AIR WAR COLLEGE

AIR UNIVERSITY

INFORMATION WARFARE:

IMPACT AND CONCERNS

James W. Mc Lendon
Colonel, USAF

A RESEARCH REPORT SUBMITTED TO THE FACULTY

IN

FULFILLMENT OF THE CURRICULUM

REQUIREMENT

Advisor: Dr. Barry Schneider

MAXWELL AIR FORCE BASE, ALABAMA
APRIL 1994

DISCLAIMER

This study represents the views of the author and does not necessarily reflect the official opinion of the Air War College or the Department of the Air Force. In accordance with Air Force Regulation 110-8, it is not copyrighted, but is the property of the United States government.

Loan copies of this document may be obtained through the interlibrary loan desk of Air University Library, Maxwell Air Force Base, Alabama 36112-5564 (telephone (334) 953-7223 or DSN 493-7223).

ABSTRACT

TITLE: INFORMATION WARFARE: Impact and Concerns

Author: James W. Mc Lendon, Colonel, USAF

Information has always been a critical factor in war. Clausewitz said "imperfect knowledge of the situation...can bring military action to a standstill." Sun Tzu indicated information is inherent in warfighting. Information warfare embodies the impact of information on military operations.

The computer age gives us the capability to absorb, evaluate, use and transmit and exchange large volumes of information at high speeds to multiple recipients simultaneously. Multiple sources of data can be correlated faster than ever. Thus, the value of information to the warfighter has been magnified to a new level.

Churchill used information warfare when he used the ENIGMA machine to read German codes during World War II. He also used information warfare through his elaborate network emanating from the London Controlling Section, for its time a very complex intelligence and deception operation.

Lessons from DESERT STORM gave impetus to this fourth dimension of warfare. It was in this conflict that the computer came of age, and presented us with new challenges, both offensively and defensively, that must be faced in the future. Not only do we have opportunities to enhance our offensive capabilities many fold, but we must consider the additional vulnerabilities to our systems that come with this added capability. The widespread availability of information technology dictates that we carefully assess the vulnerabilities of the systems we employ.

Information Warfare adds a fourth dimension of warfare to those of air, land, and sea. In this new dimension, we must stay ahead.

BIOGRAPHICAL SKETCH

Colonel James W. Mc Lendon (M.S., Troy State University) is a career intelligence officer. His experience includes national, ground tactical (mobile), and airborne operations. His overseas assignments include Taiwan (twice), Vietnam, Germany (twice), the United Kingdom, and Saudi Arabia. Stateside, he has served on the Air Force Intelligence Command (AFIC) (and its predecessors) staff three times and was the AFIC Liaison Officer to the Air Force Special Operations Command prior to attending the Air War College. Colonel Mc Lendon has commanded three intelligence squadrons, is a graduate of Squadron Officers School (residence), Air Command and Staff College (residence), and is currently a member of the 1995 Air War College class. Upon graduation from Air War College, he is being assigned to Headquarters, Air Force Special Operations Command as the Director of Intelligence.

TABLE OF CONTENTS

INFORMATION WARFARE:

IMPACT AND CONCERNS

I. INFORMATION WARFARE: OLD CONCEPT , NEW TECHNOLOGY

Given the wide realm of activities that might be included under the heading of Information Warfare, one might conclude that it is not a new concept but rather one that can be more aggressively employed today with new technology. Had the term "information warfare" existed in Churchill's day, he might have used it to describe his activities involving ULTRA. Given the availability of communications and computer technology today, the potential for information warfare seems limitless,. Unlike nuclear weaponry, however, this technology is not limited to a few nations. It is widespread and available to any country, and, in most cases, to any individual or group that wants it. It is for this reason that our pursuit of an offensive information warfare capability must not overshadow our appreciation of the need for a defensive capability.

This paper offers evidence of the need for a rigorous defensive information warfare capability. It includes a case study from World War II which demonstrates Churchill's creativity in using information warfare against the Germans and proposes that history may not have completely documented his activities in this endeavor. From World War II, we move to the Persian Gulf War where information technology was imbedded in virtually every aspect of Coalition operations. Our dependence on information mediums during the Gulf War is very evident. This dependency may also equate to yet unknown vulnerabilities, thus highlighting the need for the protection of these mediums.

Information has always been a critical factor in war. According to Clausewitz, "imperfect knowledge of the situation...can bring military action to a standstill."[1] Pick up any book on war, and the value of information becomes clear. As indicated by Sun Tzu in 500 B.C., it is inherent in warfighting.[2] It may be obvious that the more an army knows about itself and its enemy, the stronger it will be in battle. What is not so obvious are the uses that may be made of information, and how knowledge can be manipulated to reinforce the strength of an army many times over.

Information warfare embodies the impact of information, or knowledge, on military operations. It is defined as "Any action to deny, exploit, corrupt or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own information operations."[3] Additionally, in this context, information warfare "views itself as both separate realm and lucrative target. two While this definition is new, the concept isn't. It is only as we come to terms with the benefits

of the computer age that we realize the potential in conducting the operations described above.

The computer age gives us the capability to absorb, evaluate, use, transmit and exchange large volumes of information at high speeds to multiple recipients simultaneously. Multiple sources of data can be correlated faster than ever. Until recently, masses of information were transmitted in the literal, or alpha-numeric format, and had to be read and manually manipulated to be of any use. This made it difficult to sort the critical from the useful, and much of it went into the burn bag. Today, much of that same information is transmitted to the warfighter digitally and presented graphically. Little goes to waste. Thus, the value of information, its uses, and our dependence on it have been magnified to a new level.

Duane Andrews, former Assistant Secretary of Defense for C3I (Command, Control, Communications, and Intelligence), describes information today as a "strategic asset."[5] The

Tofflers go even further. In their discussion on third wave war, they refer to "knowledge warriors", describing them as "intellectuals in and out of uniform dedicated to the idea that knowledge can win, or prevent, wars."[6]

Major General Kenneth Minihan, Air Force Assistant Chief of Staff/Intelligence, describes information warfare in more objective terms, which he says is really "Information Dominance."[7] In describing Information Dominance, he puts it this way: "Information Dominance is not 'My pile of information is bigger than yours' in some sort of linear sense. It is not just a way to reduce the fog of war on our side or thicken it on the enemy's side. It is not analysis of yesterday's events, although proper application of historical analysis is important to gaining information dominance. It is something that is battled for, like air superiority. It is a way of increasing our capabilities by using that information to make right decisions, (and) apply them faster than the enemy can. It is a way to alter the enemy's entire perception of reality. It is a method of using all information at our disposal to predict (and effect) what happens tomorrow, before the enemy even jumps out of bed and thinks about what to do today." (Emphasis added.)[8] The Navy presents the bottom line view: "Information, in all its forms, is the keystone to success."[9]

The Department of Defense and all of the services are doing more than paying lip service to this new dimension. In addition to their attempts to fund extended programs in this subject, senior military leaders are taking strong positions in favor of this capability. Unfortunately, while the United States holds the lead in information technology today, other nations, including developing nations, are rapidly gaining access to this capability. This is cause for concern, and the answers are not simple.

II. WORLD WAR II CASE STUDY: CHURCHILL AND ENIGMA

INFORMATION WARFARE IN WORLD WAR II:

HOW FAR DID CHURCHILL GO?

