Chief of Staff Address

FUNDAMENTALS OF INFORMATION WARFARE--AN AIRMAN'S VIEW

NSIA-NDU Conference on
The Global Information Explosion

General Ronald R. Fogleman
United States Air Force

16 May 1995

General Ronald R. Fogleman

Chief of Staff, United States Air Force

Fundamentals of Information Warfare--An Airman's View

It's a great pleasure for me to address this particular audience. The information technology explosion that's out there sweeping the world is an important matter, not just for the military services, but also for industry, the government, and our whole way of life.

I've been looking forward to this opportunity to share with you what the Air Force is doing to capture the potential of new information realities. I will tell you right up front that I see information warfare as having both an ascending and transcending role in military operations. To understand why I say this, I will draw a little bit upon my academic background.

As I look at the history of the Second World War, I think it offers great examples of the military and civilian leadership manipulating information, even in a very crude fashion, to achieve rather spectacular results. In those days, as we thought about dominating the information spectrum, we turned to the cryptographers who were on the leading edge of these efforts, the so-called "code breakers." These specialized folks focused intently upon breaking the Japanese and German codes. In Europe, the ULTRA project -- "ULTRA" for the "ULTRA secret" -- produced

As delivered at the NSIA-NDU Conference on The Global Information Explosion, Washington, D.C., 16 May 95

spectacular results. Our code breakers literally worked miracles.

You may recall how after the Normandy invasion, the German 7th Army attempted a counterattack to drive the Allied forces from the rather tenuous beachhead that they held. But, with the help of ULTRA's ability to read the German mail and message traffic, we knew precisely what they were doing as they began to gather their forces to make this attack. So, we were able to put the British Second Tactical Air Force and the United States Ninth Tactical Air Force immediately upon these armor formations just as they massed. ULTRA gave us the critical information that allowed us to defeat the German forces before they ever came in contact with our ground forces.

Now, by comparison, if you think to December of 1944 and the Battle of the Bulge, we see an example of where the Germans were able to catch us by surprise. They used an alternative communications network and the Allies did not realize that the Germans had made this switch. It was our lack of information that really fueled the initial German success in the Battle of the Bulge. We had come to rely on ULTRA, and had developed a little bit of self-delusion -- and the Germans took advantage of it very effectively.

So, our ability to monitor the enemy's communications and use that information as an integral part of our operations is really nothing new. But, there's another example we shouldn't forget. That's how we control the information that we allow the enemy to receive. Again, I'm going back to the Second World War and talking about <u>dis</u>information, particularly

the disinformation campaign that centered on General Patton before and during the D-Day landings.

At that time, the Allies understood the other guy's ability to intercept our open signals, so we devised a rather elaborate plan that played to this emerging capability on the part of the Germans. The allies set up a fake Army headquarters and generated false communications transmissions in England. As a result, the Nazis ended up with a significant number of troops placed in the wrong positions. Even as they started to pick up indications that there was this great allied armada that was going to invade Normandy, the Germans refused to believe that there could actually be an Allied invasion of Europe led by anyone but Patton. So, we played on that expectation in a way that kept Patton associated with his fake headquarters. Even as the Germans began to get higher and higher fidelity intelligence that indicated a real attack at Normandy, their leaders were frozen in indecision and as a result tied down considerable forces in France across from the shortest invasion route from England.

Now, I think from time to time, we tend to forget about these early successes. But, with an audience like this, I'm sure you understand fully the significance of such efforts during the Second World War. And, you can begin to extrapolate and see the potential for similar operations in today's environment where we've become more and more reliant on information and the info-sphere environment.

As I reflect back on these activities, I begin to realize the tremendous advances that have come about with microchips, fiber-optics, space, and information storage over the past five decades. And I'm convinced that a tremendous potential exists in this area for a major breakthrough in the

conduct of war. In fact, as I stand back and look at the weapon systems we have today, and I try to project forward the evolution of weapons and technology into the next five to 15 years, I will tell you that I cannot see where there will be tremendous advances in the types of weapon systems we are fielding today.

For instance, the aircraft we will fly over this time frame are fundamentally the same kinds of aircraft we are flying today. Some will have more advanced avionics, more advanced stealth characteristics, or other features; but in the main, aircraft will remain fundamentally aircraft as we know them today. Ships will remain fundamentally ships as we know them today. The same holds true for tanks and armored personnel carriers.

