like to get through a set of slides with minimum interruptions. Make any essential interruption, if you need clarification, but for more general discussion, hold your fire.

Breth: Thank you, Dr. Oettinger. I first met Dr. Oettinger when he was on the Board of Visitors to the Defense Intelligence College and we were talking one night about your business, and all of a sudden I find myself here today. It's a real honor to be here, because I know whom you've had here in the past and also I've taken a look at some of your papers. The only thing I must admit to you is that I do not consider myself an expert in this business. I am someone who has found myself in the business of C^4I^2 (command, control, computers, communications, intelligence, and interoperability). You may find yourself there someday, also. Clearly it's not an easy field to work in. It encompasses much and expertise is required in several areas.

My background is basically in engineering during my undergraduate years. I went to a military college (Virginia Military Institute) and have been in the Marine Corps, serving mainly as an infantry officer. Accordingly, I've served all over the place. I served tours with the Navy, and I've been to the War Colleges and other tours with the other services. I also served a joint tour in Korea and was responsible for the war plan for the defense of Korea. Following that, I was the operations officer of the 1st Marine Expeditionary Force, which is a war fighting force of about 60,000 Marines, including a Marine division of 20,000, a Marine air wing that has 550 aircraft in it, and a logistics base. We were responsible

for readying two Marine amphibious brigades, as well as for contingencies in various parts of the world.

I remember the day when I walked in to see my boss and he said, "You're going to be the Director of Intelligence for the Marine Corps. The Commandant wants to put somebody in who has operations experience in intelligence." Since that moment I've been on the job for three years and I have found that every day you get deeper into this technical business and you learn more and it never stops. Recently, we gained a new Commandant, General Gray, whom you may have seen recently on *60 Minutes*. He is a determined leader with a wide range of experience. He recently directed me to form a C^4I^2 department for the Marine Corps and placed me in charge. All of a sudden I went from being responsible for intelligence to the C^4I^2 which I will explain.

What does C^4I^2 mean? There are people who talk about C^2, C^4I, C^3I, and all related acronyms. Don't let that confuse you, but pay attention to the basics. Go back to a "bottom line," i.e., given a rational background of one's experience, you can make good decisions if you have accurate information. For example, intelligence is processed and evaluated information. In today's world, it's not uncommon to be a deployed Marine and to have so much information that you cannot sort out the truth, since we have such high-speed processing and communications systems that will give it to you faster than you can handle it. The trick is, how do you use technology to solve problems at various echelons of command? The C^4I^2 approach is necessary.

For example, fighting Marines rarely need information that the President or higher-level policy makers will need. The Marines down there on the perimeter in Panama need to know who's 300 meters away from them, not what President Noriega's going to do tomorrow. Clearly, there is a different focus of what's important at different chains of command. The Marine focus is on the warfighting commands. That's where the battles are won or lost.

I'd like to approach this C^4I^2 from the point of view of someone who's moved from intelligence into a greater communications processing role. To do that, let me move through intelligence — talk about the threat, relate some particular focus on the Marine Corps — and then get into the communications and computer business, and approach it this way rather than start at command and control. I'll take your questions anywhere in the briefing.

First of all, let me restate that I am not an expert at C^4I^2. I've been a person at work at it. However, I think I've learned a few things by making mistakes and listening to the wise counsel of others. There can be a lot of wasted motion in this business and there can be a lot of so-called brilliant thoughts that are absolutely rife with disaster.

You probably think of the Marines coming across the beach with John Wayne as you watch *Sands of Iwo Jima* and all the rest of the old movies. We have Marines in Panama and in the Persian Gulf at risk at this moment. We have 3,000 Marines on amphibious shipping somewhere near Algiers, and we have Marines in the Indian Ocean near Sri Lanka today. We have forward deployed presence if crises develop. The nature of our service is that you never see many Marines, as they are deployed all over the world.

Marines consistently are deployed with the Navy. We can also fly and project power ashore from naval platforms. We also work with a joint task force (JTF) comprising all services who report to a commander in chief, such as the European Command or the Southern Command, who report to the Chairman of the JCS, who in turn reports to the Secretary of Defense, who reports to the President.

What is our emphasis? What's important to a Marine? I will tell you — success in combat. When you're in that kind of business you must pay attention to intelligence. If you don't have intelligence you are very inefficient. In our type of business you pay very dearly for mistakes in lives or casualties. Effective intelligence can preclude these problems.

To obtain good intelligence the Corps must be a viable part of the overall intelligence community. This first slide (figure 1) is the intelligence community. It's diverse. It's different. It's compartmented, and it's at high security levels. Each serves a different master. They have different strengths. However, when you put them all in the same bag, it is called the National Foreign Intelligence Board. I sit as a member of that board with all these organizations, with the Director of the CIA as head. These various agencies are who you would expect plus the Senate Select Committee on Intelligence, the House Select Committee on Intelligence, and the National Security Council with the President's Foreign Intelligence Advisory Board. You might ask, "What do you really need intelligence for?" You need it for decision making at all levels.

At this point I should go back to the Marine Corps mission statement (figure 2) to focus on

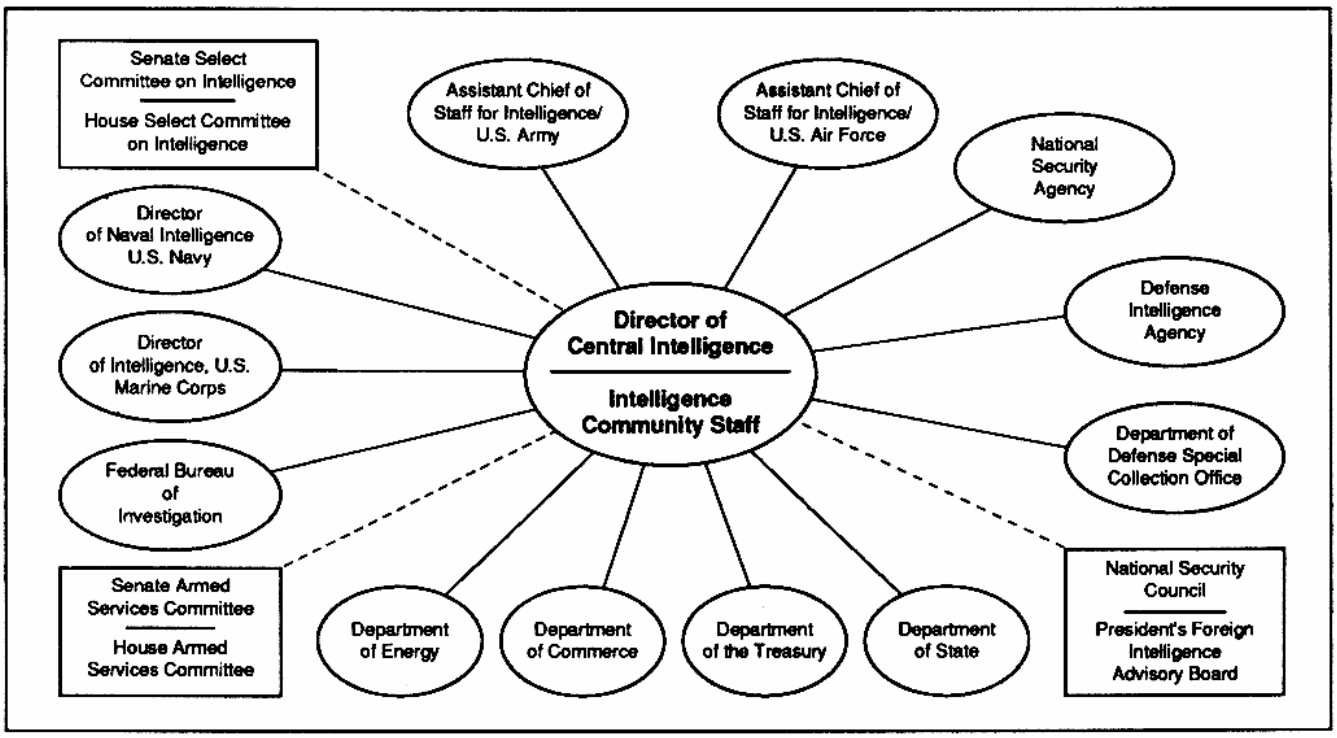

Figure 1. The Intelligence Community

The Marine Corps is an in-being combined portion of the nation's general purpose forces best suited for service as the necessary ready force of combined arms for rapid, credible response across the spectrum of conflict and civil situations.