With World War II (WWII), we saw many firsts. Some of the more significant examples were: large-scale air-to-air combat, strategic bombing--both daylight and night, the use of naval carriers to project air power, and the first and only uses of atomic bombs during hostilities. This case study asserts that we also saw the first wide-spread and well-orchestrated use of information warfare, and presents a hypothetical model for interaction between deception and cryptanalysis.

Many of us remain intrigued by the clandestine and covert operations conducted by the Allies in WWII. This study discusses two of those operations: deception and cryptanalysis based on radio intercepts. It also, and more importantly, attempts to build a model for an interactive relationship between the two that could have synergistically improved the contributions of these operations to the successful prosecution of the War. The model, though purely hypothetical, uses facts to present a case for the potential of maximizing misinformation through the integration of these two disciplines Said another way, this paper suggests that the Allied leadership, specifically Winston Churchill, found cryptanalysis necessary but not sufficient for victory. Cryptanalysis and deception were both necessary and sufficient. Hence, the logic of the model suggests that Churchill directed an offensive information warfare campaign.

THE LOGIC OF THE MODEL

The question posed is whether Prime Minister Winston Churchill would, or could, have selectively chosen to chance using the ENIGMA (the machine used by the Germans to encipher

high-grade wireless traffic)[10] to encipher notional messages and intrude on German wireless radio nets to misinform the Germans on Allied intentions, or otherwise disrupt German military operations.

Churchill's concern for the security of the ENIGMA and the knowledge that it was being used by the Allies was considerable, as will be shown later. The risk of compromising Allied use of the ENIGMA was colossal, affecting many lives and the potential outcome of many battles. On the other hand, successful deception could be equally effective.

For Churchill to have taken this step would have been boldness from "sheer necessity" in the strictest Clausewitsian terms.[11] The risk in not doing so would have had to have been greater than the risk in doing so. The logic of the model is that if Churchill directed that messages encrypted using ENIGMA be transmitted, he would only have done so out of necessity; when Britain was in dire straits.

BACKGROUND

"Deception is as old as war itself."[12] Although this statement is from WWII, it was clearly not a revelation of fact. Sun Tzu included deception as one of his tenets of warfare when he said, "All warfare is based on deception."[13] The modern complexities of war and the ensuing technological advancements enhance the means through which deception can be employed, and WWII was no exception. The use of deception during WWII has been widely publicized. At least one book, The Man Who Never Was, was published and a movie by the same title was made on a single event.[14]

Deception and its implementation occur in both the strategic and tactical spheres. The example documented above was strategic in its support of the Normandy Invasion. Tactical

deception at that time was thought to fall under three headings, visual, aural (or sonic), and radio.[15] While aural deception might apply in limited fashion to specific engagements, it is logical that visual and radio deception could be used for broader objectives at both the strategic and operational levels.

It is not surprising that most information concerning deception activities remained classified for many years after the war, and is only now coming to the attention of the public. It appears that most, if not all, of the information concerning tactical deception has been declassified. This is not the case with another stratagem used against the Germans, that of intercepting radio communications and using the ENIGMA machine to decipher the message transmissions. While previously classified documents concerning Ultra are now largely available to the public, a review of the primary sources reveals that many still contain blank pages that are marked "not releasable" while others contain portions that have been blanked out with no explanation. Thus, even though we know much more today than we did fifteen years ago about these activities, public access remains unavailable for much of it.

These continuing restrictions may well be the result of comments made on 15 April 1943 by Colonel Alfred McCormack in a memorandum to Colonel Carter W. Clarke. McCormack, then "Mr. McCormack," had earlier been appointed as Special Assistant to the Secretary of War to study the uses of Ultra and establish procedures for making the best use of this source. At the time of the memorandum, McCormack was deputy chief of the Special Branch and worked for its chief, Col Clark. The purpose of the Special Branch was to handle signals intelligence. McCormack's memorandum consists of 54 pages on the origin, functions and problems of the Special Branch, Military Intelligence Service (MIS). In this memorandum, McCormack describes, in his view, Ultra security requirements as follows:

> One lapse of security is all that is necessary to dry up a radio intercept source. Therefore, both on the officer level and below, only persons of the greatest good sense and discretion should be employed on this work. This consideration is basic since intercept information involves a different kind of secrecy than does most other classified information. It will make no difference a year from now how much the enemy knows about our present troop dispositions, about the whereabouts of our naval forces or about other similar facts that now are clearly guarded secrets. But it will make a lot of difference one year from now--and possibly many years from now--whether the enemy has learned that in April 1942 we were reading his most secret codes. Not present secrecy, not merely secrecy until the battle is over, but permanent secrecy of this operation is what we should strive for.[16]

This secrecy was maintained throughout the war. Only carefully selected individuals in Washington and in the field had access to the information produced through these intercepts. The procedures for use by field commanders and their personnel, including controls established to protect the information and its source were laid out in a letter to General Eisenhower from General Marshall on 15 March 1944.[17] These procedures lasted at least through the end of the war.

THE ORIGIN OF ULTRA

Ultra's origin begins with the delivery of a German ENIGMA machine to the British by Polish dissidents. The history and acquisition of the ENIGMA machine are quite lengthy and complex. It is sufficient here to reflect that the Poles had established a successful cryptanalytic effort against the Germans by the early 1930s, having begun their efforts in the early 1920s.[18] Using their own copy of the ENIGMA, they achieved their first successful break in reading ENIGMA ciphers in December 1932 and January 1933.[19] Between 1933 and 1939, successful reading of ENIGMA traffic was purely a Polish achievement.[20] Once the ENIGMA fell into British hands, however, they took the lead and used it successfully throughout the war.

ENTER WINSTON CHURCHILL

Winston Churchill had a profound interest in the Ultra traffic produced from ENIGMA and required that all important decrypts be provided to him.[21] His interest in codebreaking is documented as early as November 1924 when, as the chancellor of the exchequer, he requested access to intercepts.[22] In his request, he stated, "I have studied this information over a long period and more attentively than probably any other Minister has done....I attach more importance to them as a means of forming a true judgment of public policy in these spheres than to any other source of knowledge at the disposal of the State.[23] Then in September 1940, after only four months as the Prime Minister, he directed he be provided "daily all ENIGMA messages."[24] When this became overwhelming in volume, he backed off to receiving several dozen a day.[25] During a visit to Bletchley Park, the headquarters for the British cryptanalytic organization, he spoke to a crowd of the station managers and referred to them as "the geese that laid the golden eggs and never cackled. "[26] After the war, Churchill reiterated his faith in Ultra, describing it as his "secret weapon"[27] and stating his belief that "It had saved England."[28]

Churchill's concern for security of Ultra was paramount. He directed that no action be taken in response to Ultra intercepts unless cover could be provided[29] and he had, in fact, repeatedly allowed naval convoys to come under U-boat attack rather than risk compromising Ultra security.[30]

Churchill was also directly involved in the conduct of deception operations. He established the London Controlling Section (LCS) in his headquarters specifically to plan those stratagems necessary "to deceive Hitler and the German General Staff about Allied operations in the war against the Third Reich."[31]

Not only did Churchill establish the LCS, but he also personally conceived the idea for this organization after a series of successful uses of deception in the Libyan desert led to the defeat of Italian forces. In one of those instances, a small British force of 36,000 men defeated an Italian force of 310,000 using deceptive measures. Realizing he was outnumbered and about to be overrun, the British commander used inflatable rubber tanks, field guns, 2-ton trucks, and prime movers to present the image of a larger force. He employed crowds of Arabs with camels and horses to drag harrow-like equipment to stir up dust storms, and he used anti-aircraft artillery to keep the Italian reconnaissance aircraft high--precluding them from sorting out the actual order of battle on the ground. The Italians perceived a force on their right flank much larger than theirs and tried to run. Using only two divisions, the British captured 130,000 prisoners, 400 tanks, and 1290 guns. Their losses were minimal for the magnitude of the conflict--500 killed in action, 1400 wounded, and 55 missing in action.[32] This impressive event rocked London, and gave credence to further development of this capability. This action, and others similar to it, convinced Churchill that deception needed an institution so it could be applied on a broader scale. Thus, LCS was born.