There are two closely coupled areas where I do see tremendous potential for breakthrough: the ability to exploit and exchange information, and the ability to detect, fix, and target objectives on a battlefield. Because fundamentally, it will be information and the capability to move it around that will change the internal characteristics of ships, aircraft, battle tanks, and armored personnel carriers we operate on and over the battlefield. So, it's upon this foundation that the services, and the Air Force in particular, approach this emerging area of information warfare.

I think that a useful place to start is to define what I mean by information warfare, particularly since I think there is a risk in perceiving all warfare in the information age as "information warfare." In my view, I can tell you that's not the case. So, I would like to offer a definition that

focuses on the military fundamentals of information warfare, or what I've called the fifth dimension of warfare.

There are three key parts to this definition. First, information warfare (IW) includes those actions we take to gain and to exploit information on the enemy. Second, IW includes what we do to deny, to corrupt, or to destroy our adversary's information data bases. Third, how we protect our systems must also be included as part of IW. No matter how you define information warfare, we must think of it in terms of how it enhances joint warfighting. If it doesn't do so, then I'm not much interested in it, and neither are the other service chiefs. I believe that this is an important point.

I will tell you that information warfare is not the exclusive domain of the Air Force, or any other service. I think that information warfare has different meanings to a soldier, sailor, marine, or airman. For instance, the soldier's focus may be on what happens at the corps level and below. The sailor's and marine's focus is on the maritime and littoral regions. At the same time, an airman's focus is theater-wide, from the front lines to the adversary's capitol. So, you begin to see, how IW covers the entire battlefield. But, because of these divergent views and unique needs, I think it's critical that all services come to grips with and develop capabilities for their respective mediums of operations -- that is land, sea, and air. Then, it falls to the joint force commander, or the regional commander-in-chief, to integrate these capabilities to accomplish his mission.

Now, the Air Force has put considerable effort into developing our concepts. In fact, over the past four months, we've had a team travel to

every commander-in-chief (CINC) of a US unified command, and brief them on our efforts to incorporate IW into our doctrine and to integrate these concepts into our force employment. Most importantly, we want to be sure that what we are doing and how we approach the subject as an institution will be consistent with the way the CINCs intend to fight. And we want to make sure that what we are doing will meet their needs.

So, let me spend the rest of my time today focusing on what it is that we've shared with the CINCs in terms of what we are doing to leverage information technology, and then turn to how we view the offensive and defensive elements of information warfare.

As a practitioner of the profession of arms, I view information technology advances with a single-minded interest. I am motivated by the fact that throughout history, soldiers, sailors, marines, and airmen have learned one extremely valuable lesson relative to engagement with an opposing force. That is, simply put, if you can analyze, act, and assess faster than your opponent -- you will win!

I think the information explosion discussed here today is going to make dramatic changes in how this nation fights wars in the future. Such technology will allow a commander's vision and view of the battlefield to be shared at the lowest level -- to the flight for the airman, to the company on the ground, and to the ship's bridge. Simultaneously, soldiers, marines, sailors, and airmen on the front lines will be able to see and exploit opportunities as they occur.

What this means is our joint forces may enjoy what some are calling "dominant battlefield awareness." Now, we have some of this kind of

capability today. We've made significant enhancements to our ability to leverage our forces with faster command and control, and intelligence networks. Among other capabilities, these networks are dramatically reducing the time required to detect and destroy a target.

This process starts with how we gather data. Our intelligence, surveillance, and reconnaissance efforts have been significantly and dramatically improved since Desert Storm. If you are familiar with our TALON programs, you will appreciate what we're doing to reduce the sensor-to-shooter loop -- that is injecting what's detected by our space-based assets directly into the cockpit or a flight deck. We're making similar advances with the systems that operate within the earth's atmosphere. For example, our AWACS early warning aircraft have been greatly improved. Their current radar upgrade allows us to detect cruise missiles at twice the range that we could previously. The AWACS is being fitted with the Joint Tactical Information Distribution Systems, or JTIDS. We'll start the initial JTIDS operational test this August. And, I expect that we will reach full operational capability before the end of the decade.