The Marine Corps must maintain a first-to-respond posture.

Rather than being scenario-oriented, the Marines must be mission-oriented.

Figure 2. U.S. Marine Corps Mission Statement

where I'm coming from or what I pay attention to in regard to the intelligence chart. Remember, the Marine Corps is a general-purpose force, tactically oriented, and forward deployed with the Navy for a variety of contingencies. Since 1945, of the crises of our country, 88 percent of the time those crises have been answered by the Navy and the Marine Corps. As a result, we can easily predict that Marines will probably be involved in crises in the future.

Oettinger: What does that "combined" mean on the chart? Usually when I run across that it has to do with U.S. and foreign, but I suspect you mean it somewhat differently.

Breth: I mean that completely differently. It's a good point. A "combined organization" for the Marine Corps means we have our own air element integrated in combat organizations. We have an integrated combat team which is called the MAGTF. It's an acronym that stands for Marine Air-Ground Task Force, which is an organizational concept for all air formations.

The slide you're seeing shows a naval task force at sea that you are normally used to seeing in the media. Force presence can be put off a country. You don't have to go ashore. You don't need landing rights. Yes, you need to obey international law, but it gives you a force presence at sea which shows America's resolve.

When the Marines go ashore, you're used to seeing this assault amphibian tractor that carries 25 Marines. It's coming out of the landing platform dock with a helicopter on it. This particular picture you're seeing is off Beirut. The picture is representative of our forces deployed at sea.

There is another aspect of this warfare and not many people really think about it. There's warfare in the electronic spectrum. Not many people really pay attention to this and not many people understand it. It's an electronic spectrum from radio waves all the way through microwaves through infrared, through other frequencies. Lasers are in that spectrum, more clearly defined as directed energy. Our country and our adversaries must also pay attention to this emerging area of interest. In Marine C^4I^2, I must pay attention to it, or the Marine force will be at risk.

I like to use this example to state what is important with intelligence and about command and control (figure 3). Clearly, you cannot control the situation unless you have a feel for it and understand it. When you're in combat and you don't understand what's out there, how can you make good decisions that focus combat power precisely enough to achieve your mission? This is an ongoing problem at all levels of war-fighting forces. That is something that we deal with in C^4I^2 on a consistent basis. Specifically, the Navy and Marine Corps go where other services do not, and because of the evolving Third World crises there are new problems. The Third World and related low intensity crises present very difficult problems.

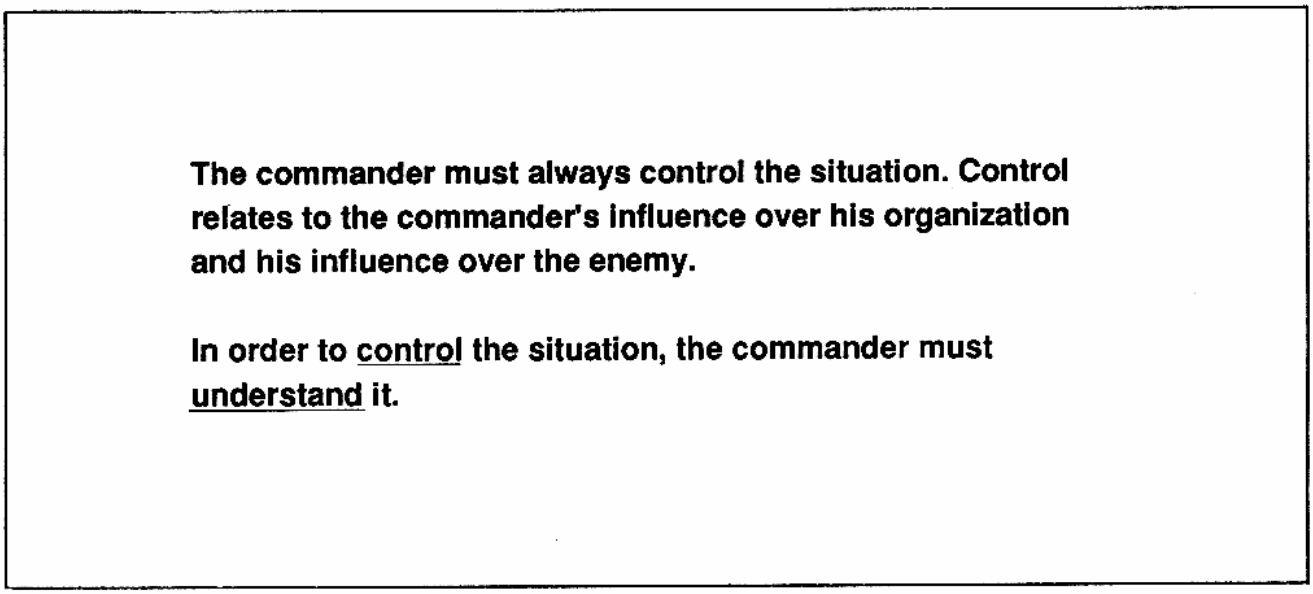

Figure 3. Command and Control

where I'm coming from or what I pay attention to in regard to the intelligence chart. Remember, the Marine Corps is a general-purpose force, tactically oriented, and forward deployed with the Navy for a variety of contingencies. Since 1945, of the crises of our country, 88 percent of the time those crises have been answered by the Navy and the Marine Corps. As a result, we can easily predict that Marines will probably be involved in crises in the future.

Oettinger: What does that "combined" mean on the chart? Usually when I run across that it has to do with U.S. and foreign, but I suspect you mean it somewhat differently.

Breth: I mean that completely differently. It's a good point. A "combined organization" for the Marine Corps means we have our own air element integrated in combat organizations. We have an integrated combat team which is called the MAGTF. It's an acronym that stands for Marine Air-Ground Task Force, which is an organizational concept for all air formations.

The slide you're seeing shows a naval task force at sea that you are normally used to seeing in the media. Force presence can be put off a country. You don't have to go ashore. You don't need landing rights. Yes, you need to obey international law, but it gives you a force presence at sea which shows America's resolve.

When the Marines go ashore, you're used to seeing this assault amphibian tractor that carries 25 Marines. It's coming out of the landing platform dock with a helicopter on it. This particular picture you're seeing is off Beirut. The picture is representative of our forces deployed at sea.

There is another aspect of this warfare and not many people really think about it. There's warfare in the electronic spectrum. Not many people really pay attention to this and not many people understand it. It's an electronic spectrum from radio waves all the way through microwaves through infrared, through other frequencies. Lasers are in that spectrum, more clearly defined as directed energy. Our country and our adversaries must also pay attention to this emerging area of interest. In Marine C^4I^2, I must pay attention to it, or the Marine force will be at risk.

I like to use this example to state what is important with intelligence and about command and control (figure 3). Clearly, you cannot control the situation unless you have a feel for it and understand it. When you're in combat and you don't understand what's out there, how can you make good decisions that focus combat power precisely enough to achieve your mission? This is an ongoing problem at all levels of war-fighting forces. That is something that we deal with in C^4I^2 on a consistent basis. Specifically, the Navy and Marine Corps go where other services do not, and because of the evolving Third World crises there are new problems. The Third World and related low intensity crises present very difficult problems.