The LCS was the first bureaucracy ever designed expressly to deceive.[33] It was "members of the LCS and hierarchs of other British and American secret bureaus"[34] who developed and executed LCS activities, referring to their weapons as "special means."[35] In this context, "special means" is "a vaguely sinister term that included a wide variety of surreptitious, sometimes murderous, always intricate operations of covert warfare designed to cloak overt military operations in secrecy and to mystify Hitler about the real intentions of the Allies."[36]

BACK TO ULTRA--ITS CONTRIBUTION

Ultra proved its value as early as mid-July 1940 when it provided forewarning of German plans to attack England. Intercepts at that time revealed Hitler's directive outlining the planned invasion of England. The invasion was to begin with an air raid. These intercepts continued, reaching a point of two to three hundred per day--all being read at Bletchley Park. On 13 August, when the air raid began, the British were more informed of the plans than were many of the Luftwaffe units.[37]

It is clear that Ultra intercepts provided the bulk of intelligence to the Allies during the war. By June 1944, 90 percent of the European intelligence summaries provided to Washington were based on Ultra information.[38] Ultra provided information on force disposition and German intentions at both the strategic and tactical levels. Ralph Bennett describes Ultra's contribution succinctly in his preface to Ultra in the West:

> For by often revealing the enemy's plans to them before they decided their own, Ultra gave the Allied Commander an unprecedented advantage in battle: since Ultra was derived from decodes of the Wehrmacht's wireless communications, there could be no doubt about its authenticity, and action based upon it could be taken with The greatest confidence. So prolific was the source that at many points the Ultra account of the campaign is almost indistinguishable from the 'total' account."[39]

It has also been described as "more precise, more trustworthy, more voluminous, more continuous, longer lasting, and available faster, at a higher level, and from more commands than any other form of intelligence."[40] It even provided information German intercepts and analysis of British and American radio networks.[41] Taking advantage of this latter knowledge, the Allies established an elaborate communications network designed expressly to transmit bogus traffic that would misinform the Germans of their intentions and operations. What would have prevented including encrypted ENIGMA messages directly to the Germans in this bogus traffic?

RADIO DECEPTION

The British and Americans used manipulation through cover and deception to target specific sources of enemy information. For example, they released false information to the world press and staged activities that "made the news." They deceived enemy air reconnaissance through the maneuver of real troops, use of controlled camouflage (both to conceal and intentionally show indiscretions), dummy equipment, and "Q" lighting (the positioning of lights to draw bombers to non-existing airfields).

Aware that German radio intercept units were targeting their transmissions, they used a three-pronged strategy against the German listening stations. First, they prepared notional radio traffic to be transmitted by special deception troops over nets established solely for the purpose of deception. Second, they sent notional radio traffic over authentic operational nets. Finally, they regulated the genuine traffic passed on authentic operational nets, creating dead time and peak traffic levels.[42] Signal troops employed in deception activities were specially trained in these operations[43] and thoroughly indoctrinated on the sensitivities that accompanied their efforts. The following statement was among the many instructions concerning security provided to them:

> You must realize that the enemy is probably listening to every message you pass on the air and is well aware that there is a possibility that he is being bluffed. It is therefore vitally important that your security is perfect; one careless mistake may disclose the whole plan.[44]

One of the most elaborate schemes employing radio deception was used in support of the First U.S. Army Group (FUSAG), a notional, fictive organization headed by General George S. Patton, Jr.[45] Conceived as a part of BODYGUARD,[46] the FUSAG was composed of more than fifty "divisions" located in southeast England. Aware that the Germans anticipated an attack by

the Allies, the purpose in establishing a non-existent FUSAG was to persuade the Germans that the attack would take place at Pas de Calais.[47]

The radio net supporting FUSAG represented the following units: a Canadian army, a U.S. army, a Canadian corps, 3 U.S. corps, a Canadian infantry division, a Canadian armored division, six U.S. infantry divisions, and four U.S. armored divisions.[48]

THE CASE

ENIGMA traffic provided the tip-offs to the planned German invasion of Britain well in advance. The speed with which Bletchley Park was reading the German ENIGMA permitted them to extract intelligence from several hundred messages a day, indicating that although the ENIGMA settings were complex and changed frequently the cryptanalysts were experts on the machine.

The ENIGMA used wheels that had to be set in the proper order for the decryption to take place. These settings were usually changed every 24 hours with minor settings changed more often. Other minor settings were made with each message. The tip-off to the receiver for these latter settings was contained in the transmission.[49] The speed with which these messages were deciphered could have provided the essential information required by the British to use the machine to other advantages.

From the volume of intercept, it is obvious the British knew their targets' organizations and frequencies. The traffic would have provided them with information on message originators, addressees, associated organizations, and formats--allowing them to reconstruct necessary elements of the German radio communications network. The German use of "standard phrases, double encipherment...their lack of an effective, protective monitoring program; and their

unshakable--even arrogant-confidence in ENIGMA"[50] make it unlikely they would have employed authentication devices in their messages. The Germans then clearly were vulnerable to deception efforts using encrypted ENIGMA messages broadcast by the nets serving the London Controlling Section. Would Churchill have taken the risks associated with exploiting this vulnerability?

DIRE STRAITS

The Battle of Britain and the Normandy Invasion were two of the most significant events in WWII. The Battle of Britain, particularly, represented a critical period for the British. The defeat of Germany in that battle required the all-out effort by Britain. The battle began with each side roughly equivalent in front-line fighters, but it was touch and go until the Luftwaffe lost its ability to mount sustained attacks.[51] The desperation facing the British during the massive air raids might have convinced Churchill at some point that it would be worth the risk to use the ENIGMA to intrude on German radio nets. Perhaps relying on the confusion and disorder he know existed among some of the Luftwaffe units,[52] his assessment as to the potential for success could lead to this risky decision.

From 13 August until mid-September, 1940, the Luftwaffe conducted raids during daylight hours and Ultra traffic revealed most, if not all, the targets that were to be hit. Interestingly, beginning in mid-September and lasting throughout October, the raids were flown at night and the only target references available through Ultra were codenames representing target locations. Had something tipped the Germans their mail was being read? On 14 November, Ultra revealed Coventry as a target and at least one British official believed naming the town instead of using a codeword was a mistake on the part of the Germans.[53] The use of codewords surely made Churchill nervous, giving him cause to question if their use of ENIGMA had been compromised.

This concern could account for his widely reported decision to take no action to evacuate Coventry, other than to alert fire, ambulance, and police units.[54]

The Normandy Invasion was the last critical juncture for the Allies. A successful invasion would bring Germany and the Third Reich to their downfall. In preparing for the invasion, BODYGUARD had already been implemented.

The infrastructure for radio deception was in place and in use. This infrastructure would also have made an excellent point of origin for intrusion into German radio nets, using the ENIGMA to encipher messages for transmission. Schemes could have been devised using notional traffic sent over the deception nets, which were known to be monitored by the Germans, to complement intrusion traffic enciphered with ENIGMA. Bletchley personnel could prepare the ENIGMA traffic and send it to the radio deception units to be transmitted verbatim on specified frequencies. The personnel employed in the radio deception were well trained for their purpose and indoctrinated in the secrecy of their work.

If Churchill saw the invasion as the last big push to defeat Germany, he may also have viewed selective use of intrusion as justified and worth the risk. Given the increasing disruption that occurs with the multiplying intensity of battle, the risk would have gradually diminished with time during the course of the fight. As the risk diminished, the opportunities would have grown. Greater opportunities would have been enticing to Churchill, especially if there were opportunities to shape the post-war world.

CONCLUSION

Much of the history of WWII may need to be rewritten because of the revelations of Ultra contributions. Revelations include those already made and those yet to be made. Considering what we now know about Ultra operations, one can assume that credit for success in a battle often

went to the wrong party. The men and women at Bletchely Park, and other locations, who were involved in providing advance warning and other information to Allied forces may never get all the credit they are due. It is now well known that "Ultra did indeed shape the character of strategy and operations--particularly operations. In no other war have commanding generals had the quality and extent of intelligence provided by Ultra."[55]

Whether Churchill actually used the ENIGMA offensively for the purposes hypothesized here may never be known. If he did not, maybe it was because it was too risky, or just too tough to do. Maybe we did not possess enough information on the keying cycles necessary to confidently exploit that avenue of deception. Or maybe we just missed a good opportunity. Absent further declassification, we cannot know for certain. While logic suggests he might have, the facts may prove otherwise.

If he did use it in this manner, it had to have been brilliant. It would have been information warfare at its best. Perhaps it was.

III . IMPACT OF INFORMATION TECHNOLOGY ON THE GULF WAR

BACKGROUND

Although the use and exchange of information has been a critical element of war since its inception, the Gulf War was the stage for the most comprehensive use of information, and information denial, to date. New technologies in this conflict enhanced the Coalition's ability to exchange and use information and highlighted the imperative of denying the adversary his ability to communicate with his forces. While in large part, these technologies were space-dependent, recent advancements in digital technology permitted the rapid processing, transmission, and display of information at all echelons, enabling decision makers to respond rapidly to developing situations on the battlefield. Some prototype systems such as JSTARS successfully made their trial run during this conflict, earning their place in history as contributors to the coalition success of this war. Architectures enabling connectivity between these many systems were non-existent when Iraq invaded Kuwait, however they were put in place during the build-up and supported the Coalition forces for the duration of the war. These architectures were clearly necessary to effectively control the myriad activities operating simultaneously in the battlefield.

For example, eleven AWACS aircraft controlled 2240 sorties a day, more than 90,000 during the war with no mid-air collisions and no friendly air engagements. Satellite connectivity permitted this same air activity to be displayed live in the Pentagon Command Center.

JSTARS tracked tanks, trucks, fixed installations, and other equipment, even though this system had not met operational capability status yet.

Satellites, microwave, and landlines handled 700,000 phone calls and 152,000 messages a day. Coalition forces avoided communications interference through successful deconfliction of

more than 35,000 frequencies. Any attempt to describe the complexities of managing this system would be an understatement. The Joint Communications-Electronic Operating Instructions (JCEOI) which was used to allocate frequencies, callsigns, callwords, and suffixes for the Gulf War, was published in over a dozen copies and weighed 85 tons in paper form.[56] This system was used for both space and terrestrial communications.

SPACE

Space assets, both military and commercial, belonging to the United States, the United Kingdom, France, and the USSR, provided the coalition with communications, navigation, surveillance, intelligence, and early warning, as well as offering live television of the war to home viewers around the world for the first time.

Using some 60 satellites, coalition forces had access to secure strategic and tactical communications in-theater and into and out of the theater of operations.[57] These satellites bridged the gap for tactical UHF and VHF signals that here-to-fore had been limited to terrestrial line-of-sight only, enabling time sensitive information to be exchanged between ground, naval, and air units spread throughout the theater. Without this capability, the communications architecture required to support the preparation and distribution of task orders and the coordinated operations of AWACS, JSTARS, and conventional intelligence collection in support of force packages in virtual and near-real-time would have been impossible. Even though there were still shortfalls at the tactical level in timeliness, precision, and volume, commanders at all levels still had access to unprecedented communications capabilities.

There are some who credit the capabilities afforded by GPS "as making the single most important contribution to the success of the conflict."[58] Using a constellation of 14 satellites, Coalition forces were able to locate and designate targets with remarkable precision, navigate

through the naked Iraqi desert better than the Iraqis themselves, and find troops in distress faster than ever before. The U.S. Army used the NAVSTAR Global Positioning System (GPS) to navigate the Iraqi desert in the middle of sand storms, surprising even the Iraqis who themselves do not venture across it for fear of becoming lost. GPS was the capability that made possible the "left hook" used to defeat Saddam Hussein's armored divisions. The use of GPS was, in large part, the result of off-the-shelf purchases acquired by special contract arrangement; these being the same systems that had been designed and marketed for recreational boat use--thus, technically available to anyone.[59] U.S. troops stationed in Saudi Arabia also received commercially purchased GPS systems from their relatives.[60] Access to GPS, and its attendant capabilities, added tremendously to the morale of coalition forces.

More than 30 military and commercial surveillance satellites were used for intelligence gathering during the war.[61] These satellites provided the coalition forces with imagery, electronic intelligence, and weather data. While these systems provided precise targeting information on enemy locations, movement, and capabilities, they were also essential in meeting another coalition objective--that of minimizing collateral damage. Precision targeting combined with the use of precision guided munitions significantly decreased civilian casualties and left structures adjacent to target intact.

INTELLIGENCE

The rapid deployment of a variety of systems to the Persian Gulf in response to the crisis there resulted in a number of stovepiped organizations, resulting in a voluminous amount of unfused and uncorrelated information being collected and disseminated. There was also a preponderance of incompatible systems deployed. This lack of integrated, all-source information and deficiency in compatibility often placed a burden on recipients who had neither the personnel

nor the skills necessary to put it all together in one product. Notwithstanding this limitation, the bulk of which involved secondary imagery production, the evidence shows that timely, quality intelligence was available to those units fortunate enough to have access to the right terminal systems. To a large degree, the impediment was the result of fielding prototype systems for which there was no proliferation of terminal capability at the time.

One of the most prolific producers of information in this category was the tactical information broadcast service (TIBS), but unfortunately the limited number of terminals dictated that only key nodes could have access to this product. Nevertheless, TIBS and its cousin, Constant Source, provided timely updates of intelligence information to various echelons, including wings and squadrons, directly from collectors and associated ground processing facilities.[62]

The RC-135 RIVET JOINT, flying in coordination with its sister ships, the E-3 AWACS and E-8 JSTARS, flew 24 hours a day to support the war. Referred to as the "ears of the storm" in contrast to the AWACS role as "eyes of the storm,"[63] the RC-135 provided real-time intelligence to theater and tactical commanders in the desert and Persian Gulf areas. Especially trained personnel used on-board sensors to identity, locate, and report Iraqi emitters that might pose a threat to Coalition forces.