Now, JTIDS alone is going to give us some pretty significant capabilities. It's not restricted just to AWACS. It also gives our warfighters a secure and jam-resistant data link between Air Force, Navy, Army, Marine units, and future coalition partners -- on land, at sea, and in the air. What that really means is all the players will have a real-time picture and awareness of both what's happening on the ground and what's going on in the air above those forces. JTIDS will give us a tremendous capability to know, at a much higher fidelity, the location of both the enemy and our own forces.

Now, we're also making similar improvements in how we plan and control air operations. Today, we're fielding CTAPS -- the Contingency Theater Automated Planning System. CTAPS will connect our command and control from the joint forces air component commander (JFACC) to the air wings and the base-level planning cells. It will allow us to generate, disseminate, and monitor the progress of the daily air tasking order much faster than we ever have been able to do before. CTAPS will also tie-in with the Combat Intelligence System which will provide us the enemy's order of battle through imagery and integrated threat data.

What does this really mean to us? During Desert Storm, it took us about 48 hours to plan and disseminate the ATO. That doesn't mean that it took 48 hours to execute a request from the field. But, it means that the deliberative process that planners went through to service targets was a 36 to 48 hour process. And you had to have someone manually intervene with an immediate air request to get inside those planning cycles. But, what the CTAPS system will do for us is take this 48-hour cycle, and compress it to 12 hours. I have to tell you, that is pretty good. And, this really isn't some pie-in-the-sky system that we're dreaming about or visualizing. This is something that is in full use in exercises, today, and will be operational across the force next year. We have a similar planning tool that has been operational with our global air mobility forces for about three years.

So, these are a couple of examples of the kinds of tools we're putting in place. They are going to do more than replace the grease pencil and butcher block paper that (General) **Chuck Horner and his staff had to use to run the air war during Desert Storm. These systems are going to help us**

dominate the information spectrum. And, I am convinced that this capability will be critical the next time our forces are employed in combat.

Now, if you recall, I described information warfare in terms of how we deny, corrupt, or destroy our adversary's information base while we protect our own. I've got to tell you that a lot of this activity has a very offensive element to it. And I think we've been doing this for some time, but perhaps we didn't use that kind of term. For example, during Desert Storm, we targeted many of the Iraqi communications nodes and physically destroyed Saddam Hussein's ability to talk to his troops through normal channels. We forced him into sub-optimum modes of communicating.

In the future, we will approach this objective by viewing our adversary's information activities as a system, and we will engage that system in a variety of ways. In fact, rather than put a precision guided munition into the central telephone exchange in Baghdad and destroy it next time, we may elect to leave it standing so we can better exploit it through our advances in information warfare. So, there will be trade-offs between lethal and non-lethal dimensions in the IW arena.

In the same manner, we've been doing some things along the way that we could properly classify as offensive information operations. There are ways that we corrupt information available to the enemy to deceive him. They include using psychological operations and our electronic warfare assets, like the Compass Call aircraft. I think that these kinds of measures that are designed to corrupt information the enemy has are really critical tools that we provide to the CINCs today. And, they open the envelope for the potential of further operations tomorrow. Again, if

you think back to what we did on D-Day with disinformation, and you consider the tremendous advances in technology since 1944, you begin to appreciate the tremendous potential that exists in this area.

Now, if we recognize an adversary's information network as a lucrative target, I will tell you that an adversary will view our data banks and weapon systems the same way. So, I think that information security -- the classic OPSEC, COMSEC, and more recently stressed computer security -- takes on a whole new level of urgency. As a result, the Air Force is taking some rather significant measures to safeguard our assets. This year, we're spending over $80 million on defensive measures alone. Now, this includes establishing a base network control center to protect access to computers and communications. This same center will permit us to see if someone has tried to gain access to our system, and hopefully will allow us to track down who tried to intrude on the system. These initiatives are important because we run a tremendous risk if we look at information warfare as something that is unique to America. It is not, and by the same token, the US military is not alone in this vulnerability.

Our commercial sector, other elements of the government, and our industrial sectors rely on information systems just as much, if not more, than the military. If you've read Tom Clancy's recent thriller, Debt of Honor, you're familiar with what may be plausible. In this fictional tale, Clancy describes the problems caused when someone infects the Stock Exchange's computers with a virus; literally bringing the stock market to a standstill. To me, Clancy's work reinforces how the information threat is more than just a unique military concern.