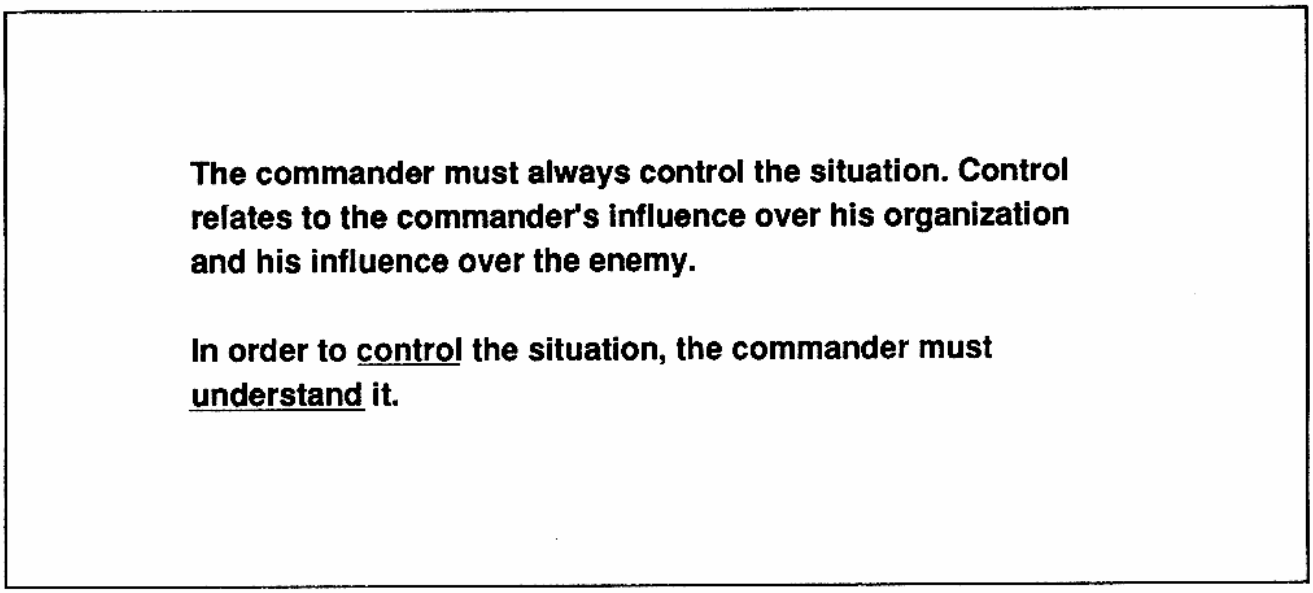

Figure 3. Command and Control

No one wants nuclear war. But if you don't invest in that capability, you cannot deter it. That investment is very costly for our country. If you spend so much money on nuclear response, you may not have money for peacetime presence, surveillance, or show of force with conventional forces. Let's bring up Sri Lanka as an example again. Which is more important: to watch the strategic weaponry of the Soviets or the Sri Lankans' situation? Obviously, air defense money will be spent to watch the former, and it should be. No one complains about that, but we must pay attention at the same time to Sri Lanka, Eritrea, the Persian Gulf, the countries across the African littoral, Central and South America, and the Philippines, and those countries are not all in the same area. The Marines and the Navy, and specifically the Marines, must be prepared for crises and limited war. My focus as director of C^4I^2 is on mid-intensity to low intensity war where Marines will most likely be committed, and we need to get in front of the problems and prepare now. If you do not do this, you will suffer disastrously, and there are examples of this. When you, in this seminar, talk about war, be prepared to talk about where it is in the spectrum of conflict. Define your situation so you can address your specific concerns.

Marine procurement programs are normally built to work in the general area of crisis response. Based on what you need to be successful, you must tailor your forces for forward deployments. That situation gives us an intelligence problem from Sri Lanka to Russia. What is the threat like? I'm not going to take a lot of time to go through all this, but here are some of the changes (figure 5). Basically, we are dealing with the Soviet-Warsaw Pact, the surrogates, the Third World, and terrorism. We know that the Soviets have a tremendous modernization program and great redundancy. What do they do with their old equipment? They store it, they give it away, or they sell it for income. That gives them availability of these weapon systems to follow on diplomatic initiatives, and lets them send advisers or maintenance teams out. If we get involved in these crises that are dictated by economic or political problems, we end up facing the Soviet equipment, or what is sometimes called a "blue-gray" database, which could be French, German, or British equipment that may be on hand.

Let me come at this in a different way. You can go from low intensity conflict to high intensity conflict very quickly, as we talked about. You can also go from non-nuclear to nuclear warfare and chemical warfare along that spectrum. Our adversaries and their strategy (and their warfighting doctrine) deal in large numbers of weapons, tanks, and aircraft, and, as an aside, their quality has improved a lot. For example, their artillery is very good, but they've been working on different, more lethal warheads. We will face the combined arms warfare (air, ground, and sea) of our adversaries, which now includes more high-speed, mobile systems, and long-range standoff capabilities.

For example, the Russians assumed that after World War II we were going to be adversaries. They took a look at our style of warfare and knew that we believe in tactical air. They watched how our fighter and close air support aircraft destroyed everything in our army's path when the Allies conquered western Europe. Also, when we went to Korea we had a terrific tactical air capability that was applied to the enemy. When we went to Vietnam we again had a terrific air campaign against North Vietnam. During this period since World War II our adversaries have developed an integrated air defense. If we fly in that defense envelope, it is extremely hazardous to our aircraft. This AA (antiaircraft) and SAM (surface-to-air missile) envelope is growing denser and denser, so much so, that many pilots are at risk to accomplish their mission, much less return. It's a great tactical development we must overcome in war.

How do you operate then? How do we operate in possible actions in low intensity conflicts where even the poorly trained fighters possess hand-held air defense weapons? It is not uncommon for this situation to happen. The capability is there to do that on a moment's notice. Another example is terrorism in our lifetime. An airliner was captured today. Weapons capabilities falling into the wrong hands can create a disastrous problem anywhere on earth. Other action going on around the world includes intelligence and electronic warfare, air-ground naval missile threats, etc. The naval missile threat you are seeing now in the evening news is a very cheap Chinese missile used as Iran targets a loaded gas platform off Kuwait.

Another poignant example was the Iraqis shooting an Exocet missile and the resultant damage on the *USS Stark*. Everywhere you see improved munitions and massive firepower. There are changes. This is a fact that you must be aware of if you deal with warfare. One side always tries to get the technological advantage over the other. We do. They do. But to stay equal and abreast is a real challenge. It can change the character of warfare very quickly.

Let's get to the Spetsnaz capability of the Soviets (figure 5). It is characterized as low-level, undercover, rear area operations that can come to Harvard, let alone Boston, or Norfolk, or Morehead City, and disrupt communications in our country before we even go to war. It's a modus operandi that the Germans used in World War II and the Russians have that capability today. For example, they are deployed and exercised in Afghanistan. This fact appears in open-source literature. Clearly, we have a very dangerous world.

Secretary of War Stanton once said, "Gentlemen do not read other people's mail." Therefore, in his time we did not have a cryptologic capability, which is the ability to listen to encrypted communications in order to decipher what our adversaries would say. This is a part of warfare today. I won't go into it much more, except to say that the Russians and our adversaries are very good at this. So when we deal with matters over the telephone and over the radios of tomorrow and today, we can assume that our adversary will listen. That leads into the communications arena and also into the technological arena.

I must go back again to intelligence, and command and control. Someone once said, "Forewarned, forearmed; to be prepared is half the victory." How nice it would have been to have had that ability at Pearl Harbor. Very shortly thereafter (I know you watched the movie, *The Battle of Midway*) Admiral Nimitz knew in advance that the Japanese would be intercepted 300 miles northwest of Midway at a certain time at a certain altitude on a certain course. He knew from an intelligence prediction approximately ten days before it happened. We put our forces out there and the Navy fought a very gallant battle and barely won an immense strategic victory. That was exact intelligence provided to a commander. There have been some other great intelligence successes. Our job in intelligence efforts is to make sure that we have that capability in the future. The Russians have that same goal. The Cubans have that same goal. Any adversary will have that same goal. That effort has bearing on command and control in any military organization.

Intelligence gaps must be filled in. What types of weapons systems do they have? Where are they? How will they use them, and when will they use them? Therefore, we will place our collection assets either on imagery, signals intelligence, or human intelligence to find it out, and then we'll get the information back, and we'll process it, and evaluate it, and then we will disseminate it to those who need it. That is the traditional intelligence cycle (figure 6). It requires the effective communications, computers, connectivity, and interoperability we are talking about.

What then is the intelligence concept of operations for the Marine Corps? I need to provide accurate intelligence that will show when, where, what, and how the enemy combat power is disposed — and how to use our combat power to defeat the enemy with the least cost to our forces. Priority of support, clearly, in peacetime to war transition, is to our forward-deployed forces who are out there today, or may go tomorrow. The rapid response forces — air, Marine Amphibious Forces — require that support. We also have the building block process of the small forces building up to a Marine Amphibious Force which is about 50,000 or 60,000 in the objective area.

Intelligence support has to be transitional for us. As we leave port, we've got to work on naval operations, and go to the amphibious objective area with the amphibious task force. We're aboard ships, so we have to work with the Navy and the commander in chief's theater intelligence architecture plans. We must be concerned with the questions of: How are we going to get intelligence? How will it work? Who will do what? If you don't think about this ahead of time, you can't just turn the switch on and say, "Give me intelligence." It's like your professor saying, "Give me your thesis today." It's very simple: we must stay in front of the situation and prepare early on.