These systems are only a sampling of those deployed to the theater to provide intelligence support. Reviews and action are ongoing to resolve the problems resulting from stovepiping and incompatible systems.

IRAQI COMMAND AND CONTROL (OR LACK THEREOF)

The Coalition not only recognized the value of information to its efforts, it also saw the benefits of denying the Iraqi command and control system its ability to function. The Coalition identified the Iraqi leadership and Iraqi command, control, and communications (C3) facilities as the two key centers of gravity.[64] While command of the air was the initial key objective, C3 facilities received priority in targeting.

The Coalition used massive airpower at the onset of hostilities to accomplish this objective. Targeting strategic military, leadership, and infrastructure facilities, the Coalition launched its attack on Iraq on 17 January 1991. Early warning sites, airfields, integrated air defense nodes, communications facilities, known Scud sites, nuclear/chemical/biological facilities, and electrical power facilities were under attack B-52s, Tomahawk land-attack missiles (TLAMs), F117s, and helicopter gunships. During the first two days, the Coalition gave no slack while conducting the most comprehensive air attack of the war. Even after the opening minutes of the war, Iraq had little of her C3 infrastructure remaining.[65] The Coalition success was so devastating that, as an Iraqi prisoner reported, "Iraqi intelligence officers were using Radio Saudi Arabia, Radio Monte Carlo, and the Voice of America as sources to brief commanders."[66] What little communications capability Iraqi tactical commanders did have, they used improperly.

Apparently concerned over Coalition communications monitoring, the Iraqis practiced strict communications security through near total emission control (EMCON). While this did have a negative impact on Coalition signals collection efforts, it also blinded Iraqi tactical units. One Iraqi brigade commander, in reflecting his surprise over the speed with which a U.S. Marine unit overran his unit in Kuwait, showed he had no idea the Marines were coming even though another Iraqi unit located adjacent to him had come under attack two hours before.[67]

Although leadership as a target was difficult to locate and survived the conflict, the successful attacks against the Iraqi C3 essentially put her leadership in the position of having no strings to pull. Trained to operate under centralized control, the Iraqi forces did not know how to function autonomously. Air defense forces became fearful of emitting because of their vulnerability to anti-radiation missiles. Believing the army, not the air force, was the determining force in battle, the Iraqis attempted to shield rather than use their aircraft. The attempts they did make in defensive counterair proved rather embarrassing.

CONCLUSION

The Gulf War clearly demonstrated the need for accurate and timely dissemination of information. Information was the hub of all activity on the Coalition side, and the lack of it caused the failure of the Iraqi military to employ its force. The communications enhancements realized with the advent of new technologies also bring about new vulnerabilities. Building defenses to these vulnerabilities is considered by some to be at odds with increasing the capabilities. The benefits enjoyed by the Coalition's ability to communicate and the impact of attacks on Iraqi C3 have been widely publicized and have to be assumed to be well known by every potential adversary on earth. We have to prepare for similar attacks, or attacks of a different medium, against our own information systems in the future.

IV: WHAT DOES THE FUTURE HOLD?

There is an information glut. There is a proliferation of modem equipped personal computers and local area networks in military organizations, industrial facilities, and private homes around the globe. And it doesn't stop there. For example, Motorola is working on a 77 satellite constellation that will provide cellular telephone service from any spot on earth within five years. With fiber optics supporting these satellites, entire countries are being wired. Turkey, for example, has moved into the information age in one big leap.[68]

As the information glut continues to grow, along with systems to accommodate it, vulnerabilities to surreptitious entry are certain to increase. The amount of information being reported is doubling every 18 months. And this growth is accelerating. Two years ago, volume was doubling every four years; three years ago, it was every four and a half years.[69] While our capacity to process information at this growth rate seems limited, technology has a way of catching up--but not necessarily in time to help for a given situation. It can be particularly difficult to process it in a readily useable form during intense, crisis situations.

For each day of the Gulf War, it took 7000 personnel working two days to produce the Air Tasking Order (ATO) for 2000 aircraft sorties to be flown on the third day. The ATO began as a 300 page document developed for transmission to Air Force, Navy, and Marine aviation, but difficulties in receipt by receiving organizations forced adjustments. Even using dedicated communications circuits, it took the Navy three to four hours to receive it. Early on, there was a 70,000-message backlog, and flash precedence messages were taking four to five days to reach their destination--some never made it. Additionally, the volume of traffic took an inordinate amount of time to read, let alone respond to.[70] It seems the greater our capability to process information, the more information there is to process. Former Vice Chairman of the JCS, Navy

Admiral David E. Jeremiah sees it this way: "Technology has fueled a change in communication, (ushering in) an era of information dominance. Global dominance will be achieved by those that most clearly understand the role of information and the power of knowledge that flows from it."[71]

The services are recognizing this, and reacting to it. In the Air Force, Information Warfare techniques are being intensively studied and incorporated at the Air Intelligence Agency (AIA). AIA looks at Information Dominance in terms of the OODA loop. The OODA loop, (Observe, Orient, Decide, Act), represents the decision cycle through which a warrior at any level must go. As you go from the strategic level to the tactical level, the time available for making a decision decreases. At the tip of the spear, it is very short. According to Major General Minihan, "As we compare friendly and adversary OODA loops, it becomes a deadly game of compression and expansion. We will use Information Warfare to expand the adversary's and compress our own action loops. If you can't think, can't hear, and can't see--and I can--you will lose every time."[72] This concentration of effort in information technology will, and should, have an impact on military doctrine.

Admiral Jeremiah has already considered this. He points out that "It is time to come to grips with a different intersection, an intersection of technology and strategic thought. ...I think that in large measure the product today, technology, drives doctrine and tactics, and to a major degree drives strategy."[73] We obviously are far from reaching full understanding of the impact of Information Warfare on doctrine, tactics, and strategy. However, the explosion of information on societies around the world, and the associated technology, dictate that we find a way to measure the impact, and look for ways to incorporate the right level of emphasis on this topic into our thinking. One area of concern is our propensity to stovepipe activities within our structures, and the negative influences this can have on military operations.

Army, Navy, and Air Force senior leaders have voiced concern with these vertical structures. It has become tradition, for example, to stovepipe several functional areas such as intelligence, logistics, and acquisition. Stovepiping often excludes the chain of command from the decision-making process and impedes synergistic benefits that are available from integrated operations. The one-base, one-boss mandate from the former Air Force Chief of Staff, General McPeak, is a significant step to overcoming some of the stovepipe inhibitors. The focus, then, should be on moving from vertical structures, or stovepipes, to horizontally integrated systems. The expected result is integrated functional areas, which should provide a better structure for identifying needs and requirements, and determining force projection priorities. In the information sphere, however, this could increase vulnerabilities to unauthorized access because it disperses the information base on a much wider scale. Some members of the U.S. military community recognize that "Interdicting, protecting, and exploiting these new pathways is what IW (Information Warfare) is all about."[74] As we place more emphasis on this new dimension, we can expect other nations to follow. Russia will probably be one of the first.

Russian senior military officials have already recognized that the integration of information technology "could generate radical changes in the organizational principles of armed forces."[75] The use of "intellectualized" weapons in the Gulf War by the coalition apparently sparked a move in the same direction in Russia. Russian military experts now believe in "a new axiom to the body of military art: For combatants contending in military conflict today, 'superiority in computers' is of precisely the same significance as superiority in tube artillery and tanks was to belligerents in earlier wars."[76] Furthermore, "superiority in the MTR [military-technical revolution] proceeds from superiority in 'information weapons': 1) reconnaissance, surveillance, and target acquisition systems, and 2) 'intelligent' command-and-control systems."[77] Russian military leaders believe the

new "formula for success" is to "First gain superiority on the air waves, then in the air, and only then by troop operations."[78] As the two former adversarial world superpowers, who by and large supplied most of the weapons to other countries around the world, pursue information warfare as new realm of combat, it is almost certain other nations will buy into the trend.

In what is probably only the beginning for nations in conflict, the Internet has already provided a medium for information warfare between two belligerent nations. During the recent border dispute between Ecuador and Peru, Ecuador used the Internet to publish government bulletins and excerpts from local media to tell its side of the conflict. In retaliation, Peru Internet used a gopher site in an attempt to neutralize Ecuadorian propaganda. [A gopher is an information system residing on the Internet that knows where everything is and, through an arrangement of nested menus, allows a user to continue choosing menu items until the sought after subject is located.][79]
The resulting verbal skirmish left both nations working to set up their own gophers.[80]

Global information systems will enable ordinary users to access an extraordinary number of databases, far beyond the Internet capability of today (which is more than a million files at databases located at universities and corporate research centers). New software technologies permit these accesses to be conducted autonomously, using "self-navigating data drones." These drones, referred to as "knowbots," are released into the Internet and search for information on their own. They can roam from network to network, clone themselves, transmit data back to their origin, and communicate with other knowbots.[81] Given this capability, one has to wonder, and perhaps be concerned, about the potential for unauthorized, or at least undesirable, access to certain data bases and computer activities.

Hackers routinely attempt to get into U.S. military systems. During the Gulf War, hackers from Denmark, Moscow, and Iraq tried to penetrate these systems.[82] Our awareness of these attempts does not necessarily prove there were no successes of which we are unaware. And, even if they failed during that conflict, can we guarantee the security of our systems during the next war?

These vulnerabilities were revealed recently when a British teenager using a personal computer at his home hacked his way into a U.S. military computer network, gained access to files containing sensitive communications relating to the dispute with North Korea over international inspections of its nuclear program, and, after reading them, placed them on the Internet. His actions made those files available to about 35 million people. Officials suspect he had access to these computers for weeks, perhaps even months, before he was caught. Interestingly, once it was known an intruder was in the system it only took a week to identify him. Unfortunately, the apparent difficulty was in detecting him. Officials added that he had also breached other defense systems.[83]

Paul Evancoe and Mark Bentley, computer virus experts, have documented their concerns over our vulnerability to computer virus warfare (CVW) by other nations. They describe in detail the vulnerability of computer systems to this danger, and claim that "CVW is a powerful stand-alone member of the non-lethal disabling technology family and is likely being developed by several countries."[84] They also point out that the intelligence community and policy makers do not focus on these threats and generally do not possess enough technical understanding to recognize CVW as a real national security threat. They believe CVW remains an abstract, non-tangible concept to most intelligence analysts and policy makers. Furthermore, they call for legislation outlawing CVW development, classifying CVW as a weapon internationally, and including it as

part of nonproliferation treaties. It is unrealistic to believe we could achieve the support of the international community in this regard, and, with our lead in technology, we probably do not want to do so. Even if we could acquire this level of cooperation, and wanted to, enforcement would be next to impossible. CVW development does not leave traces as does chemical, biological, and nuclear development. And our efforts to isolate those are not always met with success.

Some Americans believe there will be no big wars in the future because there is too much destructive power, and nobody wins. The interdependence of nations would likely result in as much damage to an aggressor as to its adversary. Whether this is true or not, the concept of national security is changing.[85] Among the threats we face today are terrorism--either state sponsored or radical element, proliferation of weapons of mass destruction, localized conflicts, and aggressors that upset the world peace balance, intense economic competition, and availability of food and water.

The U.S. military may be called upon to react, in one way or another, to any of these threats. U.S. military operations can run the gamut, from civil-military affairs assistance to forcible entry. More reliance is being placed on communications and intelligence systems in support of these activities, and as these systems become more interoperable, they may become more vulnerable. "It is becoming more and more difficult to distinguish C4 systems from intelligence systems."[86] While sophisticated anti-jam systems are being developed and deployed, these systems are still computer based. Disruption in one would affect others.

For example, for years we have needed a near-real-time intelligence system capable of providing targetable accuracy information to "shooters." The Army expects to have an airborne and ground-based SIGINT/EW system capable of doing that by the end of the decade.[87] It seems logical that other existing and developmental systems might also be interconnected. Some of these

might include the Joint Targeting Network (JTN), the Tactical Information Broadcast Service (TIBS), Tactical Receive Equipment Related Applications (TRAP), SENIOR RUBY, CONSTANT SOURCE, QUICK LOOK, Over-the-Horizon (OTH) systems, and air and ground based radar systems. The integration and wide dispersal of these systems increase the number of vulnerability points where an adversary might intrude.

The GPS may be one of the most revolutionary systems in our inventory when you consider the difference it can make in navigation and geo-positioning of assets. It is available to the public and anyone with a few hundred dollars can buy into the system. The benefits, then, that we derive from this capability may be offset somewhat by use of the system by an adversary. GPS has improved our navigation and geo-positioning accuracy in multiples, but we are not the only ones who can use it.

V. SUMMARY

Even though the anticipated national security threats of the coming decades involve less developed countries, the CVW threat and other methods of intrusion and disruption are not necessarily beyond their reach.

Opportunities to deceive and confuse through an elaborate misinformation scheme along a myriad of information paths are available to anyone. Information Warfare provides a new avenue to employ deception techniques through the use of multiple paths that create the perception and validation of truth. These activities can put new light on Winston Churchill's statement at Tehran in November 1943 concerning Allied deception efforts, "In war-time, truth is so precious that she should always be attended by a bodyguard of lies."[88]

In this vein, General Minihan proposes the prospect of "An intelligence analyst manipulating an adversary's command and control system so that reality is distorted."[89] Consider Marvin Leibstone's projection, "...tomorrow's soldier will depend more than ever on the very well known and trusted factors of mobility and C3I" (Emphasis added).[90] Imagine a scenario depicting a "left hook" in the Iraqi desert that fails because the systems in use were successfully attacked by CVW, or some other intrusion method, with the resulting disruption putting U.S. troops in a flailing posture--facing the unknown and losing confidence in their operation. One thing is sure. An Iraqi "left hook will be difficult to repeat. We have to assume Iraq, and others, will exploit the GPS to their own advantage. Information Warfare is coming of age!

World War II set the stage, but only with today's technology can we expect action in this sphere of warfare on a grand scale. Fortunately, the U.S. military senior leadership is becoming involved, and, in many cases, taking the lead on this perplexing issue. With this emphasis, we must carefully assess the vulnerabilities of the systems we employ. Systems proposals must be

thoroughly evaluated and prioritized by highest value payoff. This needs to accomplished through a more balanced investment strategy by the U.S. military that conquers our institutional prejudices that favor "killer systems" weapons.[91] Offensive systems will be at risk if we do not apply sufficient defensive considerations in this process.

"The electromagnetic spectrum will be our 'Achilles heel' if we do not pay sufficient attention to protecting our use of the spectrum and at the same time recognize that we must take away the enemy's ability to see us and to control his forces.[92] We must also interdict the opportunities for adversaries to intrude on our systems. Other nations have realized the value of offensive applications of information warfare; therefore, we must attack the issue from two directions, offensively and defensively, with almost equal accentuation.

Information Warfare adds a fourth dimension of warfare to those of air, land, and sea. When the Soviets developed a nuclear program after World War II, the U.S. was caught by surprise. In this new dimension, We must stay ahead.

---

[1] Clausewitz, Carl Von. On War. Princeton University Press, Princeton, NJ. 1984. Edited and Translated by Michael Howard and Peter Paret. P.84

[2] Sun Tzu, The Art of War, Oxford University Press, New York, NY. 1971. Translated by Samuel B. Griffith. p84.

3"Information Warfare: Pouring the Foundation," (Draft), USAF/XO, 19 Dec 94, p.i.

[4] Ibid. p.3.

[5] Toffler, Alvin and Heidi, War and Anti-War: Survival at the Dawn of the 21st Century, Little, Brown, and Company, New York, NY. 1993. p. 140.

[6] Ibid. p.139.

[7] Johnson, Craig L., "Information Warfare--Not a Paper War, Journal of Electronic Defense, Vol 17, No 8, Aug 94, p.56.

[8] Ibid.

[9] Petersen, John H., "Info Wars," Naval Institute Proceedings, Vol 119, May 93,p.85

[10] Calvocoressi, Peter, Top Secret Ultra, (New York: Pantheon Books, 1980), p. 3.

[11] Clausewitz, p. 191.

[12] Mendelsohn, John, ed., Covert Warfare: Intelligence, Counterintelligence, and Military Deception During the World War II Era, Volume 18, (New York: Garland Publishing,Inc., 1989), p. 1. Note: This book is the last in a series of 18 volumes on covert warfare edited by Mendelsohn. The content of the series is primarily composed of declassified documents residing in the National Archives. These documents included classifications up through TOP SECRET ULTRA. The quoted material in this paper from this series is usually taken from the copied material of the original documents.

[13] Griffith, Samuel B., Translator, Sun Tzu: The Art of War, (New York: Oxford University Press, 1963), p.66.
[14] See Montagu, Ewen, The Man Who Never Was, (New York: J.B. Lippincott Company, 1954).
[15] Mendelsohn, Volume 18, Chapter 1, p.1.
[16] Mendelsohn, Volume 1, Ultra Magic and the Allies, Chapter 8, "Origins, Functions, and Problems of the Special Branch, MIS," p.27.
[17] Mendelsohn, Volume 1, Chapter 4, "Synthesis of Experiences in the Use of ULTRA Intelligence by U.S. Army Field Commands in the European Theater of Operations," p.4.
[18] Kozaczuk, Wladyslaw, ENIGMA, (University Publications of America,Inc.,1984),Chapter two.
[19] Kozaczuk, p.20-21.
[20] Kozaczuk, p.95.
[21] Kozaczuk, p.165
[22] Kahn, David, Seizing the ENIGMA: The Race to Break the German U-Boat Codes, 1939-1943, (Boston: Houghton Mifflin Company, 1991), p.184.
[23] Kahn, p.184.
[24] Kahn, p.184.
[25] Kahn, p.184.
[26] Kahn, p.185.
[27] Gilbert, James L. and Ginnegan, John P., eds., U.S. Army Signals Intelligence in World War II: A Documentary History, Center of Military History, United States Army, Washington, D.C., 1993, p.175.
[28] Gilbert, p.175.
[29] Kahn, p.276.
[30] Gilbert, p.176.
[31] Brown, Anthony Cave, Bodyguard of Lies, (New York: Harper & Row, Publishers, 1975), p.2.
[32] Brown, p.50.
[33] Brown, p.45.
[34] Brown, p.2.
[35] Brown, p.2.
[36] Brown, p.2.
[37] Kozaczuk, pp.156-166.
[38] Mendelsohn, Volume 1, Chapter 3, "Use of CX/MSS ULTRA by the U.S. War Department, 1943-1945," p.17.
[39] Bennett, Ralph, Ultra in the West: The Normandy Campaign 1944-45,(New York: Charles Scribner's Sons, 1979), p.viii.
[40] Kahn, p.276.
[41] Bennett, p.42.
[42] Mendelsohn, Vol. 15, Basic Deception and the Normandy Invasion, Chapter 4,"Cover and Deception, Definition and Procedure, Exhibit '3' of C&D Report ETO," pp.1&2.
[43] Mendelsohn, Vol. 15, Chapter 6, "Cover and Deception Recommended Organization, 8 September 1944, Exhibit '5' of C&D Report ETO," p.2.
[44] Mendelsohn, Vol 15, Chapter 10, "Operations in Support of Neptune: (B)FORTITUDE NORTH, 23 February 1944, Exhibit '6' of C&D Report ETO," Appendix 'C' to SHAEF/18216/1/Ops dated 10th March 1944.
[45] Garlinski, Jozef, The Enigma War, (New York: Charles Scribner's Sons, 1980),pp. 159-160. After twice striking "shell-shocked" soldiers, Patton had gotten into trouble. General Eisenhower needed a place to put him, and, knowing the Germans kept track of his finest generals, considered Patton the perfect choice for this notional outfit. In Eisenhower's mind, placing Patton in charge would make this concoction more believable to the Germans.
[46] Brown, p.10. BODYGUARD was the covername given to the deception plan developed for NEPTUNE, the coverterm for the Normandy Invasion. It was taken from Churchill's statement at Tehran, "In wartime, truth is so precious that

she should always be attended by a bodyguard of lies."

[47] Garlinski, p.160.

[48] Mendlesohn, Vol. 15, Chapter 11, "Operations in Support of NEPTUNE: (C) FORTITUDE SOUTH I, Exhibit '6' of C&D Report ETO," Appendix B, part I.

[49] Bennett, p.4.

[50] Putney, Diane T., ed., ULTRA and the Army Air Forces in World War II, Office of Air Force History, United States Air Force, Washington, D.C., 1987, p. 97.

[51] Willmott, H.P., The Great Crusade--A New Complete History of the Second World War, (New York: The Free Press, 1989), pp.108-109.

[52] Kozaczuk, p.166.

[53] Kozaczuk, p.167.

[54] Kozaczuk, p.167.

[55] Putney, p.35. This statement was made by Associate Justice of the Supreme Court Lewis F. Powell, Jr., in an interview conducted by Dr. Richard H. Kohn, chief, Office of Air Force History, and Dr. Diane T. Putney, chief, Air Force Intelligence Service Historical Research Office. During WWII, Justice Powell was one of a select group of people chosen to integrate Ultra information into other intelligence. As an intelligence officer in the Army Air Force, He served with the 319th Bomb Group, Twelfth Air Force, and the Northwest African Air Forces. He was on General Carl Spaatz's United States Strategic Air Forces staff as Chief of Operational Intelligence, as well as being General Spaatz's Ultra officer, towards the end of the war. He made at least one visit to Bletchely Park where he stayed and worked for several weeks.

[56] Jones, David L. And Randt, Richard C., "The JOINT CEOI," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. AFCEA International Press, Fairfax, VA, Oct 1992, p.162.

[57] Anson, Sir Peter, and Cummings, Dennis, "THE FIRST SPACE WAR: The Contribution of Satellites to the Gulf War," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. AFCEA International Press, Fairfax, VA, Oct 1992, p. 121.

[58] Ibid., p.127.

[59] Peterson, p.85.

[60] Anson and Cummings, p.127.

[61] Anson and Cummings, p.130.

[62] Clapper, Jr., James R., "DESERT WAR: Crucible for Intelligence Systems," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992, p.82.

[63] Hopkins, III, Robert S., "Ears of the Storm," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992,p.65.

[64] Keaney, Thomas A. And Cohen, Eliot A., Gulf War Air Power Survey Summary Report, p.40.

[65] Campen, Alan D., "IRAQI COMMAND AND CONTROL: The Information Differential," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992, p.171.

[66] Ibid., p.172.

[67] Ibid., p.174.

[68] Petersen, p.88.

[69] Petersen, p.89.

[70] Petersen, p.86.

[71] Roos, John G., "InfoTech InfoPower, N Armed Forces Journal International, Jun 94, p.31.

[72] "Information Dominance Edges Toward New Conflict Frontier," Signal International Journal, Vol 48, No 12, Aug 94, p.37.

[73] Ops. Cit., Roos, p.31.

[74] 0pS . Cit., Johnson, p.55.
[75] FitzGerald, Mary C., The Impact of the Military-Technical Revolution on Russian Military Affairs: Volume II, Hudson Institute, Submitted in partial fulfillment of Contract #MDA903-91-C-0190, HI-4209, 20 August 1993, p.98.
[76] Ibid. p.100.
[77] Ibid. p.100.
[78] Ibid. p.100
[79] Lichty, Tom, The Official America Online for Windows Tour Guide, 2nd Ed., ver 2, p.325.
[80] Newsweek, 20 Feb 1995, p.12.
[81] Peterson, p.89.
[82] Army Times 54 No 43, 23 May 1994, p.28.
[83] Baltimore Sun, 9 Jan 1995, p.3.
[84] Evancoe, Paul and Bentley, Mark, "CVW--Computer Virus as a Weapon," Military Technology, Vol XVIII, No 5, May 94, p.40
[85] ops. Cit., Petersen, p.90
[86] Gehly, Darryl, "Controlling the Battlefield," Journal of Electronic Defense, Vol 6, No 6, Jun 93, p.48
[87] Ross, General Jimmy D., "Winning the Information War," Army, Feb 94, p. 32
[88] Brown, p.l0
[89] "Information Dominance Edges Toward New Conflict Frontier," Signal, Vol 48, No 12, Aug 94, p.39
[90] Leibstone, Marvin, "Next-Generation Soldier: Ditched, or Digitized?," Military Technology, Vol XVIII, No 7, July 94, p.59
[91] "Army Plan Fosters Dynamic Information War Framework," Signal International Journal, Vol 48, No 3, Nov 93, p.56
[92] Ops. Cit., Ross, p.28

BIBLIOGRAPHY

Anson, Sir Peter, and Cummings, Dennis, "THE FIRST SPACE WAR: The Contribution of Satellites to the Gulf War," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. AFCEA International Press, Fairfax, VA, Oct 1992.

"Army Plan Fosters Dynamic Information War Framework," *Signal International Journal,* Vol 48, No 3, Nov 93.

Bennett, Ralph, Ultra in the West: The Normandy Campaign 1944-45, (New York: Charles Scribner's Sons, 1979).

Brown, Anthony Cave, Bodyguard of Lies, (New York: Harper & Row, Publishers, 1975).

Calvocoressi, Peter, Top Secret Ultra, (New York: Pantheon Books, 1980).

Campen, Alan D., "IRAQI COMMAND AND CONTROL: The Information Differential," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992.

Clapper, Jr., James R., "DESERT WAR: Crucible for Intelligence Systems," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992.

Clausewitz, Carl Von. On War. Princeton University Press, Princeton, NJ. 1984. Edited and Translated by Michael Howard and Peter Paret.

Evancoe, Paul and Bentley, Mark, "CVW--Computer Virus as a Weapon," *Military Technology,* Vol XVIII, No 5, May 94.

FitzGerald, Mary C., The Impact of the Military-Technical Revolution on Russian Military Affairs: Volume II, Hudson Institute, Submitted in partial fulfillment of Contract #MDA903-91-C-0190, HI-4209, 20 August 1993.

Garlinski, Jozef, The Enigma War, (New York: Charles Scribner's Sons, 1980).

Gehly, Darryl, "Controlling the Battlefield," *Journal of Electronic Defense,* Vol 6, No 6, Jun 93.

Gilbert, James L. and Ginnegan, John P., eds., U.S. Army Signals Intelligence in World War II: A Documentary History, Center of Military History, United States Army, Washington, D.C., 1993.

Griffith, Samuel B., Translator, Sun Tzu: The Art of War, (New York: Oxford University Press, 1963).

Hopkins, III, Robert S., "Ears of the Storm," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War, AFCEA International Press, Fairfax, VA, Oct 1992.

"Information Dominance Edges Toward New Conflict Frontier," *Signal,* Vol 48, No 12, Aug 94.

"Information Warfare: Pouring the Foundation' (Draft), USAF/XO, 19 Dec 94.

Johnson, Craig L., "Information Warfare--Not a Paper War, *Journal of Electronic Defense,* Vol 17, No 8, Aug 94.

Jones, David L. And Randt, Richard C., "The JOINT CEOI," The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War. AFCEA International Press, Fairfax, VA, Oct 1992.

Kahn, David, Seizing the ENIGMA: The Race to Break the German U-Boat Codes, 1939-1943, (Boston: Houghton Mifflin Company, 1991).

Keaney, Thomas A. And Cohen, Eliot A., Gulf War Air Power Survey Summary Report.

Kozaczuk, Wladyslaw, ENIGMA, (University Publications of America,Inc., 1984).

Leibstone, Marvin, "Next-Generation Soldier: Ditched, or Digitized?," *Military Technology, Vo* l XVIII, No 7, July 94.

Montagu, Ewen, The Man Who Never Was, (New York: J.B. Lippincott Company, 1954).

Petersen, John H., "Info Wars," *Naval Institute Proceedings,* Vol 119, May 93.

Putney, Diane T., ed., ULTRA and the Army Air Forces in World War II, Office of Air Force History, United States Air Force, Washington, D.C., 1987.

Roos, John G., "InfoTech InfoPower," *Armed Forces Journal International,* Jun 94.

Ross, General Jimmy D., "Winning the Information War," *Army,* Feb 94.

Toffler, Alvin and Heidi, War and Anti-War: Survival at the Dawn of the 21st Century, Little, Brown, and Company, New York, NY. 1993.

Willmott, H.P., The Great Crusade--A New Complete History of the Second World War, (New York: The Free Press, 1989).

03 Sept 97