As I look at information warfare and how it relates to the services, I'm reminded of a story about a football team. It seems that during one of the games, the local team had to put in a back-up quarterback late in the fourth quarter. They were ahead, and they were just trying to hang on. So, they put this relatively untested young man into the game, and all he had to do was avoid making a mistake and the team would win. So, the coach grabbed the guy as he was about to go on the field, and said, "OK, here's what I want you to do. Run the ball three times, and then punt. So, the kid understood that and goes out onto the field.

Well, his first run gains 20 yards -- great. On the second play, he gains 30 yards. Now, this is going a lot better than he ever expected. And on the third play, he gains 30 more yards. Now, they are down on the 10 yard line, the fans are going crazy, and it appears they're going to wrap this thing up. All he has to do is score, and he'll seal the victory for sure. So, the center snaps the ball to him and he punts. Everyone is stunned by this. His coach pulls him over to the sidelines and asks him what he was thinking. And the quarterback replied, "I was thinking that since you didn't change that play, I must have the dumbest coach around."

So, it's not enough to make a gameplan and go with it. You've got to act and react to what's happening around you. So, I think that what we're doing today with information warfare is a little bit like that football game. IW gives us the ability to plan faster with better information, so that we can call the optimum play. It may allow us to know what defensive stunt the other team is going to use. It may allow us to give our opponent false information on what play we're about to use. And, most importantly, it may allow us to call an audible and adjust to a fluid situation.

But unlike the game that I just described, when America sends her military forces into action, we don't want a close, exciting game and we don't want an inexperienced quarterback. This nation has come to expect in our military operations nothing but blow-outs -- 100 to nothing is a good score. And, I believe that exploiting this new and emerging information technology is going to be the key to making this happen.

So, as we approach tomorrow, we need to do more as a service and with the other services. Let me touch just briefly on what we're doing in terms of how we're changing the way we organize, train, and equip our forces.

First, in terms of organizing, in September of 1993, the United States Air Force stood up the Air Force Information Warfare Center in San Antonio, Texas. Now, this center has over 1,000 men and women chartered to support IW planning, intelligence gathering, weapon system analysis, and related activities. This group will be a source of IW support teams to go out and assist the CINCs and JFACCs during crises or exercises. They will help build information warfare into the air campaign planning and execution. And I will tell you that the Air Force is not alone in this. The Army has an IW Center down at Fort Belvoir and the Navy has created a center at Fort Meade.

Additionally, the Air Force is adjusting our training and education programs to include IW concepts. We've had a course for our major air command and numbered air force staffs to give them some basic understanding of the issues. And now, we're incorporating IW into our doctrine, so that airmen everywhere will share a common foundation and a common terminology. And we're adjusting our mid- and senior-level

professional military education schools at Maxwell Air Force Base, Alabama. And, of course, you see part of this effort here today. We have four Air Force officers attending the inaugural class of the National Defense University's School for Information Warfare.

Finally, and most significantly, we are beginning to procure weapon systems with a mindset that places high priority on maximizing their performance as an information warfare platform. One example of that is the United States' new air superiority fighter, the F-22.

This aircraft is the first platform to be built around information technologies. This was an established objective when we started the program, not something added after the fact. Now, a lot of people have heard about the F-22's stealth. You've heard about its supercruise capability -- that is the ability to cruise faster than the speed of sound in military power. And possibly you've heard about the fact that it has tremendous agility in the air-to-air arena.

But, you cannot begin to appreciate its potential until you sit in the concept demonstrator and see how the F-22's integrated avionics work. The quality of the composite picture that's compiled from a variety of sources will literally water your eyes, particularly if you're an old time fighter pilot. For the first time, you'll be able to sit there with those flat glass displays and have tremendous situational awareness readily available to you. That is something we've needed for years, and we're finally in the process of getting it. It will allow our pilots to act and assess faster even when outnumbered. And I tell you it isn't just a concept -- it's being put into production today!