The acronym TENCAP stands for tactical exploitation of national capabilities. As you know, there is lots of junk flying around in space. There are very important items that you read about. There's a terrific intelligence capability in space. It's nice to have the President receive the product, but it's also nice to have that forward-deployed Marine out there know what that system can do for him and get him those products.

Oettinger: A footnote on that, that will get you backward into the record of the last eight years, is that TENCAP integration is talked of in an innocuous sort of way as a fait accompli. If you look back to eight, seven, six years ago, you will see a great deal of complaint about the left hand, and the right hand, and so on, and that innocent-sounding phrase is a result of a great deal of head knocking. You can see the traps there in the record.

Breth: It's a success story. It's effort completed by many people several years ago. This was a great

- **Soviet Warsaw Pact, Soviet surrogates, Third World area, terrorism**
- **Low to high intensity conflict**
- **Non-nuclear to nuclear / chemical / biological warfare**
- **Massive numbers of forces and weapons**
- **Comprehensive combined arms warfare capability**
  - high-speed, mobile systems; long-range / standoff weapons
  - intelligence / electronic warfare capability
  - air / ground / naval missile threats
  - improved munitions
  - massive firepower
- **Modern weapons**
  - quantity and quality
  - R&D and technology transfer
  - air threat particularly dangerous
  - extensive anti-aircraft artillery and surface-to-air missile air defense capability
- **Nuclear / Chemical / Biological warfare capability**
  - extensive arsenal
  - best equipped force to maintain operations on a contaminated battlefield
  - future use by terrorists
- **Spetsnaz capability**
  - exploit rear area vulnerability
  - combined with other operations

Figure 5. The Threat

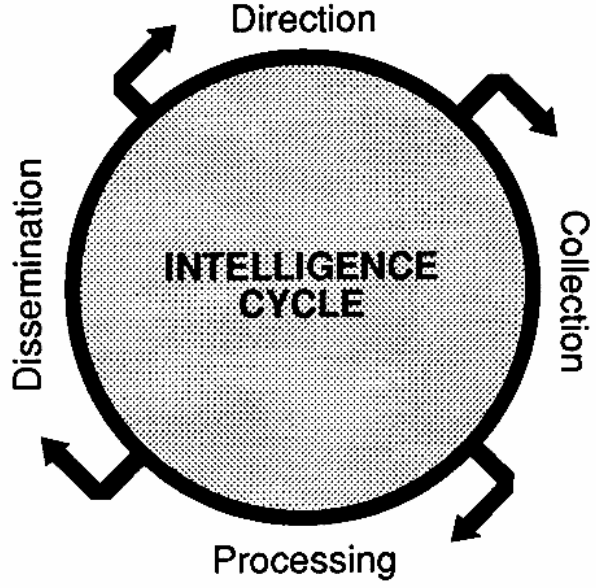

Figure 6. Intelligence Cycle

effort and there are some great success stories. Unfortunately, I just can't tell you.

When we Marines go ashore we have to have a stand-alone capability. Of course, those ships will also be useful. When we get ashore, it may be in a scenario where we're the only forces ashore, so we have to have a set of expeditionary equipment out there that will do the job: weapons, command and control, intelligence, logistics, mess halls, the whole business. We must prepare to operate in all threat modes from peace, to crisis, to war — low intensity and high intensity. And we must pay attention to the air, ground, and rear area threats.

In the intelligence milieu, signals intelligence incorporates communications intelligence, and electronic intelligence of categorizing emitters. For example, every radar has a signature. Imagery is the picture receiver. For example, in the state of the art today, it's not uncommon to transmit over fiber optics a picture taken with your camera and put it through a modem which is connected to a field radio and send it over those relays to another modem and get that photograph to a distant source very quickly. That technology is available today.

Do you know where it came from? It came from American business. It didn't come from the CIA and its deep black world. There are some clever folks out there today in business. Something we can get into later on is the younger generation's familiarity with electronics, and computers, and video games. There are also some ingenious people who do garage type work, who can provide some things in communications and information processing. Intelligence also includes human intelligence, reconnaissance and surveillance, and TENCAP.

You will also hear the term "all-source analysis" in intelligence. We need to take all information and put it together and analyze what it means. This is a very difficult technological challenge. And then, we must get it to the commander who needs it, when he needs it, in a usable form in a near-real time fashion. You can have fused intelligence, but if you don't get it to the person who needs it, all the effort may be wasted.

In this intelligence requirements chart (figure 7), real time means now. Near-real time means in a few seconds or minutes. For example, when carrier air in Korea, and Air Force air in Korea, were fighting in North Korea, they would be given their missions to bomb a target. Very shortly thereafter, within hours, they would put up a photo reconnaissance plane which would fly over that target to take a look at the target to see the damage. He would return, and they would process the film, and that night they'd take a look. "No, you didn't hit that tank. You didn't hit that rail yard. You didn't do this. Go back and do this again." That cycle would sometimes take days. We are required to accomplish that effort now in hours and minutes.

Take, for example, an enemy tactical missile system with no nuclear warhead on it which can move into position to fire within a few minutes. If you even know about the exact tactic, to fly your attack aircraft there with great speed and to attack the target is just about impossible unless you have very timely, accurate intelligence. Clearly, the character of warfare has changed. The only way you can survive in warfare today is to be able to pass information quickly. You can see that the command and control and intelligence efforts must be integrated.

What is meant by area of interest and area of influence? Area of interest means you have to watch out very deep, because of the lethality and speed. The area of influence is what I as a commander can do with my Marines and their weaponry. For example, if I can take an F-18D with 500-pound bombs on it, and place a tanker in the air, and refuel the F-18 and get it out to a thousand miles, that is my area of influence. If I can't get any further, it is to that limit. For a rifleman it's the range of his rifle. For an artilleryman it's the range of his artillery cannon. For an aircraft it's as far as you can accomplish the mission and return.

Let me give you a scenario of what I'm talking about for intelligence requirements. I was reading some of your past proceedings today. The North American Defense Command is very interested when somebody comes through that radar scope, and they react accordingly. With today's high-yield, long-range weaponry entering that radar envelope, by the time someone launches a standoff missile at us it could be too late. Another example is Marines in Norway. If we had our air control equipment there and we were waiting for the Russian bombers, which are very fast, to come into the radar screen, by the time we discerned that fact and gave the mission order to the intercept plane to take off, our enemy could have fired his weapons and we would never have touched it. In these two scenarios you can see we must have a deeper, long-range look to get intelligence so that we can react properly.

For example, it would be much better to watch the enemy airfields with imagery — to watch when they deploy those bombers, to watch them loading the weapons and see what type of warheads will be on those planes. It would be great if we could hear

the pilots talking to each other when they took off and when they're airborne, and you would then cue your sensors to watch. Accordingly, you would change the weaponry on your aircraft, and intercept the enemy before they could launch their weapons. That is the character of warfare today, which clearly presents a terrific challenge for intelligence and command and control experts.

As you can see, intelligence requirements are much different today. I don't want to spend a lot more time on it. Therefore, let me get into the C^4 area because this is also an important area of concern. In the C^4 business we must be interoperable with our Marines, Air Force, Army, and Navy, our commanders in chief, and also our allies. As an example, let's say that we all agree to buy the same radio with the same speed rates and frequency bands, but the French don't want to do that. They want to buy Thompson equipment which is different. It's like putting a metric bolt into an American standard system. It doesn't work and it is a problem. We can go through example after example. NATO has a terrific problem. Americans in Korea have that problem. We have the same problem with the Japanese when we operate, and you can expect that problem almost everywhere. How do we solve the problem? Believe me, it is not easy.

How about communications and connectivity? We were talking about this at lunch. Every service buys equipment and not necessarily the same equipment. However, there's a move to do so, for obvious reasons — money, cheaper procurement, interoperability, and spare parts. We need to do that. For example, let's say the Army gets a lot of money and they make a decision to field some equipment. We don't in the Marines, and the Air Force may wait two years, and the Navy may wait three other years. Stop at a point in time and envision a force where they all are working together. The Marines are at 75 words per minute. The Navy's at 2400 words per minute on their processing machine. The Air Force is with the Marines at 75 on the ground, but 9600 in the air, and the Army has one unit at 75, because one came from Colorado and has old equipment, and the one from Fort Bragg has new equipment, 9600 words per minute. Believe me, this is not a far-fetched situation.

These are real-world problems, and to solve these problems you must be, once again, "in front of them." Equipment is fielded at different rates and at different times. That is a problem that we must understand in all the services, and when you talk about joint service operations, this is an extremely critical part of it. You just can't control a situation if you don't understand.

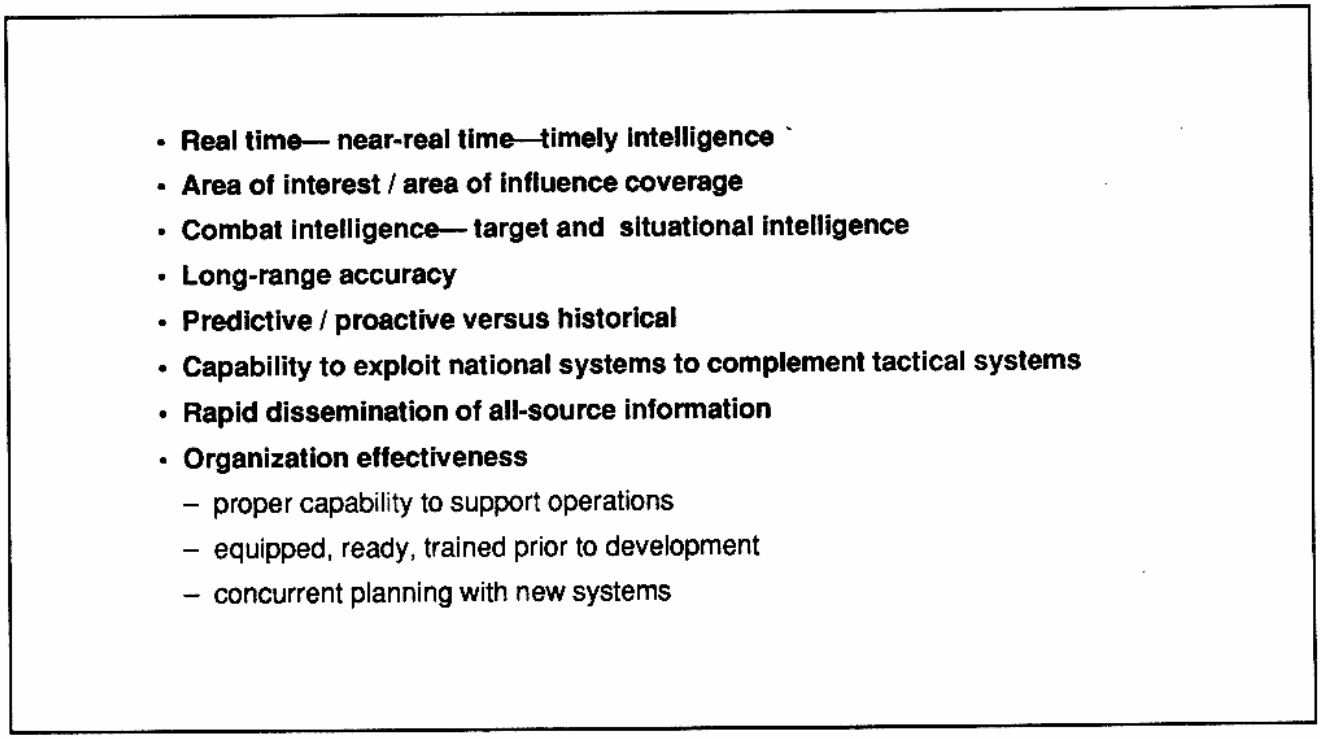

Figure 7. Intelligence Requirements

We Marines want mobile, rugged expeditionary equipment. The fielding of equipment is a problem, because not every service has the same needs. For example, the Marines must drag it through the surf and salt water. You know this beautiful ad where they show the truck driving through the surf? That truck can turn into a throwaway. Have you ever seen what salt water will do to the bearings on a tank or a truck? One of the things that it really doesn't show you is that after we make those big beautiful assaults, within 24 hours you'd better pull the wheels off those trucks and repack the joints. Have you ever seen what salt water can do to communications equipment? As you can see, in some circumstances the services are dissimilar, and in some we have the same requirements for equipment.

I don't know how much you've gotten into C^3CM — command, control, communications, and countermeasures, i.e., protecting our communications and destroying theirs. This is an art that's very important today. We must have good operations security and deny the enemy knowledge about our intentions. Tactical deception is important to deceive them about where we are and what we're up to. The C^4I^2 effort must be concerned about operations, communications, and computer security plus tactical deception.

Operations, intelligence, and the communications interface are absolutely vital, so when we plan an operation we really need three important advocates there. General George Patton said, "My two (intelligence) tells me what I should do. My four (logistics) tells me I can do it, and I tell my three (operations) what to do." It is applicable today. "My intel guys tell me what I should do, and my C^4 and my logistics guys tell me what I can do, and then I tell my operations officer what to do." It's changed somewhat, and that's because of the character of warfare and technology. Essentially, C^4 and intel have gained in importance and cannot be overlooked.

Ensuring that C^4I^2 is a force multiplier is an ongoing challenge. If I had to admit something to you, I would say intelligence can never be good enough. For example, just ask your stockbroker. He needs good intelligence plus computer power and communications.

Student: Could you please elaborate a little bit on antiterrorism warning?

Breth: There are two categories of terrorism: domestic and international terrorism. The FBI is responsible for domestic terrorism and they watch that like a hawk. The international intelligence effort falls under a different jurisdiction.

As a service intelligence chief, I primarily watch exterior to the United States to take care of our Navy and Marines to provide early warning. We're constantly assessing the situation. It takes fusion of data from police agencies and other intelligence agencies to integrate it and know what's going on. For example, you might want to ask, do I know where Lieutenant Colonel Higgins is? I can assure you today that a team of people is very hard at work on that. We know that if you are an American, and if you can avoid going to Athens, Greece, it would be a good idea at present. If you're thinking about going on a long tour in Turkey, I would pay attention. This is not the time to go to Kuwait and Saudi Arabia, unless you have a specific purpose. For example, the place with the most bombs and the most shooting, recently, is Peru. If you travel to Colombia, you know that you're going to be in an area that has a lot of narco-terrorism. There are a lot of influences that affect terrorism. This will not go away for a long time. To stay in front of this problem is a tough one.

Student: How does the average tourist find that out?

Breth: Do you voraciously read the newspaper?

Student: No.

Breth: You're making a mistake. You need to read world news and world happenings. That's the best intelligence you can get. Our media reports events faster than we sometimes do through the military intelligence command and control system. The media is another influence of C^4I. If you traveled to the White House today you would see one of their best news sources — you'd see a TV there. It's simple — you need all sources. I'm not so sure the veracity is going to be important, but you, as a civilian, need to be well read, especially if you're a world traveler. That is just prudent action.

Student: You say Turkey?

Breth: For example, if you have read the news — I don't have it here in front of me today — I can show you news articles on that country. If you take a look at the *Washington Post* every day, there's a second page that says "World News." You must read it on a consistent basis. One thing about intelligence is, you just don't get intelligence reports that focus — "There it is." The intelligence experts who know what they're doing watch things, and trends, and developments just like a broker in a stock brokerage firm watches prices of stocks going up and

down. To be alert for terrorism, to get ahead of the problem, or at least be aware of it, what you need to do is watch the news. It will appear there. Find somebody you know here who travels to the Middle East a lot. I guarantee you he or she is going to pay attention to the situation.

McLaughlin: Let me note that there is an account by Admiral Hilton a couple of years ago in the proceedings* about getting CNN (the Cable News Network) installed in a National Military Command Center so they would know what was happening.

Breth: It's true. They have their own satellites. They have their own communication paths and are very effective. They have investment out there in the world. They have the connectivity. You'll see live reports. It may not be accurate, but it may be close — and it may well be accurate. Our system will evaluate it, but at least you'll get early warning. This is not to say we don't have high-speed systems, but our systems are sometimes focused on different priorities. Our investment in where we do business is very important. We do different things than CNN, and we use CNN's products.

McLaughlin: Do other countries pay attention to terrorism?

Breth: Other countries pay attention to this pretty well, too. The Europeans really pay attention to the news across the world on terrorism. Different governments have different viewpoints on terrorism. Some don't care. Some care greatly. It's the U.S. State Department that works very heavily trying to engender that cooperation for us, and they've been very successful at it.

Recently, my Commandant gave me some mission orders. "I want you to combine reconnaissance, surveillance, remotely piloted vehicles, and selected intelligence functions into a larger consolidated reconnaissance and surveillance outfit. We've got to re-examine our tactical command and control, communications, and intelligence structure for changes that will make it more suitable for fluid maneuver on the battlefield, as well as more survivable in the face of new threat weapons and tactics." To that end, we set about and have fielded some new equipment.

The Commandant then said, "Breth, put C^4 and I^2 together in the Marine Corps. Remember, I told you: command, control, computers, communications, intelligence, and interoperability. You're responsible, General." Remember now, I just learned the intelligence business. Now I'm working with information systems that serve payrolls, planning, and tactical databases, and electronic warfare, and I'm not feeling very comfortable about this because I'm dealing with technology that is changing rapidly and I have to find out what's essential for the Marine Corps. I have to watch what the other services are doing. I have to see what OSD C^3I wants and I have to take a look at what Congress will allow us to do. I also need to take a look at how to spend our money wisely and field those systems, and do it as soon as I can. Then, when it's out there, I have to make sure our Marines are trained to use it. I also must make sure there are the maintenance and the spares to repair our systems. It's a real challenge to make sure that the products come out and are reliable, useful, and supported. C^4I^2 is a terrific challenge.

Oettinger: At the risk of belaboring the obvious, there's something I want to underscore here and also perhaps to plant some questions regarding some of the slides. What is remarkable about what General Breth has just said is that the scope of his responsibility as he's outlined it here, in any of the other services or at another Defense Department level, or with any of the other people we heard discussed here, is something that would be splattered across umpteen people in umpteen pieces of an organization. He's saying, "No, this is on my platter." So we have an opportunity which is unique in this semester and across our record of discussing balances and trade-offs among these things with one man in whose head these conflicts are going on unsullied by turf, budget, or whatever, because it's all his. I hope as we question him later, we'll take advantage of that sort of unique opportunity.

Breth: We need C^4I^2 global links. For example, a Marine in CONUS has to work with the Navy through the naval communications station up through the fleet SATCOM, then communicate directly with a CINC, and then link back up with an intelligence service via satellite. At the same time, our Marines may be collocated with a carrier battle group, or a surface action group for gunfire, and an amphibious task force. Our helicopters could be going ashore to rescue some people from an embassy. In a given theater of operations, JCS em-

*Rear Admiral Robert Hilton, "Roles of the Joint Chiefs of Staff in Crisis Management," in *Seminar on Command, Control, Communications and Intelligence: Guest Presentations, Spring 1985*. Program on Information Resources Policy, Harvard University, Cambridge, MA: February 1986.

ploys the JTF commander, an Air Force airplane, and an Army commander. That's the real world.

Now, how about connectivity and interoperability and the intelligence flow along with command and control matters? What do you really need? What is essential? As you recall, we must assess the battlefield quickly and accurately in the air and the deep search. It must be done on-line. You've got to integrate the automated data systems with communications, because it's changed from when you used to just pick up the phone and say, "Hey, Joe, switch up on different frequencies." Digital information flow is tremendous. If you don't have the same system, all you get is a funny sound in your ear. For example, the Army's developed a massive system for fire support. So have we in the Marines. Because we realized this, we're back at it again to integrate and to get interoperable. A naval example is that the Navy carrier battle group can interface at the same data rate with an amphibious task force, hopefully with a surface action group, and unless the ships that deploy are outfitted properly before they deploy it won't work. In other words, these are disparities that can happen if you don't pay attention early on and prepare for connectivity and interoperability.

There is more of an effort to get at this than I've ever seen before, and that's because everybody sees this crushing problem in front of us. I'm sure that you've heard Jerry Tuttle tell you that, and I'm sure you've heard many others relate similar stories. It's what we can do in the near term with a limited amount of money, and what we had better do over the long term. It's very important because we are investing in tomorrow.

From an operator's point of view, what are some of the problems with C^4I^2? One, the avalanche of superfluous information which paralyzes the headquarters. That can absolutely happen. It's not uncommon to be operating as a joint task force somewhere, and receive reports that are what the President desires, the SecDef wants, the JCS can use, the CINC might want, the fleet commander might want, and that you don't need!

For example, the Marine on the line in Panama wants to know what's 300 meters in front of him. He doesn't want to know when President Noriega will get a bank loan from Spain. How do you build filters? That's part of this C^4I^2 problem.

Another typical problem, because of the technology today, is excessive reporting requirements at all echelons. I can give you example after example of questions by superiors asking, "What's going on? Give me a situation report." The guy's busy fighting a war and he is supposed to disengage and sit down and write reports. Every service has this problem.

I can tell you as a company commander in Vietnam when we had an engagement, I had a good Marine next to me write radio reports. One of those reports that we tracked, for example, got back to the White House within 45 minutes. You say, "Why?" That was because President Johnson had a son-in-law who was a Marine and he was in the area. So he wanted to know a lot of extraneous information. My question — who used it? Was it necessary?

Vulnerability to enemy signal intelligence and electronic warfare is a fact of life. We need mobile, modular command posts (CPs). The enemy has a targeting capability to pick up your signature and launch a weapon system at you and you'd better move.

The C^3 countermeasures business is really getting important. We need to protect our C^3I systems, and as the enemy works against us we need to make sure those systems degrade very slowly and are robust. Yet, at the same time, we need to be able to counter enemy C^3I systems, including targeting — we need to deny him; we need to deceive him; we need to degrade him, maybe by jamming; or we need to destroy him. This is a particular part of warfare.

I guess the bottom line is, does your system work better than the enemy's? Frank Snyder and I were talking about the decision cycle through the process of operations. The requirement is to speed that up: to evaluate, decide, and act before the enemy does.

Oettinger: You don't see that very often, and I like it. More often you see a perfectionist view — you've got to know everything. This is a very modest but very important statement. It is a comparative one. It talks about an inch, not about perfection, and I would say that most of what you read in the literature, in a lot of those tech things, has that perfectionist image. This objective may even be attainable, and it's very unusual in that ocean of perfectionist nonsense.

Breth: This is my goal: to make sure that can happen. I'm not there yet, but I'm having some success, and in some places I'm not. Another fact of life is that the Air Force doesn't do it alone, the Navy doesn't do it alone, and neither do the Army or the Marines. We, in the services, really have to work together. The same is applicable to our National Command Authority, to our intelligence

agencies, to our State Department, and to our national fabric. The integration of effort is more important than ever before if we are to be successful.

In closing, I must pay attention to the Marine Corps C^4I^2, because we know we're probably going to be in low intensity conflict. We're going to be forward deployed and we won't have much time to get ready, and we must have good intelligence and connectivity to do what we're told to do. If we don't get in front of the problem now, we will be at risk when we have to go.

That completes my long brief. Let's discuss some C^4I^2 topics of interest to you.

Student: I want to ask a question about countermeasures and operational security on some of these issues. When the U.S. military is planning an operation overseas, or maybe just planning a rehearsal of an operation — the rehearsal to take place in the United States — and they don't want the media to find out, do these people come to you or your opposite numbers in the other services and ask what the intelligence people on the other side are likely to be looking for? If you were the Soviet intelligence people, how would you find out about this? What security measures do we need to take, or is there not much of a connection?

Breth: A good, but a very sophisticated question. We know what we need to do, and if we were going to work against them we can assume that they would do other things. Our access to what they do is in some cases very, very good. So, we know what they're doing, and that gives us clear objectives to work around. Let me give you an example. One of the greatest initiatives that General Bill Odom, who heads the National Security Agency, has taken is in the area of communications security. His people, through their research and development, have been able to field a device called the STU-III (secure telephone unit) telephone. It looks like an AT&T telephone, and it has crypto in it that allows the keys to be changed every day, so that when you make a normal telephone call it's inexpensive and you're secure. In other words, the enemy with its capability cannot break that code. It allows you to talk and maintain security. In sum, we operate effectively if we deny the enemy any forewarning and we practice that often.

Our adversaries watch for capability and they watch for intention. The earlier they can discern our capability and our intentions, the more success they will have, and the more disastrous our results will be. Every military force goes through that process.

The Soviets, who have a closed society, have a great advantage because they're very controlled. We have an open society that has media and the press is everywhere. I'm not criticizing it, I'm just saying you must understand the nature of the United States. When a ship is at sea, or when an airplane's in the air, not a whole lot of Americans are seeing it and reporters don't report. There's an advantage there for us. We must pay attention to operations security and deception. As you might expect, we have plans and we exercise that. Is it good enough? My personal opinion is, "No," because it can never be good enough. We need to work at it more than ever before because the technology and the capabilities of today tell us that we must, now more than ever before.

Oettinger: You may have noticed in the last couple of weeks an article in the *Sunday Times* about NSA and its attempts to sell STU-III and other technology to the private sector, and it is meeting terrible skepticism. In light of the discussion of the importance of economic intelligence, the dimensions of what General Breth is talking about are not limited to inside the Marine Corps, but include the financial and business communities as well. You're talking about major problems.

Breth: When you want information security with computers and you want to embed it, it's a very expensive process and the technology is moving in that regard too. Communications security, information security, and operational security and deception go hand in hand. You cannot leave out a piece or you'll pay.

Oettinger: Forgive me for jumping in, but this is not run of the mill any more than what Rae Huffstutler said way back.* There's a certain amount of heresy in it. I doubt if General Breth is very popular in his own organization or elsewhere, where ecumenical notions are not widely accepted.

Breth: I guess you're right. I'm the guy who must tell a commander, "I think you're making a great mistake." That's my lot in life as the C^4I^2 Director, and commanders don't like it because it's painful sometimes. It's painful to take anti-terrorism measures. It's painful to inspect after hours. It's painful to make sure you have communications devices. It's painful to buy more expensive equipment. It's painful to enforce standards. But you either do it right, or you don't do it right. Sure, it is easier to decree a band-aid for something than a complete fix.

---

*See Mr. Huffstutler's presentation earlier in this volume.

Remember now, I deal with some people in this community who are just great Americans and they do care. The intelligence officer's lot in life is to be a person of integrity and to tell it like it is, or he shouldn't be in the business. But there's a price to pay. It's sort of like bad news does not improve with age. It's a fascinating challenge. This C^4I^2 business is terribly complex, and technology is exploding, and it's hard for anyone to watch what is happening with the research and development. It's difficult to watch what's happening in industry, and it's hard to watch what's happening in the other services, and to stake a position and say, "Let's do this." It is a dynamic and ever-changing environment.

McLaughlin: The last time the Marine Corps deployed forces — in Grenada — I know there are certain constraints, but there was a lot of post-operational critiquing about intelligence for the operation; command, control, and communications. Can you comment on any of that?

Breth: Yes, I can; however, I'm not going to do a postmortem. I was not there, but there are some basic facts that are reported. I don't know if you're well briefed on it, but you know the old joint service commercial, Army, Navy, Air Force, Marines, at halftime at football games? That's who went down there, as well as the special forces who were there early. So you actually had five. What you really had was a sea-based operation augmented by an airborne operation. The Navy-Marine expeditionary unit on board the amphibious ready group and a carrier were on their way to the Mediterranean. There was good operational security. It diverted and went somewhere else — down to Grenada. The decision was made to make that a joint service operation. That unit had already been at sea with all of its plans to go to Beirut. The contingency package and their orders went to that ship for those Marines out in the carrier.

It was also decided to divide the island in half. The Air Force was going to support the Army in an airborne operation where they took the troops out of the airborne corps, and they, in fact, did drop at the same time the Marines conducted an amphibious operation on the other part of the island. What really happened is that it was short notice, compartmented to provide the operational security, which means only certain people knew about it, and when they executed, the robustness of the communications, and the communications paths, were different and resulted in some interoperability problems.

"Why did the soldier have to use his AT&T card in the telephone to call back to Fort Bragg to get air support for his unit?" Once again, the telephone's a wonderful instrument, but it didn't work in this case. Normally at sea you have a certain type of communications, as you well know. There's high frequency, very high frequency, ultra high frequency, and different comm paths that you can use, and you can use teletype, or you can use digital streams, or you can use voice. It can either be secure or unsecure. It depends also on what type of encryption you use.

As a result, you had several different forces than you normally have. The Air Force and Army normally work very closely together. The Navy and the Marine Corps work very closely together. And you'll hear, for example, about the air-land battle strategy between the Air Force and the Army. In the Marine Corps and the Navy, you'll hear about the maritime strategy. We're on a sea-based platform. The interoperability of that communications equipment and the apportionment of the satellite channels and many of those things were very constrained and the interoperability problem was there.

In spite of all those problems, the operation was very successful. Could it have been better? Probably. It gets into the planning for the operation of C^4I^2 for proper intelligence, proper connectivity, and proper interoperability. We do joint exercises all the time, but the task organization was different. The operators who made the decision knew that before they executed it to protect the operational security of that command.

Were there failures? Probably, and some judgments came out of that. But I think that one of the things that came out was that we learned several lessons again. They're not new lessons: if you plan properly and train properly you can execute properly. It was a lesson that we really must pay attention to, but I think it gave an advantage to OSD, C^3I, and Congress to ensure standards are met in the future when we field systems for interoperability. I think that was a clear outcome.

There were some fragile links in that operation, but yet many positive points. A lot of people, in spite of those problems, used great initiative and solved a lot of problems, and that must be stated. Sometimes you can think things are absolutely horrible, and you will find that people who have great knowledge and great initiative will solve lots of problems that you'll never see. I'm convinced that happened down there, because I've talked to Army, and Air Force, and Navy people as well as Marines.

Student: I'm interested in your organizational merger, specifically the C^4I^2 merger. Even though your tasking came from the Commandant, and obviously you're going to get a lot of support when you have that level of direction within the Marine Corps, in our earlier discussion you mentioned that there was some resistance to the merging of the functions. Where did that resistance come from and in what form? That's question number one. Question number two is, is the merger of C^3 and I filtering down to other organizational levels within the Marines? And I guess my third question deals with interoperability. In your one chart (figure 8) you had a realistic and pretty complex scenario depicted, showing potential involvement of all four services simultaneously in a pretty elaborate set of circumstances. From a systems management perspective, which I'm sure you guys are heavily involved in, has the merger of C^3I or C^4I^2 in the Marine Corps really helped you that much in working system interoperability problems in light of the fact that the other services have not taken the same measures? In other words, are the folks with whom your people have to deal with on interoperability issues still kind of messed up? Within the Air Force C^3I is spread out.

Breth: I would like to tell you that, in the spirit of the Marine Corps, the Marines have solved the problem and everything is wonderful, but I can't yet. It's a tough problem that will remain. The question I think you properly asked is, "How do you get at it?" What works and what doesn't, and how are we approaching it?

Let me get to the first question. Was there resistance? The C^4I^2 merger that I handled in the department essentially came from two divisions at Headquarters, Marine Corps. Headquarters, Marine Corps is not a warfighting organization; its responsibility is to train and equip the forces in peacetime, to chop those forces, or to turn them over to a warfighting CINC. So my job then, in the C^4I arena, is to make sure that the forces are trained and equipped properly.

The Commandant formed two other organizations I need to talk about. One of them works at long-range requirements. What is the enemy doing? What are our long-range requirements? What are our mid-range requirements — say, five years out? What are our requirements for a warfighting structure in C^4I? Then they pass them to this other organization which does the research and development and the service procurement of those items. I have the oversight responsibility for C^4I in that linkage. There's a triad.

The staff is similar to that of a commercial organization, just as there's a sales department or production department, there's an accounting department, and there's an information systems department. In the military staff, normally, traditionally, the G-1 is personnel, the G-2 is intelligence, the G-3 is operations, the G-4 is logistics, and the G-6 is the communications, electronic information systems guy. So really what the Commandant did was to put the C^4 and intel together. Yes, there was resistance. First of all, the intelligence community said, "What is C^4I? It means that you're not the service intelligence guy and you're now paying attention to C^4I and C^4 matters and intelligence is no longer important. If you're dedicating your time to C^4 you cannot be dedicating it to intelligence." The C^4 guy said, "If you're working for intelligence, you're going to be dedicating all your time to intelligence; you certainly won't be paying attention to command, control, computers, and interoperability." At the executive levels they said, "What is C^4I^2?" In fact there was resistance, and it went from top to bottom, and across functional lines.

Let me tell you how we approached it. First of all, in command, control, communications, and computers those guys do a lot of specialized things. And so do the intelligence guys — the HUMINT guys, and the imagery guys, and you say, "Why put them in the same room?" There is a dysfunctional relationship here, and yet there is a place where they need to come together. What we've done is, we've taken those branches and we've stripped out of them what we thought had a common base, and we built a central focal point. I call it the C^4I^2 ops branch. It's composed of information systems, communications, and intelligence, and they work C^4I^2 issues that need to be closely coordinated. They work the interoperability issues and then they go out and work with the intelligence and the C^4 divisions.

We have found that there's a tremendous amount of excitement. The first thing we found was, "Hey, you do care. You're not so bad. I really like you. Yeah, that is a problem, and I've been trying to figure out how to work that for a long time." The first thing that happens is you start communicating. I wouldn't say they were armed camps, but you had two camps with no communications paths. You're talking about Ford and Mercedes. They're really different, but when you put them together there's a lot of commonality. We have made progress when

we have a staff action and the guy says, "Hey, what's the impact on intelligence?" For the first time we're articulating requirements to the communicators, and the communicators are taking a look at intelligence. For example, we might have a data system that the intelligence folks use, when all of a sudden, because of technology, the C^4I people know a lot more about this. We're finding that we're not buying separate sets of equipment; we're putting it together. That's starting to work and we are having an impact.

The commanders were able to go to our commanders and say, "This is what's important to you in communications, dissemination, intelligence, and processing." So our service to the field is having a great response. Our people are learning that other people are really great pros and we should have been talking a long time ago. At least we have control over the interoperability to get at the tough issues and I believe we are winning.

We've had some success with our systems. For example, we could take a bar chart up here, with time going across, and we could list every system and when we're trying to field it. We could list communications systems, information processing systems, intelligence, and we could take a look at when we're trying to field those, and then ask, "Are they interoperable?" Before anybody fields the system, he's got to go through our matrix. So I, in fact, have control. Can I make it work? Can I control it? Time will tell.

We're not there yet and we're still dealing with resistance, but it is much less. The interoperability issue is what we're after. I believe an austere budget is going to force that, more so than ever before. You cannot go the sole source, service way to do things. You will not get away with it. I'm sure that Jerry Tuttle, and if you have somebody over from the Congress, will tell you the same thing. We want that to happen. If it doesn't we're in trouble.

We're on our way, but I will tell you honestly that figuring out how to do this and how to get at this problem in an organizational structure is my greatest challenge. As I leave, how do I grow my replacement, so that he won't have to go through the same things I did? Otherwise there will be no continuity. Yes, there is a challenge.

Student: I have a question going back to the *Mayaguez* incident. One of the criticisms that has come out of that incident was that there was apparently an attempt to connect the commander on the scene all the way back to Washington. Could you talk a little bit about that? I was wondering if you were familiar with that setup and whether you had any comments to make about that — the mistakes they made there and the lessons that were learned.

Breth: First of all, I was not there. I've studied it a lot and I had many friends there. Yes, that did happen. And the patch between the A-7 pilot and the President was in effect on UHF. The command authority has that privilege and it can be exercised, and I'm sure in the future it may be exercised again sometime.

The more you operate together the more you understand each other. That's why I think the intent of the DOD Reorganization Act is to make us operate together so problems like that don't occur. That is coming along very well.

Snyder: I might inject that what you heard underscores the fact that the Marine Corps is really a walking interoperability machine. We've used the Marine Corps in a variety of ways. The Navy and the Air Force operate one kind of radio and the Army operates the other, and the Marine Corps always carries the two sets. Unfortunately, with the *Mayaguez*, the helicopter lost one of their sets. As a result of that, we invented a new radio, but the Marine Corps, for reasons you've heard, pick and choose. They always do it at sort of the least common denominator level and provide a lot of interoperability for all the services. If you want to talk to the Army, you essentially figure out how to do it with the Marine Corps. They're the leaders.

Breth: Let me give you an example. In our expeditionary plans to go to Norway with carrier aircraft, the E-3A, and also the F-16s that go up there, we know that we have the only connectivity that talks to everybody. We're trying to solve that problem to get everybody together, although we hope that everyone would not rely on us for that. We've done pretty well with that over the years.

I'm not here to tell you that the Marines always do things right, but we sure try to. Our greatest challenge is to watch what everybody else is doing. We're small, we make prudent decisions. But you've got to know your business if you're going to be a good account executive. You've got to know your business if you're going to be a corporate executive. You'd better know your business if you're going to put your life and those of others on the line.

Oettinger: It's interesting to look back a few years in the proceedings of this seminar. I think you'll find an account of General Cushman's visit to the Army installation at Fort Leavenworth and his expression of amazement and delight at finding some

company-level folk who had gone out to Radio Shack and bootlegged themselves together some electronic system of the kind General Breth is describing. The problem was to keep this initiative from getting squashed, and to let it develop further. There's a kind of a milestone here in terms of what you're describing and that's becoming the norm, at least in the Marine Corps, rather than the exception. You see the organization adapting itself in part to the kind of people that can manage the technology. You are a different breed.

Snyder: I didn't hear the answer to one aspect of the earlier question: that is, whether you foresee, in operational units, the merger of tactical J-2 and J-6, the intel and the communicator? As you point out properly, the Commandant's headquarters is a different kettle of fish. Do you see the utility of it working down at the unit level of operations?

Breth: Not as a C^4I^2 function, because that's a drastic change. But I believe we're seeing a closer coordination of requirements, and at the command post, the command center, where the command and control is done, intelligence is integrated better and needs to be integrated better with communications, which is going to force that to happen. I showed the slide of an old truck with its maps and those guys putting them up; you can't do that anymore. The requirement to put that information together is causing that to happen no matter what you call it: surveillance, reconnaissance, intelligence center integrated with operational fire support control, to make targeting a very important position.

For example, what should I strike now? What needs to be done? The commander may be off inspecting a unit. You need maybe a young captain or a master sergeant saying, "Sir, the intelligence shows this." You cannot do things like that unless you have intelligence and communications integrated. If you don't, the character of decision-making will slow down and you will fall out of your decision loop, and your C^4I^2 effectiveness will not be as good as you want it to be.

Student: Does the Army really have integrated C^3I, or more C^3 and less I? That's the tendency. At OSD, there's a C^3I authority, but he's really the C^3 czar.

Breth: They have an architecture that shows maneuver control, fire support control, intelligence, electronic warfare, and there's one other; it used to be logistics. It's sort of a triad when it's all connected together. So the question is, yes, it's big and they've got a discipline matrix on how to approach it. Their requirements are much more detailed and manifest than ours, and yet, at the same time, they must be able to work with the Air Force. I think that's a link about which I asked, "What are you doing?" Because as a Marine I'm interested in how we, on our ground, can integrate with our air. That means lessons learned.

Oettinger: I get worried a little bit about the pendulum going too far. I push integration and the fact that computers and communications and all this information stuff can't be pulled apart, etc., etc. When all is said and done, the scope of what is defined by what we call information resources is so vast that even if there were no such things in the civilian world as antitrust laws, or in the military world as separate services or pieces of the services, the world is too big to pull it all into one ball of wax. There have to be pieces, and the question is, how do we work the pieces? What I hear here is that in a smaller, leaner organization you have a tendency to put a lot more things together. I think that's a general Marine Corps tendency, because they've got fewer officers and smaller staffs, so people tend to have broader responsibilities, not only in this area. It seems one is looking at a Marine Corps characteristic necessary in a lot of areas as it translates itself into this particular area. Is that accurate?

Breth: I think that's an accurate assessment. It really is. We think we can get away with it. There's probably a better way to say it. We're having a tough time, too, but we look at others who are doing it well. We look at our brothers in the Navy and also the Air Force and the Army, how they're approaching it, and there are some good methodologies and there is fine work being done by everybody. It's a tough problem.

Snyder: The Navy's tried it twice, in my estimation: once down at NAV and once in Europe. It only lasted a few months. It boggled the minds of the new people, and they saw it wasn't an effective proposal.

Student: The other day I read an article, I believe it was in the *New York Times*, which was saying that the technologies that the military uses today are often very far behind similar technologies in the private sector. They gave one example about some branch of the military that had just procured certain IBM computers that were no longer sold or supported in the private sector at all; they were dinosaurs. Do you observe this difficulty with your

people and the people in other services? And how do you deal with it?

Breth: That can happen. That's because you're dealing with a large organization — or organizations — that have procurement at various levels and maybe have different requirements.

Clearly, there are government constraints on procurement. Sometimes procurement decisions are made that seem to be absolute folly. The system is trying to do away with that, and that's a challenge to the procurement system and all the people involved. In many areas we're ahead, especially in research and development for the armed forces. More than often, the investment has been transferred into the civilian sector. I think that's one of the by-products we see of SDI. I'm not here advertising SDI, but I see that as a by-product perhaps. Without a doubt there are clear benefits to our country from the R&D investment of SDI.

Oettinger: Thank you so much for a wonderful talk.