The F-22 is just one of many Air Force programs that we're continuing to push forward. You see the same thought processes in the space-based infrared system, in our Joint STARS, and in our precision munitions program. As we move forward, we are establishing an additional requirement for our weapon systems -- that is security against the information threat -- that's being written into the requirements documents.

This new mindset is found throughout our acquisition strategy. We are changing how we view our modernization needs. We're taking another look at IW capabilities, like those associated with command and control, and we're treating them more like force structure than support structure. It's part of how we've got to change the way we do business to incorporate the fundamentals of information warfare.

And, this broad approach means that we must get the lawyers involved. Now, when I first heard about bringing in the lawyers, I thought we had really slipped off the deep end, one more time. And I do apologize if I offend any lawyers out there. I always have held lawyers in fairly high esteem. But then, the more I thought about this thing of bringing the lawyers into the equation, the more I realized we need their expertise. Because exploiting the information spectrum will readily cross international borders, we must be cognizant of what the law allows and will not allow.

When do you begin information warfare in the spin up to a conflict? When do you begin to go out there and intrude in somebody's banking system? When do you begin to get into somebody's telecommunications system? These are all very difficult questions. Clearly, information

warfare is not something that is focused solely on the confines of a constrained battle area. While we will fight in a theater, information warfare will force us to be engaged worldwide. And so, we must have some good advice as we pursue this capability.

I appreciate this opportunity to share with you what the Air Force is doing to try and keep up with the information technology explosion. The American way of war has very strong roots in understanding the value of exploiting information to deny information to our adversary, to corrupt what data he has, and to exploit what we know.

World War II was filled with many examples of information warfare. Perhaps Winston Churchill offered the best summary of its importance. At the Tehran conference, when discussing the Allied plans to manipulate information before D-Day, many of these same ethical questions came up. When do we do it? How do we do it? Who are the innocent victims of this thing? And Churchill addressing the other allied leaders said, "In wartime, truth is so precious that she should always be attended by a bodyguard of lies."[1] Something to think about. Later, there was a book written with that title by Anthony Brown. If you read his thick volume, it's rather chilling to see what was possible in that era, and then think about how much more is possible today with the technology that's available.

Today and in the future, information warfare is, in fact, going to be this nation's bodyguard. It is essential for the success of our joint forces. To succeed, we're going to need help from a lot of people including all the very interested people in this room. You understand the far-reaching

---

[1] Anthony Cave Brown, Bodyguard of Lies, Harper and Row, (New York, New York) 1975, p. 10.

implications of systems like LANDSAT or SATCOM which are readily available and widely employed at relatively low cost. You appreciate the potential for information technology to allow an adversary to build small, capable, autonomous operating systems that can threaten U.S. forces on land, sea, or in the air. Such devices might operate relatively unseen and unobserved until they unleash their destructive power.

So, I will tell you that those in the military services need your help. Don't be bashful about giving it. And, I think you'll find us very open and receptive to the advice and assistance you're willing to give.

IRIS Record

Key Information

Main: FOGLEMAN, RONALD R.

Document Type: **Papers**
Call Number: **168.7677-472**
IRIS Number: **01179193**
Accessions Notes: Ref 01174718
Old Accession Nbr:
Title:
Beginning Date:
End Date:
Publication Date: **1995/05/16**
Classification: ***Unclassif***

Rcvd:		Rel	
Indexer ID: **80**		Entered Date:	**2010/11/05**
QC ID:		QC'd Date::	
Scanner ID:		Scanned Date:	
Acc ID	**42**	Acc Date:	**20100504**

Media Roll #: First Frame: Last Frame: Linear Feet: **0.08**
Old MFlm Roll # Audio Rec:
NUMPAGE
Title Extensions:

Abstract Contains copies of remarks as delivered by Gen Fogleman at National Security Industrial Association-National Defense University Conference on Global Information Explosion, 16 May 1995, titled; Fundamentals of Information Warfare--An Airmans View.

Descriptive Notes: In personal collection of Gen Ronald R. Fogleman (USAF Retired). FULL TEXT DOCUMENT IS AVAILABLE IN ELECTRONIC FORM VIA CLASSIFIED NETWORK.

Major Command:

Doc Link http://hra-2k-4f58121/h$/168.7677-472/19950516/01179193.pdf

Administrative Markings

No Administrative Markings Listed
Security Review Information: