T.C

YEDİTEPE UNIVERSITY

GRADUATE INSTITUTE OF SOCIAL SCIENCES

THE IMPACT OF THE ELECTRONIC INTELLIGENCE –ELINT- IN THE FUTURE BATTLEFIELD

by

Mustafa KAYAR

Supervisor

Assoc. Prof. Dr. Mesut Hakkı CAŞIN

Submitted to the Graduate Institute of Social Sciences
In partial fulfillment of the requirements for the degree of
Master of
Business Administration

ISTANBUL, 2004

THE IMPACT OF THE ELECTRONIC INTELLIGENCE -ELINT- IN THE FUTURE BATTLEFIELD

by

Mustafa KAYAR

Approved by:

Assoc. Prof. Dr. Mesut Hakkı CAŞIN : ....
(Supervisor)

Assoc. Prof. Dr. Ali Fuat BOROVALI : ....

Asst. Prof. Dr. Mehmet YAHYAGİL : ....

Date of Approval by the Administrative Council of the Institute 01.03./2004

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AAA : Anti-Aircraft Artillery
AAW : Anti-Air Warfare
ABCCC : Airborne Battlefield Command and Control Center
ACTD : Advanced Concept Technology Demonstrations
AEHF : Advanced Extreme High Frequency
AFB : Air Force Base
AFRL : Air Force Research Laboratory
AOC : Air Operation Center
ARPA : Advance Research Projects Agency
ASAT : Anti-Satellite
ATR : Automatic Target Recognition
AWACS : Airborne Warning and Control System
AWS : Advanced Wideband Satellite
C^2 : Command and Control
C^2W : Command and Control Warfare
C^3 : Command, Control, Communications
C^4I : Command, Control, Communications, Computers And Intelligence
C^4ISR : Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAP : Combat Air Patrol
CGS : Common Ground Segment
CIS : Communications and Information Systems
COMINT : Communications Intelligence
CONOPS : Concept of Operations
CONV HAE : Conventional High Altitude Endurance
DARO : Defense Airborne Reconnaissance Office
DARPA : Defense Advance Research Projects Agency
DBA : Dominant Battlefield Awareness
DF : Direction Finding
DMSP : Defense Meteorological Satellite Program
DOD : Department of Defense
DSCS : Defence Satellite Communications System
DSP : Defense Support Program
EA : Electronic Attack
ECCM : Electronic Counter-Counter Measures
ECM : Electronic Countermeasures
EIW : Economic Information Warfare
ELINT : Electronic Intelligence
EO : Electro-Optical
EO/IR : Electro-Optical/Infrared
EOB : Electronic Order of Battle
EP : Electronic Protection
EPDS : Electronic Processing and Dissemination System

ER	: Electronic Reconnaissance
ES	: Electronic Support
EW	: Electronic Warfare
EWIS	: Electronic Warfare Integrated System
FEAF	: Far East Air Force
GCS	: Ground Control Station/Segment
GPS	: Global Positioning System
GRAB	: Galactic Radiation Background Experiment
HAE	: High Altitude Endurance
IBW	: Intelligence Based Warfare
IMINT	: Imagery Intelligence
IOSA	: Integrated Overhead SIGINT Architecture
IR	: Infrared
ISR	: Intelligence, Surveillance and Reconnaissance
ITEC	: Information, Technology, Electronics and Communications
IW	: Information Warfare
JDAM	: Joint Direct Attack Munitions
JSTARS	: Joint Surveillance Target Attack Radar System
JTF	: Joint Task Force
LIDAR	: Light-Detection and Ranging
MAV	: Micro Air Vehicle
NATO	: North Atlantic Treaty Organization
NRO	: National Reconnaissance Office
OEF	: Operation Enduring Freedom
OIF	: Operation Iraqi Freedom
OODA	: Observe, Orient, Decide, and Act
PACAF	: Pacific Air Force
PHOTINT	: Photographic Intelligence
PLGRs	: Precision Lightweight GPS Receivers
PSYOPS	: Psychological Operations
PSYW	: Psychological Warfare
R&D	: Research and Development
RAF	: Royal Air Force
RISTA	: Reconnaissance, Intelligence, Surveillance, and Target Acquisition
RSTA	: Reconnaissance, Surveillance, and Target Acquisition
SAC	: Strategic Air Command
SAM	: Surface-To-Air Missile
SAR	: Synthetic Aperture Radar
SATCOM	: Satellite Communications
SBIRS	: Space-Based Infrared System
SBL	: Space Based Laser
SBR	: Space Based Radar
SEAD	: Suppression Of Enemy Air Defenses
SIGINT	: Signals Intelligence
SLAR	: Side Looking Airborne Radar

SLEP	: Service Life Enhancement Program
SOF	: Special Operation Force
TAC	: Tactical Air Command
TUAV	: Tactical Unmanned Aerial Vehicle
UAV	: Unmanned Aerial Vehicle
UCAV	: Uninhabited Combat Aerial Vehicle
UFO	: Ultra–High Frequency Follow–on
UGV	: Unmanned Ground Vehicle
UHF	: Ultra-High Frequency
US	: United States
USAF	: United States Air Force
USCENTCOM	: United States Central Command
VHF	: Very High Frequency
WGS	: Wideband Gapfiller Satellites
WWII	: World War II

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my supervisor **Associated Prof. Dr. Mesut Hakkı Caşın** for his invaluable comments, his advices and help throughout my study. His knowledge and guiding insights into strategic studies have provided me a new sound perspective. It was a great honor for me to study with him.

I would thank to **Associated Prof. Dr. Abdülkadir Varoğlu (Colonel, War College)** for giving the opportunity to study in Yeditepe University in the context of institutional framework (Turkish Armed Forces).

I want to thank Mr. **Bedrettin Dalan**, the founder of the university, for his services to the Atatürk's Turkish youth, establishing opportunities in such a marvelous university with its precious academic personnel, contemporary educational system and modern buildings.

I would like to express my best regards to the **Prof. Dr. Doğan Altuner**, the Dean of Yeditepe University Graduate School of Social Sciences, for his support throughout the Master of Business Administrative (MBA), and to the **Ret. Maj. Gen. Rıza Küçükoğlu**, the Secretary General of Yeditepe University, for his help.

I would like to thank all academic members of the University, especially **Prof. Dr. Erhan Adal, Asst. Prof. Gaye Gencer, Asst. Prof. Tuba Dumlu, Asst. Prof. Çetin Kaya, Nilgün Bilsel, Ali Bahçuvan, Cahit Yılmaz, Orlando Calumeno** for sharing their knowledge.

I also would like to express my best regards to Turkish Nation, Command of the Turkish Land Forces, Command of the Land Forces Academy, and Command of the Infantry School for providing this chance to attend the master of business administration program and improve myself. I believe that, as Atatürk has targeted, our nation will go beyond the level of contemporary nations with these well-educated personnel.

February 2004, Mustafa KAYAR

ABSTRACT

Electronic technology has come to play an increasingly important role in military operations. To need information about enemy will be integral to any future conflict. Simply information warfare will dominate future war. Command and control warfare (C^2W) and electronic warfare (EW) are the core of information warfare. Electronic warfare in its broadest sense goes far beyond electronic intelligence (ELINT). Satellites, aircrafts, unmanned aerial vehicles, ships, and land vehicles are used as a platform for electronic intelligence.

In order to be effective at future war, intelligence must be integrated the tactical, operational, and strategic levels and used as part of campaign planning. Mutually supportive, intelligence enhances C^2W effects against enemy. The intelligence must be timely to support the current mission. Out of date or inaccurate data could lead to disaster for the commander's overall mission. Electronic intelligence (ELINT) sensors provide accurate and timely intelligence for the commanders.

The implementation of information technology is essential to provide the automation necessary to transfer, process, and store the large volumes of data on the future battlefield. Electronic intelligence (ELINT) will play a significant role in the support developed to allow commanders to plan and maneuver faster than an adversary. Signal intelligence (SIGINT) and electronic intelligence (ELINT) sensors enable target detection and accurate location, on a large scale, in a short time.

Airborne, ship-based, and land-based ELINT are currently used. The development of space-based and unmanned aerial vehicles electronic intelligence (ELINT) systems will be more affect the future battlefield. Other sensor platforms will continue to be used.

New technology will offer the potential to achieve military objectives in different ways and indeed provide means to do completely new things. Maintaining close collaboration with allied partners, and with the civil sector, will be vital in order to maximize the achievement of the objectives and maintain a technological lead over potential adversaries whilst minimizing costs.

ÖZET

Askeri operasyonlarda, elektronik teknolojinin önemi gittikçe artmaktadır. Çıkacak herhangi bir sorunda düşman hakkında bilgi elde etmek çok önemlidir. Basitçe gelecek savaşlarda bilgi belirleyici rol oynayacaktır. Komuta-kontrol savaşı ve elektronik savaş bilgi savaşlarının en önemli kısmını teşkil etmektedir. Elektronik savaşın en geniş anlamda uygulanmasında elektronik istihbarat gittikçe artan oranda rol üstlenmektedir. Uydular, insansız hava araçları, gemiler, uçaklar ve kara araçları elektronik istihbarat için platform olarak kullanılmaktadır.

Gelecek savaşlarda etkin olabilmek için taktik, operatif ve stratejik seviyedeki planlamalarda istihbarat etkin kullanılmalıdır. Düşmana karşı etkili komuta-kontrol için istihbarat çok önemlidir. Vazifenin ifası için zamanında sağlanan istihbarat inisiyatif kazandırır. Zamanı geçmiş ve doğru olmayan bilgi komutanın vazifesini yapmasına engel teşkil eder. Elektronik istihbarat sensörleri komutana doğru ve zamanında bilgi sağlarlar.

Gelecek savaşlarda bilginin transferi, işlenmesi ve depolanması için bilgi teknolojilerinin otomasyonunun sağlanması zorunludur. Elektronik istihbarat komutana düşmanlarından daha hızlı planlama ve manevra yapabilmesi için önemli bir rol oynayacaktır. Muhabere ve elektronik istihbarat sensörleri hedefin çok kısa sürede doğru tespitini yapacaklardır.

Hava, deniz ve karadan elektronik istihbarat hala kullanılmaktadır. Gelişmekte olan uydu ve insansız hava araçları üzerinden elektronik istihbarat faaliyetleri ise gelecek savaş ortamında daha etkili olacaklardır. Diğer elektronik istihbarat platformları da geliştirilerek kullanılmaya devam edilecektir.

Askeri hedeflere ulaşabilmek için ileri teknolojik gelişmeler çeşitli farklılıklar sunmaktadır. Müttefiklerle ve sivil sektör ile sıkı işbirliği içerisinde bulunmak, askeri harcamaların en alt seviyede tutularak hedeflere ulaşmanın en üst düzeyde gerçekleşebilmesi ve potansiyel düşmanlara karşı üstünlük sağlanabilmesi için hayati öneme sahiptir.

"In God we trust, all others we monitor."
-ELINT intercept operator's motto.

1. INTRODUCTION

With the passing of time, electronic technology has come to play an increasingly important role in military operations. The electronic era, and with it the first steps in the introduction of electronics into weapons, goes back to the time when radio and the radio direction finder were first used to give the platform position. The second step was the introduction of radar for the detection, and location in angle and in range, of hostile platforms, and its subsequent use to increase the accuracy of artillery. The last step, and probably the most lethal one, has been the use of electronic devices for precision guidance of missiles.

The effectiveness of electronically guided weapon systems, expressed in terms of kill probability, has risen to values very close to unity, thus leaving undefended targets little hope of escape. Consequently, almost all effective weapons now employ electronic guidance devices.[1]

The enduring lesson from recent conflicts since the Gulf War is that what can be seen can be hit, and what can be hit can be killed. The function of "seeing" is now much more sophisticated and entails electronic, optical, and acoustic ELINT sensors that can have global coverage. These sensors can be linked in real time to computer-controlled weapon systems with unparalleled accuracy and lethality.[2]

The fruitfulness of countermeasure techniques has quickly become apparent. They have been developed to the point that they can seriously degrade the performance of nearly all weapon systems. The inevitable next step has been the development of counter-countermeasures to try to restore the original effectiveness of the weapon sensors.

The techniques and technologies that lead to the construction of devices capable of electronically countering a weapon system, and to the development of counter-countermeasures, go under the name "electronic warfare". However, given the basic harmlessness of these electronic systems ("Electrons don't make holes", at least as long as

[1] Neri, Flippo, "Introduction to Electronic Defense Systems", Artech House, Boston, 1991, p. 1-2.
[2] Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001, p. 16-17.

no directed-energy weapons are available), the name "electronic defense" seems more appropriate[3].

However, this is not enough. The decisive advantage on the modern battlefield will go to the commander who can gather and exploit information most effectively. While this is greatly assisted by the technologies associated with the information revolution, the human element is arguably the most significant. For example if computers and communications systems are used to reinforce hierarchical information flows –and therefore perpetuate the information overloads and bottlenecks –it is the fault of humans, not technology.[4]

Commanders of the past have adopted most of their practices because the technology available simply did not allow them to do more. The information revolution will change that. Commanders can have unparalleled information available to them; they can see the full extent of the battlefield, even if spans the globe. Careful thought must now be given to what practices are the most efficient. Just because it can be done, does not mean that it should.

1.1. DEFINITION OF THE PROBLEM

ELINT is almost as old as man's attempts to use radio signals. But especially when the United States (US) and Soviet Union stood astride the globe eyeing each other warily, the development of strategic reconnaissance/ELINT satellites, aircrafts, and UAVs were seen easily, except for their key role in the political area at the time two superpowers brought the world on the brink of war. In the first place, ELINT has been unveiled the secret roles and impacts of military revolution. With grounding this phenomenon, this research aims the development of ELINT concomitant with the military perspective. More importantly, it has been suggested that ELINT have such an important position that seriously affect the future battlefield.

After the cold war ended in 1991, the technology has improved quickly. So, the first Gulf War has heralded the uncertain nature of the future battlefield and the integrated role of ELINT activity on platform of space, UAV, and aircraft systems.

---

[3] Neri, Flippo, "Introduction to Electronic Defense Systems", Artech House, Boston, 1991, p. 1-3.

1.2. OBJECTIVES OF THE STUDY

A descriptive study is committed in order to determine the common characteristics of the ELINT and to assess the impacts of the ELINT by analyzing the means, usage and its platforms like as satellites, aircraft, and UAVs.

The main objective of the study is to clarify the impact of the ELINT on the future battlefield. The other objective is to build up an essential base for future studies.

1.3. SCOPE OF THE STUDY

The main scope of this study is search for the characteristics of the ELINT and its impacts on the future battlefield. However, in order to determine their mentioned role, this study begins with the digitized battlefield of future's war platform. In order to portray the future battlefield, American and other foresight studies of the future battlefield are examined. While doing so, the emphasis is given to the technological priorities determined. As it is a new dimension of war and one of the most important factors in future information or net-centric war, space and unmanned air vehicles are also examined as a part of the study.

The project report starts with an introductory chapter to draw the framework of the study.

Chapter 2 is about the definition and the characteristics of the future digitized battlefield. The chapter begins with the definition of future war, and information revolution. Information warfare, Network-centric warfare, Command, control system, Parallel war, Intelligence-based warfare, technological dimension on the future battlefield, dominate battlefield awareness, future weapons system, military advanced in information technology, and how the information technology effect the military operations are explained in this chapter.

Chapter 3 presents the electronic warfare and electronic intelligence. This chapter has brief history of electronic warfare and electronic intelligence especially from dawn of radio signals to now on. Subsequently, at the end of World War II, the United States and the Soviet Union stood astride the globe eyeing each other warily. They, of all the combatants,

---

[4] Allard, C., "Command, Control, and the Common Defense", Yale University Press, New Haven, U.S.A., 1990, p. 263-264.

had emerged stronger than when they entered the war. They alone had the power to shape the postwar world. This inevitably brought the two superpowers increasingly into conflict which also caused them to leap to develop new technological breakthrough – ELINT capabilities.

Chapter 4 presents a brief summary of the characteristics of radar, and their contributions to the conduct of war are analyzed in detail. This chapter also focuses on the vulnerability of radar and on the future trends.

Chapter 5 firstly presents definitions of ELINT satellites, battlespace dominance and surveillance, and space surveillance network sensors. After brushing upon the basic features of a satellite, the development of the U.S. ELINT satellites and successively the Soviet ELINT satellites is examined. Future US space ELINT program like GPS, meteorological satellites, defense support program, MILSTAR, on land spy satellites, micro and nano ELINT satellites, and areas for future progress are analyzed in detail.

Chapter 6 presents definitions of unmanned aerial vehicles, and historical development. US Navy's UAV program, US Air Force UAV program, Strikestar UAV as a force multiplier, integration of space-based ELINT systems and UAV, uninhabitet combat aerial vehicles, micro unmanned aerial vehicles, and next generation of UAV are analyzed in detail.

Chapter 7 presents relation with Air Force and ELINT, air Force C^4ISR resources and requirements, theater air control system, air operation center, control and reporting center, airborne warning and control system, airborne battlefield command and control center, Air Force radar (ELINT) system and River Joint, Airspace control and integration with air operations, friendly and enemy combat identification, and Operation Iraqi Freedom and development of Air Force ELINT.

Chapter 8 presents relation with Navy and ELINT, command and control on Navy forces, importance of information network, operational capabilities enabled by information technology, networked specific emitter identification, automatic target recognition and ELINT sensors, radar technologies for future naval warfare, and US Navy's unmanned aerial vehicles program and ELINT.

Chapter 9 presents relation with Army and ELINT, modernization and ELINT, Army C4I system, providing operational intelligence for the warfighter, GENESIS II and Digital Bridge, Land warrior system, the warfighter information network tactical, and Army ELINT satellites and UAV.

1.4. METHODOLOGY

In the first step, all interested areas have been selected, and program planned with time diagram. In the second step, in order to reach required information, literature review, internet survey and interview with signal commanders in the Land Force has been used. Many books, articles and military magazines have been examined to determine the characteristics of ELINT, Future War, Radars, Satellites, UAVs, Aircraft and Land-based systems and their impact on future battlefield.

While analyzing, as the United States ELINT capabilities are given on the conceptual approaches that are obtained by utilizing existing and uncovered academic resources. By taking into consideration the rational and objective methodological criterion in the study, the possible parameters belonging to the ELINT and the ELINT platforms like satellites etc. are tried to be uncovered. As in all of the scientific studies, there may be some deficiencies in this study but we hope that it will be very helpful to the future academicians.

In the third step, this thesis is prepared and in the last step, although there may be some deficiencies in this academic study like in all of the studies, is presented to the future academicians. I hope that it will be helpful to all researchers.

2. THE FUTURE'S WARS PLATFORM: DIGITIZED BATTLEFIELD

Technology has always pioneered the creation of new concepts, and the improvement of strategies presented new battle techniques and tactics. So, as the interaction between technology and strategy makes the unbelievable developments continuous, it also shapes up the important principles of the international foreign policy targets and preservation of peace.[5] Throughout history, technological, political, and social advances have caused profound shifts in military doctrine, organization, strategy, and tactics. In recent history, six revolutions in military affairs have radically altered the conduct and character of war. The first five were;[6]

- The institution of universal military obligation (the French Revolution of 1978),
- The Industrial Revolution of the mid-nineteenth century,
- The managerial revolution of the late nineteenth century,
- The mechanized revolution occurring between 1919-1939,
- And the scientific revolution that followed shortly afterwards, culminating in the production of the atomic bomb.

Even before the Cold War ended, the Army was realizing that the information revolution promised potentially radical improvements in the effectiveness of ground forces, as well as significant changes in their organization.[7] Then, in the early 1970s, the introduction -an *information revolution* centered on the concept that the dominant factor in war is the ability to collect, analyze, disseminate, and act upon battlefield information.[8]

The Soviet Union first called attention to this issue in the 1970s with discussion in military journals of what it called the *military technical revolution*. By the 1980s, the label had been altered in the United States to the *revolution in military affairs*, but the core theme

[5] Caşın, M. Hakkı, "Digital Revolution for the Military: The Effects of the Electronics Revolution in the 21st Century on the International Security Strategy", Armed Forces Communications and Electronics Association, AFCEA, Ankara, September 1995, p.6-7.
[6] Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001, p. 2.
[7] Nardulli, Bruce R. and Thomas L. McNaugher, "Transforming America's Military - The Army: Toward the Objective Force", Ed. Hans Binnendijk, NDU, U.S.A., June 2002, p. 51-52.
[8] Reimer, D. "Foreword - War in the Information Age: New Challenges for U.S. Security Policy", Ed.R.Pfaltzgraff and R.Shultz, Brassey's, Washington D.C., U.S.A., 1997.

remained the same: given what the information revolution was doing to commercial firms, surely it could work radical change in military forces.[9]

These advances in technology have produced an environment on the modern battlefield that is characterized by continuous, 24-hour action; increased volume, lethality, range, and precision of fire; smaller more effective units due to better integration of technology; a disjunction between greater dispersion of more mobile, faster units and an increased tendency for combat in built-up areas with congestion of forces in short ranges; and a further dichotomy between greater invisibility, due to dispersion and speed, and increased risk of detection, due to larger numbers of more capable battlefield sensors.

Arguably, therefore, the most significant technological revolution in warfare will be in the role of information and knowledge, and, in particular, in the degree of situational awareness made possible by the increasing number of communications and information systems supporting combat forces. However, not all armies will be able (or will choose) to take advantage of this revolution, and today's Information Age army must be prepared to deal with broad spectrum of threats from Agrarian, Industrial, and Information Age adversaries.[10]

The information revolution, with the associated provision of information technology, favors networks rather than hierarchies; it diffuses and redistributes power; it crosses borders and redraws boundaries of offices and responsibilities; and it expands horizons. This is particularly true in the civilian environment, where organizations have become more democratic in information distribution and have realized considerable efficiencies.[11]

The network form is very different from the institutional form. While institutions (large ones in particular) are traditionally built around hierarchies and aim to act on their own, multi-organizational networks consist of (often small) organizations or parts of institutions that have linked together to act jointly. The information revolution favors the growth of such networks by making it possible for diverse, dispersed actors to communicate, consult,

---

[9] Nardulli, Bruce R. and Thomas L. McNaugher, Ibid, p. 51-52.
[10] Toffler, A., and H. Toffler, "War and Anti-War: Survival at the Dawn of the 21st Century", Little Brown, Boston, MA, U.S.A., 1993.
[11] Toffler Alvin, "Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century", Bantam Books, New York, U.S.A., 1990.

coordinate, and operate together across greater distances and on the basis of more and better information than ever before.[12]

The information revolution is a harbinger of notable changes in the conduct of war. As Martin van Creveld said in *Command in War*, "The history of command can thus be understood in terms of a race between the demand for information and the ability of command systems to meet it." The revolution in military affairs surrounding information dominance is as important and vital as the advent of steam propulsion, the radio, radar, the tank, or the airplane.[13] For warfare, the major lesson from the commercial world is that in the Information Age conflict will largely be about knowledge and mastery of the network and networked organizations will provide major advantage in conflict. However, these concepts can be an anathema to military commanders who tend to see command and information (and even communications in many armies) following the same hierarchical lines. In a nonhierarchical, network model, command and information flow must necessarily diverge. Sensors, commanders, and weapon systems are connected via a networked grid that ensures that situational awareness data can be shared by all elements, regardless of whether they belong to the same unit. Command lines need no network; command and control are directed in accordance with the order of battle. Therefore, the adoption of these new technologies will not only significantly affect the way armies are commanded and controlled, but it will also change the way they are organized and trained.[14]

Leveraging technology to dominate information, and to put that information where it is needed when it is needed, will be a significant force multiplier. Likewise, gaining complete access to needed information--and validating that information--will limit misinformation, enhance the opportunity for peace, and provide the basis for success in battle and speedy resolutions to crises.[15]

---

[12] Arquilla, J., and D. Ronvelt, "Cyberwar Is Coming!", Rand, Santa Monica, California, U.S.A., 1992, p.3-4.
[13] Atkins, Robert L., Duane A. Lamb, Marlene L. Barger, Larry N. Adair, and Michael J. Tiernan, "2025 In-Time Information Integration System (I3S)", U.S. Air Force, April 1996, p. 9, Available on site: http://www.au.af.mil/au/2025/volume1
[14] Frater, Michael R., and Michael Ryan, Ibid, p. 2.
[15] Atkins, Robert L., et al., Ibid., p. 7.

Modern armed forces must be able to defeat adversaries across a wide range of operations such as conventional warfighting, peace enforcement, peacekeeping, counterterrorism, humanitarian assistance, and civil support.

A key component of full-spectrum dominance is *information superiority* –the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority can therefore be defined as that degree of dominance in the information domain which permits the conduct of operations without effective opposition. Superior information is to be converted to superior knowledge which, when combined with organizational and doctrinal adaptation, relevant training and experience, and proper command and control mechanisms and tools, is to achieve *decision superiority.* Current capabilities for maneuver, strike, logistics, and protection will become dominant maneuver, precision engagement, focused logistics, and full-dimensional protection.[16]

- *Dominant maneuver:* This defined as the ability of joint forces to gain positional advantage with decisive speed and overwhelming operational tempo in the achievement of assigned military tasks. Widely dispersed joint air, land, sea, amphibious, special operations, and space forces, capable of scaling and massing force or forces and the effects of fire as required for either combat or noncombat operations, will secure advantage across the range of military operations through the application of information, deception, engagement, mobility, and countermobility capabilities.
- *Precision engagement:* This is the ability of joint forces to locate, observe, discern, and track objectives or targets; select, organize, and use the correct systems; generate desired effects; assess results; and reengage with decisive speed and overwhelming operational tempo as required, throughout the full range of military operations.
- *Focused logistic:* This is the ability to provide the joint force the right personnel, equipment, and supplies in the right place, at the right time, and in the right quantity, across the full range of military operations. This will be made possible through real-time, networked information systems providing total asset visibility as part of a common relevant operational picture, effectively linking the operator and logistician across service and support agencies.

[16] Frater, Michael R., and Michael Ryan, Ibid, p. 3.

- *Full-dimensional protection:* This ability of the joint force to protect its personnel and other assets required to decisively execute assigned tasks. Full-dimensional protection is achieved through the tailored selection and application of multilayered active and passive measures, within the domains of air, land, sea, and space, and information across the range of military operations with an acceptable level of risk.

In this sense, the artillery branch, for example, exploits satellites and electronics to use the global positioning system to lay in its artillery pieces and to add speed and precision to aiming artillery tubes. Information technologies have been used to improve the accuracy and rate of fire of the tank.[17]

2.1. INFORMATION WARFARE

The term information warfare is relatively new, but the role that information and information technologies have played in warfare in the more general sense has been crucial almost since the beginning of recorded history.[18] Although information warfare is a newly introduced concept, information has always been a critical factor in war. Clausewitz said 'imperfect knowledge of the situation, can bring military action to a standstill'.[19]

Nearly 2000 years ago, the Romans, striving to secure their borders and mobilize troops quickly, developed some yet undeciphered precursor of Morse Code to send messages via flashing mirrors the entire length of the Empire in a single day. Aerial surveillance (via balloon) combined with telegraphic communication back to a field command center began as early as the Civil War, providing a tactical advantage to the forces commanding the new technology. More recently, and more ominously, the federal government took over the entire US telephone system during World War I based upon military and information security considerations. Even in those times, the notion had arisen that in an age of total war the public networks would be totally involved.

[17] Steele, Dennis, "The Hooah Guide to Army Digitization", Army Magazine, U.S.A., September 2001, p. 19-40.
[18] Sweeney, Dan, "Information Warfare", America's Network Magazine, Vol. 105, Issue 18, U.S.A., 1 December 2001, p. 26.
[19] McLendon, J.W., "Battlefield of Future: Chapter 7, Information Warfare Impacts and Concerns", Air Force Press, Maxwell, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles

Where the present differs from the past is in the way that information technologies, including the public networks, have becomes tools of war instead of merely supporting conventional military operations.[20] Information warfare may be defined as: "actions taken to achieve information superiority by affecting adversary information, information-based process, information systems, and computer-based networks while defending one's own information, information-based process, information systems, and computer-based networks".[21] The more information is central to military proficiency, the greater the ostensible logic of attacking another side's information systems. Even if these information systems remain intact, simply slowing them down or reducing their fidelity can help. An information system, however, is not a simple mechanism but the combination of sensors, networks, processors, command centers, and operators.[22]

It is now widely accepted that military capabilities will be decisive to the extent that the military can enjoy information dominance over its foes extant and potential.[23] Information warfare is emerging as a potent new element of strategy. Information warfare is an attack on an adversary's entire information of military, command and control, and indeed decision-making systems.[24]

Information dominance may be defined as superiority in the generation, manipulation, and use of information sufficient to afford its possessors *military* dominance. But information dominance *per se* is not particularly meaningful, for three reasons. First, unlike air combat, where one air force can keep another one grounded (e.g., Coalition forces in the Gulf War), information power on one side does not prevent its use on the other (with some specialized exceptions such as radio-electronic combat). Second, every side to a conflict has its own requirement for information depending on its strategy, operations, and tactics. A modern (information age) force needs more information just to function than does a pre-modern force. In Somalia, the United States enjoyed information superiority at the tactical level its forces could see objects from great distances. But, its insight at the operational level and

---

[20] Sweeney, Dan, Ibid, p. 26.
[21] U.S. Army field Manual FM 100-6, "Information Operations", August 1996.
[22] Libicki, Martin C., "Information Dominance", National Defense University, U.S.A., November 1997, Available on site: http://www.ndu.edu/inss/strforum/SF132/forum132.html
[23] Libicki, Martin C., Ibid.
[24] Blackwell, J., "Battlefield of Future: Overview: Information Warare Issues", Air Force Press, Maxwell, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles

the political level was inferior to what its adversaries enjoyed. Third, as Sun Tzu observed 2500 years ago, the most important knowledge one can bring to the battlefield is knowledge of self, and second, a corresponding insight of the other side. Human knowledge forges strategy; machine knowledge produces tactics. Poor strategy can rarely be saved by tactical information superiority.[25]

As we look to the future, the growth of information technologies seems limitless. Hardly a day goes by without a breakthrough of some kind in information-related technologies. For this reason, it is likely both any armed forces and their enemy will have information-based systems far more advanced than those currently available. Both of them could have:[26]

- Global satellite networks with voice, data, and imaging capabilities 50 times greater than today (based on advances in data compression, processing, frequency management, miniaturization, and sensors). Although the military will control a limited number, commercial interests will own most platforms.
- Autonomous weapons, enabled by artificial intelligence, automatic target recognition algorithms, and multispectral miniature sensors.
- Sophisticated computer viruses and equally sophisticated encryption protocols.
- Data fusion at rates 10^4 times faster and more accurate than today, based on advances in processing and software.
- Data storage capabilities at 10^3 times greater than today (due to miniaturization).

Because of the advances, an information campaign will be integral to any future conflict. Simply stated, information will dominate future war. Wars will be won by the side that enjoys and can exploit: cheap information while making information expensive for its opponent; accurate information within its own organization while providing or inserting inaccurate data in its opponent's system; near-real-time information while delaying its opponent's information loop; massive amounts of data while restricting data available to its opponent; and pertinent information while filtering out unnecessary data.[27]

---

[25] Libicki, Martin C., Ibid.
[26] Barnett, Jeffery R., "Future War - An Assessment of Aerospace Campaigns in 2010", Air University Press, Maxwell Air Force Base, Alabama, U.S.A., January 1996, p.2.
[27] Barnett, Jeffery R., Ibid, p. 3.

Table 2.1: Information Warfare – What is New, What is effective[28]

FORM	SUBTYPE	IS IT NEW?	EFFECTIVENESS
C²W	Anti-head	Command systems rather than commanders are the target.	New technologies of dispersion and replication suggest that tomorrow's command centers can be protected.
	Anti-neck	Hard wired com munication links matter.	New techniques (e.g., redundancy, efficient error encoding) permit operations under reduced bit flows.
IBW		The cheaper the more can be thrown into a system that looks for targets	The United States will build the first system of seeking systems, but, stealth aside, pays too little attention to hiding.
EW	Anti-radar	Around since WW II	Dispersed generators and collectors will survive attack better than monolithic systems.
	Anti-comms	Around since WW II	Spread spectrum, frequency hopping, and directional antennas all suggest communications will get through.
	Cryptography	Digital code making is now easy.	New code making technologies (DES, PKE) favor code makers over code breakers.
Psychological Warfare	Anti-will	No.	Propaganda must adapt first to CNN, then to Me-TV.
	Anti-troop	No.	Propaganda techniques must adapt to DBS and Me-TV.
	Anti-commander	No.	The basic calculus of deception will still be difficult.
	Kulturkampf	Old history.	Clash of civilizations?
Hacker Warfare		Yes.	All societies are be coming potentially more vulnerable but good house-keeping can secure systems.
Economic Information Warfare	Economic	Yes.	Very few countries are yet that dependent on high-bandwidth information flows.
	Techno-Imperialism	Since the 1970s.	Trade and war involve competition, but trade is not war.
Cyber-Warfare	Info-Terrorism	Dirty linen is dirty linen whether paper or computer files.	The threat may be a good reason for tough privacy laws.
	Semantic	Yes.	Too soon to tell.
	Simula-warfare	Approaching virtual reality.	If both sides are civilized enough to simulate warfare, why would they fight at all?
	Gibson-warfare	Yes.	The stuff of science fiction.

[28] Barnett, Jeffery R., Ibid, p. 3.

Information warfare in its broadest sense goes far beyond electronic communications. The modern information warrior approaches information in a limited number of ways. He gathers information about the enemy, ideally without making his own surveillance techniques known. He then uses that information to enhance his decision-making process and to control automated weapons systems. In addition, he disseminates information to confuse or disable the enemy's own information systems such as radar or satellite surveillance, and to sap enemy morale, a subspecies of infowar known as PSYOPS (for psychological operations).[29]

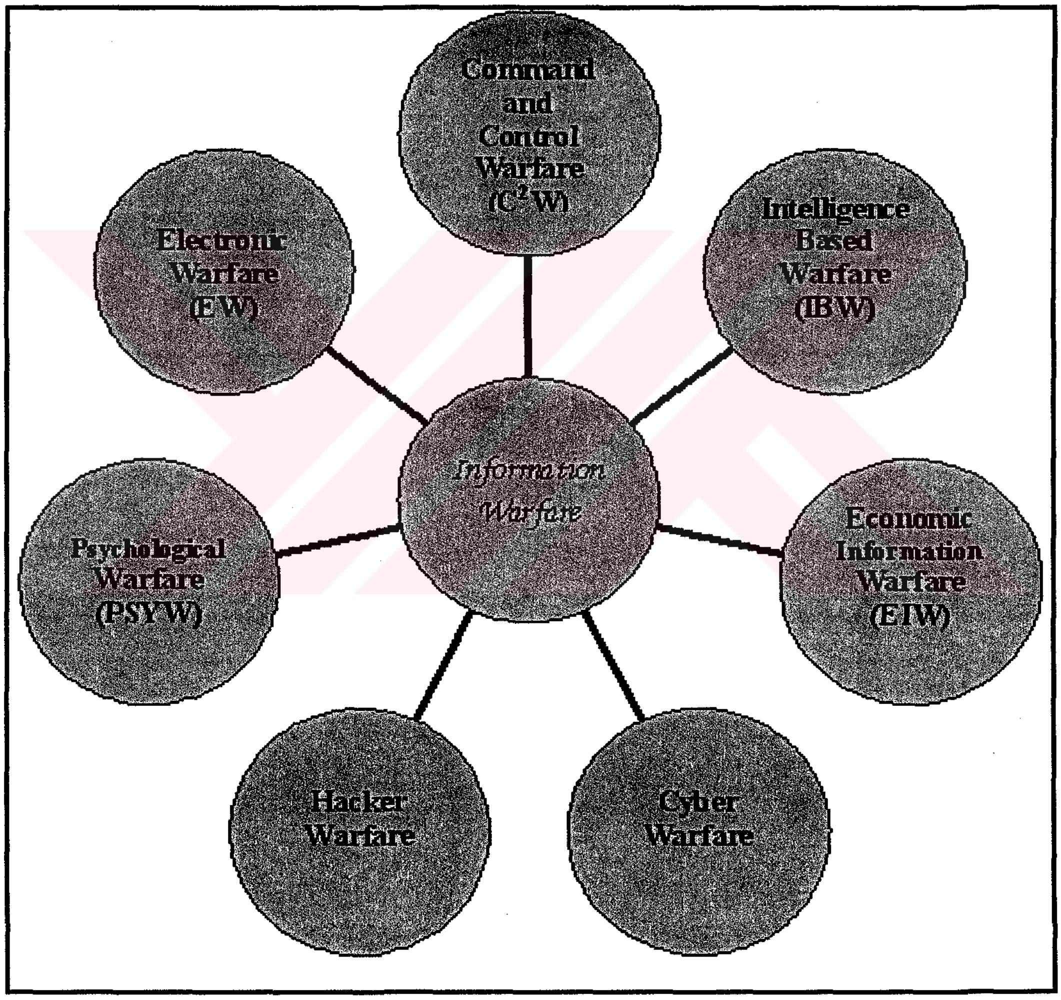


Figure 2.1: Seven Forms of Information Warfare vie for the Position of Central Metaphor.

While the Information Age has produced a revolution in military operations that provides a great promise of decisive advantage on the modern battlefield to the commander who can gather and exploit information most effectively, there is a significant dark side to the

[29] Sweeney, Dan, Ibid, p. 26.

information revolution. As communications and information systems become vital to military and civilian society, they can become major targets in the war and can also serve as a major means for conducting offensive operations. Consequently, the military adoption of information technology creates a new vulnerability –the same information technology that provides the fuel for the networks that support modern commanders also provides the fuel for the major means for their destruction. An increased reliance on communications and information systems increases this vulnerability. So, while automated command systems to increase commanders' situational awareness, they can also be turned against them and used to contribute to their uncertainty.

Movement through the C^2 cycle on the modern battlefield depends heavily on the use of the electromagnetic spectrum; whether for surveillance and target acquisition, passage of information, processing of information, or destruction of adversary forces. This reliance is a vulnerability that must be exploited in attacking adversary command systems, while being protected in own-force systems. Operations to counter the C^2 cycle are generally termed *information warfare (IW),* which is a term that recognizes a range of actions taken during conflict to achieve information superiority over an adversary.[30]

The US does not have a monopoly on this insight. The impact of information technologies on war is well understood abroad. According to one Chinese defense intellectual:[31] "In hi-tech warfare, tactical effectiveness no longer depends on the size of forces or the extent of firepower and motorized forces, but more on the control systems over the war theater and efficiency in utilizing information from the theater. Superiority in numbers and strength no longer plays a decisive role."

Military theorists in Russia hold a similar view. Major General Vladimir I. Slipchenko, the leading Russian military theoretician:[32] "The impending sixth generation of warfare, with its centerpiece of superior data-processing to support precision smart weaponry, will radically change military capabilities and, once again, radically change the character of warfare."

---

[30] Frater, Michael R., and Michael Ryan, Ibid, p. 11.
[31] Barnett, Jeffery R., Ibid, p. 3.
[32] Slipchenko, Vladimir I., "A Russian Analysis of Warfare Leading to the Sixth Generation", Field Artillery, October 1993, p. 38.

Military professionals should feel comfortable envisioning campaigns focused on information. Although an information focus brings new targets and weapons to war, it nevertheless mirrors traditional military concepts in at least six general ways:[33]

1. As with all forms of warfare, information war (IW) will have offensive and defensive aspects. Militaries will both prosecute information war and defend against its use by the enemy.
2. Information war will be conducted at the strategic, operational, and tactical levels of war. Decision makers at each level will orchestrate information campaigns. They'll attack information infrastructures at the national, theater, and unit levels.
3. Information war will both support other military campaigns and operate independently. For example, naval air forces have both independent and supporting missions.
4. Information war will be an imperative for victory. Even as past victories were possible only through supremacy of the air, land, or sea, future victories will be doubtful without information supremacy.
5. Military forces must be capable of operations despite successful enemy IW. Because perfect defenses against IW are an unreasonable expectation, units must continue functioning despite corrupted information.
6. Information war will have distinct mission types. As with conventional military forces, no one type of IW will suffice to describe all its ramifications. For example, just as aerospace power has distinct mission types, IW will have subsets. Table 2.2 illustrates this point in more detail.

Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-networked systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries in cyberspace offers further anonymity. Information warfare is also relatively cheap to wage as compared to conventional warfare. The technology required to mount attacks is relatively simple and ubiquitous. During an information warfare engagement, the demand for information will

[33] Barnett, Jeffery R., Ibid, p. 3-4.

dramatically increase while the capacity of the information infrastructure to provide information may decrease.[34]

Table 2.2: Comparisons between aerospace war and information war

TYPICAL AEROSPACE MISSIONS	ANALOGS IN INFORMATION WAR
Counterair, Counter Space	Counter Information
Strategic Attack	Destroy/Distort National Information Network
Interdiction	Target C^4I Nodes
Close Air Support	Jam
Airlift	Transmit Information to Theater
Air Refueling	Update Databases in Flight
Electronic Combat	Insert Viruses, Corrupt Data
Surveillance & Reconnaissance	Understand Enemy's Information Architecture

The warfighting application of information warfare in military operations is called *command and control warfare* (C^2W). The aim of C^2W is to influence, deny C^2 capabilities against such actions. C^2W therefore comprises two major branches: C^2-attack and C^2-protect.[35]

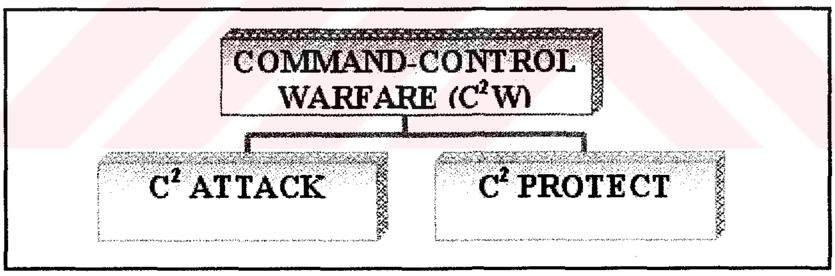


Figure 2.2: C^2W Major Branches

The information warrior relies on many techniques and technologies to collect information. Old-fashioned human intelligence provided by agents on the ground and even gleaned from open sources such as newspapers and broadcasts is still in many cases the best. But human intelligence has been increasingly supplemented by information collected electronically (ELINT and etc.). These means include physical methods such as satellite optical surveillance, on which the US heavily reliant today; radar, the mainstay of military

[34] Defense Science Board, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)", Defense Science Board, Washington, D.C., U.S.A., November 1996. Available on site: http://www.au.af.mil/au/awc/awcgate/infowar
[35] Frater, Michael R., and Michael Ryan, Ibid, p. 11-12.

operations in the field because of the ease with which it can be combined with advanced weapons control systems; infrared sensors, especially useful for detecting concealed troops in the field; satellite interception of microwave over-the-horizon spill, useful for picking up cellular backhaul, but less useful for landline telephony which largely relies on a fiber optic backbone today; stray field emanations from computing equipment, dubbed TEMPEST by the intelligence community; the venerable phone tap; and various means for tapping into optical networks.

Less used techniques include laser doppler acoustical surveillance where conversations can be picked up off of a vibrating structure (such as a window pane) over considerable distances; and small flying robot drones containing acoustical and video sensors and endowed with some measure of artificial intelligence. These are still largely experimental but potentially of enormous significance.[36]

In modern information warfare the public networks are considered just another battlefield to be monitored as assiduously as troop movements on the ground -only in this case, it means scanning traffic at routers and switches as well as along copper and fiber optic cables. Examples of info-war electronic intelligence (ELINT) abound. Satellite cameras feed information to image enhancement and pattern analysis software for resolving images. Radar receivers have their own kind of specific intelligence for rejecting spurious signals. Taps on public networks use sophisticated search engines to isolate text transmissions containing keywords, and speech recognition algorithms to detect such words in continuous speech.[37]

2.2. NETWORK-CENTRIC WARFARE

Recent operations in Afghanistan and Iraq illustrate the kinds of operation we may face in the future. The Americans describe this approach, to which they are giving a very high priority, as *network-centric warfare*. The Gulf War demonstrated how new technologies could be harnessed to produce military effect, with vastly greater speed and precision, at

[36] Sweeney, Dan, "Information Warfare", America's Network Magazine, Vol. 105, Issue 18, U.S.A., 1 December 2001, p. 26.
[37] Sweeney, Dan, Ibid, p. 26.

much reduced direct cost.[38] Perhaps the most useful elaboration of the impact of information technology is the emerging concept of *network-centric warfare.* In the platform-centric warfare, the sensing and engaging capability normally resides on the weapon system (shooter), and there is only a limited capability for the weapon to engage targets because it can only use the situational awareness generated by its own sensor. If a weapon is able to engage a target located by a remote sensor, the passage of weapon data is normally via stovepipe communications systems. (i.e., they connect the single weapon directly to a single sensor). By contrast, in network-centric warfare, sensors and shooters are connected by a ubiquitous network through which weapons can engage targets based on a situational awareness that is shared with other platforms.[39] Network centric capability encompasses the elements required to provide the capability to deliver controlled and precise military effect -rapidly, reliably and at will. At its heart are three elements: ELINT and other sensors (to gather information); a network (to fuse, communicate and exploit the information); and finally strike assets to give military effect to the information.[40] Combat power can therefore be applied with fewer weapons and sensors are interconnected, it does not mean that targets can be engaged randomly or without authority; control is still essential to ensure that targets are engaged in accordance with the operational plan.

While there may continue to be a role for direct links from sensor to shooter (i.e., ELINT sensor to fighter plane), the ultimate aim of network-centric warfare is that the employment of future precision weapons is designed around information. No single sensor has the ability to direct the application of these precision weapons data must be integrated from a number of sensors, and databases.[41] The gathering, processing and distribution of accurate, timely and relevant information to the right user at the right time (whether that be in real time, in seconds or in minutes) will result in a common understanding among commanders at all levels a "shared situational awareness" to lift the "fog of war".[42]

---

[38] Ministry of Defence, "The New Chapter To The Strategic Defence Review: A Progress Report", Speeches & Statements, Secretary of State for Defence, London, U.K., 23 May 2002, Available on site: http://news.mod.uk/news_press_notice.asp
[39] Frater, Michael R., and Michael Ryan, Ibid, p. 4.
[40] Ministry of Defence, Ibid.
[41] Frater, Michael R., and Michael Ryan, Ibid, p. 4-5.
[42] Ministry of Defence, Ibid.

The U.S. Navy's emerging network-centric concept holds that the conjunction of communications, sensors (ELINT etc.), and weapons systems is more important than the individual aircraft, ships, or submarines on which they are deployed. The U.S. Navy's Cooperative Engagement Capability permits many ships (notably their radars and fire control systems) to act as one at Carrier operations in March 1996 off Taiwan.[43]

On the modern battlefield, the network is a considerable force multiplier. Commanders will be unfettered by communications and unconstrained to information centers (command posts). The information network must be ubiquitous across the battle space and must be fluid, flexible, robust, redundant, and real-time; have integrity and security; have access and capacity; and be joint and coalition capable.[44] Developing a networked capability will be fundamental to joint and coalition warfighting in the information age. It offers the potential for dramatic increases in tempo -the ability to decide and act more quickly and with greater agility, control and precision.

It is define network-centric warfare as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared situational awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization".[45]

Figure 2.3 illustrates the three interlocking grids of network-centric warfare (the information grid, the sensor grid, and the engagement grid), and the three major types of participants (sensors, command elements, and shooters). The information grid provides the infrastructure through which information is received, processes, transported, stored, and protected. The sensor grid contains all sensors (including ELINT sensors), whether they are specialized devices mounted on weapons systems, carried by individual soldiers, or embedded into equipment. The engagement grid consists of all available weapons systems that are tasked to create the necessary battlefield effect. Proponents of network-centric

[43] Libicki, Martin C., Ibid.
[44] Frater, Michael R., and Michael Ryan, Ibid, p. 4-5.
[45] Albert, D., J. Gartska, and F. Stein, "Network Centric Warfare", CCRP Publication Series, DoD, Washington D.C., U.S.A., 1999.

warfare envisage that these three grids will exist in space, in the air, on land, and on and under the sea.[46]

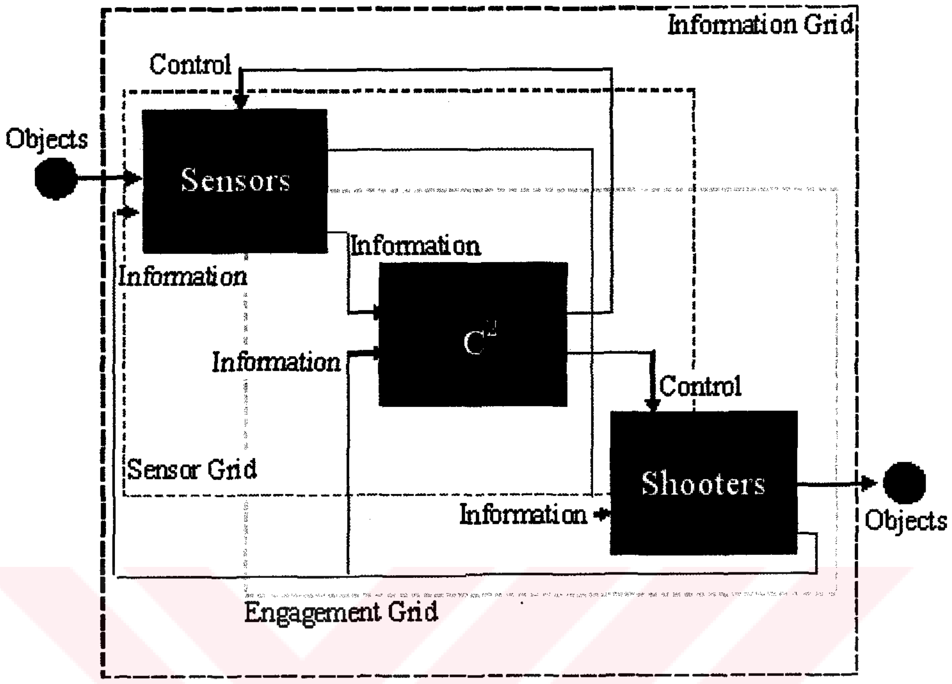


Figure 2.3 The grid arrangement of network-centric warfare.[47]

Compare the frustrations of Gulf War Scud-hunting a decade ago with recent US successes in Afghanistan in coordinating the product of aerial reconnaissance in real time so that decisions could be taken in Tampa and targets attacked with precision munitions in a matter of minutes. Arguably, the United States' ability to:[48]

- maintain constant coverage of a target area in Afghanistan;
- transmit a constant stream of real time imagery back to decision makers;
- and subsequently engage targets by stand-off weapon is the first real example of network centric warfare.

Network-centric warfare is not currently part of military doctrine. However, the concept has considerable merit philosophically and it is most likely that future land warfare will embrace most, if not all, of the above concepts. The employment of tactical network based

[46] Frater, Michael R., and Michael Ryan, Ibid, p. 4-5.
[47] Cebrowski, A., and J. Garstka, "Network-Centric Warfare", CCRP Publication Series, DoD, Washington D.C., U.S.A., 1997.
[48] Ministry of Defence, Ibid.

on wireless, nonnodal communications has the advantage that armies can disperse as required and then mass effects rapidly at an appropriate time and place. Less reliance is required on large information processing centers, which can be distributed to increase physical survivability without sacrificing processing power.[49]

The most significant effect of electronic warfare will be on the ability of a commander to acquire information, prepare and disseminate plans, and then control their execution. This is the business of *command and control* (C^2), which has become increasingly dependent on reliable communications and effective information systems.

The two terms command and control are inextricably linked –command is hollow without an ability to control; control is toothless without the authority of command therefore, the business of commander is most often referred to as command and control (C^2), which can described as the process of and means for exercise of authority of a commander over assigned forces in the accomplishment of the commander's mission. The military doctrine adds that command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.[50]

2.2.1. The Command and Control (C^2) Cycle

Command and control systems are the core of a modern and efficient decision-making process, because the management of crises as well as of military operations poses more and more problems, which extend far beyond the capability of a human decision-maker, whatever his skills. This requirement for tools to manage crises and conduct operations is becoming more acute at all levels of the decision-making chain, in particular at the higher political level, and this for reasons that often have little to do with actual operational requirements.[51] U.S. Department of Defense defines C^2 Warfare as 'the military strategy that implements information warfare on the battlefield and integrates physical destruction.

---

[49] Frater, Michael R., and Michael Ryan, Ibid, p. 5-6.
[50] Frater, Michael R., and Michael Ryan, Ibid, p. 5-6.
[51] Mermet, François, "The Role of European Ground and Air Forces After the Cold War: European Political-Military Analysis and Decision-Making", Ed. Gert de Nooy, Netherlands Institute of International Relations: Clingendael, Netherlands, 1997, p. 37.

Its objective is to decapitate the enemy's command structure from its body of command forces'.[52] The interdependence of various elements of a command system is illustrated by the C^2 cycle shown in Figure 2.4. Although a very simple model, the C^2 cycle is a useful mechanism for developing a framework for the application of command and control at any level. Here it is useful to visualize the impact that communications and information systems have on the modern battlefield.

The C^2 cycle is also called the *decision cycle* for the elements of observation, orientation (understanding), decision and action. While the cycle is continuous, it can be considered to start with surveillance and target acquisition, or observation, from which the commander receives a wide range of information from the many sensors and systems deployed. This information is invariably reported in digital form, and the rapid increase in the number of sensors and surveillance systems is predominantly responsible for the explosion in digital transmission requirements on the modern battlefield. It should be noted that surveillance data can only reach the commander if effective, survivable communications systems are available from the sensor system through to the data processing facilities in the command post.

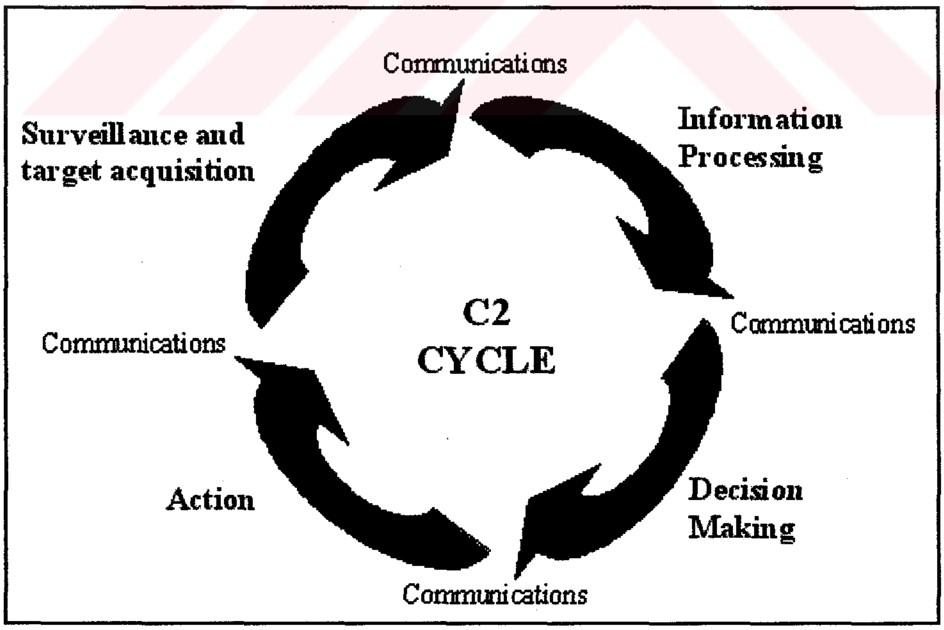


Figure 2.4.: The C^2 cycle.

[52] Waltz, E., "Information Warfare: Principles and Operations", Artech House Inc. London, U.K., 1998, p. 17.

The term battlefield digitization has been adopted to refer to the automation, through digital networks and processes, of command and control operations across the full breadth of the battle space. This integration of ground, air, and space nodes (sensors, communications, command, and weapons nodes) into a seamless digital network requires the fully compatible digital exchange of data and common operating pictures to all nodes. Security, compatibility, and interoperability factors dominate the drive toward full digitization across the entire battle space.[53]

Attacks facilitated by advances in information, C^2, penetration, and precision will occur within the first 24 hours of conflict and continually thereafter. This compressed, broad, and precise attack should leave the opponent paralyzed, unable to either coordinate an effective defense or mount an orchestrated offense. The potential for parallel war will only increase in the future. Information, C^2, penetration, and precision will allow targeting of each target type at the outset of hostilities. Advances in the underlying technologies will multiply the number of targets struck.

The primary problem of command and control is as knowing where one's forces were and secondarily, in what shape.[54] A fighter pilot, posited that conflict was a matter of observing the battlespace, orienting yourself in it, deciding what to do, and doing it (his Observe, Orient, Decide, and Act (OODA loop); those who could run the cycle better and faster would win. *Where* and *when* are the two key attributes of command and control.

The U.S. Air Force's new expeditionary warfare concept seeks the ability to conduct distributed collaborative planning literally across the world even up to the point that the missions of entire air wings could be reprogrammed even as aircraft are warming up for takeoff. Other initiatives, such as sensor-to-shooter, permit imagery from space and airborne assets to be conveyed to pilots in real time. Scud-hunting techniques under development seek to coordinate multiple aircraft so as to acquire, illuminate, and engage

[53] Frater, Michael R., and Michael Ryan, Ibid, p. 7-9.
[54] Creveld, Professor Martin Van, "Command in War", Harvard University Press, Cambridge, MA, U.S.A., 1987.

enemy targets literally within minutes. If successful, these efforts could couple the firepower of concentrated forces with the agility of small teams.[55]

2.2.2. Command Systems

While the term C^2 remains in common use to refer to the process and means for the exercise of authority, the field has spawned many variations in terminology. (Figure 2.5)

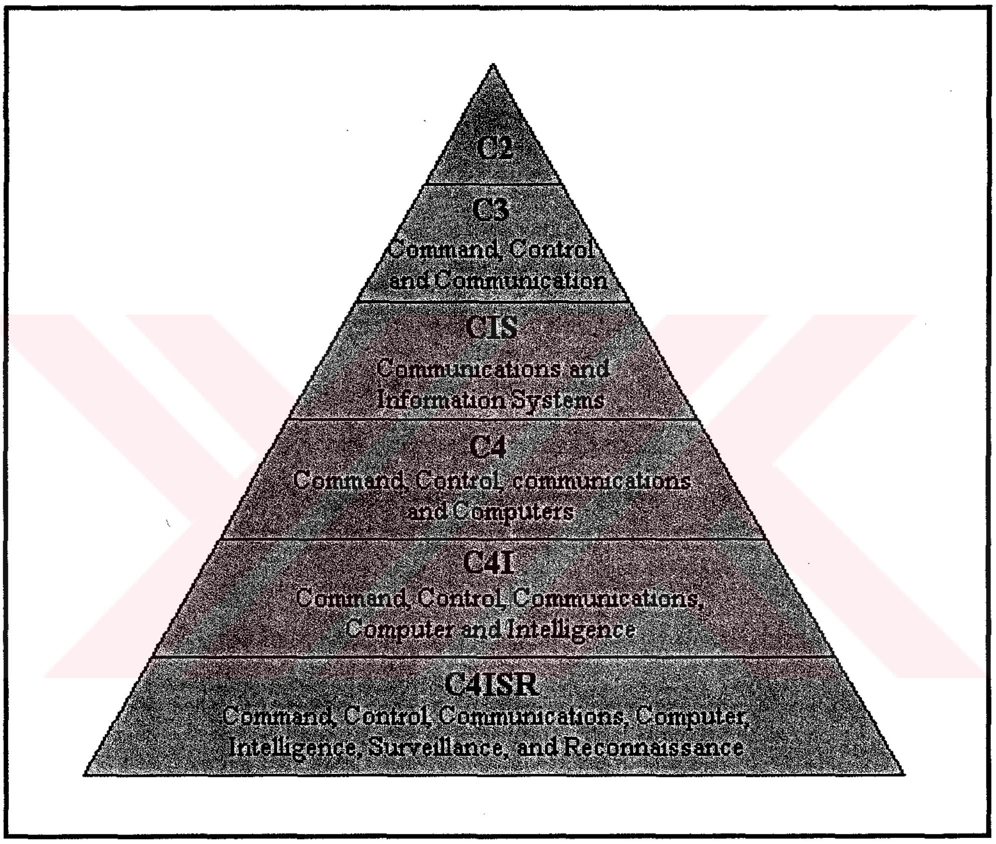


Figure 2.5: Various Command System Terms

Each of these terms can be justified by its emphasis on particular vital elements of the command and control process. For example, without intelligence, surveillance, and reconnaissance, commanders are blind; without communications they are isolated, and so on. In the interest of brevity, we will simply consider the C^2 cycle and bring together all of the systems that support it into the generic term of *command systems*.

[55] Libicki, Martin C., Ibid.

To be successful on the modern battlefield, a commander and staff must be able to move through the C^2 cycle faster than any adversary. Success in modern warfare depends on tempo, lethality, and survivability. Command systems must therefore be agile and responsive to change in threat and must be able to cope with the influx of huge amounts of information from intelligence and surveillance systems, both tactical and strategic. In recent conflicts, this has overloaded tactical communications systems as well as the labor-intensive intelligence process, making it extremely difficult for the commander to process and analyze information in a timely manner. The implementation of automated battlefield information systems offers the only viable solution to process information and to prepare and disseminate plans within a realistic time frame.[56]

The implementation of information systems and information technology is essential to provide the automation necessary to transfer, process, and store the large volumes of data on the future battlefield. Technology will play a significant role in the support developed to allow commanders to plan and maneuver faster than an adversary. Information systems and technology might be expected to improve several thousand times in the next 20 years and will greatly increase the scope, volume, accuracy, and speed of information available to commanders.

Gathering and synthesizing data into information, correlating information, and sharing knowledge call for sophisticated computer systems and advanced telecommunication networks. The systems must employ advanced parallel and distributive processing techniques. They must also employ secure broadband communications to dynamically link systems, collection resources, producers and users. The systems also must be compatible across all users. Both computer systems and telecommunication networks must be highly responsive to human and machine interfaces, innovations, and interventions and they must automatically learn to adapt to changing needs. All systems must be accessible via

[56] Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001, p. 9-10.

interactive voice commands, advanced modems, cellular-type devices, and other as yet unknown technologies that will emerge.[57]

The speed, fidelity, and breadth of modern information systems offer orders of magnitude increases in military efficiency. This efficiency will only increase in the future. As a result, information efficiency will be a key factor in future war and will become an area of conflict. Commanders always seek to observe-orient-decide-act (the "OODA" loop) faster than their opponents. This drive towards near-real-time C^2 will open interesting opportunities for operational art. Commanders will exploit their opponents' drives toward near-real-time decisions. Because, near-real-time decisions will require heavy degrees of automation and decision protocols, commanders at all levels will strive to drive their opponent's snap decisions towards poor decisions, usually by presenting false indications of intent or reality.

Advances in hardware, software, and bandwidth driven by the private sector are certain. Their impact on future conflict will be profound. Simply stated, the ability to rapidly exploit observations of friendly and enemy positions and capabilities, at levels superior to that of the enemy, will be decisive at the operational and tactical levels of wars. For this reason, there will doubtless be a fight over information in any future war. Winning this information war with integrated, redundant, secure, and exercised networks will be imperative to victory.[58]

The integrated C^4I system is assessed to enhance the capabilities of military units that will create military effectiveness.[59] The next step in the development of the system is the integration of reconnaissance and surveillance functions to the C4I system. The integration of sensors to the whole system is assessed as a painstaking fashion but many critical ingredients have been deployed and in development which includes:[60]

---

[57] Atkins, Robert L., Duane A. Lamb, Marlene L. Barger, Larry N. Adair, and Michael J. Tiernan, "2025 In-Time Information Integration System (I3S)", U.S. Air Force, April 1996, p. 7, Available on site: http://www.au.af.mil/au/2025/volume1
[58] Barnett, Jeffery R., Ibid, p. 7-10.
[59] Lin, H.S., "Realizing the Potential of C4I", National Academy Pres, Washington, D.C., U.S.A., 1999, p. 214.
[60] McConnell, K., M. Meermans, "Nowhere to hide: A Prescription For Attacking Fleeting, Mobile Battlefield Targets", Armed Forces Journal, U.S.A, July 2001.

- Signal intelligence (SIGINT) and electronic intelligence (ELINT) sensors, and reporting improvements that enable target detection and accurate location, on a large scale, in a short time.
- Airborne and space-based literal imaging systems, synthetic aperture radar (SAR) and electro-optical (EO) that have increased area collection capabilities and deliver better resolution, improved exploitation and dissemination, and ability to locate targets accurately.
- Unmanned aerial vehicles (UAVs) with ELINT sensors that can support weapon targeting.
- Affordable data links to efficiently transmit command and control (C^2) and targeting data to attack platforms.
- Significant inventories of smart weapons and sub-munitions that can efficiently attack ground targets.

Tomorrow's C^4I systems will have to adapt their response to the dimension of events, that is, be able on their own to:[61]

- Proceed to the fusion of intelligence data at the decision-maker's hierarchical level,
- Proceed to the timely discrimination, for the decision-maker, of those items of information that can contribute to the decision-making process,
- Reduce uncertainties,
- Supply specific or integrated forces equally well,
- Display data and follows the evolution of information in order to anticipate,
- Display suggestions for decisions as a function of the evolution.

A partial, limited transformation could occur if a military force acquires new technologies (such as new command, control, communications, computers, intelligence, surveillance, and reconnaissance [C^4ISR] systems and smart munitions) but does not change in other significant ways. A more ambitious transformation might replace old weapons with new weapons but not acquire different platforms. The combination of new technologies and

---

[61] Mermet, François, "The Role of European Ground and Air Forces After the Cold War: European Political-Military Analysis and Decision-Making", Ed. Gert de Nooy, Netherlands Institute of International Relations 'Clingendael', Netherlands, 1997, p. 37.

weapons might lead to new operational doctrines for employing forces on the battlefield but not produce major alterations in force structures and organizations, such as the mix of divisions and air wings. As a result of such changes, a military force might improve greatly in combat power and versatility, enough to "transform" what counts: its operational style, battlefield performance, and ability to win wars. Yet to the casual observer, its outward appearance might not be much different from its predecessor.[62]

2.3. COMMAND AND CONTROL WARFARE

Command and control warfare (C^2W) is the military strategy that implements information warfare (IW) on the battlefield. Its objective is to attack the command and control (C^2) decision-making capabilities of an adversary while protecting friendly C^2.[63] It integrates physical destruction into its litany of available tools. Its objective is to "decapitate the enemy's command structure from its body of combat forces". Tools used to perform this task, which can be referred to as the "five pillars of C^2W", include operations security, military deception, psychological operations, electronic warfare, and physical destruction (Figure 2.6).[64]

The key considerations underlying this strategy are that commanders must protect the command and control of deployed friendly forces while at the same time seeking to deny, deceive, disrupt, or, if necessary, destroy the command and control capabilities of the enemy. The goal of this action is to get inside the decision-making cycle of the opponent, thus forcing the enemy to lose the initiative and resort to a reactive mode of operation.[65]

Operations Security; is a process used for denying adversaries information about friendly intentions, capabilities, or limitations.

Military Deception; involves actions taken to mislead enemy decision makers or protect friendly capabilities. Its stated goal is to cause the enemy decision maker to respond in a manner that assists in the accomplishment of friendly objectives.

---

[62] Kugler, Richard L. and Hans Binnendijk, "Transforming America's Military - Choosing A Strategy", Ed. Hans Binnendijk, National Defense University, U.S.A., June 2002.
[63] Hutcherson, Norman B., "Command & Control Warfare", Air University Press, Maxwell, Alabama, U.S.A., September 1994, p. xiii.
[64] Hutcherson, Norman B., Ibid, p. 21.
[65] Hutcherson, Norman B., Ibid, p. 21.

Psychological Operations; convey specific information and indicators to an adversary audience to affect or influence their "emotions, motives, objective reasoning, and behavior.

Electronic Warfare; is any military action that involves the use of "electromagnetic or directed energy" to attack an enemy or control the electromagnetic spectrum.

Physical Destruction; requires the ability to identify, locate and prioritize enemy targets accurately and then to destroy them selectively.

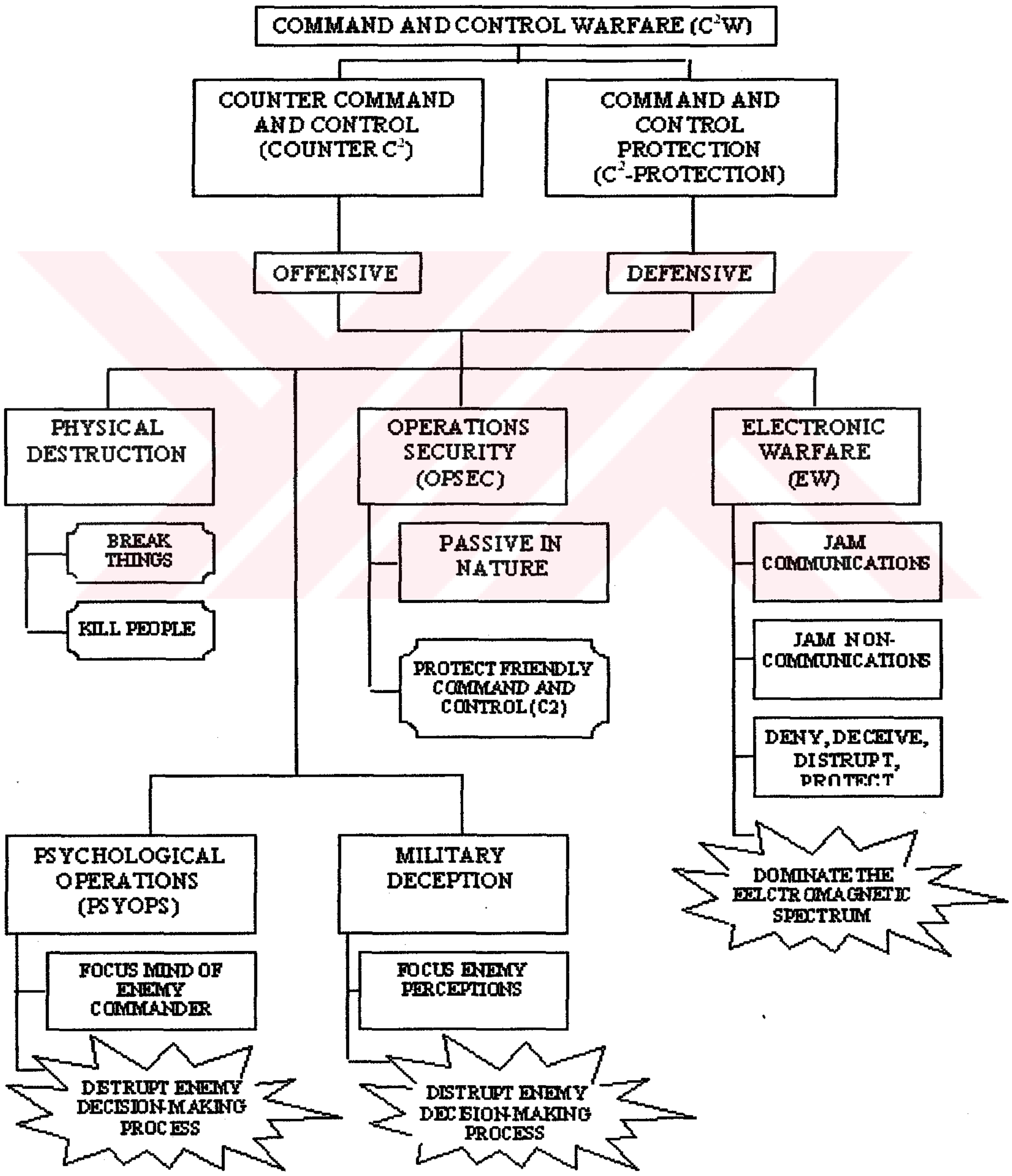


Figure 2.6: The Five Pillars of Command and Control Warfare

2.4. THE INTELLIGENCE-BASED WARFARE

In order for the five C^2W tools to be effective, intelligence must be integrated the tactical, operational, and strategic levels and used as part of campaign planning. Mutually supportive, intelligence enhances C^2W effects against enemy. The intelligence must be timely to support the current mission. Out of date or inaccurate data could lead to disaster for the commander's overall mission. Since it is the adversary's situations, intentions, and capabilities that are targeted, time and accuracy is of the essence.[66] Intelligence-Based Warfare (IBW) occurs when intelligence is fed directly into operations (notably, targeting and battle damage assessment), rather than used as an input for overall command and control. In contrast to the other forms of warfare discussed so far, IBW results directly in the application of steel to target (rather than corrupted bytes).[67]

Intelligence-based warfare deals with all the means including sensors used in order to obtain the tactical picture of the battlefield and the systems which process, evaluate and distribute this information to the military units.[68] As sensors grow more acute and reliable, as they proliferate in type and number, and as they become capable of feeding fire-control systems in real time and near-real time, the task of developing, maintaining, and exploiting systems that sense the battlespace, assess its composition, and send the results to shooters assumes increasing importance for tomorrow's militaries.[69] Achieving this accuracy and timeliness requires all-source intelligence and support from all available intelligence-related agencies. Sources include human intelligence (HUMINT), signal intelligence (SIGINT), imagery intelligence (IMINT), and photographic intelligence (PHOTINT) provided not only by defense agencies but analysis centers and scientific and technical intelligence production centers.[70]

Signals intelligence (SIGINT) is rapidly evolving from a strategic/technical assets, used to monitor radio and radar emissions across the border in support of long-term policy and

---

[66] Hutcherson, Norman B., Ibid, p. 29.
[67] Libicki, Martin, Ibid.
[68] Bilgin, H., "Siber Terörizme Karşı Tedbirler", Unpublished Thesis, Harp Akademileri, İstanbul, 2001, p. 22.
[69] Libicki, Martin, Ibid.
[70] Hutcherson, Norman B., Ibid, p. 29.

planning, to real-time tactical asset with a direct impact on decision-making by hands-on commanders.

COMINT (communication intelligence) and ELINT (electronic intelligence), the two components that make up SIGINT, are expanding more and more toward each other in terms of the digital-processing techniques they use. Communications and radar frequency bands are also overlapping with certain radars employing lower frequency and certain radios going up in the electromagnetic spectrum. Communications transmissions are increasingly of the frequency-hopping type, and there is a tendency to use data communications instead of voice, leading to the need for COMINT to make of emitter databases just like ELINT has been doing. This makes it easier and more appropriate to build integrated COMINT/ELINT (together, SIGINT) sensor suites which can for instance be packaged together in a single SIGINT pod for airborne applications.[71]

Intelligence is the end product that results from the "collection, processing, integrations, analysis, evaluation and interpretation of available information. A key distinction is the difference between data, which are the "representation of facts, concepts, or instructions in a formalized manner", and information, which is "unevaluated material of every description". This key distinction makes it readily apparent why well-trained intelligence personnel, no matter how greatly their collection functions are automated, are a critical requirement for war fighters in the field. Intelligence, like command and control warfare, is a thinking person's activity. Without the critical "man in loop" it becomes a useless regurgitation of previously reported "facts" that may or may not be relevant.[72]

Lessons regarding the applicability of intelligence to the five pillars of C^2W that arise out of the above examples include (1) a firm foundation of intelligence support to operations is critical, (2) timely intelligence support requires preparations focused on meeting the needs of the supported unit, (3) success depends on good intelligence and the intelligence collector's ability and (4) all of these efforts must be focused on the commander's intent. It is important that intelligence agencies have a basic understanding of the commander's operational plans and objectives. It is equally important that commanders and operators

[71] Hewish, Mark, and Joris J. Lok, "The Intelligent War", Jane's International Defense Review, Vol.30, Essex, UK, December 1997, p. 28.
[72] Hutcherson, Norman B., Ibid, p. 29.

understand the basic capabilities and limitations of the intelligence agencies that provide them support (Table 2.3).[73]

Table 2.3: Intelligence Support to Command and Control Warfare

PHYSICAL DESTRUCTION	ELECTRONIC WARFARE	OPERATIONS SECURITY	MILITARY DECEPTION	PSYCHOLOGICAL OPERATIONS
Target identification	Target location	Friendly vulnerability assessments	Identification of deception targets	Identification of enemy perceptions, strengths, and vulnerabilities
Target location	Electronic preparation of the battlefield	Identification of C2 (enemy C2W) threat	Selective of believable story	Selection of a focus for PSYOP campaign efforts
Time for optimal attack	Frequencies, critical nodes, modulations, and link distances	Denial of friendly capabilities and intentions	Identification of enemy order of battle to include intelligence collection system	Identification of enemy order of battle to include key commanders and their associated C2 support systems
Battle damage assessment	Time for optimal attack	Evaluation of deception efforts.	Placement of assets	Placement of assets
Intelligence preparation of the battlefield	Battle damage assessment		Analysis/feedback	Analysis/feedback
	Joint restricted frequency list			

Intelligence is critical to C^2W planning and execution. In striving to achieve information dominance, the commander's goal is to extend the adversary's decision-making and execution activity beyond that of friendly processes. Intelligence assessments of vulnerabilities of command and control targets allow planners to identify and select the appropriate tools for C^2W operations. Intelligence monitoring activities, prior to and during a military operation, provide planners with the necessary information to tailor operations and to gauge the effectiveness of the overall campaign. Estimates of adversary capabilities to exploit friendly vulnerabilities allow planners to determine priorities of hostile targets while increasing protective measures.[74]

The aim of the IBW is to avoid the surprises of war and to help commanders to shape the operation plans. A perfect intelligence provides the coordination and synchronization of the operations. When the battle begins, on one site there is forces which understood their

[73] Hutcherson, Norman B., Ibid, p. 30.
[74] Hutcherson, Norman B., Ibid., p. 31.

tasks and ready for the battle on the other hand there is forces living chaos and shock.[75] Despite differences in cognitive methods and purpose, systems that collect and disseminate information acquired from inanimate systems can be attacked and confounded by methods that are effective on C^2 systems. Although the purposes of situational awareness (an intelligence attribute), and battlespace visibility (a targeting attribute) are different, the means by which each is realized are converging.[76]

2.4.1. Offensive IBW

Sharp increases in the ratio of power to price of information technologies, in particular those concentrated on distributed systems, suggest new architectures for gathering and distributing information. Platforms that host operator, sensor, and weapon together will give way to distributed systems in which each element is separate but linked electronically. The local-decision loops of industrial age warfare (e.g., a tank gunner uses infrared [IR] sights to detect a target and fire an accurate round) will yield to global loops (e.g., a target is detected through a fusion of sensor readings; the operator fires a remotely piloted missile to a calculated location). Because networking permits the logging of all readings and subsequent findings (some more correct than others), it can generate lessons learned more efficiently than a system that depends on voluntary human reporting.[77]

The evolution of IBW may be understood as a shift in what intelligence is useful for. Traditionally, the commander uses intelligence to gauge the disposition, location, and general intentions of the other side. The object of intelligence is to prevent surprise a known component of information warfare and to permit the commander to shape battle plans. Good intelligence allows coordination of operations; great intelligence allows coherence, which is a higher level of synchrony.[78] The goals of intelligence are met when battle is joined; when one side understands its tasks and is prepared to carry them out while the other reels from confusion and shock thus, situational awareness.

---

[75] Kılıçaraslan, M.A., "Bilgi Harbi Nedir?", Unpublished Thesis, Harp Akademileri, İstanbul, 2000, p. 11.
[76] Libicki, Martin, Ibid.
[77] Libicki, Martin, Ibid.
[78] Cooper, Jeff, "Toward a Theory of Coherent Operations," SRS Technologies Magazine, U.S.A., 30 June 1994.

Today's information systems reveal far more than yesterday's could, permitting a degree of knowledge about the battlespace that accords with situational awareness. The side that can see the other side's tank column coming can dispose itself more favorably for an encounter. The side that can see each tank and pinpoint its location to within the effective radius of an incoming warhead can avoid engaging the other side directly but can fire munitions to a known, continually updated set of points from stand-off distances. This shift in intelligence from preparing a battlefield to mastering a battlefield is reflected in newly formed reporting chains for this kind of information. Although the direct reporting chain to the national command authority will continue, new channels to successively lower echelons (and, eventually, to the weapons themselves) are being etched. An apparent loss in status perceived by the intelligence apparatus (thus one resisted) is turning out to offer a large gain in functionality.

Tomorrow's battlefield environment will feature a mixed architecture of sensors at various levels of coverage and resolution that *collectively* illuminate it thoroughly. In order to lay out what may become a complex architecture, sensors can be separated into four groups:[79]

1. far stand-off sensors (mostly space but also seismic and acoustic sensors);
2. near stand-off sensors (e.g., unmanned aerial vehicles [UAVs] with multispectral, passive microwave, synthetic aperture radar [SAR], and electronic intelligence [ELINT] capabilities, as well as similarly equipped offshore buoys and surface-based radar);
3. in-place sensors (e.g., acoustic, gravimetric, biochemical, ground-based optical);
4. weapons sensors (e.g., IR, reflected radar, and light-detection and ranging [LIDAR]).

This complexity illustrates the magnitude and complexity of the task for those who would evade detailed surveillance. Most forms of deception work against one or two sensors - smoke works for some, radar-reflecting paint for others, quieting for yet others- but fooling overlapping and multivariate coverage is considerably more difficult. The task of assessing what individual sensor technologies will have to offer over the next decade or so is relatively straightforward; globally available technologies will come in many types for use by all. The task of translating readings into militarily useful data is more difficult and calls

[79] Kılıçaraslan, M.A., Ibid, p. 11; Libicki, Martin, Ibid.

for analysis of individual outputs, effective fusion of disparate readings, and, ultimately, integration of them into seamless, cue-filter-pinpoint systems.[80]

2.4.2. Defensive IBW

Equally difficult to predict are defenses developed to preserve invisibility or, at least, widen the distance between image and reality on the battlefield. IBW systems can be attacked in several ways. On one hand, an enemy would be well advised to make great efforts against sensor aircraft (such as AWACS or JSTARS). On the other, using sensors that are too cheap to kill may be wiser. Sensors can also be attacked by disabling the systems they use, and their systems can be overridden or corrupted with EW. When sensor readings are technically accurate, countering IBW requires distorting the links between what sensors read and what the sensor systems conclude. In high-density realms (e.g., urban areas, villages crowded together, forests, mountains, jungles, and brown water) counterstrategies may rely on the exploitation or multiplication of the confusing clutter. In realms where the assets of daily civilian commercial life are abundant, military assets would need to be chosen so they could be confused with civilian assets.

For the foreseeable future, battlefield sensors will not be able to look at all information at the same time in sufficient detail. Thus, the sensor system will need to use a combination of cuing, filtering, and pinpointing (e.g. as a JSTARS system does to indicate a group of moving vehicles so UAVs can be dispatched to identify each of them).

Information technology can be viewed as a valuable contributor to the art of finding targets; it can also be viewed as merely a second-best system to use when the primary target detection devices –a soldier up close –are too scarce, expensive, and vulnerable to be used this way. Open environments (tomorrow's free-fire zones) aside, whether high-tech finders will necessarily always emerge triumphant over low-tech hiders remains unclear.[81]

---

[80] Libicki, Martin, Ibid.
[81] Libicki, Martin, Ibid.

2.5. PARALLEL WAR

Future aerospace operations against the enemy at all levels of war and across all target categories must occur almost simultaneously. Near-simultaneous attacks across the enemy target set will be the hallmark of future aerospace operations. Failure to conduct aggressive and overwhelming attacks across all facets of enemy power would waste a decisive capability.

The *theory* of near-simultaneous attack across multiple target sets is nothing new. Airmen have recognized it for decades. A large number of attacks in a day have far more effect than the same number of attacks spread over weeks or months. In his report to President Truman at the end of WWII, Gen Hap Arnold asserted that strategic air assault is wasted in sporadic attacks that allow the enemy to readjust or recuperate.[82]

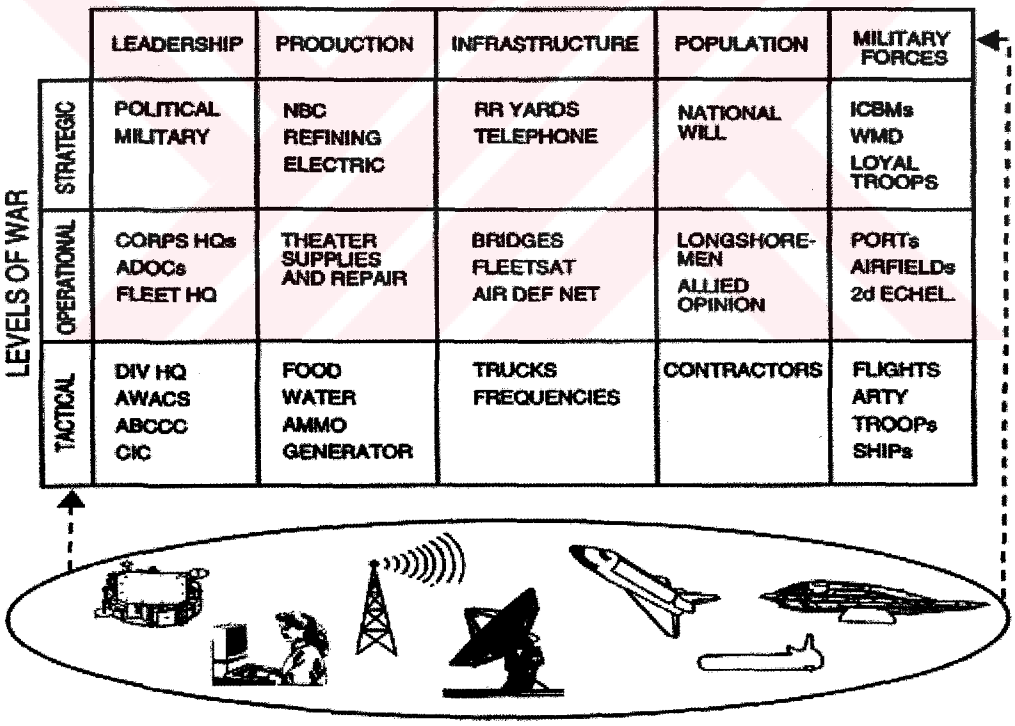


Figure 2.7: Target Categories.

Historically, however, airmen lacked the military capabilities to implement near-simultaneous attack. During all of 1942–1943, for example, the Eighth Air Force attacked

[82] Barnett, Jeffery R., Ibid, p. 10.

a total of only 124 distinct targets. At this low attack rate (averaging six days between attacks), the Germans had ample time to repair and adapt between raids.

Contrast this WWII rate of attack with the 1991 Gulf War. In the first 24 hours of Operation Desert Storm, coalition air forces attacked 148 discrete targets. Fifty of these targets were attacked within the first 90 minutes. Targets ranged from national command and control nodes (strategic) to key bridges (operational) to individual naval units (tactical). The goal was to cripple the entire system to the point it could no longer efficiently operate, and to do so at rates high enough that the Iraqis could not repair or adapt. Coalition forces, knowing an incredible amount about Iraq, efficiently orchestrated thousands of sorties, reached key vulnerabilities with high certainty, and, once in the target area, hit specific targets. The end result was near-simultaneous attack across hundreds of key Iraqi targets. Under this intense attack, Iraq was unable to either regain the initiative or orchestrate a cohesive defense.

Such targeting, conducted against the spectrum of targets in a compressed time period, is called *parallel war.* The goal of parallel war is to simultaneously attack enemy centers of gravity across all levels of war (strategic, operational, and tactical) at rates faster than the enemy can repair and adapt. This is a new method of war. Previous generations of military strategists could not prosecute parallel war. They had only the sketchiest knowledge of the enemy's key strategic and operational targets. The enemy was opaque prior to contact.[83]

Even when military commanders knew what to target, they had to first "roll back" an enemy's defenses before attacking key centers of gravity. But modern technology is changing these long-held axioms of war. As demonstrated in the Gulf War, modern penetration and precision can place these centers of gravity under massive attack on day one of the war, and do so faster than an enemy can react. Most importantly, modern command and control systems can plan and direct this offensive in near real time. These attributes of parallel war distinguish it from anything seen in military history.

[83] Barnett, Jeffery R., "Future War - An Assessment of Aerospace Campaigns in 2010", Air University Press, Maxwell Air Force Base, Alabama, U.S.A., January 1996, p. 11.

The Iraqi commanders had difficulty carrying out orders for a coordinated movement of their forces. Their command posts, air shelters, and even tanks buried in the sand were vulnerable to elimination by precision penetrating bomb attack.[84]

Parallel war is enabled by emerging advances in *four key technologies:* [85]

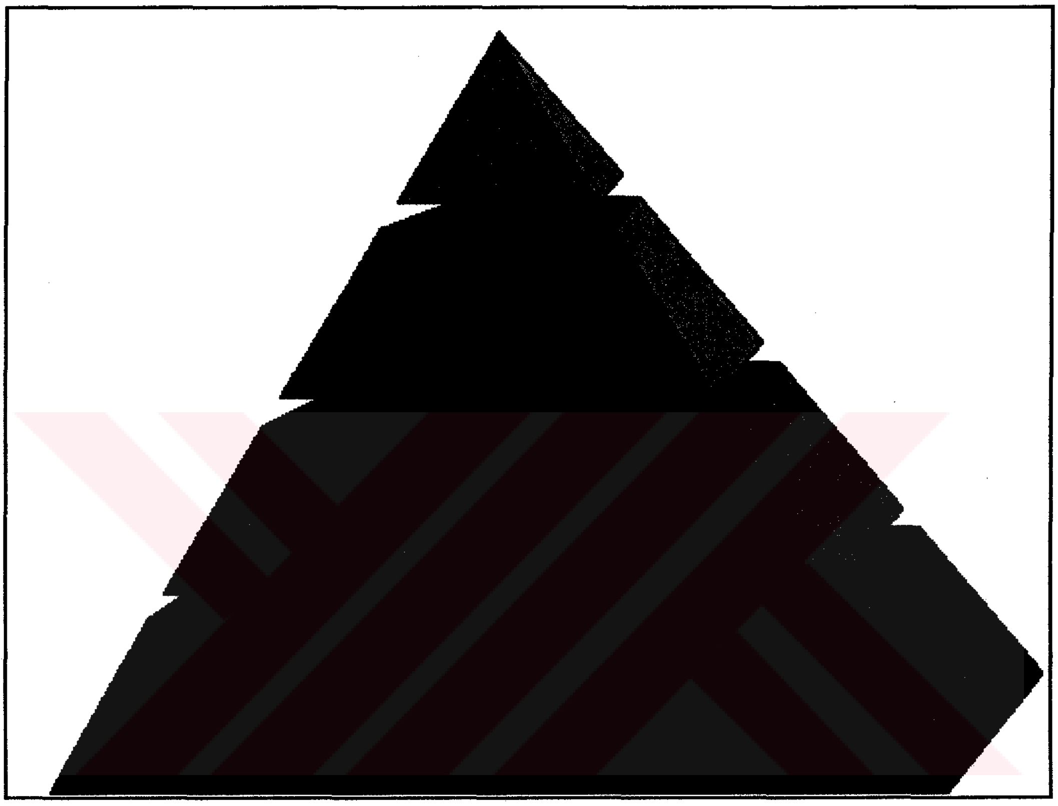


Figure 2.8: Parallel War's Four Key Technologies.

1. *Information:* By 2010, well into the Information Age, aerospace planners will detect an incredible amount of information about the target state. They will never know everything, but they will detect orders of magnitude more about the enemy than in past wars. At the strategic level of war, they should observe the connectivity among the national leadership, the architecture of the national communications grid, and the position of elite troops who are key to regime protection, among other things. At the operational level of war, they should see the location and connectivity of key corps and air defense headquarters, the naval order of battle, the location and LOCs of theater-level supplies, and the coordinates of critical nodes in airfields and ports. At the tactical

[84] Barnett, Jeffery R., Ibid, p. 15.
[85] Barnett, Jeffery R., Ibid, p. 11-15.

level of war, they should know where most of the enemy's unit headquarters are, their communications centers and means, and the individual locations and readiness levels of squadrons, divisions, and ships.

2. *Command & Control (C^2):* Future commanders will use the Information Age's revolutionary advances in information transfer, storage, recognition, and filtering to orchestrate attacks and defenses. Theater-wide taskings will flow with unprecedented fidelity and speed. Commanders will convert "the understanding of the battlespace into missions and assignments designed to alter, control, and dominate that space."[86]
3. *Penetration:* Units will launch penetrating platforms against these targets. Enabled by stealth, hypersonic, and/or electronic warfare technologies, these platforms will penetrate in significant numbers. While defenses will certainly defeat some attackers, others will get through at rates higher than previously experienced.
4. *Precision:* Once over the target area, penetrating platforms will deliver brilliant munitions. Deliveries will be highly accurate. Target locations will be measured within feet. Circular error of probability will be less than a meter. Brilliant sensors will have the ability to distinguish between tanks and trucks, between parked bombers and decoys. Because of this precision, fixed and mobile targets will be struck by the thousands.

2.6. MILITARY ADVANCE IN INFORMATION TECHNOLOGY

2.6.1. Know the Enemy

Some of the most dramatic changes in the capabilities of forces to gather, evaluate, and disseminate information involve increased knowledge of the enemy. In general these capabilities are into two broad areas:[87]

- Ubiquitous, near real-time surveillance sensors using multiple phenomena.
- Processors and communication systems that enable fusion, transfer, and display of information from these sensors.

---

[86] Owens, Adm. William A., "The Emerging System of Systems," Proceedings Magazine, U.S.A., May 1995, p.38.

[87] Harshberger, Edward and Ochmanek, David, "Information and Warfare: New Opportunities For U.S. Military Forces", Ed: Zalmay M. Halizad, John P. White, The Changing Role of Information in Warfare", RAND, California U.S.A., 1999, p. 163.

In combination, these new capabilities have fundamentally altered the state of knowledge that commanders have about the location and disposition of enemy forces. Improved information capabilities can also provide commanders with vital clues bout an enemy's *intent*. Such information has been rare in the past, but, when attained, often critically important.

Spaceborne sensors have steadily improved since the 1960's, and today they can provide nearly constant coverage of many of the military activities of potential opponents. This knowledge of the situation on the ground, covering thousands of square kilometers and delivered in "real time", arises from new sensors, such as the moving target indicator radar aboard the Joint Surveillance Target Attack Radar System (JSTARS). By exploiting breakthroughs in radar technology and signal processing, the JSTARS aircraft is able to detect and locate moving vehicles with some precision. This picture can be enhanced by integrating information from other sensors, such as synthetic aperture radar (on board JSTARS) or other imaging sensors that can be carried by smaller unmanned aerial vehicles (UAVs). Because of these types of systems, knowledge of enemy movements beyond the horizon of friendly ground forces is orders of magnitude more accurate, timely, and reliable than ever before.[88]

And the types of information available are many. The Predator UAV sends back a real-time video feed from optical sensors. Rivet Joint and other aircraft gather information on radar, radio, and other emissions of enemy forces, the analysis of which can help identify unit and equipment type and location. To deal with this massive flow of disparate types of data, military forces are aided by the same kinds of information processing and display technologies that are revolutionizing the workplace. Military forces can tap into the same digital satellite communication systems that carry civilian traffic every day and can augment these capabilities with secure military systems, such as the Military Strategical and Tactical Relay System and the Global Broadcast System. In the theater, specialized and common digital communications systems, such as the Joint Tactical Information Distribution System, can bring together most-if not all- of these information sources coherently on common displays in multiple command centers. The net result of the mix of these systems is a dramatically improved picture of the operational battlefield for military

[88] Harshberger, Edward and Ochmanek, David, Ibid, p. 164.

leaders and staffs at many levels of command. This knowledge reduces the likelihood of surprise at the operational and tactical levels, increase the commander's decision timelines, and moves commanders closer to an understanding of enemy intent, a critical step toward thwarting that intent and enforcing own.[89]

2.6.2. Know Yourself

Throughout history, as the scale and geographic scope of military operations have grown, one of the greatest roadblocks to effective operations has been uncertainty about the disposition of one's own forces. In a stressful, unfamiliar, and changing environment, forces can simply get lost. This has led to catastrophic consequences in the past, among them failure to support other forces effectively when those forces come under fire; exposure of a unit's flanks to attack; and at times, losses due to "friendly fire".

Enhanced knowledge of position, coupled with improved means of communication, can dramatically change the nature of ground forces' operations. When creating operational plans, higher-level commanders can effectively monitor and coordinate the location and movement of all of their forces. This capability has the potential to reduce substantially the possibility of casualties by "friendly fire" –development that will be furthered by improved Identification Friend or Foe capabilities for both air and ground forces.[90]

2.6.3. Know the Ground, Know the Weather

In a time when commercial aircraft fly in almost any weather and roads are (generally) quickly cleared during snowstorms, it is often easy to forget the dramatic effects that weather and terrain continue to have on military operations. For a mechanized ground force, the difference between the rate of mechanized advance on an open plain and that through a swamp can be the difference between success and failure. Coordination of an infantry assault in driving rain is qualitatively different from the same maneuver in good weather.

[89] Harshberger, Edward and Ochmanek, David, Ibid, p. 164-165.
[90] Harshberger, Edward and Ochmanek, David, Ibid, p. 166-167.

So it is not surprising that timely and accurate information on the operating environment remains at the top of the list of military commanders' need. For this reason, the defense establishment maintains global weather observation and forecasting networks, augmenting the capability of civilian weather satellites with military system that focus on areas of greatest interest. All four military services participate in this activity, and high-quality weather information is available to forces worldwide, 24 hours a day.

Beyond predicting the weather, forces are, to an increasing extent, doing something about it. Obviously, the weather can not be controlled, but new systems are enabling some military forces to operate more effectively in spite of adverse weather conditions. Since the dawn of military aviation, effective reconnaissance and attack operations have depended on clear weather: Air crews had to be able to see their targets to photograph or attack them effectively. Even the laser-guided bombs that proved so accurate in Operation Desert Storm, Bosnia, and elsewhere can only be delivered through fairly clear skies. As sensors and processors become smaller, cheaper, and more capable, increasing numbers of munitions will be fielded that find and home in on their targets autonomously. Radar sensors on satellites and aircraft are also enabling forces to conduct reconnaissance of enemy forces and targets at night and through clouds.

Forces are also benefiting from enhanced knowledge of terrain. Digital information includes digital versions of standards maps (allowing such information to be used on computer displays), digital wide-area photography, and Digitized Terrain Elevation Data – vertical profiles of terrain features. Used in combination, these sources of topographic information are allowing forces to "know the terrain" by creating three-dimensional imagery for use in mission planning, mission rehearsal, and training system.[91]

2.6.4. Know When Victory Is Endangered

In particular, as commanders adjust their forces, training, and operations to take advantage of increased knowledge and better communications, the impact of losing these capabilities can become more serious. Attempts by an adversary to deny the commanders timely and accurate information can take many forms. Most straightforward are those that might be

[91] Harshberger, Edward and Ochmanek, David, Ibid, p. 167-169.

termed traditional approaches: electronic jamming, physical destruction of sensors and control mean, deception, and disinformation. Some aspect of new capabilities do, in fact, appear susceptible to these means: For example, GPS signals are quite weak and can be jammed under some circumstances, and satellite communications generally rely on relatively few ground stations.[92]

However, a more ominous aspect of new information systems is their susceptibility to more subtle attacks. The amount of computer-based information, the automation that handling this information requires, and the increased connectivity of systems means that a capable opponent might attempt to use the information and information systems as weapons, by inserting computer viruses or false information into information networks. The effects of such attacks could be manifested at all levels of warfare, from strategic to tactical.[93]

For the present and near the future, the United States appears to have a distinct advantage in almost all areas of this two-sided struggle for information dominance. In the area of traditional means, the United States' conventional military capabilities stand alone –even in 1991 and 2003, the systematic destruction, jamming, and spoofing of Iraq's surveillance and control systems was an unquestioned success. And development and reliance on computer and communication systems have paid a dividend in terms of knowledge of system vulnerabilities and the means to exploit and reduce these. As knowledge of advanced information systems spreads, however, it will become increasingly difficult to maintain this lopsided advantage.[94]

2.7. HOW NEW INFORMATION CAPABILITIES MIGHT AFFECT MILITARY OPERATIONS

The commercial sector now leads the military sector in research investment and in the development of certain critical technologies. This is most obvious in the area of Information, Technology, Electronics and Communications (ITEC), where the rate of technology advance and innovation is driven by a world economy increasingly dependent

[92] Harshberger, Edward and Ochmanek, David, Ibid, p. 169.
[93] Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson, "Strategic Information Warfare: A New Face of War", Santa Monica, RAND, California U.S.A., 1996.
[94] Harshberger, Edward and Ochmanek, David, Ibid, p. 169-170.

on knowledge and information. In the context of defense, advances in civil ITEC will have a major impact on future Command, Control, Communications and Intelligence (C^3I) systems, and will also be significant in such systems as new sensors and weapons. Another field of relevance to defense where there is substantial civil activity is biotechnology, where advances will have broad significance in the areas of chemical and biological defense, human performance and medical treatments. And the development of space-based systems, originally driven by the US and others (notably Russia and China) for defense purposes, is now becoming a commercial activity, potentially bringing significant capability to a wider range of nations and organizations.[95]

Technological advance will increase the range of military options available to potential adversaries, some of whom may be prepared to adopt alternative weapons or unconventional strategies based on more widely available technology. Maintaining an edge in the field of ITEC will require our own unique, intelligent and inventive use of architectures, mathematical algorithms and programmes to be as advanced as possible.[96] At the tactical level, information is critical for assuring that systems that are meant to attack the enemy have targets to shoot at; that when hey shoot, they do so accurately; and that what they are shooting at is, in fact, what they think it is. A fighter pilot may see a "blip" on his radar scope. This blip constitutes a datum -a piece of evidence to be used for reasoning or inference. The pilot may use other data- the location and form of the blip, its direction and velocity, responses to electronic interrogation -to help inform his or her judgment about whether the source of the blip is a mountain, a cloud, an electronic anomaly on the scope, or an aircraft- friendly or enemy. Some of these data can be used to guide a weapon to the target if the pilot decides to attack the source of the blip. All of this takes place at the engagement and tactical levels.[97]

The rapid pace of development will lead to rapid obsolescence of many equipments embedded in defense systems, resulting in more technology insertion and upgrade in weapons, sensors and C^3I systems, and consequently there may be fewer resources devoted

---

95 Ministry of Defence, "The Future Strategic Context for Defence - The Technological Dimension", Secretary of State for Defence, London, U.K., November 2001, Available on site: http://www.mod.uk/issues/strategic_context/physical.htm
96 Ministry of Defence, Ibid.
97 Harshberger, Edward and Ochmanek, David, Ibid, p. 171.

to other areas such as equipment platforms where technological changes take place more slowly. Greater availability of technology is likely to result in acceleration in the rate at which new threats develop. It will be important to minimize the lead time between the emergence of a new weapon or threat and the development of counter-measures (or counter counter-measures), and to be able rapidly to amend military doctrine, concepts and training as necessary.[98]

Information is also a key to survivability on the battlefield, just as information is needed to locate, identify, and engage targets, it is also useful in helping combatants determine whether or not they are someone else's target. It is thought that the crews of most of the aircrafts lost in combat are not aware that they have been engaged by the enemy until the final seconds of engagement. In the airmen's lexicon, these victims had inadequate "situational awareness", which has been shown in training to be at least as important as major aircraft performance parameters in determining the results of air-to-air combat. The importance of maintaining situational awareness has been a major factor in the design and equipping of combat aircraft, leading to the development of radar warning receivers, longer-range radars, and "bubble" canopies.[99]

Information Age armies will develop a shared situational awareness based on common, up-to-date, near-complete friendly and enemy information distributed among all elements of a task force. First, operational and tactical commanders will know where their enemies are and are not. Of course, this *knowledge* will never be absolute, and it is folly to assume it ever will become *perfect*. It will be, however, of an order of magnitude better than that achieved even during the Gulf War II, information age armies will know where their own forces are, much more accurately than before -and deny this critical information to the enemy. Last, this enemy and friendly information will be distributed among the forces of all dimensions -land, sea, air, and space- to create a common perception of the battlefield among the commanders and staffs of information age armies.[100]

---

[98] Ministry of Defence, Ibid.
[99] Harshberger, Edward and Ochmanek, David, Ibid, p. 171.
[100] Sullivan, Gordon R. and James M. Dubik, "War in the Information Age," Military Review, U.S.A., April 1994, p. 56.

In the current and future strategic environment, equipment is much more likely to see operational use than during the Cold War, and in a wider range of circumstances and environmental conditions. As a result, equipment will need to be designed with utility for a wide range of circumstances. Additionally, capability gaps and risks of being out-matched will become apparent more quickly. This will provide opportunities for technology to be developed or adapted accordingly, as long as sufficiently responsive acquisition processes are in place.

New technology will offer the potential to achieve military objectives in different ways and indeed provide means to do completely new things (e.g. unmanned systems might be used for operations deemed too risky for humans). Consequently new technology will, in some cases, require the development of new doctrine and concepts of operation. Military advantage will rest with those who most effectively identify and exploit technology. This will place a premium on the ability to generate and identify opportunities, adapt them for military use and integrate them rapidly into equipment platforms, weapons systems and force structures.[101]

Moving further into the future, there are a number of areas that will offer potential for significant technological advance. The technological possibilities and their implications might include:

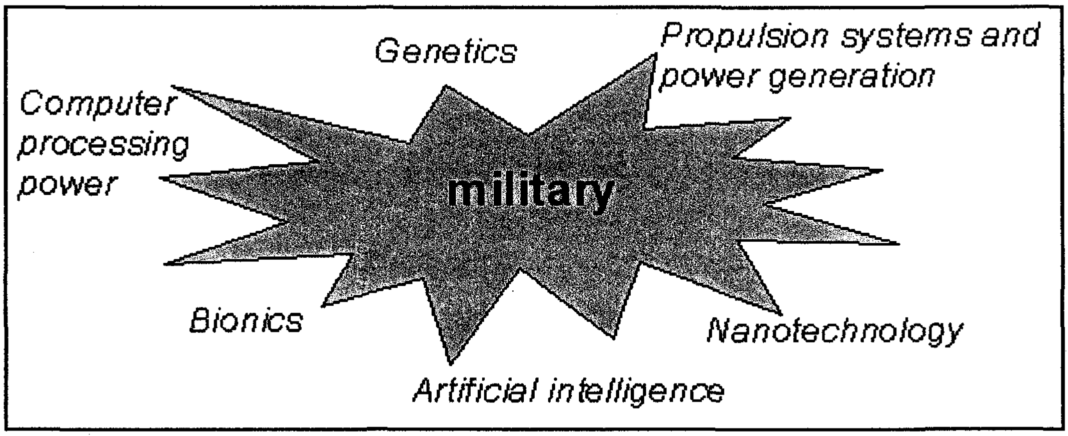


Figure 2.9: The Technological Possibilities and Their Implications.

Computer processing power: Increases in processing power will continue apace. Moreover, quantum processing, if successful, will revolutionize computer processing

[101] Ministry of Defence Ibid.

power to a staggering degree, with implications for weapons, sensors (ELINT and other), communications, and information operations and countermeasures. The fusion in real time of multi-sensor information to enable high assurance recognition of hostile targets. Another use may be quantum cryptography, offering the prospect of perfectly secure communication.

Propulsion systems and power generation: Further significant advances will be made in alternative propulsion systems and power generation, such as electric and solar power and improved energy storage based on nanotechnology. Long endurance remotely deployed systems and micro unmanned airborne vehicles (UAVs) will be possible.

Bionics: Direct and indirect electronic-brain links to improve the performance of the brain to handle, perceive or view data, originally driven by medical considerations such as treatment of sight and hearing defects, will emerge. Techniques will include both implanted equipment and surface or remote equipment.

Artificial intelligence: By 2030 machines will be developing which have an advanced ability to gather information on their surroundings, and which, acting autonomously, can make intelligent judgments (including judgments on risks) in response to that information. This will have obvious implications in many areas especially for military intelligence (ELINT, SIGINT etc.), surveillance, target acquisition and reconnaissance and support to military decision-making.

Genetics: It is possible that some might attempt to harness the function of specific genes for genetic warfare or biogenetic terrorism, such as targeting food sources, against which we would need to develop defensive measures. It is also possible that new antibiotic-resistant diseases could develop or be developed, increasing levels of sickness and likelihood of death.

Nanotechnology: Nanotechnology will allow the miniaturization of sensors (ELINT and other) and equipment. This will affect many technologies, and opens up a wide range of new possibilities. Postulated systems, some possibly further out than 2030, include nano-solar cells offering more efficient electricity generation than present systems, and nano-robots for many potential purposes. Combined with increases in processing power these systems will have widespread application including in micro-platforms for reconnaissance.

2.8. DOMINATE BATTLEFIELD AWARENESS

It is well within the realm of technical possibility to observe practically everything of operational significance about a battlefield. Admiral William Owens called this concept *dominant battlefield awareness*. This concept has three components. First, platforms continuously surveil the area of interest. A mixture of aircraft, satellites, and UAVs, equipped with multispectral sensors (ELINT and etc.), establishes 24-hour, all-weather coverage of the battle area. Unattended ground sensors sniff/watch/listen/ report along areas of possible maneuver. SOSUS-type sensors listen for underwater threats. Second, data generated by these sensors are fused and filtered through wide-area automatic target recognition software. This software cues more refined systems to specifically identify emitters and high-signature targets (e.g., armored formations or logistics points). Lastly, this information is disseminated to weapon systems. This dissemination takes advantage of large bandwidth and digital compression technologies. It transmits via direct broadcast satellites. The result of these three steps is dominant battlefield awareness.

Dominant battlefield awareness does not mean *perfect* knowledge of all enemy locations and intentions. Knowledge of *everything,* distributed to *everybody,* is impossible to attain. Plans based upon such an impossible standard are doomed to failure. Rather, dominant battlefield awareness is *an attempt to exploit order-of-magnitude increases in what's identifiable about a battlefield.*

Throughout military history, what commanders have not known about an adversary has dominated our image of war. The armies of generals Lee and Meade *bumped* into each other at Gettysburg. In 1914, the German army didn't even know the British Expeditionary Force was on the continent until they ran into the BEF at Mons. Hitler kept panzer divisions in reserve near Calais, waiting for the "real" cross-channel invasion. Saddam's army had little knowledge of Gen H. Norman Schwarzkopf's deployment to the west for the "left hook." In each of these cases, commanders had little information on whole armies maneuvering in front of them. In today's Information Age, such military ignorance is *impossible* if one fields an integrated mix of ELINT and other sensors, filters, and disseminators -and protects this architecture from effective enemy interference.[102]

2.9. FUTURE WEAPON SYSTEMS

To envision this future war, planners should start with possible future weapon systems as their baseline—*not* what is currently on the ramp and in procurement. As the WWII experience shows, most of today's weapons will be obsolete for a 2010 war. For example, it is very unlikely that today's models of cruise missiles and satellites will reflect the state of the art in 2010. Nor will bombers. Just as advances in engine technologies made the 1925 Curtiss B-2 bomber obsolete in WWII, advances in information technologies will bypass the avionics, computers, and munitions in today's Northrop B-2 bomber.

Although today's weapons will become obsolete, today's thinking will not. The doctrines developed today will be critical. If the World War II analogy holds, doctrines developed today will guide rearmament and initial operations in the next war.

When projecting a major conflict with a peer, planners must expect both sides to employ significant numbers of advanced-technology aerospace systems. These systems will include:[103]

Atmospheric and space-based reconnaissance and communications systems: These systems will vary in quality and quantity between opponents. They will, at a minimum, be able to detect massive force movements and relay this information in near real time despite significant enemy countermeasures.

Information Age command and control systems: Future C^2 will devise and direct integrated taskings with high fidelity in near real time. They'll be heavily automated and dispersed. Attacks on any single node of this structure will not have catastrophic effects.

Stealth aircraft and stealth cruise missiles: The stealth technology is assessed as a revolution in air warfare. The development of stealth aircraft reduces radar determining

[102] Barnett, Jeffery R., "Future War - An Assessment of Aerospace Campaigns in 2010", Air University Press, Maxwell Air Force Base, Alabama, U.S.A., January 1996.
[103] Barnett, Jeffery R., Ibid.

range from a few hundred kilometers to a bit more than a dozen kilometers.[104] These very low-observable weapons will use state-of-the-art electronic warfare systems to further increase their chances of penetration. Stealthy cruise missiles will be inexpensive, allowing their employment in massive numbers.[105] Further advances in stealth aerospace weapons will make sudden attacks realistic and disable the air defense warning system and entire air defense systems.

Precision weapons: Reflecting current trends in sensor technologies, precision weapons will have less than one meter accuracy with brilliant munitions. They will guide independently of external positioning systems (e.g., global positioning system [GPS]), and they will have automatic target recognition capabilities. Some of these weapons will retain their accuracy regardless of weather or darkness.[106] Attacking ground-based sensors such as radar systems with special precision-guided missiles was tested during the Gulf War by coalition forces.

2.10. REQUIRED FLEXIBILITIES FOR FUTURE WARFARE

Future warfare will also require specific flexibilities within weapon systems. Decisions made today will affect that flexibility. Therefore, today's acquisition considerations for aerospace forces should include these factors:[107]

Information: Platforms must have the ability to incorporate/upgrade the latest information hardware and software, employ information obtained by off-board sensors, and transmit information garnered by onboard sensors to other weapon systems. Systems must also be able to operate despite a corrupted information environment.

Long range: Aerospace platforms should be based as far from enemy stealth systems as possible. Distance either puts a base out of enemy stealth range or gives layered defenses more opportunities to detect and target enemy attacks. Short-range systems will contribute only in very low-threat environments.

---

[104] Shenxia, Z., Z. Changzai, "Chinese Views of Future Warfare, Part Four, The Revolution in Military Affairs: The Military Revolution in Air Power", Ed.: M. Pillsbury, National Defense University Press, U.S.A., 1996.
[105] Barnett, Jeffery R., Ibid.
[106] Barnett, Jeffery R., Ibid.
[107] Barnett, Jeffery R., Ibid.

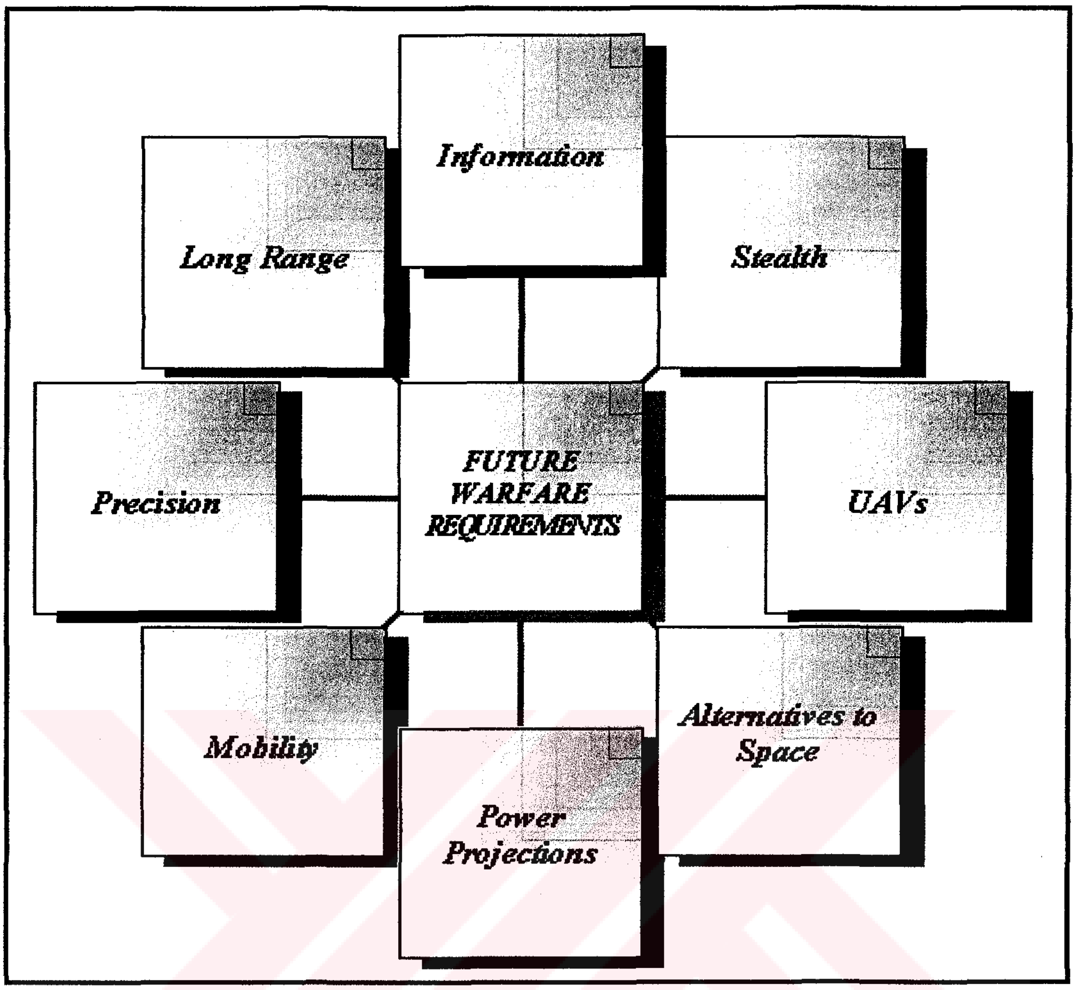


Figure 2.10: Future Warfare Requirements

Stealth: High-signature aerospace weapons won't survive in future war. Weapon systems must emphasize passive sensing, minimal reflectivity, and discrete emissions. If platforms have these characteristics but their support structures (e.g., tankers, AWACS, fixed air bases) do not, the platform as a weapon system will not survive.

Precision: Manned aerospace platforms will become increasingly expensive. Driven by their need to incorporate long range, stealth, data processing, and mobility, there's no way they will also be cheap. This expense will drive down inventories. At the same time, target sets are expanding (better C^2 will allow dispersion; the possibility of strategic attack adds to the number of targets). There's also the desirability of conducting near-simultaneous attack across all levels of war. Precision is required to reconcile these trends. Each sortie must kill multiple targets.

UAVs: UAVs' inherent stealthiness and minimal basing requirements allow low-signature operations. They are increasingly capable of long-endurance flights. They can perform strike, communications, and surveillance missions. While manned platforms will remain mandatory for certain types of missions, UAVs will make decisive contributions to future aerospace operations if employed skillfully in large numbers.

Mobility: One result of the Information Age will be the enemy's near-certain detection of fixed facilities. To offset this information, future commanders will need the flexibility to move land-based aerospace forces between bases. Such mobility requires a lean support structure. This concept affects how we envision munitions, C^2, maintenance, POL, and support equipment.

Alternatives to space: Satellites in fixed orbits will be exceedingly vulnerable in the future. Military operations dependent on satellite support rest on a dubious assumption of satellite survivability. We need alternatives to space-borne architectures. These alternatives should emphasize HALE UAVs and fiber-optic cable.

Power projection: Ubiquitous sensors and transmission devices will give our future military commanders extensive information on the enemy's scheme of maneuver. Unfortunately, the enemy will also have substantial information about our forces. This information will make either side's invasion forces exceptionally vulnerable when they mass to attack. Mobile defenses accompanying massed forces will be inadequate to stop interdiction forces emphasizing state-of-the-art information, C^2, penetration, and precision. It is at this point, very early in the battle, that wars will be won or lost. Therefore, future US weapons must be capable of *day one* operations. US weapons must have the capacity to strike with overwhelming force from the first day of the war.[108]

[108] Barnett, Jeffery R., Ibid.

3. ELECTRONIC WARFARE

Electronic warfare can be defined as "the use of the electromagnetic spectrum to degrade or destroy an adversary's combat capability (including degrading or preventing the use of the electromagnetic spectrum as well as degrading the performance of adversary equipment, personnel, and facilities); or to protect friendly combat capability (including protection friendly use of the electromagnetic spectrum as well as friendly equipment, personnel, and facilities that may be vulnerable to attack via the electromagnetic spectrum)."[109]

The concept of Electronic warfare or EW is not new. It was practiced as early as the WW II albeit in a different way. The Germans used EW effectively to confuse British Radar operators and quietly slipped two battle cruisers through the English Channel. Winston Churchill even called it the "Battle of the beams" and 'Wizard war". ECM (Electronic Counter Measures) and EW (Electronic Warfare) are today of the most important aspects of warfare.[110] The Germans made changes in the navigation beams used to guide their night attacks on England. British scientists were able, through careful detective work, to intercept the German beams and develop techniques to corrupt the German navigation data and defeat the night attacks. The British used electronic intercepts integrated with other forms of intelligence to identify the frequency and the purpose of the German transmission.[111]

Domination of the electromagnetic spectrum is a crucial component of most modern military operations. There are few battlefield elements that do not rely on communications and information systems. The C^2 cycle depends very heavily on the electromagnetic spectrum to maximize the effectiveness of surveillance and target acquisition, communications, and information systems. If these systems are destroyed, degraded, or deceived, the commanders and staff are unable to prosecute war adequately. Without

---

[109] Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001, p. 13.
[110] Raj, Manoj, "Airborne Electronic Countermeasures", Air Combat Information Group, U.S.A., January 2003, Available on site: http://www.acig.org/artman/publish/article_56.shtml
[111] Allan, C.T., "Electronic Warfare: Foundation of Information Operations", U.S.A., November 1999, Available on site: http://www.infowar.com/MIL_C4I

communications on the modern battlefield, the commander is deaf, dumb, and blind. Therefore, the capability to conduct electronic combat and dominate the electromagnetic spectrum is now a recognized component of any modern force structure.[112] EW is assessed as one of the most important concepts for the conduct of war because of the increasing importance of C^4I and electronic dependency of armed forces. The increasing amounts of digital data and information for C^4I are leading to a reassessment of military communication systems in favor of new concepts based on communications technologies.[113]

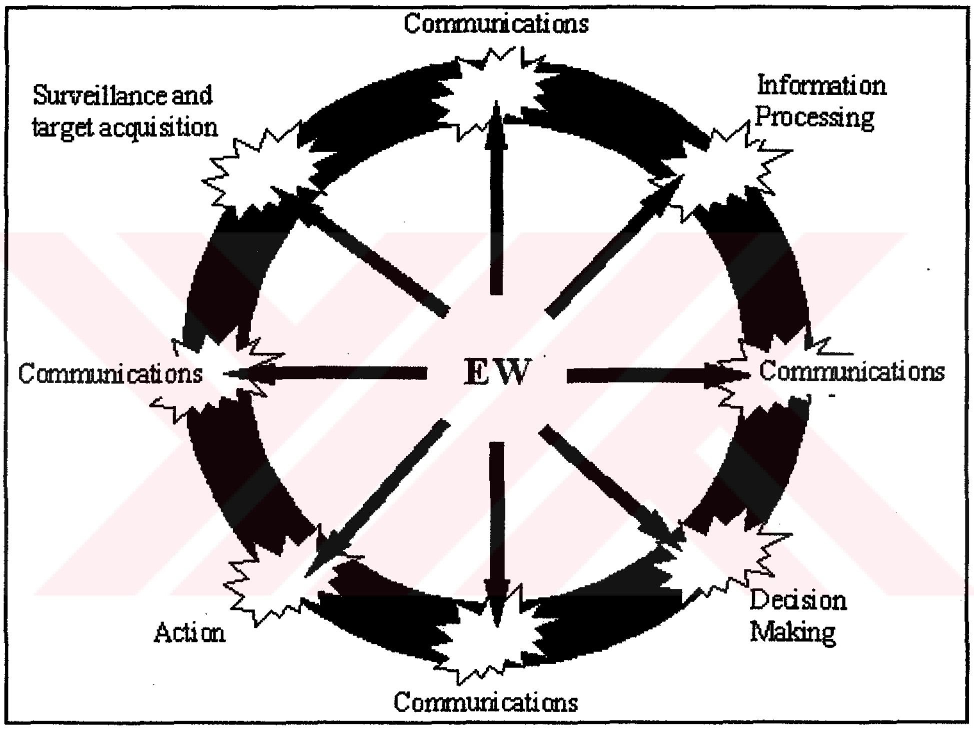


Figure 3.1: The potential impact of EW on the C^2 cycle.

Figure 3.1 illustrates how electronic warfare pervades all aspects of the modern battlefield and has the potential to impact on all elements of the C^2 cycle. In summary, EW resources are used to monitor adversary activities in the electromagnetic spectrum, indicate adversary strength and dispositions, give warning of adversary intentions, decisive and disrupt

[112] Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001, p. 12.
[113] Ingerman, S., "Data Flow", A Newsletter of RAD Data Communications, No: 44, U.S.A., Autumn 1999, p. 6, Available on site: http://www.rad.com/data/pages_6/page7.htm

sensors and command and control processes, and safeguard friendly use of the electromagnetic spectrum.[114]

EW uses physical principles in order to attack electronic devices such as radars, and communication links. Key areas covered include mathematical models for active, passive and active-passive jamming signals; jamming methods based on the use of false radar and thermal targets; the effectiveness of specific jamming methods; mathematical definitions of electronic anti-aircraft defense systems as targets; and the reduction of radar detectability.[115] Although EW is targeted against the technology, the ultimate affect is on a commander's ability to move through the C^2 cycle. The human element of the command system is both the strongest and weakest link and can fairly rapidly be enshrouded in the fog of war if supporting communications and information systems are disrupted, degraded, or deceived.[116]

EW activities are applicable across the whole spectrum of military operations and are not confined to warfare, conventional or otherwise. In peacetime, armies attempt to intercept, locate, and identify the source of a potential adversary's electronic emissions. Analysis may then reveal details of capabilities as well as vulnerabilities that can be used to gain an advantage in times of conflict.

EW is an area of considerable innovation. Inevitably, and often very rapidly, advantages gained by technological or procedural change are met with equally effective countermeasures. In order to maintain the edge in any future conflict, information on friendly methods of electronic protection and attack must be safeguarded.[117] Electronic counter-measures (ECM) on the other hand are ways that the opposition tries to deny the use and advantage of the use of the electromagnetic spectrum. In simpler terms EW/ECM is a complex and technological game of ping-pong; with one side trying to outdo the other.[118]

---

[114] Frater, Michael R., and Michael Ryan, Ibid, p. 13.
[115] Vakin, S.A., et. al., "Fundamentals of Electronic Warfare", Artech House, London, U.K., 2001.
[116] Frater, Michael R., and Michael Ryan, Ibid, p. 13.
[117] Frater, Michael R., and Michael Ryan, Ibid, p. 12-14.
[118] Raj, Manoj, "Airborne Electronic Countermeasures", Air Combat Information Group, U.S.A., January 2003, Available on site: http://www.acig.org/artman/publish/article_56.shtml

The rapidly developing EW capabilities in the Asia-Pacific region reflect the widespread efforts to achieve national self-reliance, the general recognition of the value of EW as a force multiplier, the defense modernization programs (which necessarily include significant electronic components), and the ability of many countries in the region to indigenously produce advanced electronic systems (or the desire to promote the development of indigenous electronic sectors through local design and production). ELINT is an essential ingredient in both the design and operation of EW capabilities.[119]

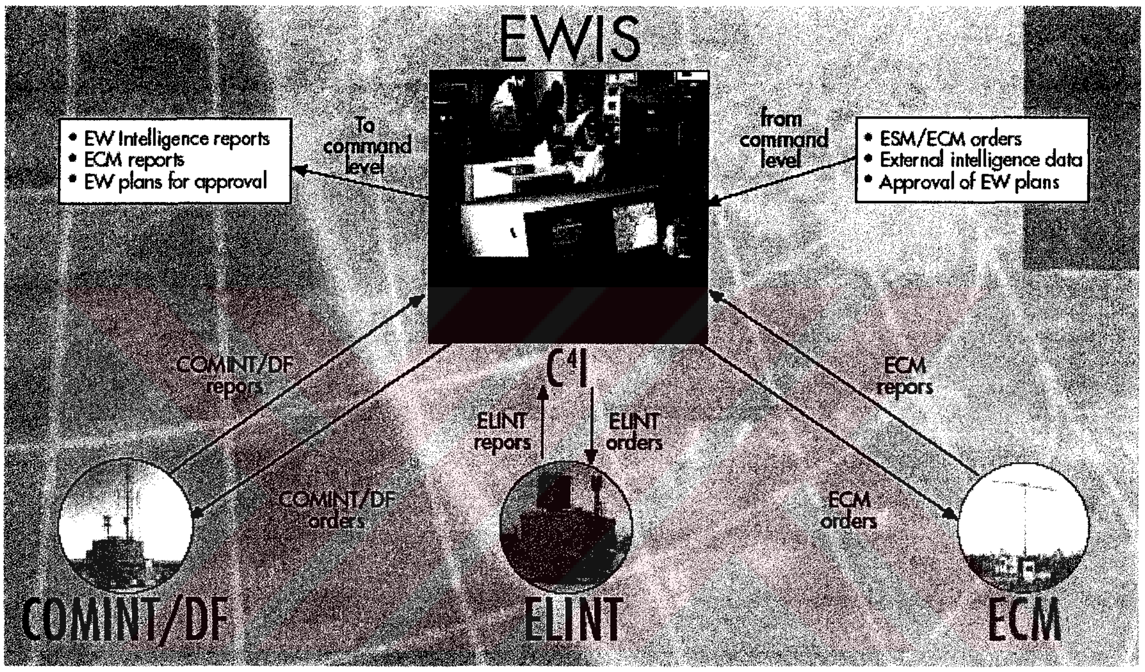


Figure 3.2: The Electronic Warfare Integrated System (EWIS)

The major components of the *electronic warfare integrated system* (EWIS) are:[120]

1. **C^{4}I:** The Command, Control, Communication, Computer and Intelligence Systems (C^{4}I) control the EWIS operation and form the interface with the command level. It is the link between the various system elements and the human factor, which delivers the dramatic power boosting of the integrated system. The C4I process EW intelligence gathered by the COMINT/DF and ELINT stations and assigns missions

[119] Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm
[120] Tadiran Electronic System Ltd. "Electronic Warfare Integrated System (EWIS)", Tadiran Electronic System Ltd., Holon, Israel, 2003. Available on site: http://www.tadsys.com/EWIS.pdf

to the ECM stations. A user friendly interface is utilized to facilitate efficient, accurate and timely operation.

2. **ELINT:** Electronic Intelligence (ELINT) stations complement the COMINT/DF stations by detection, interception, classification, location, analysis and identification of non-communication transmitters. Together they cover a complete spectrum of operational and tactical threats required for the generation of the Electronic Order of Battle (EOB).
3. **COMINT/DF:** Communication Intelligence and Direction Finding (COMINT/DF) stations provide services over a wide range of frequency bands (HF, VHF & UHF). Their advanced demodulation, classification and agile signal detection capabilities are combined with smart location techniques and supply a full, multifaceted, real time display of the EW arena activity.
4. **ECM:** The Electronic Countermeasure stations are the active elements of the EWIS, capable of interfering with hostile communications and electronic systems, or inserting false information in order to disturb its operation. They can jam communication equipment and networks, imitate and retransmit enemy's communication.

EW is a major facets in every area of a modern air warfare campaigns, including close air support (CAS), air-to-air, battlefield air interdiction (BAI), strikes against command and control targets, and destruction or suppression of enemy air defenses (DEAD and SEAD). Among all these, it is the last two that simply cannot succeed without ECM.

3.1. COMMUNICATIONS AND NONCOMMUNICATIONS EW

EW is normally divided into two main areas: communications EW and non-communications EW. Communications EW is almost as old as electronic communications itself and, on the battlefield, is mostly concerned with communications sources that transmit in frequency bands between HF and SHF. The intercept and analysis of transmissions are usually more important than the measurement of transmitter characteristics. Noncommunications EW has been developed since the early employment of radars in World War II and is primarily concerned with platform protection, and normally specifically oriented towards radar systems in the UHF and higher bands. In non-communications EW, the measurement of emitter characteristics is central as they are used to detect the presence of, and possibly identify, a piece of equipment and-or its performance.[121]

EW against communicators is generally more difficult to wage than EW against radars. The signal strength of communications weakens with the distance to the transmitter squared (versus the fourth power with radar). While radars try to illuminate a target (and therefore send a beam into the assets of the other side), communicators try to avoid the other side entirely and thus point in specific directions. Communicators move toward frequency- hopping, spread-spectrum, and code-division multiple access technologies, which are difficult to jam and intercept. Communications to and from known locations (e.g., satellites, UAVs) can use digital technologies to focus on frontal signals and discard jamming that comes from the sides. Digital compression techniques coupled with signal redundancy mean that bit streams can be recovered intact, even if large parts are destroyed.[122]

One can see from this why electronic warfare is shrouded by so much secrecy. The principles of electronic warfare are not complex, nor are the technologies. What are precious are the frequencies used by sensors in weapons systems and the frequency-hopping plans that are employed by communications systems. Just as precious is information about the capabilities of jamming units; their range, their agility at moving from frequency to frequency, their sensitivity to frequency.[123]

EW is also used to geolocate the emitter. The noisier the environment, the more difficult the task is. One defense is to multiply sources of background electronic clutter shaped to foil intercept techniques that rely on distinguishing real signal patterns. Voice calls have certain patterns in terms of who talks when and what percentage of the time is filled with blank time (e.g., listening). Encryption techniques can mask blank time patterns. False emitters can generate false conversations from random locations.

[121] Frater, Michael R., and Michael Ryan, Ibid, p. 14.
[122] Libicki, Martin, "What is Information Warfare", National Defense University, August 1995, Available on site: http://www.iwar.org.uk/iwar/resources/ndu/infowar
[123] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 286.

As suggested above, the work of finding targets is likely to shift from manned platforms to distributed systems of sensors. Despite the impending necessity of distributed systems often heavily used communications links between many sensors, command systems, and dispersed weapons. In a trivial comparison, an F-18, with its pilot, FLIR sensors, and attached weapons, can link all three with wires or in the pilot's mind and is therefore far more resistant to jamming. In sensor-rich environments, EW –expressed by jamming or by soft- kill –can assume a new importance. Interference with communications from local sensors, for instance, can create virtual blank areas through which opposing systems can move with less chance of detection. The success of this tactic critically depends on the architecture of the distributed sensor system to be disrupted. A system that relies exclusively on distributed local sensors (intercommunicating or relaying signals by low power to switches) is the most vulnerable. A system that interleaves local and stand-off sensors are more robust, particularly where coverage varies and overlap is common.[124]

As an aside, EW is also associated with *signals intelligence* (SIGINT), which contains two main subcomponents:

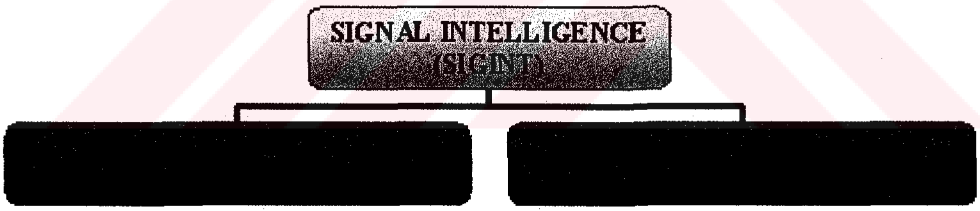


Figure 3.3: SIGINT Main Subcomponents.

To a large extent, these mirror the functional areas of communications and non-communications EW, but take place in the strategic environment rather than the tactical one.[125]

[124] Libicki, Martin, Ibid.
[125] Frater, Michael R., and Michael Ryan, Ibid, p. 15.

3.2. EW SUBDIVISION

There are three fundamental subdivisions within EW that are applicable to both communications and non-communications EW, albeit with the different degrees of emphasis noted earlier:

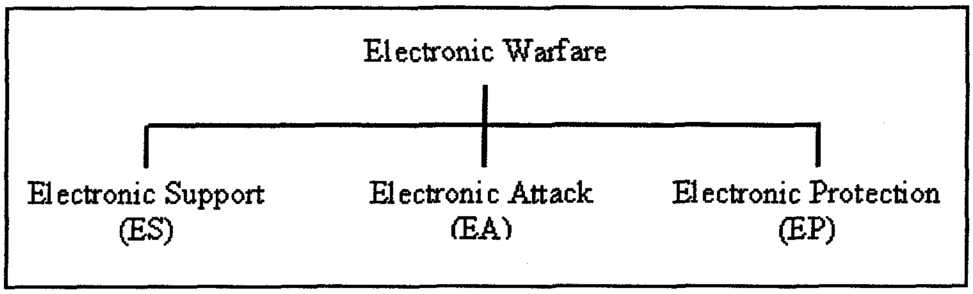


Figure 3.4: Major subdivisions of EW.[126]

Electronic Attack: Formerly known as electronic countermeasures (ECM), is the division of EW involving the use of electromagnetic energy to attack personnel, facilities, or equipment with the intent of degrading or destroying adversary combat capability. EA comprises jamming, electronic deception, and neutralization.[127] Jamming involves the deliberate radiation, re-radiation, or reflection of electromagnetic energy with the object of impairing the use of electronic devices, equipment, or systems being used by an enemy. Jamming includes both the denial and falsification of information. This can be accomplished electronically through the use of high-powered transmitters or mechanically through the use of chaff to confuse and saturate enemy radars.

Deception involves the deliberate radiation, re-radiation, alteration, suppression, absorption, denial, enhancement, or reflection of electromagnetic energy in a manner intended to convey misleading information to an enemy or to enemy electromagnetic-dependent weapons, thereby degrading or neutralizing the enemy's combat capability. Among the types of electromagnetic deception are:[128]

---

[126] Ünal A. N., "Elektronik Saldırı", Ulusal Strateji Dergisi, Yıl: 3, Sayı: 17 CNR, Istanbul, 2001, p.46.
[127] Nemzetvédelmi, Zrínyi Miklós, "Advanced Military Technology Related Research Work at Electronic Warfare", National Defense University, U.S.A., 2002, Available on site: http://www.zmka.hu/tanszekek/ehc/konferencia/may/makkay.htm
[128] Public Affairs Office, "Naval Special Warfare and Special Operations", United States Naval Academy, U.S.A., 2003, Available on site: http://www.usna.edu/Training_probook/spring03/proman

1. Manipulative Deception: Actions to prevent revealing electromagnetic telltale indicators or convey misleading indicators that may be used by hostile forces.
2. Simulative Deception: Actions to simulate friendly, notional, or actual capabilities to mislead hostile forces.
3. Imitative Deception: The introduction of electromagnetic energy into enemy systems that imitates enemy emissions.

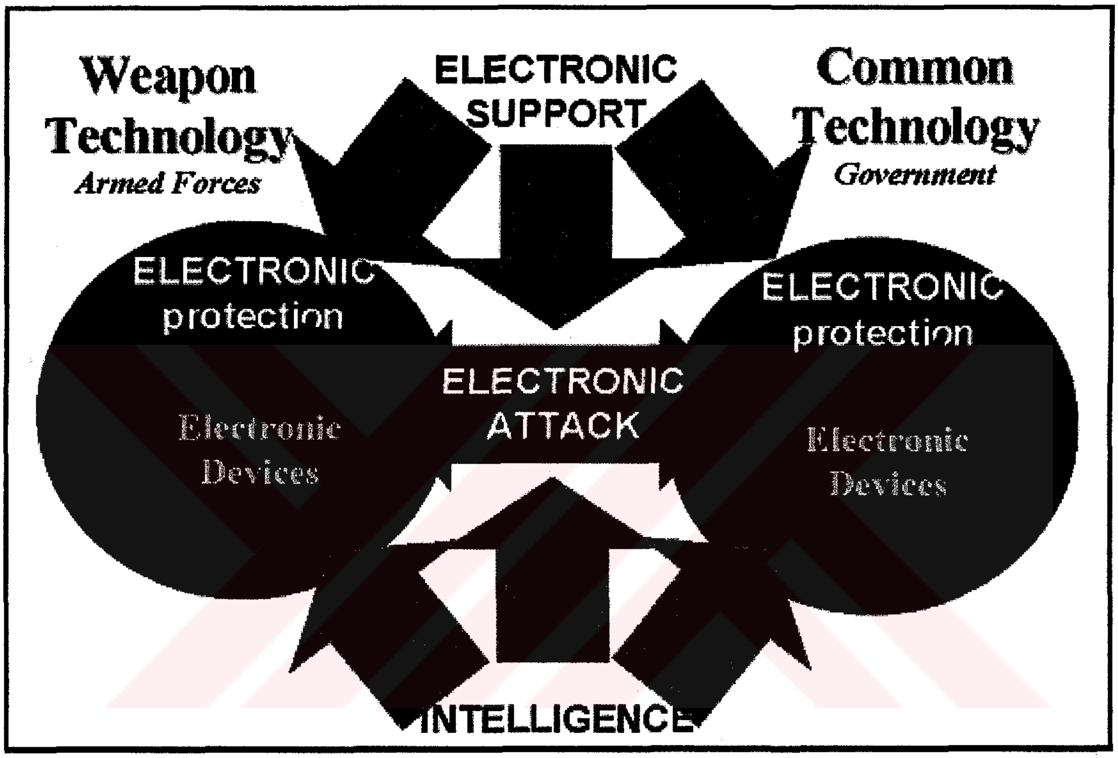


Figure 3.5: The main parts of electronic warfare

Neutralization describes the use of very high levels of electromagnetic energy to disrupt or permanently damage electronic equipment.

Electronic Support: Formerly known as electronic support measures (ESM), is the division of EW involving actions tasked by, or under the direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional an unintentional radiated electromagnetic energy for the purposes of immediate threat recognition and constructing an electronic order of battle. An electronic order or battle includes information on the nature and the deployment of all electromagnetic emitting equipment of military force, including equipment types, frequencies, modes of operation, locations, and other relevant data.[129] During combat, ES can identify order of battle changes, targeting information, threats to friendly units, and potential targets for EA.

Locating the source of threat signals is one of the objectives of ES. This is primarily achieved using bearings to the received signal. Lines of Bearing (LOB) and cross-fixing are two ways that these bearings can be used to help locate a threat. The intensity and mode of operation of the signal can also assist in locating the emitter. Often, ES information can be correlated with contact information from other sources to more accurately determine the classification and location of contacts.

ES provides early detections of enemy radiations at long ranges. This facet of EW is completely passive and consists of receivers that gather, process, and display all signals of interest required to meet a specific mission requirement.[130] To determine which contacts represent a threat, analysis of received signals consists of reviewing the following parameters in figure 3.6.

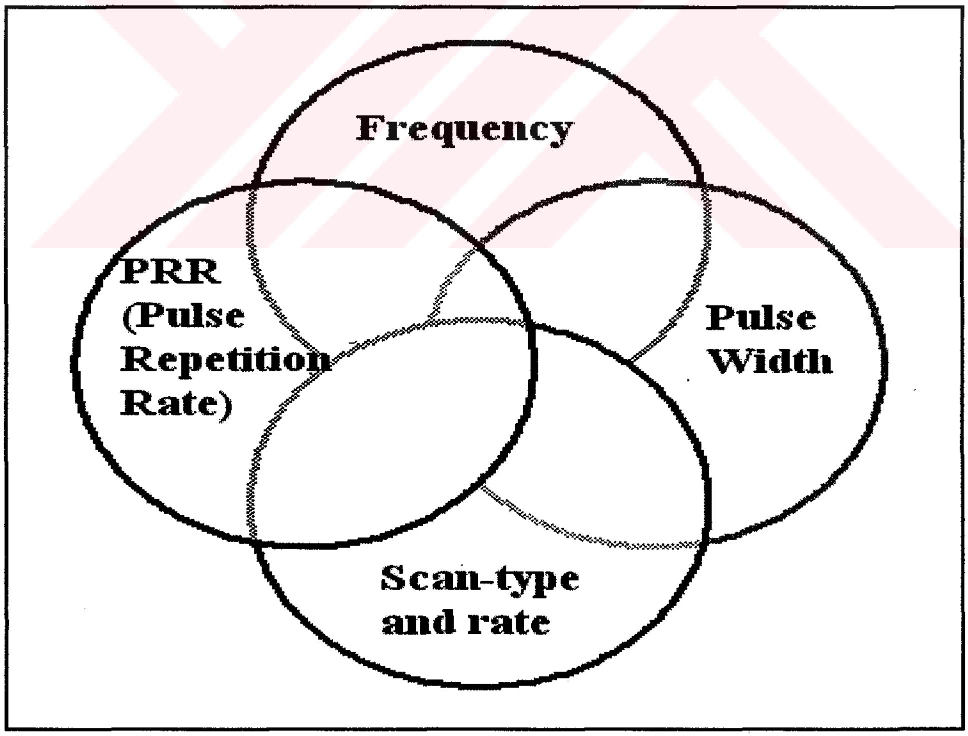


Figure 3.6: The Parameters of Received Signals

[129] Nemzetvédelmi, Zrínyi Miklós, Ibid.
[130] Public Affairs Office, "Naval Special Warfare and Special Operations", United States Naval Academy, U.S.A., 2003, Available on site: http://www.usna.edu/Training_probook/spring03/proman

Electronic Protection: Formerly known as electronic protection measures (EPM) or electronic counter-countermeasures (ECCM), comprises those actions taken to protect personnel, facilities, and equipment from any effects of friendly or adversary employment of EW that degrade, neutralize, or destroy friendly combat capability.[131] EP can be technical (such as encryption devices), procedural (such as training operators to work through jamming), or tactical (such as terrain masking of antennas). Effective EP is achieved through good training, sound procedures, and thorough planning for alternative communications means. The measures used must be continually adjusted to the tactical situation. When the enemy's EA efforts change in focus or method, EP efforts must be adapted. This facet of electronic warfare includes both *anti-EA* and *anti-ES measures*.[132]

Anti-EA measures include system techniques and frequency control, i.e. the ability of fire control radar to operate at various frequencies to prevent jamming of a single effective frequency.

Anti-ES measures include tactical evasion and Emissions Control (EMCON): (1) Tactical evasion is the routing of forces so that the enemy is unable to use his EW equipment effectively, the stationing of forces such that they are difficult to locate, or the use of ships as decoys. (2) Emissions Control (EMCON) is perhaps the best anti-ES measure and this involves having a thorough knowledge of the enemy's ES capabilities and applying total or partial EMCON to your unit/units so as to deny the enemy the use of his equipment. The drawback is the possibility of “blinding” friendly units by denying the use of active detection methods. EMCON is the selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security (OPSEC), detection by enemy sensors; to minimize mutual interference among friendly systems; and/or to execute a military deception plan.

Electronics are available and used everywhere. They are objective of enemy's EA that is why they must be protected and supported by friendly electronic warfare measures. Enemy's Signal Intelligence (COMINT, ELINT etc.) also tries to catch electronic devices. We must be expert of electronic devices used in all military and related common

[131] Frater, Michael R., and Michael Ryan, Ibid, p. 15-16.
[132] Public Affairs Office, Ibid.

technology. There are new EW robots -like a spider. It is not bad because even the spider can sense a minimum of changing in own cobweb, flying over the future's battlefield. The vertical takeoff or landing (VTOL) air vehicle can extremely improve EW capability of 21st century force. They are remote controlled by computer for a distance. This is the air vehicle what about EW experts are dreaming for a long time. They can carry EW equipment to the necessary position at under minimum flying weather conditions. They can fly when situation can not allows flying by manned aircraft.[133]

3.3. INTEGRATED INTELLIGENCE SUPPORT

Integration is absolutely critical to C^4I as in every warfare area. Planning, execution, and evaluation of both counter-C^4I and C^4I-protection are necessary by commanders at all echelons. The C^4I operational commander must have the best available intelligence on enemy situations, intentions and capabilities in order to weigh the potential advantage of specific actions. C^4I plans and operations must also be coordinated with other potentially affected intelligence and counterintelligence activities.

Intelligence to support C^4I activities is the result of the collection, evaluation, analysis, and interpretation of all available information that concerns one or more aspects of foreign nations or areas. Intelligence support generally includes[134]:

- Developing and maintaining databases in sufficient detail to support C^4I in geographic areas of potential conflict.
- Identifying critical C^4I nodes, links and sensors of potentially hostile nations.
- Assessing the capabilities, limitations, and vulnerabilities of potential C^4I targets.
- Identifying the key political and military leaders in potentially hostile nations, including psychological profiles of leaders to support (as a minimum) the PSYOP element of C^4I.
- Estimating hostile counter-C^4I capabilities to assist in determining the vulnerability. C^4I capabilities and the impact on forces and friendly military operations.
- Providing accurate direction finding (or geo-location, if available) information on pulsed and continuous wave signals.

---

[133] Nemzetvédelmi, Zrínyi Miklós, Ibid.
[134] Public Affairs Office, Ibid.

- Supporting Battle Damage Assessments (BDA).

Therefore it is assessed that C^4ISR systems would be more important than before for the future battlefield. According to military experts of the United States: "…with the support of an advanced C^4ISR backbone, the United States will be able to respond rapidly to any conflict…".[135]

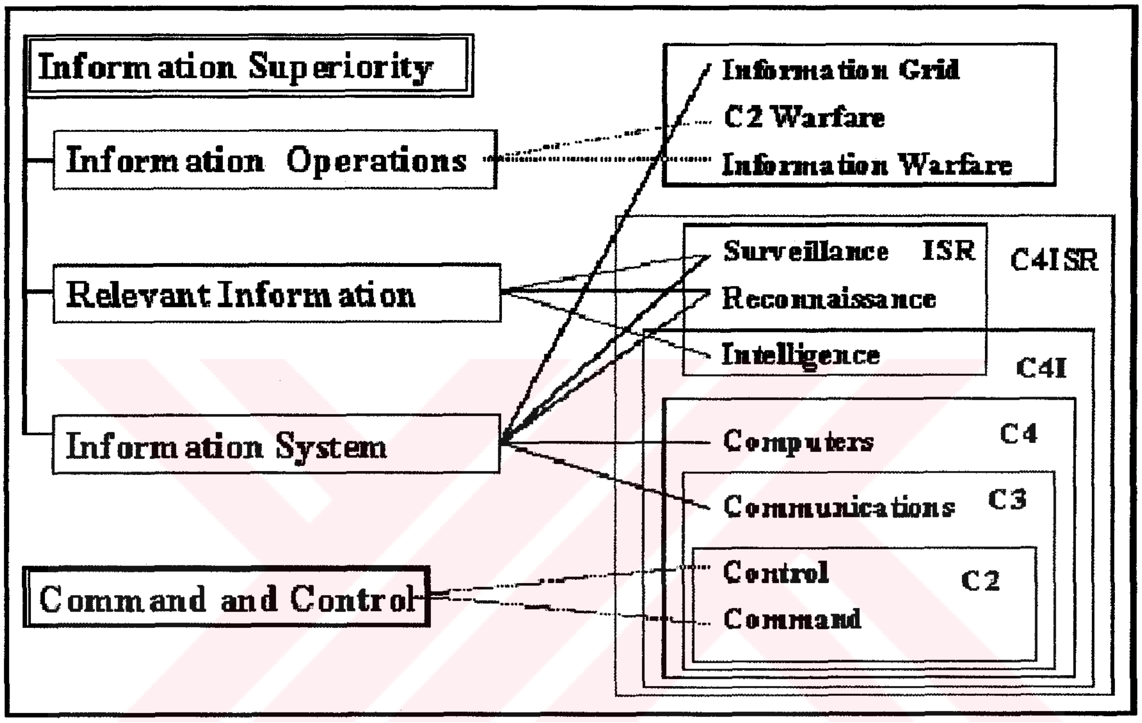


Figure 3.7: Elements of Information Superiority.[136]

And also the Russian military thinks that, superiority for the future battlefield proceeds from superiority in C^4ISR systems:[137] (1) reconnaissance, surveillance, and target acquisition (RSTA) systems, and (2) intelligent, command and control (C^2) systems. Indeed Chinese military thinks that: "Key information weapons include precision-guided weapons systems and electronic warfare weapons systems as well as C^4I systems (communications, guidance, control, computer, and intelligence) which form the central nervous system". Furthermore the US Army's report states that advances in information

[135] Cohen, W.S., "Annual Report to the President and the Congress", DTIC, Washington, D.C., U.S.A., 1999, Available on site: http://www.dtic.mil/execsec/adr1999/index.html
[136] Steele, Robert D., "A New Approach to Collection, Sharing and Analysis", OSSA: Open Source Solutions Academy, Fairfax, VA, U.S.A., 2000.
[137] FitzGerald, M.C., "Russian Views on IW, EW, and Command and Control: Implications for the 21st Century", CCRP, Department of Defence, Washington, D.C., U.S.A., 1996, Available on site: http://www.dodccrp.org/1999CCRTS/pdf_files/track_5/089fitzg.pdf

management and distribution will facilitate the horizontal integration of the battlefield functions and aid commanders in tailoring forces and arranging them on land...[138]

Furthermore scientific studies are funded by all countries about the future battlefield. As an example according to a study about C^4ISR Analytic Performance Evaluation: "One role of C^2 is to select the appropriate strike platforms and weapons to attack targets. This allocation dynamically changes through the scenario as a function of battle phase, ISR system capability, remaining enemy targets, and remaining inventory of strike platforms and weapons.[139]

3.4. SIGNALS INTELLIGENCE (SIGINT)

If electronic warfare is the control and manipulation of the electromagnetic spectrum, and the spectrum is the environment in which information, data, and energy lives, then the collection, interpretation and communication of this information enables the other elements of EW. Central to the EW support mission are the military's electronic and signals intelligence capabilities.[140]

The collection of electromagnetic intelligence by an adversary, directed towards a specific plan of operations, is of concern to military planners. The broad spectrum of this intelligence collection is referred to as Signals Intelligence (SIGINT), a key area of intelligence gathering frequently used by forward deployed naval forces. SIGINT is divided into two major functional categories:[141]

Communications intelligence (COMINT): The intelligence collected by the interception of any communications methods. Some examples are seen in Figure 3.8.

---

[138] Schneider, B.R., "Battlefield of Future: Principles of War for the Battlefield of Future", Air Force Press, Maxwell, U.S.A., 1998, Available on site: http://www.airpower.maxwell.af.mil/airchronicles/battle/chp1.html

[139] Parker, S., H. Neimeier, "C4ISR Analytic Performance Evaluation Models", MIT Publication, U.S.A., August 1998, Available on site: http://www.mitre.org/pubs/edge/august_98/cape.html

[140] Pitts, Joseph R., "What is Electronic Warfare?", A Speech to the Lexington Institute, Washington, D.C., U.S.A., 22 October 2003, Available on site: http://www.house.gov/pitts/Commentary from.htm

[141] Neri, Flippo, "Introduction to Electronic Defense Systems", Artech House, Boston, 1991, p 321-322.

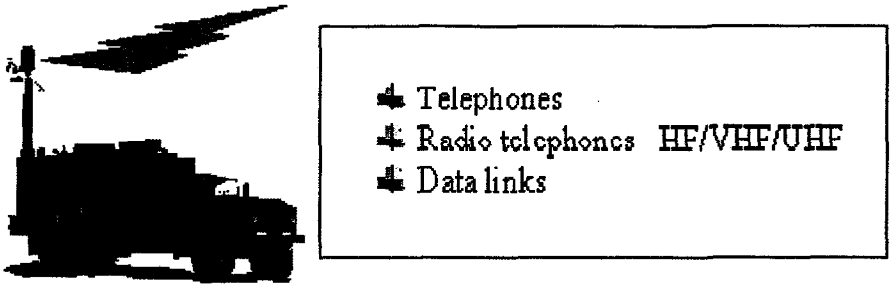


Figure 3.8: Examples of COMINT methods.

Electronics intelligence (ELINT): The intelligence collected through the interception of any Noncommunications electronics systems. Examples include in Figure 3.9.

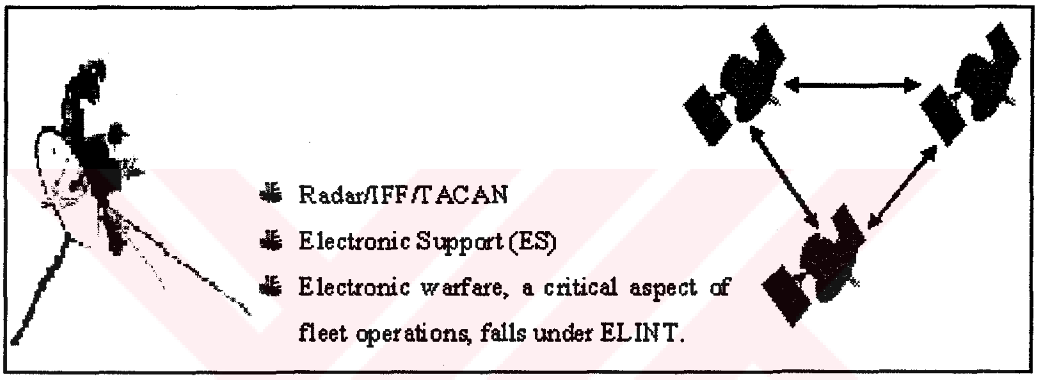


Figure 3.9: Examples of ELINT methods.

Sending and receiving signals and communications continues to take major leaps forward. The implications of the advances made in these areas include the ability to:[142]

1. send and receive signals and communication real time;
2. listen and jam enemy communications; and
3. process and manipulate data through the use of sophisticated algorithms. Advances in electronic and signals intelligence have raised the profile of vital assets, such as the RC 135 Rivet Joint, EP-3, RC-12 (Guardrail Common Senor), U-2, and Unmanned Aerial Vehicles (UAVs).

Further electronic and signals intelligence capabilities are enhanced by advances made in the networking services. This allows the military to leverage the strengths of each branch of the service to accomplish a mission while shielding the weaknesses from the enemy.

[142] Pitts, Joseph R., Ibid.

Unfortunately, electronic (ELINT) and signals (SIGINT) intelligence is generally overlooked when discussing the merits of EW. Discussions of EW typically focus on the other two elements: electronic protection and electronic attack. Without the value and necessity of EW support being articulated as the foundation of EW, it is difficult to effectively promote the other elements and understand the enormous value they have in accomplishing supremacy of a battle space. While electronic (ELINT) and signals (SIGINT) intelligence is not solely EW, it must be seen, understood and communicated as part of the foundation of EW.[143]

Sophisticated SIGINT and EW capabilities are in fact integral to the operation of the modern weapons systems which are currently being acquired throughout the Asia-Pacific region. Modern missile systems, for example, simply cannot be effectively utilized without real-time intelligence and surveillance information, supported by a thorough and comprehensive catalogue of the electromagnetic environment in the area of operations.[144]

Most of the countries in the Asia-Pacific region have recently acquired long-range anti-ship missiles, such as Harpoon or Exocet, which are designed for use at beyond-line-of-sight or over-the-horizon ranges. SIGINT is invaluable to the effective operation of these systems. HF and VHF DF systems provide the principal means of detecting and locating enemy ships; analysis of the communications and radar emissions is a primary means of determining the nationality, class, and even the identity of particular ships; and, together with other electro-optical techniques, a means of precision-guidance of the missiles to the targeted ships. Modern air defense systems utilize ELINT together with active radar for threat warning and location. A whole class of anti-radiation missiles ARMs) exists for attacking radars on the basis of their signal emissions (frequency, power, pulse rates, and characteristics, and so forth). It has been widely recognized that defense operations on the modern electronic battlefield simply cannot be effectively conducted without full and real-time intelligence concerning the adversary's electronic order of battle (EOB) that is, catalogues of the plethora of communications systems, radars, and other electro-magnetic emitters which might be expected in area of operations.

143 Pitts, Joseph R., Ibid.

144 Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm

Moreover, countries in the region attempting to achieve greater defense self-reliance generally recognize the value of capitalizing on 'force multipliers', of which electronic warfare is one of the most potent. The acquisition of EW systems can be traded off against that of expensive platforms to achieve greater defense capabilities within given budgetary and other resource constraints. In the Asia-Pacific region, Japan is clearly the leader with respect to the acquisition of advanced EW equipment. All of the major platforms of the JASDF and JMSDF have advanced ESM systems for detecting, identifying and informing counter-measures against electronic threats.[145]

3.5. ELECTRONIC INTELLIGENCE (ELINT) SYSTEMS

The mission of this class of equipment is mainly strategic, but also tactical. In their strategic role, ELINT systems are capable of providing information about the technological status of a potentially hostile country and on its military activity. This information will have to be translated into plans that can have an impact on the political, military, and industrial sphere.

Detection of signals generated by new equipment of higher quality or by the use of a new frequency band must lead to the initiation of military and industrial programs for the neutralization, if necessary, of these new threats. Detection of unusual electromagnetic activity, or of the movement toward borders of a quantity of radar equipment, may suggest some political moves are required to clarify the situation.

However, ELINT systems have an important tactical objective, as well as a strategic one. Given the enormous amount of precise and detailed information known about emitters, an ELINT system is capable of following the displacement of one single piece of equipment and of providing a very accurate EOB. Furthermore, the available sensors are so precise that an ELINT system can be the principal supplier of information for the libraries to be loaded into the ESM, RWR, and ECM devices.[146]

---

[145] Cereijo, Manuel, Ibid.
[146] Neri, Flippo, "Introduction to Electronic Defense Systems", Artech House, Boston, 1991, p 321-322.

3.5.1. ELINT Sensors

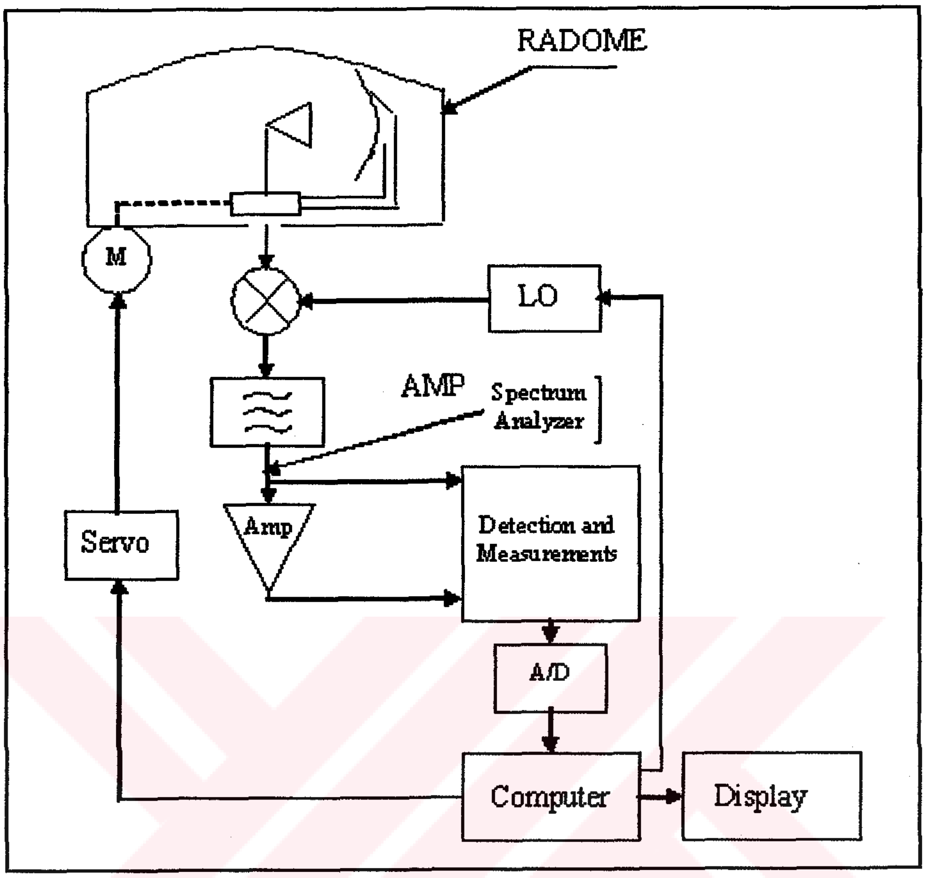


Figure 3.10: Block diagram of an ELINT system.

Figure 3.10 shows the block diagram of an ELINT sensor. Since its task is not to give immediate warning, but rather to give very precise measurements, well protected from interference, an ELINT system is usually of the super heterodyne type, with a directive, rotating, receiving antenna, which can be trained in directions of interest by means of servomechanisms. This configuration provides ELINT systems with a high sensitivity that allows detection ranges of a few hundred kilometers. In order to minimize the range restriction resulting from the curvature of the earth, this equipment is often installed at elevated sites. Thus the receiver has the capability of measuring many parameters with great precision, to the point of being able to identify a specific device (finger printing), and, after integration with other data, may be able to identify the platform on which the devices is installed. An ELINT system generally has several IF bands at its disposal and is capable of analyzing the spectra of single emissions. It can load very long pulse buffers stores to enable accurate analyses to be performed in delayed time. An operator may see the results on a display in both tabular and graphic form. The enormous mass of data is extracted by the ELINT processing centers, either by a protected link or on recorded tapes and discs.[147]

3.5.2. The ELINT Processing Center

An ELINT processing center (Figure 3.11) has the following functions:

- Gathering of data and information.
- Generation of a data base.
- Generation of strategic information.
- Generation of tactical information (libraries for ED system).

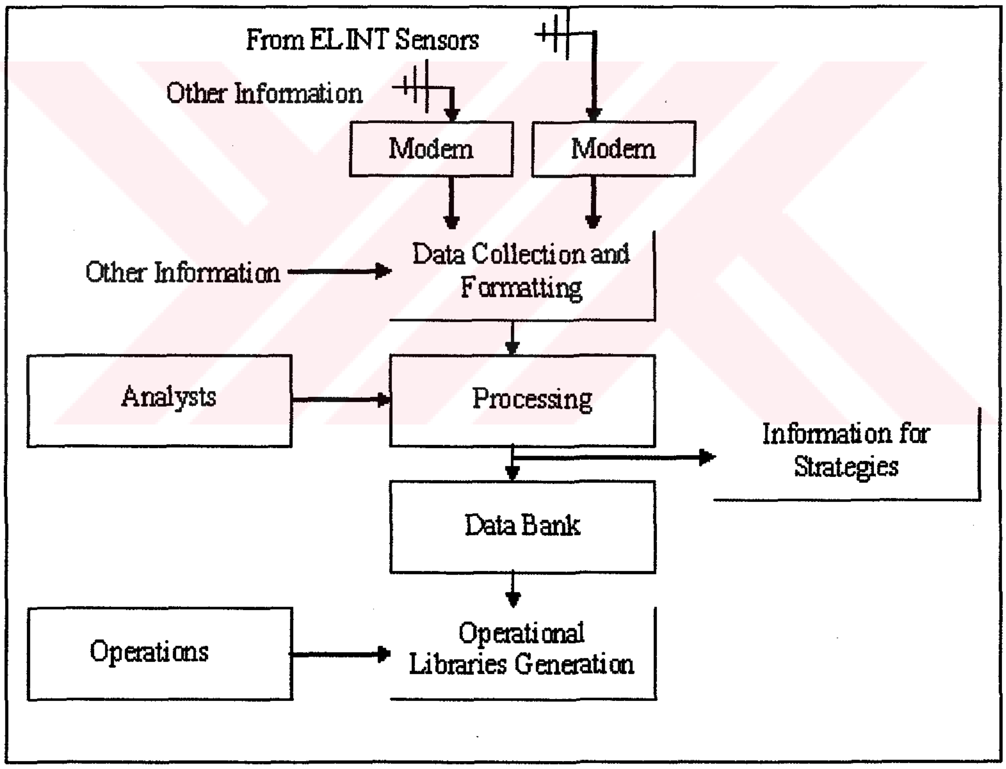


Figure 3.11: Diagram of an ELINT processing center.

To perform these functions, the ELINT processing center must be able to receive information from both ELINT and other ES sensors, and from other intelligence organizations. All information is formatted, that is, rendered homogeneous to allow subsequent digital processing. It must be correlated, filtered, and analyzed by experts to

[147] Neri, Flippo, Ibid, p 322.

extract potential strategic information and to add to data base memory. Once the data base has been formed, depending on the political-military situation, operations experts will prepare libraries for the various operational departments that will insert them into the memories of ED equipment.[148]

3.6. THE HISTORY OF EW AND ELINT

3.6.1. The Dawn of EW and ELINT

The electronic warfare is almost as old as the use of electronic for military purposes. At the time of the Russo-Japanese War, in 1904-1905, the Russian and Japanese fleets were well equipped with WT (wireless telegraph) sets. The Japanese navy used the WT freely and effectively to control the fleet, even though such transmissions often alerted the Russians to the presence of Japanese ships. The Russian Navy on the other hand tightly controlled its use of WT and exploited its passive and active modes tactically: a number of Russian ships avoided trouble when they heard Japanese signals traffic before they were spotted, and the Russians disrupted Japanese operations on several occasions by jamming their communications with WT.[149]

In World War I it consisted of jamming and intelligence analysis of radio and morse transmissions used by ground formations. Radios were too heavy and bulky for the World War I airplanes. During the inter-war years technological developments reduced the weight of radios and just prior to the outbreak of World War II radar was developed. Radar allowed for the detection and tracking of aircraft.[150] During World War II, the British, using the Enigma machine, had almost perfect access to German operational codes. They therefore knew, at the same time that the German field commander did, that the Luftwaffe had been ordered to destroy the city of Coventry in centre England.[151] By 1944 the use of EW became widespread within the RAF's Bomber Command. The main purpose of

[148] Neri, Flippo, Ibid, p. 322-324.
[149] Raj, Manoj, "Airborne Electronic Countermeasures", Air Combat Information Group, U.S.A., January 2003, Available on site: http://www.acig.org/artman/publish/article_56.shtml
[150] Nederveen, Gilles Van, "Sparks Over Vietnam - The EB-66 and the Early Struggle of Tactical Electronic Warfare", Airpower Research Institute, ARI Paper 2000-03, U.S.A., 2000, p.4, Available on site: http://www.airpower.maxwell.af.mil/airchronicles/ct/research/sparks
[151] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 324.

different devices used was to confuse and dilute German defenses, make large bombers inconspicious and make small aircraft look like large bombers, or make aircraft to appear as moving at very low speeds.[152] Airborne electronic warfare was used extensively by the United States Army Air Force (USAAF) in both the European and Pacific theaters during World War II. Its purpose was to ensure that bombers got through the enemy's radar-guided defenses to bomb targets in Japan or Germany.[153]

Before radar countermeasures could be conducted effectively considerable knowledge of enemy radar emissions, referred to as ELINT (electronic intelligence) or RADINT (radar intelligence), needed to be collected and analyzed. Specially modified aircraft, equipped with radar investigational equipment, for the most part bombers, such as the B-24 or B-17, and were used to "ferret" out enemy signals. B-24s and B-17s were outfitted with jamming equipment and these accompanied the bomber streams. With electronic intelligence the jammers could be tuned to the correct frequencies blinding the enemy's radar or electronic aids during the bombing missions. Much of this jamming capability would be jettisoned in the swift demobilization that took place after V-J Day.[154] The belief that the peace would be maintained or war waged by atomic bombs that could be carried by a single aircraft able to penetrate any enemy's defenses fostered the idea that jamming aircraft would no longer be needed.

3.6.2. Korean War, EW and ELINT

The Korean War in 1950 found the U.S. unprepared for electronic warfare. Although lacking jamming capability, the U.S. did have some electronic reconnaissance capability when the Korean conflict began. It was limited to strategic bomber units, since atomic bombing missions still needed to get through enemy defenses with atomic bombs. The Air Force mapped electronic radar sites so bombers could reach their targets undetected or at least with minimal exposure to an enemy's air defense system. Tactical air forces, in contrast, relied on speed, maneuverability, and the cover of darkness to carry out their

[152] Raj, Manoj, Ibid.
[153] Nederveen, Gilles Van, Ibid, p.4.
[154] Streetly, Martin, "Airborne Electronic Warfare, History, Techniques and Tactics", Jane Publishing Group, New York, NY, U.S.A., 1988.

interdiction missions. They did not develop electronic countermeasures to defeat the enemy electronic ground defenses consisting of radar-controlled guns and searchlights.[155]

During the Korean War, Far East Air Force (FEAF), operating from Japan and South Korea, faced a formidable number of Soviet supplied air defense systems on the Korean battlefield. Initially both FEAF and SAC (which controlled the B-29 bombers) were unwilling to use the small number of jammers in the USAF inventory for fear of revealing U.S. capabilities. However, in 1952 as North Korean radar-guided guns began to take their toll on B-26 night intruder strikes and B-29 bombing raids, this tactic was changed. B-29 raids flew with jammer equipment fitted on board. The tactical aircraft unfortunately did not have jammers. FEAF and Fifth Air Force had one RB-26, which could locate North Korean radar signals and then photograph the actual radars for later strikes, but this system was too cumbersome to be effective in North Korean combat. Fifth Air Force began to convert more B-26s in an effort to build both an electronic reconnaissance and jammer force for its tactical bomber units.

The Korean War was a reminder that tactical air forces required sophisticated electronic reconnaissance capabilities in order to operate in enemy airspace.[156] Strategic Air Command's RB-29 and RB-45 aircraft were pressed into service to collect ELINT over North Korea and neighboring communist countries.[157] Similar electronic reconnaissance missions were flown around the Soviet Union to help ensure that strategic bombers would be able to reach their targets. Since the end of World War II, Strategic Air Command had flown modified bombers as strategic electronic reconnaissance aircraft. The most important were the RB-29, RB-50, RB-45, RB-36, and RB-47. The ELINT data collected underwent lengthy and comprehensive analysis at Offutt AFB.[158]

After the Korean War, electronic warfare continued to develop as a series of electronic countermeasures (ECM) to enemy radar and communications systems were introduced. By the late fifties, however, modern air defense systems employed a large number of radars integrated through a complex command and control communications net. This linking of

---

[155] Nederveen, Gilles Van, Ibid., p.4.
[156] Nederveen, Gilles Van, Ibid, p.6.
[157] Futrell, Robert F., "The USAF in Korea 1950-1953", Office of USAF History, Washington, D.C., 1983, p.545-556.
[158] Nederveen, Gilles Van, Ibid, p. 6-7.

air defense weapons radars and command posts allowed an air defense commander to direct more assets towards penetrators, making detection and destruction of attackers all the more likely. In the context of tactical electronic warfare (EW), the term tactical retained its classic distinction from the term strategic. It connoted a greater sense of immediacy -the application of EW during and in direct support of tactical air operations.[159]

3.6.3. United States-Vietnam War, EW and ELINT

Tactical Air Command (TAC) became involved in the growing operations in Southeast Asia. Starting in 1965 the command sent RB-66Cs as the sole tactical electronic intelligence (ELINT) collection aircraft for the Air Force. Navy collection aircraft operated in the Gulf of Tonkin, but carrier space was limited. Larger aircraft like the EC-121K "Warning Star" operated from Da Nang AB, South Vietnam after 1967. The RB-66C jamming capability was also used against the North Vietnamese air defense system. In fact, tactical electronic reconnaissance efforts in support of USAF operations over North Vietnam were limited to the RB-66C. C-130B-II variants carried out a limited number of ELINT/COMINT collection missions, but, due to survivability concerns, they could not enter North Vietnamese air space. Although EB-57s assigned to Air Defense Command carried jamming gear to act as radar targets for fighters and radar sites stateside, they were not deployed to Vietnam.[160] The USAF deployed RB-66Cs aircraft to Tan Son Nhut Air Base, South Vietnam from Shaw to provide PACAF (Pacific Air Force) an electronic intelligence (ELINT) capability over Vietnam.

So long as the USAF was involved in Vietnam it had to continue to rely on the EB-66 fleet for electronic reconnaissance and jamming missions over the northern provinces of North Vietnam. Two to four EB-66s usually took part in this jamming, depending upon such factors as weather, the area to be reconnoitered, and North Vietnamese defenses. When the drones were flying at low altitude into the SAM defenses protecting Hanoi and Haiphong, the EB-66s aligned themselves with the programmed flight path so that the most dangerous of the North Vietnamese acquisition and missile system radars would be transmitting directly into the jamming beam. The EB-66C was assigned to this duty since its steerable

---

[159] Nederveen, Gilles Van, Ibid, p. 4-5.
[160] Nederveen, Gilles Van, Ibid, p. 17-18.

antennas concentrated jamming at greater signal strength than the omnidirectional E model antennas.[161]

The original mission of the EB-66C was in performance of the classic electronic reconnaissance role. It gathered ELINT data for the identification, analysis, and location of radars making up the enemy order of battle. However, as SAM sites proliferated and the threat to strike aircraft multiplied, emphasis was diverted from ELINT to real-time electronic reconnaissance in support of strike sorties. In May 1965, the North Vietnamese air defense network was still in an embryonic phase and tactical electronic reconnaissance aircraft operated over most of the country with relative impunity. Penetration and peripheral reconnaissance were performed in a continuing effort to monitor the growth of the radar order of battle in the ensuring months. When performing ELINT collection missions, as prescribed by flight planners, hostile radar emissions were located and recorded for subsequent analysis. When a radar emission was intercepted, the EWO responsible for the frequency band in which it was operating took a series of relative bearings to the transmitter site. The converging bearings were later manually plotted to determine the site location. The time required to acquire the necessary data for location and analysis was primarily a function of aircraft speed and distance to the site. Normally, it varied from six to ten minutes for the EB-66C. Other variables such as EWO operator technique and ground site transmission patterns also affected the data collection times. The ELINT gathering task retained its traditional primacy during the early operational phase of the EB-66C in Southeast Asia.

The EB-66E support to drone operations used a variety of jamming packages to provide across-the-board jamming against enemy early-warning, acquisition, ground control intercept, SAM, and fire control radars. The best jamming position for the EB-66E was when the drone was between the radar and EB-66 aircraft. For missions in the Hanoi-Haiphong area, the orbit was immediately offshore. In lower route packages EB-66Es were positioned either on the east or west side of North Vietnam or on both sides to cover opposing look angles. A key to successful support of drone operations was, knowing the location of the drone in relation to the primary threat radars. Until 1969 the EB-66s and DC-130 drone director aircraft lacked secure in-flight communications which hindered

[161] Nederveen, Gilles Van, Ibid, p. 59.

even the most effective positioning of the jammer aircraft. [162] As the Vietnam War came to an end in 1974, and the last EB-66C/Es were retired. With the retirement of the EB-66 fleet in 1974, however, the US Navy's EA-6B was the most capable electronic warfare platform in the U.S. inventory.

Electronic warfare, by its very nature, is dynamic. For every development, there is a countermeasure. Therefore, electronic warfare is never constant and establishing an effectiveness rate is difficult at best. During the Vietnam War, however, the USAF Security Service was tasked by the Chief of Staff in 1967 to produce an electronic warfare study that examined the effectiveness of electronic warfare, including jamming, over North Vietnam. But since so much jamming occurred simultaneously, from USAF EB-66s and pods and the Navy, the Security Service was not able to establish the extent to which each individual system had contributed to the total effort. It was nevertheless recognized in the study that electronic warfare had saved aircraft from enemy air defense threats and was thus considered the cornerstone of any future air operations.[163]

3.6.4. Arab-Israel War

Immediately after the WWII, the development of the EW was slow, but it received an immense boast during the US engagement in SEA, and also due to appearance of large numbers of Soviet-built SAMs in the Middle East, where these were continuously confronting the Israeli Air Force during the Arab-Israel War. Initially during these conflicts, the western systems were foremost used to identify the threat and advise the pilot to take necessary steps to counter it. Subsequently their sophistication increased, and the simple systems were made capable of not only detecting the threat, but also countering it by electronic countermeasures.

Already at this time - during the early 1970s - it became common for every new radar to soon be followed by a system of appropriate electronic countermeasures (ECM), and in turn every ECM-system to be followed by the system of electronic counter-counter-measures (ECCM), that in turn was followed by the further development of the radar and the ECCM-systems so these can counter the ECM. Initially, such modifications were

[162] Nederveen, Gilles Van, Ibid, p. 38-39.
[163] Nederveen, Gilles Van, Ibid, p. 83.

crude, and problematic to deploy, but today it is possible to modify any of the three components - radar, ECM, and the ECCM - in a matter of few hours. That is, unless a new threat incorporates some new kind of fundamental advance in technology.[164] During the Vietnam War pod protection had improved with each new electronic development, however, North Vietnamese air defenses used an older type radar acquisition system than the newer Soviet systems. The pod protection approach proved ineffective during the Arab-Israeli 1973 Yom Kippur War, when older U.S. designed pods failed to jam the SA-6 "Gainful" SAMs. The SA-6s radars operated in a portion of the frequency spectrum never used before by the Soviets. Israeli Air Force pilots attempted to compensate for their lack of jamming capability by flying lower to get under the SA-6's radar coverage. This tactic placed them into the heart of the ZSU-23-4 (a mobile AAA gun) threat envelope and accounted for high Israeli losses.[165] During 1973 Arab-Israeli War, Israeli electronic warfare specialist managed to disrupt communication between Syria and Egypt by precisely overlaying the Arab Morse code with their own pulses.[166]

The SA-6 caused a considerable surprise for the Israelis -and the West in total- as at the time these had no ECM-system capable of effective countermeasures against the CW (continuous-wave) radars. The SA-6 initially caused to the Israeli Air Force to avoid flying into certain areas, or to fly in a very specific manner -which then exposed the Israeli aircraft to other weapons, foremost MiG-21 interceptors and ZSU-23-4 radar-guided guns, that caused even more losses. This situation -as well as the heavy overclaiming of the number of Israeli aircraft shot down by Arab SAMs- caused such a shock in Israel and in the West, that most of the observers failed to observe the fact that already a more careful choice of tactics decreased the rate of losses to SA-6 almost to nil by the end of the first week of the war. In fact, subsequently the MiGs and ZSU-23-4s scored more kills against Israeli aircraft than the SA-6s.

After an emergency airlift of U.S. ALQ-101/119 pods programmed to counter the SA-6 radar, the Israeli Air Force was able to reestablish air superiority. And the appearance of

[164] Raj, Manoj, "Airborne Electronic Countermeasures", Air Combat Information Group, U.S.A., January 2003, Available on site: http://www.acig.org/artman/publish/article_56.shtml
[165] Cordesman, Anthony H., and Abraham R. Wagner, "The Lessons of Modern War - Volume 1: The Arab-Israeli Conflicts 1973-1989", Westview Press, Boulder, CO, U.S.A., 1990, p. 20-25.
[166] Munro, Neil, "The Quick and the Dead", St. Martin's Press, New York, N.Y., U.S.A., 1991, p. 100.

the SA-6 was a reason for a large number of important developments that were to follow, one of which was the development of *low-observable* or *stealth* aircraft, while others were a fast series of new technologies developed in the arena of ECM and ECCM. This development is characteristic for the *ping-pong* game the EW actually is, and which - for all practical purposes - is being continued right into our days. The only difference now is, that the electronic warfare today is less a matter of "East vs. West" conflict, and far more the question of competition between different companies from the defense sectors of different states.[167]

3.6.5. Cold War (Related to Turkey), EW and ELINT

The United States had tremendous geographical advantages in ELINT task. U.S. aircraft based Europe, Turkey, Iran, Pakistan, Korea, Japan, and the United States could probe virtually any portion of the Soviet periphery, from the North Cape of Norway to the Bering Strait. The Soviets were unable to reach either coast of the United States because their aircraft lacked the range to travel that distance and return.[168]

US intelligence intercept site (ELINT) was perched on a 200 meter cliff overlooking the Black Sea called "Boztepe" in Trabzon and only 100 kilometers from the border of Soviet Georgia to the north east and only 150 kilometers from Soviet Armenia to the east. The Russian Soviet Federation was only 150 kilometers due north across the Black Sea. The Ukraine Soviet Socialist Republic was only 200 kilometers to the North West across the Black sea.

Among the first American units was the USAF Security Service TUSLOG (Turkish-U.S. Logistics) Detachment-3 in Ankara. That group rapidly moved to create Detachments 3-1 in Trabzon and 3-2 in Samsun, Turkey. Both were operating by 1956.[169]

---

[167] Raj, Manoj, Ibid.
[168] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 306.
[169] Gallimore, Jack M., "Jack's Journal", Clemmons NC, U.S.A., 18 November 2001, p.36, Available on site: http://www.aipress.com/jackmem_06.BOZTEPE.pdf

In addition to the L-Band to X-Band surveillance equipment like US had at Hof, Germany, the Trabzon ELINT station had 4 full Telemetry receiving stations that covered HF to UHF frequencies, basically 1 Mhz to 1000 Mhz.[170]

Figure 3.12: United States ELINT station in Boztepe-Trabzon

The C-130 (reconnaissance aircraft) departed Incirlik on a reconnaissance mission along the Turkish-Soviet Armenian border. It was to fly from Adana to Trabzon, Turkey on the Black Sea coast, turn right and fly to Van, Turkey. From Van, the pilot was to reverse course and fly a race-track pattern between Van and Trabzon.[171]

The growth of ELINT systems in East Germany in both size and sophistication, combined with data learned about Soviet air defense systems from Arab-Israeli wars, prompted USAFE to request and receive its own share of what came to be considered as a precious asset.

At the conclusion of the 1973 Arab-Israeli War, the USAF entered into a period of doctrinal realignments. During the Vietnam War a series of modified fighters had been developed which could acquire the emission of SAM and AAA radars and launch guided weapons at these sites. In the seventies the Air Force believed that these aircraft, called

[170] Gallimore, Jack M., Ibid, p. 41.
[171] Gallimore, Jack M., Ibid, p.39.

Wild Weasels, could precede strike aircraft to their targets. This concept was known as suppression of enemy air defenses (SEAD). The Wild Weasel would destroy or, at the very least, suppress enemy radar systems allowing strike fighters to reach their targets. However, USAFE faced a bigger challenge as the U.S. military focus shifted back to the Central Front in West Germany after the Vietnam War. The Soviet Union had emplaced an integrated air defense system of such magnitude that, for SEAD to work, a part of the radar network would have to be jammed. Before it could be jammed the radars had to mapped and catalogued. PACAF faced a similar challenge in Korea. The first priority was therefore to obtain some type of ELINT collector.[172]

Electronic reconnaissance (ER) missions are flown to acquire information on the enemy's electronic system such as radars and communications nets. The electronic intelligence (ELINT) information these flights gather is charted to produce a comprehensive overview of an enemy's electronic network, referred to as its electronic order of battle (EOB). In the Cold War years ferret flights captured and identified signals emanating from the constantly changing equipment of adversaries. The purpose was to pinpoint the transmitting stations before the Soviets, Chinese, or others were alerted to the presence of the collecting aircraft.[173] ELINT collection requires sensitive receivers, direction finding (DF) equipment to pinpoint the location of sites, and sophisticated equipment to measure the operating characteristics of electronic systems.[174]

In tactical air command (TAC)'s view electronic reconnaissance was to provide warning of AAA/SAM radar activity to help strike forces initiate evasive maneuvers, guide strike aircraft away from SAM infested areas, help hunter-killer teams in suppressing enemy radar and SAM sites, and gauge the effectiveness of jamming on enemy systems. These reconnaissance missions were to be performed in support of air operations and they were distinct and separate from strategic intelligence collection efforts. They were to be oriented to information collection that had an immediate and significant effect on the conduct of tactical air operations. The product of the electronic intercept and direction finding activity was to be used initially to counter the enemy and, as a second priority, to provide inputs for

---

[172] Nederveen, Gilles Van, Ibid, p. 86.
[173] Lashmar, Paul, "Spyflights of the Cold War", Sutton Publishing Ltd., Gloucestershire, U.S.A., 1996.
[174] Wiley, Richard G., "Electronic Intelligence: The Interception of Radar Signals", ARTECH House, Dedham, MA, U.S.A., 1985, p.2-3.

intelligence efforts. The data gathered through tactical electronic reconnaissance is not analyzed for signal parameters or subject to complex electronic signal breakdown, but instead is used to detect tactical advantages over the battlefield.[175] During the Cold War period of 1945-1977, a total of more than 40 U.S. reconnaissance aircraft were shot down.[176]

3.6.6. Operation Desert Storm (Gulf War-I)

Iraq was not prepared for air forces that had modern, near-real time targeting capability, sustained air superiority, the ability to sustain massed offensive attack strength over the battlefield, modern sensors and all-weather combat systems, effective passive and active countermeasures against ground based air defenses, and precision-guided weapons capable of killing at ranges outside the coverage of Iraq's short-ranged air defenses.[177]

At the beginning of Operation Desert Shield force deployment; there essentially was no existing US military command, control, communications, and computer (C^4) infrastructure in the region. Iraq's passivity gave the Coalition the time it needed. The Coalition had the time to deploy both the aircraft it needed, and the required support systems and C^4I/BM capabilities. By mid-January, the Coalition had established the largest C^4 network ever assembled.[178]

The first deployments to theater included US airborne warning and control system (AWACS) aircraft to enhance the development of an *air picture* for coalition military leadership and forces. This knowledge not only was critical to the defense of Saudi Arabia against air threats, but also helped monitor Iraqi training activity and improve coalition understanding of the Iraqi air force's readiness levels and sortie-generation capability. Behind the initial air defense force deployments came a plethora of reconnaissance and surveillance aircraft to monitor Iraqi activities and define orders of battle. These included RF-4s, RC-135s, TR-1s, P-3s, E-2s, RF-5s, and specially configured F-14s and Tornado

---

[175] Nederveen, Gilles Van, Ibid, p. 6.
[176] Gallimore, Jack M., "Jack's Journal", Clemmons NC, U.S.A., 18 November 2001, p. 38, Available on site: http://www.aipress.com/jackmem_06.BOZTEPE.pdf
[177] Cordesman, Anthony H., "Struggle for Air Supremacy", CSIS, Washington, D.C., U.S.A., 15 October 1994, p.406, Available on site: www.csis.org_burke_reports_941015lessonsgulfIV-chap06
[178] Department of Defense, "Conduct of the Persian Gulf War: Final Report", Department of Defense, Washington D.C., U.S.A., April, 1992, p 140, Available on site: http://www.defenselink.mil/ezecsec/

GR1As--a total of more than 100 such aircraft. Additionally, Pioneer unmanned aerial vehicles flew nearly 300 reconnaissance and ELINT sorties.[179] Two experimental E-8 joint surveillance target attack radar system (JSTARS) aircraft contributed theirs own brand of near-real-time battlefield reconnaissance. Though using them was a risky gambit (because of their developmental status), these aircraft provided tracking of both friendly and enemy forces, thus reducing fratricide and making possible some spectacular -usually one-sided- air-to-ground engagements such as the one that produced the now-famous "highway of death." On top of all that, a significant array of military and civilian space systems augmented air-breathing reconnaissance and surveillance systems, providing meteorological information and imagery of various types.

The first Iraqi targets attacked were air defense, leadership (including command, control, communications, and intelligence [C^3I]), and electrical grids, all of which had the highest priority because of their impact on the Iraqis' flow of information. The integrated air defense command and control (C^2) system, known as Kari, provided tracking and targeting information for Iraqi fighter and surface-to-air missile (SAM) engagements of coalition aircraft. Breaking down this flow of information would fragment the enemy's air defense effort, forcing his SAMs into autonomous mode and leaving his interceptors virtually helpless. This situation allowed coalition aircraft to exploit Iraqi airspace at will. Leadership C^3I targets provided linkages between the highly centralized decision-making elements (principally Saddam) and both the Iraqi population and the fielded military forces. Disrupting these systems would upset and discredit the regime, while simultaneously reducing its capability to control military forces.[180]

To build and maintain this pressure, the US brought a tremendous array of electronic warfare systems to the fight. Other coalition partners contributed a few systems, such as the British Tornado GR1As, but the US provided the vast majority. Before and during the war, satellites and airborne systems collected electronic intelligence (ELINT), finding and fixing C3I nodes of all types for later attention from less benign systems such as the USAF's 61 F-4Gs and 12 specially configured F-16 Wild Weasels, highly sophisticated systems capable of detecting and destroying electronic radiation sources (especially radar

[179] Keaney, Thomas A., and Eliot A. Cohen, "Gulf War Air Power Survey Summary Report", Department of the Air Force, Washington, D.C., U.S.A., 1993, p. 184-195.
[180] Keaney, Thomas A., and Eliot A. Cohen, Ibid, p. 36-37.

emissions) with high-speed antiradiation missiles (HARM) and Shrike antiradiation missiles. The Navy and Marines contributed less sophisticated -yet very capable- F/A-18, EA-6B, and A-7 HARM and Shrike shooters. These aircraft could detect and shoot at radiation sources but, lacking some of the information available to the Weasels, could never be sure they had released their missiles within range of the target. Many strike aircraft carried their own ELINT and electronic jamming equipment to counter Iraqi attempts to track and shoot them with radar-guided systems; additionally, EF-111s, EC-130s, and EA-6Bs accompanied most strike packages, employing even more sophisticated (and powerful) jamming equipment.[181] The Iraqi Army was unable to challenge the U.S. for two reasons: first, their intelligence was so poor that they were not aware of a multidivisional force maneuvering within miles of their front lines; second, both their strategic and tactical communications had been so badly damaged that the chain of command no longer functioned well enough to assure control during a counterattack.[182] The apparent Iraqi fears that radiating was both futile and dangerous were certainly well founded, if not totally accurate. The enemy's ability to collect and use information was severely disrupted, but creating that deficit represents only half the battle.[183]

US air forces dominated every aspect of reconnaissance, electronic warfare, and command and control activity. They flew 90% of all reconnaissance missions, 96% of all command and control missions, and 97% of all electronic warfare missions.[184]

These figures on sortie numbers reflect the fact that US forces had superior numbers and power projection capabilities. They also reflect the fact that the air battles in Desert Storm were dominated by US air forces that were high technology forces, and which integrated attack and air defense aircraft with a complex mix of command and control, reconnaissance and targeting, intelligence, electronic warfare, and refueling and support aircraft.

---

[181] Keaney, Thomas A., and Eliot A. Cohen, Ibid, p. 195-197.
[182] Friedman, George & Meredith, “The Future of War”, Crown Publishers Inc., New York, U.S.A., 1996, p. 301.
[183] Mann, Col Edward, “Desert Storm: The First Information War?”, Aerospace Power Journal, U.S.A., Winter 1994, Available on site: http://www.iwar.org.uk/iwar/resources/airchronicles/man1.htm
[184] Cordesman, Anthony H., “Struggle for Air Supremacy”, CSIS, Washington, D.C., U.S.A., 15 October 1994, p.411, Available on site: www.csis.org/burke/reports/

Table 3.1: The Impact of Coalition Air Forces: Electronic Warfare and C^4 Missions.[185]

	Reconnaissance			C^4				Electronic Warfare				
	Recce	SLAR	Observ	Total	ABCCC Early Warning	C4	Tot	ECM	ESM	EW	Total	TOT
US												
Air Force	869	0	442	1,311	201	379	24	604	0	190	1,388	1,578
Navy	1,190	0	241	1,431	1,143	0	0	1,143	5	260	0	265
Marine Corps	3	0	0	3	157	0	0	157	0	17	326	343
Special Forces	2	0	0	2	0	0	0	0	0	0	84	84
Army	0	147	0	147	0	0	0	0	6	547	15	568
Subtotal	2,064	147	683	2,894	1,501	379	24	1,904	11	1,014	1,813	2,838
Saudi Arabia	118	0	0	118	0	85	0	85	0	0	0	0
U.K.	156	0	0	156	0	80	0	80				
France	62	0	0	62	0	0	0	0	0	0	0	0
Canada	0	0	0	0	0	0	0	0	0	0	0	0
Kuwait	0	0	0	0	0	0	0	0	0	0	0	0
Bahrain	0	0	0	0	0	0	0	0	0	0	0	0
Italy	0	0	0	0	0	0	0	0	0	0	0	0
UAE	6	0	0	6	0	0	0	0	0	0	0	0
Qatar	0	0	0	0	0	0	0	0	0	0	0	0
Subtotal	336	0	0	336	0	85	0	85	0	80	0	80
Total	2,406	147	683	3,236	1,501	464	24	1,989	11	1,094	1,813	2,918

ABCCC=Airborne battlefield command and control center. ECM=Electronic countermeasures. ESM=Electronic support measures or intelligence. C4=Command, control, communications, and computers. CAP=Combat air patrol SLAR=Side looking airborne radar.

Table 3.1 shows that the US had an effective monopoly of medium and long range bombers (F-111 and B-52G), the only "stealth" aircraft (F-117A), the only forward air control aircraft, the only gunships, and the only dedicated tank-killing close air support aircraft. The US had a near monopoly of dedicated electronic warfare aircraft like the EA-6B and EF-111, and while the Tornado and Mirage 2000 are excellent combat aircraft, the

[185] Cordesman, Anthony H., Ibid, p. 434-436.

F-14B, F-15C, F-15E, and A-6E had an important margin of superiority in terms of strike and beyond visual range combat capabilities.[186]

US air units were located in more than 20 different locations in Saudi Arabia by the time that Desert Storm began. Even a comparatively small deployment like the US presence in Turkey involved over 130 planes. These included 28 F-15Cs for air superiority operations; a mix of 46 F-18C, F-111E, and F-4 strike airplanes; and a mix of 32 RF-4C, F-18C, and EF-111A Wild Weasel and electronic warfare aircraft. It also included 30 other support aircraft for AWACS, reconnaissance, tanking, and intelligence gathering.[187]

Coalition electronic warfare (EW) capabilities played a critical role in winning air supremacy, and in allowing Coalition strike/attack aircraft to survive over the battlefield. At the same time, it is not possible to transform this lesson of the Gulf War into some precise ranking of the importance of electronic warfare capabilities relative to other Coalition activities. Much of the unclassified data on electronic warfare provides only a limited or inaccurate picture of the role of such systems.[188] More generally, the electronic warfare effort was only part of the effort to "blind" the Iraqi Air Force and ground-based air defenses. It interacted with a massive series of strikes on Iraqi air sensors and command and control facilities, the F-4G Wild Weasel, Tornadoes, and other aircraft using antiradiation missiles. Further, special intelligence aircraft to the rear monitored Iraq communications and Iraqi radar activity. Some of these Coalition aircraft could instantly detect Iraqi radar activity, characterize the emitter, and locate it from deep behind the battlefield. They played a role in "blinding" the Iraqi forces by allowing the ABCCC and AWACS aircraft to guide strike/attack aircraft away from emitters and vector in aircraft with anti-radiation missiles.

Two key Coalition strike systems -the F-117 and cruise missile- did not require extensive protection from electronic warfare, although the F-117 had protection from EF-111 jammers even in flying missions that minimized exposure to Iraqi radars. It used such support on the first day of the war, and in some of its later attack sorties.[189] Virtually all of

---

[186] Cordesman, Anthony H., Ibid, p. 411.
[187] Cordesman, Anthony H., Ibid, p.411.
[188] Morse, Stan, ed., "Gulf Air War Debrief', Aerospace Magazine, London, U.K., 1991, p. 36-37.
[189] Electronic Defense Magazine, Washington, U.S.A., May, 1991, p. 37-39.

the other strike/attack aircraft and helicopters, however, were protected by on-board EW electronics in the aircraft, pods mounted on the aircraft, and specialized electronic warfare aircraft that flew as escorts.

Many aircraft carried their own electronic warfare protection. This was true of many British, French, Saudi and US aircraft -although the RAF was forced into a crash upgrade effort to provide electronic warfare capability. The RAF's Tornado GR1 did have the Marconi Sky Shadow jamming/deception pod, a radar warning and homing receiver, and dispensable chaff and flares. However, the RAF air defense variants of the Tornado F3 had a radar warning and homing receiver, but were not rigged to carry expendable chaff and flare countermeasures before the Gulf War, although the same aircraft supplied to the RSAF had such capability. This experience illustrates the level of risk inherent in underfunding first line combat forces in peacetime.[190]

Specialized electronic warfare aircraft played a major role in the war for air supremacy. As Table 3.2 shows, the Coalition flew nearly 3,000 dedicated missions in this role, in addition to the tens of thousands of sorties other aircraft from other aircraft with their on-board EW systems or pods. Virtually all of these specialized electronic warfare aircraft were US aircraft. The US flew all but 80 of fixed-wing electronic warfare sorties during the Gulf War, which were flown by British Nimrod aircraft in the naval defense role.[191] The only other specialized electronic warfare activity came from a French DC-8 Sarigue, a French EC-160, and two modified SA-330 Puma helicopters- whose function and activity level remains classified.[192]

According to observation-orientation-decision-action (OODA) loop theory, this kind of offensive effort can "enmesh the adversary in a world of uncertainty, doubt, mistrust, confusion, disorder, fear, panic, chaos . . . and/or fold back inside himself so that he cannot cope with events/efforts as they unfold." This factor probably contributed greatly to the mass desertions and surrenders of Iraqi troops and almost certainly to their general ineffectiveness as a cohesive fighting force.

---

190 Price, Alfred, "EW additions for the RAF", Military Technology Magazine, U.S.A., December 1991, p. 82-84.
191 Keaney, Thomas A. and Eliot A. Cohen, "Gulf War Air Power Survey: Summary Report", Department of the Air Force, Washington, D.C., U.S.A., 1993, p. 195-197.
192 Morse, Stan, ed., Ibid, p. 36-37.

Table 3.2: US. Electronic Warfare Aircraft in the Gulf War.[193]

Type/Location	Service	Type	Number on 20 Jan 1991	Total Sorties Flown in War By All Aircraft of Type
EF-111A Raven				
At-Taif, Saudi Arabia	USAF	EF-111A	18	
Incirlik, Turkey	USAF	EF-111A	18	
Total			36	1,105
EC-130H				
King Fahd Saudi Arabia	USAF	EC-130H	2	
Riyadh, Saudi Arabia	USAF	EC-130H	7	
Bateen, UAE	USAF	EC-130H	6	
Incirlik, Turkey	USAF	EC-130H	3	
Total			18	450
EA-6B Prowler				
Aircraft Carriers	USN	EA-6B	27	1,126
Shaikh Isa Bahrain	USMC	EA-6B	12	504
F-4G Wild Weasel				
Shaikh Isa, Bahrain	USAF	F-4G	48	
Incirlik, Turkey	USAF	F-4G	12	
Total			60	2,683
F-16C				
Incirlik, Turkey	USAF	F-16C	13	--
RC-135V Rivet Joint				
	USAF	EC-135	?	24(?)
NAVY				
Jiddah, Saudi Arabia	USNavy	EA-3B	2	-
Bahrain Itnl., Bahrain	USNavy	EP-3E	2	-
Masirah, Oman	USNavy	EP-3E	1	-
Bahrain Itnl., Bahrain	USNavy	P-3B(RP)	2	-
Total			7	
EC-130H Compass Call				
	USSOCCENT	EC-130	8	450

Of course, this disruption of the adversary's flow of information represents only one side of the equation. The real objective is to complete one's own OODA cycles faster than the

193 Cordesman, Anthony H., Ibid, p. 468-469.

adversary completes his; thus, while "stretching-out the adversary's cycle time," one must also "compress his own." Although caught somewhat flat-footed in August 1990, the coalition immediately began working this part of the equation and continued with a vengeance until the air war began in Jan. 1991.

The OODA loop can be thought of as being the C^2 loop. It is actually being referred that all aspects of what we call C^3I (or C^4I -the fourth C standing for computers). Logically, then, (1) intelligence provides observation (in accordance with command elements' requirements); (2) working together, intelligence and command elements provide orientation (i.e., they determine what to observe, which observed information is of greatest value, and how it is to be used in making decisions); (3) command elements make necessary decisions and direct the actions required to execute those decisions; and (4) field units and their discrete elements (aircraft, tanks, people, etc.) execute the directed actions (and contribute to observation through postaction reports, at which point the cycle begins again). All these elements are interconnected through the communications element of C^4I. The whole can be only as strong as the weakest link. Even though at least one of its links was very weak indeed (i.e., orientation, discussed below), the coalition -after weathering a slow start- would eventually dominate in every element of this cycle.[194]

The US employed two drones to support the electronic warfare mission by decoying radars, providing tactical deception, and designating targets. The BQM-74 was a drone used to decoy radars, and create confusion, by providing false targets. It was used extensively on the first night of Desert Storm and aided Wild Weasel targeting. It provoked a major reaction from Iraq anti-aircraft guns and missile batteries and surveillance radars.[195]

The TALD, or tactical air-launched decoy, was used extensively by US Navy and USMC aircraft during Desert Storm, and met roughly the same mission need as the BQM-74.[196]

---

[194] Mann, Col Edward, “Desert Storm: The First Information War?”, Aerospace Power Journal, U.S.A., Winter 1994, Available on site: http://www.iwar.org.uk/iwar/resources/airchronicles/man1.htm
[195] Eliot A. Cohen, “Gulf War Air Power Survey”, Volume IV, Part I, Department of the Air Force, Washington, D.C., U.S.A., 1993, p. 102-103.
[196] Eliot A. Cohen, Ibid, p. 103-104.

The EF-111 uses the AN/ALQ-99E jamming subsystem, which scans across frequency bands under computer or manual control. When threats are identified, it initiates countermeasures either automatically or under EW officer's control. The EF-111 jammed the radars in the integrated Iraqi KARI air defense net. The EF-111 often operated in direct support role because Iraqi air defenses were too weak to require stand-off jamming. The EF-111 operated in the heavily defended areas around Baghdad, H2/H-3 and Scud launch zones during the war. The EF-111 has terrain-following capability and is able to keep up with strike/attack aircraft even in demanding high speed mission profiles. The EF-111 had no combat losses and only one non-combat loss. EA-6B's capabilities are similar to EF-111. EA-6B jammed the radars in the integrated Iraqi KARI air defense net and tracking radars. They launched TALD decoys to lead Iraqi radar operators to emit, and jammed to force increased radar activity, so Iraqis could be attacked by HARM. They often operated in direct support role because Iraqi air defenses were too weak to require stand-off jamming. They operated in the heavily defended areas around Baghdad during the war. Some speed problems in keeping up with strike/attack aircraft. EA-6B could fire a maximum of two HARMs. It accompanied virtually all USN air strikes into Iraq. They were currently being upgraded along with the EF-111.[197]

F-4G Wild Weasel were used to accompany Coalition strike packages early in war, and then acted as "Weasel Police" to continuously suppress Iraqi radars by patrolling the area over the battlefield. It used HARMs to attack Iraqi radars, particularly air defense radars. Navy EW Aircrafts performed a wide range of naval jamming and electronic warfare functions. RC-135V Rivet Joint worked with AWACS and ground stations as electronic intelligence collection platform that provided enhanced awareness of enemy air and ground activity. They precisely located and characterize enemy radio and radar activity. They provided direct near-real time support to theater and tactical commanders in some cases. RC-135V flew standoff missions as close to Iraqi airspace as threats permitted. EC-130H Compass Call was used confuses and disrupts Iraqi command and control communications, in either a manual or automatic mode. They gathered intelligence on Iraqi communications, and disrupted Iraqi voice systems. They provided 24 hour a day surveillance of Iraqi communications for 44 days. Air EW activity limited by lack of Iraqi air activity, but

---

[197] Cordesman, Anthony H., Ibid, p. 468-469.

effectively jammed tactical air, anti-aircraft, artillery, surface-to-air missile, and battlefield communications. They supported EW training of US and Egyptian forces during Desert Shield.[198]

3.6.7. Kosovo Crisis, EW & ELINT

NATO launched military operations only as a last resort when it was clear that the diplomatic track would not deliver a solution, whilst at the same time the humanitarian situation on the ground had deteriorated to such an extent that outside intervention became essential in order to avert a humanitarian catastrophe.

Targets for air strikes were selected by the NATO Military Authorities, acting in accordance with guidance agreed by the North Atlantic Council on broad sets of targets and the requirement to minimize collateral damage. The North Atlantic Council was not involved in the detailed process of target selection. Individual Allies were responsible for the clearance of the targets assigned to them by NATO.

Various systems were employed to assess battlefield damage, all complementary to each other rather than being mutually exclusive. Reconnaissance aircraft, Unmanned Aerial Vehicles, satellite imagery and other intelligence gathering systems all provided data that could be used to assess the amount of damage caused by the NATO bombing campaign.[199]

In the light of our experience during the air campaign, the UK national Battle Damage Assessment/targeting process has been fully reviewed and a series of recommendations for follow-up action highlighted. These include:

- the need to ensure the most appropriate mix of Intelligence, Surveillance and Reconnaissance assets is available to provide Battle Damage Assessment;
- sufficient background information should be compiled to enable the accurate assessment of the impact of operations and of an adversary's remaining capability;
- and the limitations of the human eye and weapons systems video should be recognized and, where possible, supporting intelligence material obtained.

---

[198] Cordesman, Anthony H., Ibid, p. 468-469.
[199] Secretary of State for Defence, "Kosovo: Lessons From The Crisis", Ministry of Defence, London, U.K., 2002, Available on site: http://www.mod.uk/publications/kosovo_lessons/chapter7.htm

The E-3D aircraft, although originally designed as AEW aircraft, were employed in the Airborne Warning and Control (AWACS) role as part of a complex command and control operation guiding hundreds of Alliance aircraft in what had become the busiest airspace in the world. This stretched the aircraft's resources, and the long term sustainability of using the aircraft in this role is being addressed.

The United States was very pleased with the performance of its GPS-guided JDAM, which was used accurately and effectively in all weathers.

NATO encountered significant difficulty in locating and positively identifying mobile ground targets. Given the long period over which the crisis had been developing, the Yugoslav/Serbian security forces had had time to disperse their personnel, equipment and logistics resources. In order to engage such targets more effectively, Allies and partners need to look to acquire/develop:

- An improved Intelligence, Surveillance and Reconnaissance capability, to enable us to detect the right targets, in all weathers, and to distribute the intelligence to those who need it in timely fashion. Our planned all-weather Airborne Stand Off Radar (ASTOR) aircraft will greatly enhance our battlefield surveillance capability, alongside existing Allied capabilities such as the US JSTARS and Unmanned Aerial Vehicles, including the UK Army's PHOENIX and planned successor systems such as SENDER and SPECTATOR. As technology advances, it should also become easier to detect where assets have been concealed;
- Improved real-time "sensor-to-shooter" communications/data links (ELINT sensors to enable faster communication between intelligence gathering assets and the means of attacking the target e.g. a pilot in an aircraft on patrol);

Electronic Warfare (EW) and Suppression of Enemy Air Defense (SEAD) capabilities were vital force enablers during the air campaign. The first stage of the air operation was aimed at (and succeeded in) degrading the Yugoslav Integrated Air Defense System, but as a threat remained, force packages were escorted by EW and SEAD-capable aircraft to counter these threats as they arose. The bulk of this effort was provided by the United States, although other Allies, including the UK to a very limited extent, played a role.[200]

3.6.8. Operation to Afghanistan

The coalition presses Taliban in Afghanistan with SEAD, ELINT, and electronic attack. At press time, the US-led campaign against the Afghanistan had entered a stage where small numbers of grounds troops -special-operations forces. This followed nearly two weeks of steady bombing of military targets in which aircraft armed with precision-guided weapons continued to do most of the work.

A variety of US fixed-wing combat aircraft are taking part in the operations. US Air Force (USAF) B-1Bs, B-2s, and B-52s are seeing combat, as are US Navy F/A-18s and F-14s -all of which are dropping GPS- and laser-guided munitions on targets: air-defense sites; airfields (and on the aircraft on the ground themselves); military garrisons and training camps; command, control, and communications sites; maintenance and storage facilities. Early results seemed impressive, as demonstrated by the reconnaissance photos taken for bomb-damage assessment. The US had also begun AC-130H/U gunship sorties followed by BLU-82 *daisy cutter* fuel-air munitions attacks by MC-130 Combat Talons.[201]

Based on aircraft carriers in the Indian Ocean and supporting the strike aircraft are EA-6B Prowlers for escort and communications jamming - using the aircraft's AN/ALQ-99 and AN/USQ-113(V) jammers, respectively - and E-2C Hawkeyes for airborne early warning and most probably some command-and-control responsibilities, as in Operation Allied Force over the former Yugoslavia. Also in theater, according to sources, are USAF RC-135 Rivet Joint signals-intelligence (SIGINT) aircraft; EC-130H Compass Call communications-jamming and -deception planes; EC-130E Commando Solo aircraft, which broadcast messages and drop leaflets to the Afghan people from the US military; and U-2 high-altitude spy planes. There have also been reports of Predator unmanned

[200] Secretary of State for Defence, "Kosovo: Lessons From The Crisis", Ministry of Defence, London, U.K., 2002, Available on site: http://www.mod.uk/publications/kosovo_lessons/chapter7.htm
[201] Chaisson, Kernan, and Brendan P. Rivers, with Patrick Brunet, "Lead Story: US-Led War on Terror Staged Over Afghanistan", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

aerial vehicles providing surveillance and reconnaissance support, as well as actually serving a strike platform for the first time.

Figure 3.13: Royal Air Force Nimrod R1 Reconnaissance Planes

According to the UK Ministry of Defence, in addition to Royal Navy vessels in the Indian Ocean, Royal Air Force Canberra PR9 and Nimrod R1 aircraft are also supporting the strikes by performing reconnaissance missions, while E-3D Sentry aircraft are providing additional airborne early warning to augment the Hawkeyes.[202]

France also sent intelligence aircraft to support the campaign, namely the C-160G Transall Gabriel and the Mirage IV P, a reconnaissance version of the nuclear bomber. The Gabriel is a twin-engine transport aircraft adapted for the SIGINT mission and carries a crew of 20. The ELINT system is very close to the Astac pod carried on the Mirage F-1CR. It features automatic interception, analysis, identification, and localization of radar emitters. The COMINT capabilities of the aircraft have gained more importance in recent years, and could be useful for tracking the Taliban V/UHF and SATCOM systems they favor. The Gabriel is reportedly fitted with a very accurate interferometer system. The antennas of this system, called Diadema, are located on top of the airframe. The aircraft is also fitted with two high-resolution cameras protected under special blisters aft of the wing.

Communications were similar but there was no similarity threat wise. The Taliban do not have nearly the air defenses of other recent US foes like Iraq and the former Yugoslavia,

[202] Chaisson, Kernan, and Brendan P. Rivers, with Patrick Brunet, Ibid.

but for the first two days, the effort concentrated on taking down what air defenses there were. By day three, US declared that they had achieved air superiority over Afghanistan. There were no reports of challenges by Taliban aircraft, so strikes concentrated on destroying aircraft on the ground, as well as making their airfields unusable.[203]

EW is so important for a number of reasons. EW is narrowly defined to make it synonymous with electronic attack – blinding the enemy, including the use of radar or communications jamming. This lends itself to a platform-centric definition of EW centered on aircraft, such as the EA-6B Prowler. The Prowler is US military's only dedicated radar jamming aircraft. Its mission is essential. It tells commanders when, where, and how to strike the enemy.[204] Taliban forces are not a major EW power. Nobody can fly without Prowlers. While the EA-6B Prowler proved invaluable in the suppression of enemy air defenses (SEAD) during Operation Allied Force over Kosovo. The USQ-113(V) communications jammer is also a very capable SIGINT collector.

The ongoing air campaign has seen some of the most sophisticated intelligence-gathering assets in Western arsenals put to use against one of the least modern armed forces in the world. In addition to the questions this raises in certain circles, one could rightly wonder whether this is the proper application of force, or simply the application of whatever force happens to be available.[205]

3.6.9. Operation Iraqi Freedom (Gulf War-II)

Even during Desert Storm, US used to be one plane, one target, in Operation Iraqi Freedom US used one bomb, one target. More operations planning were done during OIF than ever before. If coalition forces positively identified a target during a morning mission, it was likely struck by sundown. Crucial to the successful prosecution of those targets was a multitude of Intelligence, Surveillance and Reconnaissance (ISR) systems. The Air Force

[203] Chaisson, Kernan, and Brendan P. Rivers, with Patrick Brunet, Ibid.
[204] Pitts, Joseph R., "What is Electronic Warfare?", A Speech to the Lexington Institute, Washington, D.C., U.S.A., 22 October 2003, Available on site: http://www.house.gov/pitts/Commentary from.htm
[205] Chaisson, Kernan, and Brendan P. Rivers, with Patrick Brunet, Ibid.

and Central Command used ISR Manager (ISRM) during OIF to enhance their command and control of the conflict.[206]

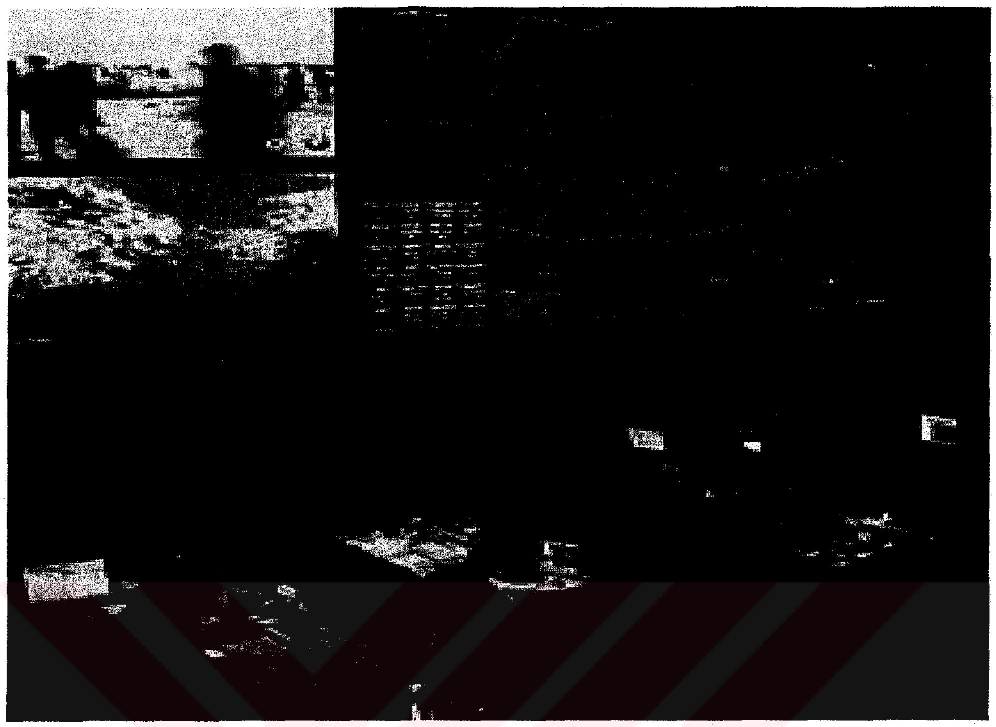


Figure 3.14: Operation Center in Operation Iraqi Freedom

Massive Air Operations Centers (AOC) enable targeteers to plan air campaigns in a fraction of the time once required. The Prince Sultan AOC has been disbanded, leaving five major AOCs throughout the world. The one used for Operation Iraqi Freedom (OIF) is at Al Udeid Air Base in Qatar, and the others are at Osan Air Base, South Korea; Hickam Air Base, HI; Davis-Monthan Air Force Base, AZ; and Ramstein Air Base, Germany.[207]

US Secretary of Defense Donald Rumsfeld and General Tommy Franks, the commander of the US Central Command (USCENTCOM) and the overall commander of the coalition forces summarized these lessons in testimony to Congress on July 9, 2003. Secretary Rumsfeld summarized the key lessons as follows:[208]

---

[206] Cordesman, Anthony H., "The Lessons of the Iraq War: Executive Summary", Center for Strategic and International Studies, Washington, DC, U.S.A., 21 July 2003, p.6. Available on site: http://www.csis.org/features/iraq_instantlessons_exec.pdf

[207] Clarke, Patrick E., "Nerve Centers for Air Warfare", Volume: 7, Issue: 7, U.S.A., 01 September 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=183

[208] Cordesman, Anthony H., Ibid, p. 6.

"...In less than a month, they had developed and were executing a war plan for Afghanistan employing a range of capabilities from the most advanced (such as laser-guided weapons), to the antique (40 year-old B-52s updated with modern electronics) to the rudimentary (a cavalry charge) they and our Afghan and coalition allies drove the Taliban and Al-Qaeda from power in a matter of months. The plan they developed for Operation Iraqi Freedom was even more innovative and transformational employing an unprecedented combination of speed, precision, surprise, and flexibility.

I'd say some key lessons so far include:

- The importance of ***speed***, and the ability to get inside the enemy's decision cycle and strike before he is able to mount a coherent defense;
- The importance of ***jointness***, and the ability of U.S. forces to fight, not as individual deconflicted services, but as a truly joint force—maximizing the power and lethality they bring to bear;
- The importance of ***intelligence***—and the ability to act on intelligence rapidly, in minutes, instead of days and even hours;
- And the importance of ***precision***, and the ability to deliver devastating damage to enemy positions, while sparing civilian lives and the civilian infrastructure.

Another lesson is that in the 21st century *overmatching power* is more important than *overwhelming force*. In the past, under the doctrine of overwhelming force, force tended to be measured in terms of mass the number of troops that were committed to a particular conflict. In the 21st century, mass may no longer be the best measure of power in a conflict."

General Franks added the following points:[209] "Decisive combat in Iraq saw a maturing of joint force operations in many ways. Some capabilities reached new performance levels. From a Joint Integration perspective, our experience in Operations Southern and Northern Watch, and Enduring Freedom helped to develop a joint culture in our headquarters and in our components. These operations helped to improve joint interoperability and improve our joint C^4I networks as joint force synergy was taken to new levels of sophistication. We saw

[209] Cordesman, Anthony H., Ibid, p. 7.

jointness, precision munitions, C^2, equipment readiness, state of training of the troops, and Coalition support as clear "winners" during Operation Iraqi Freedom (OIF).

Advanced technologies employed during OEF were also critical. The command and control of air, ground, naval, and SOF from 7,000 miles away was a unique experience in warfare as our forces achieved unprecedented real time situational awareness and C^2 connectivity. We learned that precision-guided munitions represent a force multiplier. Low collateral damage during both OEF and OIF was a fundamental factor in achieving our objectives. Early in OEF we saw the need for an unmanned sensor-to-shooter capability to support time-sensitive targeting. The armed Predator demonstrates great potential and will be a high payoff system in the future. Blue Force Tracking and enhanced C^4I systems increase lethality and decrease response time, and also represent transformational technologies. We will continue with development of Global Hawk as an unmanned, high-altitude, long loiter time, beyond line-of-sight multi-sensor UAV, and will work to incorporate laser designation and delivery of precision weaponry from that platform."

In an interview following the war, Secretary of Defense Rumsfeld's director of the Office for Force Transformation, Arthur K. Cebrowski summarized the initial lessons of the war in the following evolutionary terms:[210]

- The growing implementation of network-centric warfare and its role in shifting the balance of power through new forms of air-land battle and dynamics. A long process driven by better sensors, good networked intelligence, high-speed decisionmaking, and the ability to exploit the noncontiguous battlefield the battlefield without a front.
- The need for increased connectively in net-centric warfare.
- A possible reduced dependence on helicopters on the battlefield for vertical lift.
- The increased value of Special Forces and the need the ability to work with friendly local forces, and provide more SOF-like forces to support IS&R.
- The need for still further improvements in joint planning.
- Increased need for strategic mobility, possibly merging inter- and intra-theater lift, providing high-speed sealift, and possibly airships.

[210] Fulghum, David A., "Fast Forward," Aviation Week Magazine, U.S.A., 28 April 2003, p.34.

- The need to accelerate the speed of command and control.

Key concepts like *network-centric* or *net-centric* warfare emerged well over a decade, as did the common use of the term "revolution in military affairs. The idea of using a wide range of synchronized forms of attack or parallel warfare was a key part of the war plan for the first Gulf War.[211]

New tactics and technology used in the Iraqi War, and projected for future force transformation, have taken decades to evolve. If U.S. progress over the last 10 years seems remarkably fast, at least part of the reason is that so many foreign armies have stood still or regressed and that so many Americans forget or never knew the past history of current developments. In practice, America's "new way of war" has been relatively conservative. Then US military services have never forced it to sacrifice proven force elements before the new ones were ready; the resulting process of change has mixed new and old methods of warfighting; and it has been measured and pragmatic.[212]

If one looks at the asymmetries in the Coalition-Iraqi military balance, it is clear after the fact that the United States and Britain did deploy "decisive" force relative to the weaknesses in Iraqi forces, Air dominance; superior intelligence, reconnaissance, and targeting; far more effective and survivable command and control; precision strike capability; far more rapid and adaptive cycles of decision-making; and far more rapid cycles of land maneuver were pitted against an incompetent enemy leadership whose forces had many deep structural weaknesses.[213] Once again, dramatic changes took place in the quality of their execution during the Iraq War. The United States had vastly improved every aspect of its intelligence, targeting, and command and control capabilities since the last Gulf War, in addition to having spent some 12 years in surveillance of Iraqi operations and military developments. Its combination of imagery, electronic intelligence, signals intelligence, and human intelligence was honed in Afghanistan, and improved

---

[211] Cordesman, Anthony H., Ibid, p. 12.
[212] Krause, Merrick E., "Decision Dominance: Exploiting Transformational Asymmetries," Defense Horizons Magazine, No. 23, Center for Technology and National Security Policy, National Defense University, Washington, D.C., U.S.A., February 2003.
[213] Loeb, Vernon, "Commander Defends Iraq War Comments," Washington Post, U.S.A., 8 May 2003, p.18

communications and command and intelligence fusion at every level gave it near real-time day and night situational awareness.[214]

Space is scarcely a traditional fundamental of war. But it has been a fundamental ever since the United States first made use of satellites for intelligence purposes. In the Iraq War, the United States used space for battle management, for communications, to locate its forces and guide its weapons, and to perform a wide range of other missions. It built upon the lessons of the Gulf War and Afghan War and on progress in worldwide communications dating back to the days of Vietnam. At the same time, this was the first large-scale war in which the United States could fight with 24-hour continuing intelligence satellite and sensor coverage over the battlefield, as well as the first major conflict where it could take advantage of full 24-hour coverage by global positioning satellite (GPS) system.[215] United States made use of more than 50 satellites during the war, including the two dozen satellites in the GPS system.

Space provided a wide range of intelligence (ELINT etc.), targeting, and battle damage assessment capabilities. It was the key to effective command and control and to netted global military communications. The range of space-based communications and sensor assets, and the vast bandwidth the United States could bring to managing global military operations, allowed it to achieve near-real-time command and control and intelligence collection, processing, and dissemination. At the same time, GPS allowed U.S. and British forces to locate friendly and enemy forces and both target and guide weapons. The United States also made use of satellites to locate missile launches, predict their target, and provide warning.[216]

The space effort in the Iraq War benefited from improved communications, integration, data processing and analytic methods, and command and control at every level. National, theater, and tactical intelligence had much better integration, processing, and dissemination than during the Gulf War, building on the lessons of that conflict and Afghanistan.[217]

---

[214] Cordesman, Anthony H., Ibid, p.20.
[215] Cordesman, Anthony H., Ibid, p.22.
[216] Loeb, Vernon, "Intense, Coordinated Air War Backs Baghdad Campaign", Washington Post, U.S.A., 6 April 2003, p.24.
[217] Cordesman, Anthony H., Ibid, p.23.

The importance of the global positioning satellite system is illustrated by the fact that when GPS was introduced into the U.S. Army during the Gulf War, there was a maximum of one receiver per company or 180 men. In the Iraq War, there were more than 100,000 Precision Lightweight GPS Receivers (PLGRs) for the land forces and at least one per nine-man squad. The marines had fewer units, but still had 5,400, or roughly one per platoon (3--5 squads.) Moreover, a number of marines carried their own civilian GPS units.[218]

Although Iraq had at least four jammers designed to jam the Coalition GPS system, these seem to have been destroyed early in the war and to have had little operational effectiveness. The jammers were successfully attacked by B-1Bs and F-117s; at least some seem to have been attacked with GPS- guided weapons.[219]

The dust storms in the Iraq War highlighted the value of radar imaging versus infrared and electro-optical imaging. The JSATS proved particularly valuable in tracking Iraqi land forces at a time when other sensors had severe limits. Aircraft and UAVs do, however, have limits in terms of coverage and the ability to provide continuous coverage on a "24/7" basis.

The Iraq War is scarcely the only war in which weather has had a powerful impact on US imaging capabilities, however, and it is just as important to "own the weather" as to own the night. As a result, there seems to be good reason why the US should reevaluate the need for a robust radar satellite program.[220]

The Coalition applied C^4I and IS&R systems, however, in a form of joint warfare that had an unparalleled degree of near-realtime situational awareness that shortened the "kill chain" from targeting to strike, and the sensors-to-shooter gap from days to hours in the Gulf War to hours to minutes in the Iraq War.[221] At this point, there is no way to analyze the relative role of space, UAVs, fixedwing aircraft, SIGINT, ELINT, imagery, Special Forces, and human intelligence in detail. It is clear, however, that the resulting mosaic of

---

[218] Schiesel, Seth, "On the Ground in Iraq: The Best Compass Is in the Sky," New York Times, U.S.A., 17 April 2003.
[219] Trimble, Stephen, "GPS is Surviving Jamming Threat, Pentagon Says," Aerospace Daily, U.S.A., 22 April 2003.
[220] Hacket, James T., "Tracking Targets from Space," Washington Times, U.S.A., 8 July 2003, p. 18.
[221] Goure, Daniel, and Christopher M. Szara, "Air and Space Power in the New Millennium", Center for Strategic and International Studies (CSIS), Washington, D.C., U.S.A., 1997.

intelligence and senor data was far better than in the Gulf War, and was processed and disseminated far more quickly. The time-consuming and relatively rigid process of sortie planning and targeting that shaped the Air Traffic Order in the Gulf War was replaced with a far quicker and more responsive system.[222]

The evolution of precision air strike technology greatly improved Coalition capabilities in carrying out these strikes. Even in the Gulf War, only a small number of aircraft like the F-117, F-111, and F-15E were properly equipped for advanced precision strike missions. In the Iraq War, virtually all U.S. aircraft had the avionics necessary to make use of a wide variety of precision weapons by acquiring targets, illuminating them when necessary, using GPS guidance, and acquiring targeting coordinates from the ground. To put these differences in perspective, only one out of five strike aircraft could launch laserguided bombs in the Gulf War; all strike aircraft could launch laser-guided bombs in the Iraq War.[223]

The onboard sensors and computer systems on these aircraft were much more capable both in executing preplanned strikes and in the dynamics of acquiring and killing. The integration of intelligence assets into target planning and the speed of execution made precision strikes more effective. All-weather coverage was better, and while the term "all-weather" will probably always seem at least somewhat ironic in air combat, field reports so far indicate that it was a far more realistic description in the Iraq War than in previous conflicts.

A combination of UAVs and better sensor aircraft, systems like the E-8C, and improved infrared and radar sensors interacted with better command and control to allow the effective use of both better delivery platforms and better precision weapons. For example, experimental use was made of the E-8C JSTARS to target Iraqi armor even under sandstorm conditions. Dust and sand did present problems in some cases. Still, the

---

[222] Cordesman, Anthony H., Ibid, p.30-31.
[223] Scarborough, Rowan, "Myers Says: Annihilation of Iraqi Army wasn't Goal", Washington Times, U.S.A., 30 June 2003.

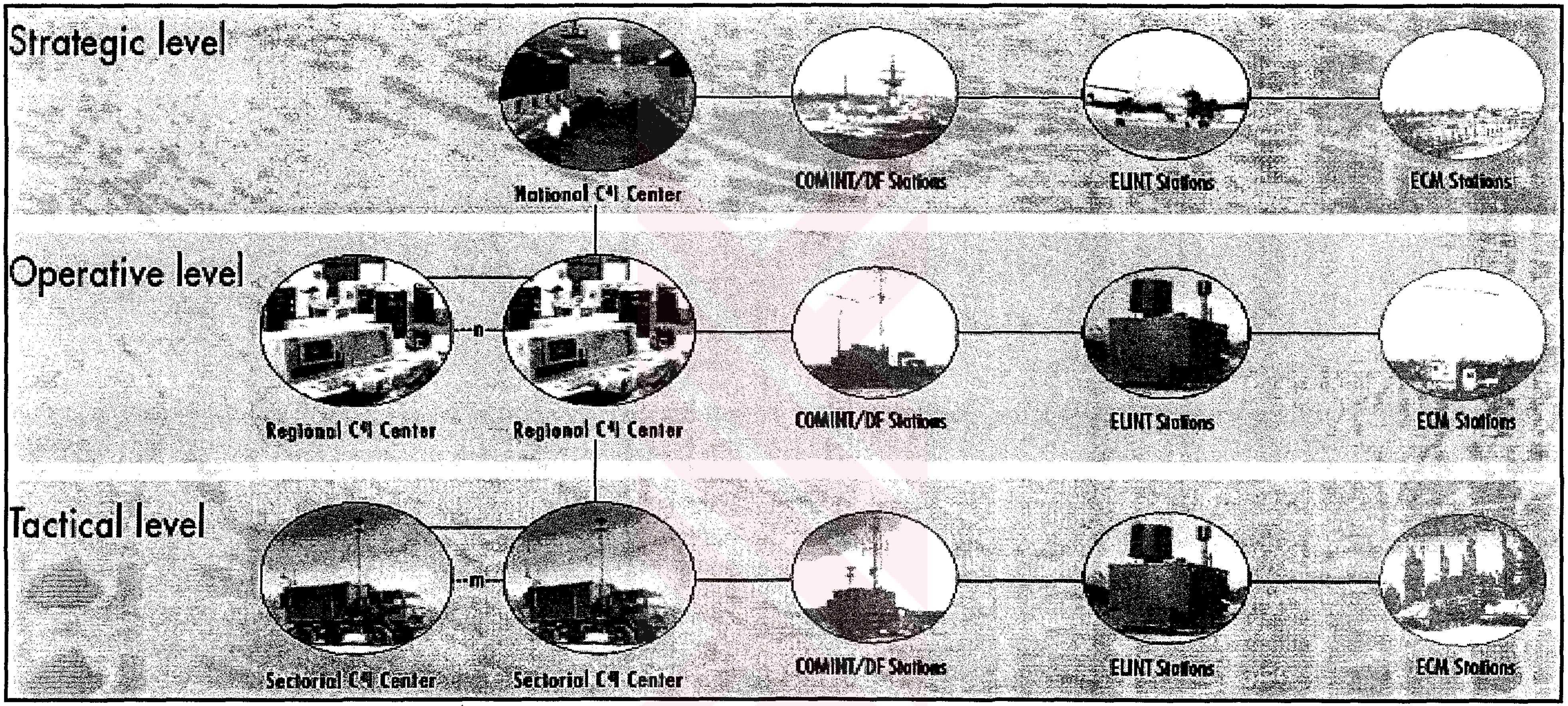
widespread dissemination of laser illuminators to ground forces and SOF units allowed them to call in precision close air support, as did giving those GPS targeting capability.[224]

There are no combat operations data available in a form where that makes it possible to precisely define the role of sensor aircraft like the E-8C JSTARS, or Joint Surveillance and Target Attack Radar System. It is clear, however, that extensive use was made of JSTARS. The Coalition's air dominance allowed it to be deployed forward and nearer the battle space, where it could track Iraqi armored and vehicle movements over hundreds of square miles, and it was used to cover the greater Baghdad area. The "fusion of intelligence" from the E-8C and other sources enabled the coalition to locate and target Iraq forces under weather conditions the Iraqis felt protected them from the air. Aircraft like the RC-135 Rivet Joint, for example, could characterize and locate the source of Iraqi military communications.[225]

While no sortie data are available on the Coalition's use of UAVs, the nature and importance of the data they collected, or the specifics of the role they played in joint operations, it is clear that they had a major impact. The Coalition used more than a dozen types of UAVs in the conflict, building on the U.S. success in using such systems in Afghanistan.[226] The UAVs included larger systems like the Predator, Global Hawk, and the Pointer, the three systems the United States used in Afghanistan. The United States had used the Pioneer in the Gulf War. In the Iraq War, the Coalition also made use of new tactical systems like the U.S. Army Hunter and Shadow, the Marine Corp's Dragon Eye, and the USAF Force Protection Surveillance System. The change was particularly important in the case of field commanders, who had only one type of UAV available in the Gulf War but had 10 types available in the Iraq War. Both the US military services and the Britain Ministry of Defense concluded that the value of these UAVs was one of the major lessons of the war.[227]

---

[224] Cordesman, Anthony H., Ibid, p.42-43.
[225] Grahm, Bradley, and Vernon Loeb, "An Air War of Might, Coordination, and Risks", Washington Post, Washington, D.C., U.S.A., 27 April 2003, p. A1.
[226] Schmidt, Eric, "In the Skies Over Iraq, Silent Observers Become Futuristic Weapons," New York Times, U.S.A., 18 April 2003.
[227] British Ministry of Defense, "Operations in Iraq: First Reflections", Ministry of Defense, London, U.K., July 2003, Available on site: http://www.mod.uk/



C^4I

The Command, Control, Communication, Computer and Intelligence Systems (C4I) control the EWIS operation and form the interface with the command level. It is the link between the various system elements and the human factor, which delivers the dramatic power boosting of the integrated system. The C4I process EW intelligence gathered by the COMINT/DF and ELINT stations and assigns missions to the ECM stations. A user friendly interface is utilized to facilitate efficient, accurate and timely operation.

COMINT/DF

Communication Intelligence and Direction Finding (COMINT/DF) stations provide services over a wide range of frequency bands (HF, VHF & UHF). Their advanced demodulation, classification and agile signal detection capabilities are combined with smart location techniques and supply a full, multifaceted, real time display of the EW arena activity.

ELINT

Electronic Intelligence (ELINT) stations complement the COMINT/DF stations by detection, interception, classification, location, analysis and identification of non-communication transmitters. Together they cover a complete spectrum of operational and tactical threats required for the generation of the Electronic Order of Battle (EOB).

ECM

The Electronic Countermeasure stations are the active elements of the EWIS, capable of interfering with hostile communications and electronic systems, or inserting false information in order to disturb its operation. They can jam communication equipment and networks, imitate and retransmit enemy's communication.

4. RADAR AND ELINT

A large portion of the EW community deals with radars (both search and target), and worries about jamming and counterjamming.[228] Radar works by sending out a radio wave at a very high frequency. When the radio signal hits raindrops part of the signal bounces back to the radar. The signal travels at the speed of light (over 350,000 kilometers per second). Knowing exactly how fast the signal is traveling, means that we can tell how far away the rain is by timing how long it takes for the signal to travel to the rain and then bounce back to the radar. This happens so fast that most radars send out about 1000 signals (called pulses) each second.

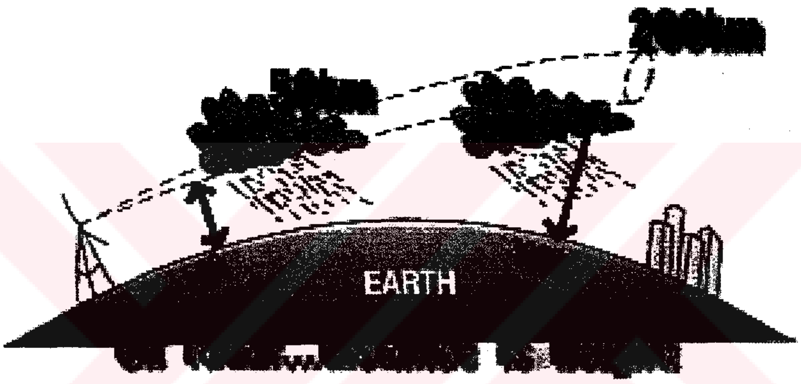


Figure 4.1: Radar signals.

Radar is an active remote sensing system which means that it provides its own source of energy to produce an image. It therefore does not require sunlight (as do optical systems) and data can be acquired either by day or by night. Furthermore, due to the specific wavelength of radar, cloud cover can be penetrated without any effect on the imagery.[229]

Offense and defense keep coming up with new techniques. Traditional radars generate a signal at one frequency; knowing the frequency makes it easy to jam a return signal. More modern radars hop from one outgoing frequency band to the next. To counter radars, today's jammers must be able to acquire the incoming signal, determine its frequency, tune the outgoing jamming signal accordingly, and send a blur back quickly enough to

[228] Libicki, Martin, "What is Information Warfare", National Defense University, U.S.A., August 1995, Available on site: http://www.iwar.org.uk/iwar/resources/ndu/infowar
[229] Inggs, M.R., and Lord, R.T., "Applications of Satellite Imaging Radar", University of Cape Town, South Africa, 2002, Available on site: http://rrsg.ee.uct.ac.za/applications/applications.html

minimize the length and strength of the reflected signal. Jamming aircraft that are riding in formation with attack aircraft often wipe out return signals (which weaken as the fourth power of the distance between radar and target) by overpowering them, but doing so makes jammers very visible so they must protect themselves. Coalition forces in the Gulf developed new synergies using jamming aircraft en masse. Radars make themselves targets because of their outgoing signals; antiradiation missiles (e.g., the HARM) force radars either to be turned off or to rely on chirping and sputtering. The aborted Tacit Rainbow missile was designed to loiter in an attack area until a radar turned itself on; the outgoing signal gave the missile an incoming beacon, and away it went. As digitization improves, radar can acquire a target by generating a transient pulse and analyzing the return signal before a false jamming signal overwhelms the reflection.

The cheaper digital manipulation becomes, the more logic favors the separation of an emitter from a collector. Emitters, the targets of antiradiation missiles, would proliferate, to ensure the survival of the system and to act as sponges for expensive missiles. The missiles would create a large virtual dish out of a collection of overlapping small ones. Because outgoing signals will be more complex, collection algorithms too will grow in complexity, but the ability of jammers to cover the more complex circle adequately may lag. Dispersing the collection surface will also make radars less inviting targets.[230]

4.1. ADVANCED RADAR SYSTEMS

4.1.1. Radial Velocity Discrimination

In many circumstances, it is beneficial to know both the range and the radial velocity of the target. Since the relative radial velocity is the range rate, a measurement of the radial velocity can be used to predict the target's range in the near future. For example, it allows the prediction of when a target will be inside the effective range of a weapon system. Radial velocity discrimination can also be used to eliminate unnecessary targets from the

[230] Libicki, Martin,Ibid.

display. For example, sea clutter or buildings. There are three methods used which can give simultaneous measurement of range and range rate. [231]

Differentiation: This system simply measures the range at fixed intervals and computes the rate of change between the measurements. For example, if a target is at 1500 m for the first measurement and at 1492 m for the next measurement made 1 sec later, the range rate is -8 m/s. Light detection and ranging (LIDAR) systems use this method. Accuracy is improved by taken several quick measurements and computing the average rate of change. The intervals cannot be chosen to be too small however, since the target must be able to change range during the measurement interval.

Moving Target Indicator (MTI): This system measures changes in the phase of the returned signal to determine motion of the target. In order to measure the phase, a sample of the transmitter pulse is fed into a *phase comparator,* which also samples the return signal. The output of the phase comparator is used to modulate the display information. Returns will be the largest and positive when they are in-phase the largest negative value when out of phase.

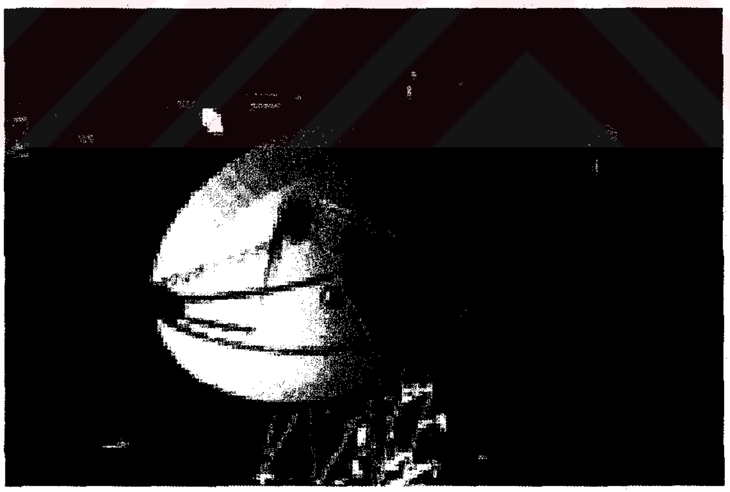


Figure 4.2: An example of radar.

When the range to a target is changing, the phase comparison output will be varying between its extreme values, as well as moving in range. One full cycle of phase shift is completed as the range changes by one-half wavelength of the radar. This is because the

[231] Federation of American Scientist Web Page, "Advanced Radar Systems", U.S.A., Available on site: http://www.fas.org/man/dod-101/navy/docs/es310/syllabus.htm

radar signal travels both to and from the target, so that the change total distance traveled by the radar pulse changes by a factor of two. For a typical radar wavelength of 3 cm, it is clear that the phase comparison output will be rapidly varying for targets whose range is changing.

The fact that stationary targets have a fixed value of phase difference can be exploited to remove them from the display. This is accomplished by a cancellation circuit. The MTI processor takes a sample from the phase comparison output and averages it over a few cycles. Moving targets will average to zero, while stationary targets will have non-zero averages. The average signal is then subtracted from the output before it is displayed, thereby canceling out the stationary targets.

Figure 4.3: Pulsed Doppler radar.

Pulse Doppler Radar: This system adds additional processing equipment to the basic pulsed radar system. A sample of the transmitted signal is directed to mixer, which also samples the output from the receiver. The output of the mixer is the Doppler shift. The Doppler shift is passed to a filter which modifies the display information accordingly.[232] As a truck approaches, Doppler's sound becomes louder and louder and higher and higher pitched. As it leaves, the sound quickly declines in volume and frequency. Sounds propagate as waves, at frequencies below two hundred kilohertz.[233]

---

[232] Federation of American Scientist Web Page, Ibid.

[233] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 320-321.

The most common application is to color code the return information on the PPI display. The Doppler shift is sorted into categories, for example positive, zero and negative, which are then associated with colors. In this example, only three colors are used: white, grey and black. (It can be used other colors like red, blue etc.)[234] By measuring shifts in the frequency of waves, it is possible to measure motion; how fast something is moving, and whether it is moving toward you or away from you. This can be done in any spectrum. Astronomers, for example, can examine the wavelength of light coming from stars to determine if the shift is toward the white or red (movement away) or toward the black or blue (movement toward you). In the radar spectra, Doppler radar can measure changes in frequency to determine speed.[235]

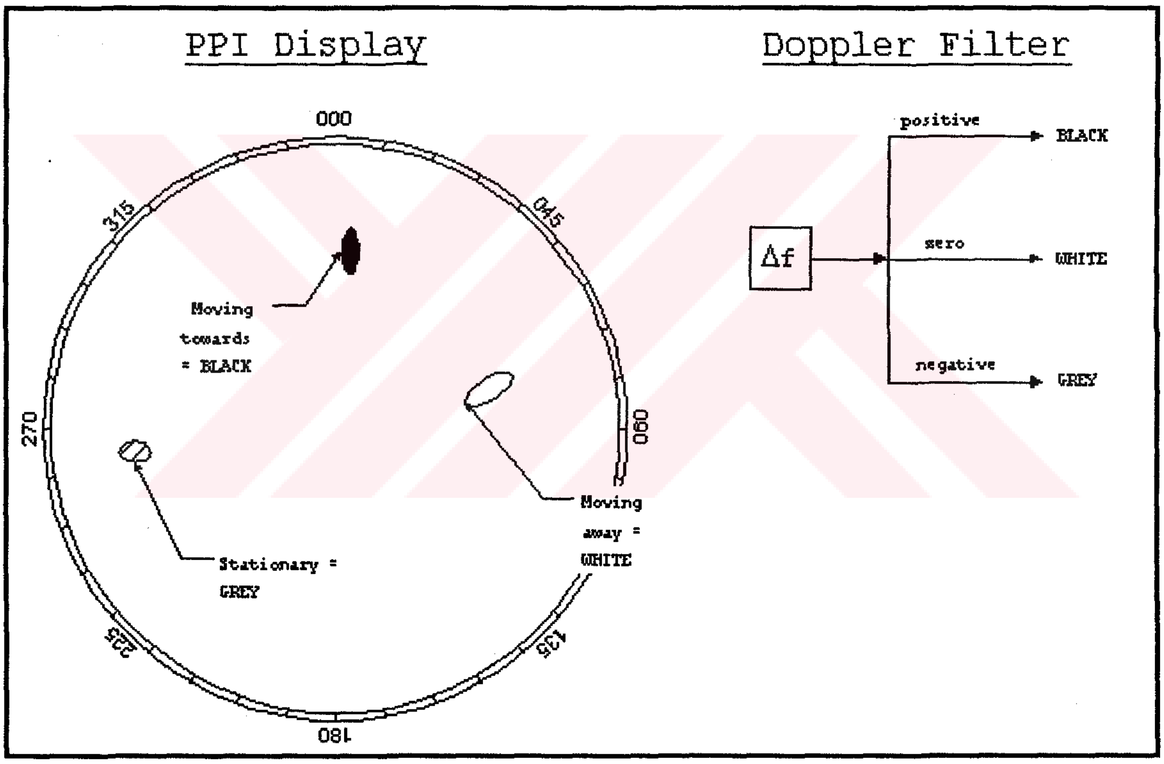


Figure 4.4: Pulsed Doppler display.

Pulsed Doppler radar systems are used in numerous military applications. They are also the standard weather radar throughout the country. The pulsed Doppler radar can detect and graphically display information about the relative motion of winds inside of storm cells

---

[234] Federation of American Scientist Web Page, Ibid.
[235] Friedman, George & Meredith, Ibid, p. 320-321.

and has proved useful in detecting tornadoes. A Doppler velocity display of a tornado will show the two colors which correspond to opposite directions of motion side-by-side.[236]

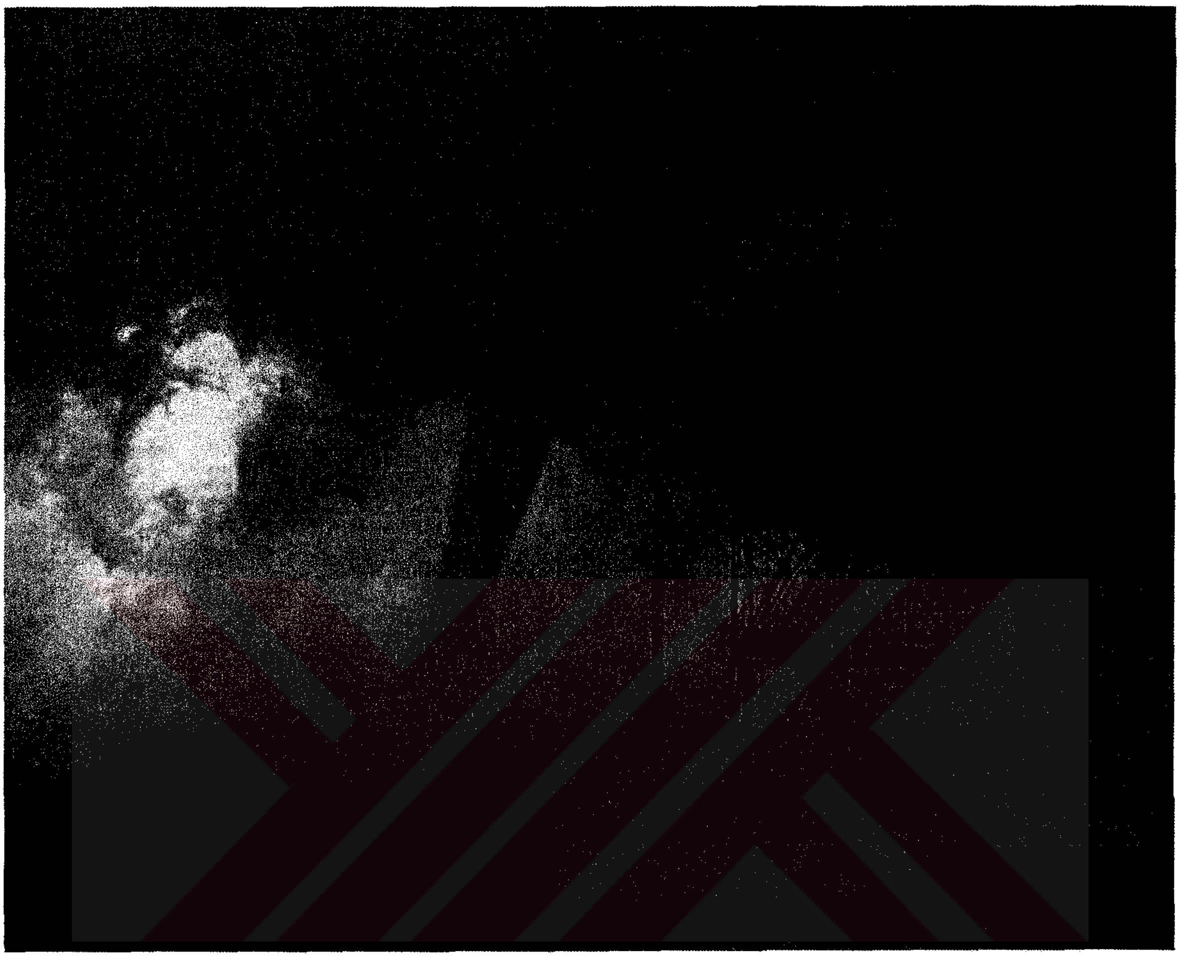


Figure 4.5: Nexrad Doppler

4.1.2. Synthetic Aperture Radar (SAR)

Synthetic Aperture Radar (SAR) is a technique for creating high resolution images of the earth's surface. Over the area of the surface being observed, these images represent the backscattered microwave energy, the characteristics of which depend on the properties of the surface, such as its slope, roughness, humidity, textural inhomogeneities and dielectric constant.[237] Synthetic aperture radar (SAR) is currently the principal means for acquiring ELINT sensor data for target recognition. SAR's advantages include ***all-weather capability, high resolution***, and ***imaging at a distance***. *Infrared sensing*, on the other hand,

[236] Federation of American Scientist Web Page, Ibid.
[237] Inggs, M.R., and Lord, R.T., "Applications of Satellite Imaging Radar", University of Cape Town, South Africa, 2002, Available on site: http://rrsg.ee.uct.ac.za/applications/applications.html

demands proximity, but can provide extremely useful information at high resolution by passive means. It must be assumed that the suite of available sensor modalities will expand, and that ATR methods will be able to provide generic, multisensor recognition capabilities.[238]

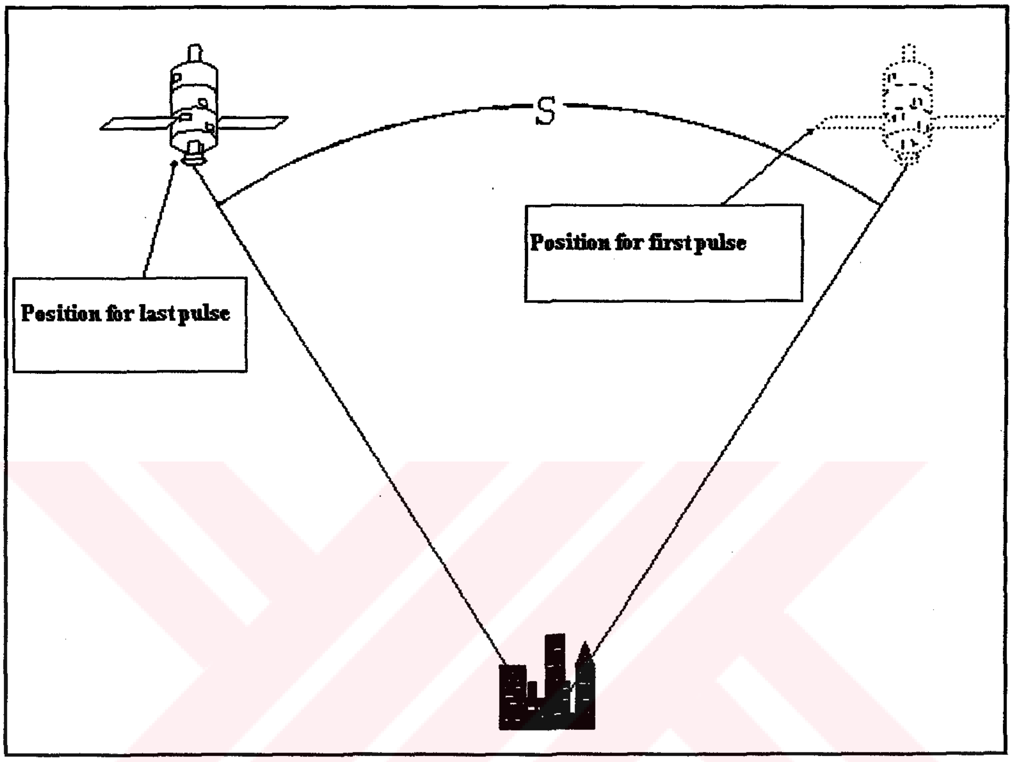


Figure 4.6: Synthetic aperture

It may also incorporate additional facilities to provide Ground Moving-Target Indication (GMTI), allowing them to detect and track vehicles traveling along roads on across country. Techniques such as Interferometric Moving Target Focusing (IMTF) provides imagery of mobile targets and detect vehicle vibration that can aid classification. 3D SAR can detect 10.000 feet height illegal immigrants, smugglers and terrorists, also allowing targets that are buried or hidden in dense woodland.[239] These dependencies allow SAR imagery to be used in conjunction with models of the scattering mechanism to measure various characteristics of the earth's surface, such as topography. SAR has become a

---

238 Naval Studies Board, "Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st-Century Force, Volume 3: Information in Warfare", National Academy of Science, Washington, D.C., U.S.A., 1997, Available on site: http://www.nap.edu/html/tech_21st/iwindex.htm

239 Caşın, M. Hakkı, "Digital Revolution for the Military: The Effects of the Electronics Revolution in the 21st Century on the International Security Strategy", Armed Forces Communications and Electronics Association, AFCEA, Ankara, September 1995, p.15.

valuable remote sensing tool for both military and civilian users. Military SAR applications include intelligence gathering, battlefield reconnaissance and weapons guidance.[240]

Synthetic aperture radar (SAR) uses the motion of the transmitter/receiver to generate a large effective aperture. In order to accomplish this, the system must store several returns taken while the antenna is moving and then reconstruct them as if they came simultaneously. If the transmitter/receiver moves a total distance S during the period of data collection, during which several return pulses are stored, then the effective aperture upon reconstruction is also S (Figure 4.6). The large synthetic aperture creates a very narrow beamwidth which can be calculated by the usual beamwidth formula, substituting the synthetic aperture for the physical antenna aperture. For most radar antennas the beamwidth is sufficiently large so that the cross range resolution is fairly large at normal detection ranges. As such, these systems cannot resolve the detail of the objects they detect.

The most frequent application of SAR is with satellite radar systems. Because the satellite is traveling at high velocity, the accuracy of these systems can be made very high. Furthermore, if the target is fixed in location, the period for data collection can be made very long without introducing significant error. Therefore satellite SAR is used for the imaging of fixed objects like terrain, cities, military bases, etc.[241]

Technology advances are anticipated in the following three areas:

- Better sensing methods,
- Better algorithmic methods for performing recognition, and
- Faster and better computer processing.

In the area of improved sensing, SAR image formation methods can be considerably improved. New methods for improving the resolution, for coherently adjusting, and improving the combination of raw signal data, and for adaptively forming the best image

[240] Inggs, M.R., and Lord, R.T., "Applications of Satellite Imaging Radar", University of Cape Town, South Africa, 2002, Available on site: http://rrsg.ee.uct.ac.za/applications/applications.html
[241] Federation of American Scientist Web Page, Ibid.

promise to dramatically improve SAR capabilities for ATR applications. While the capability does not exist today, it may be possible in the future to form SAR images of moving objects. Some progress has been made in this area, but the algorithms are more delicate. It is reasonable to expect that developments will occur to permit high-accuracy radar imaging of moving objects at long distances. Much of the investment in ATR development has focused on the inverse SAR (ISAR) modality, such as imaging a moving ship from a fixed radar platform. These algorithmic methods for image formation, applied to other targets such as moving ground targets, may prove useful for achieving high-resolution imaging of moving targets at a distance, although at this point, the use of ISAR techniques for general ATR applications is only in the earliest stages of development.

Inexpensive infrared (IR) sensors, especially ultraminiaturized ELINT and other sensors, are likely to be available in the near future. Depth sensing, by light detection and ranging (LIDAR), and chemical analyses from a distance might also enable a wealth of discrimination capabilities. ATR is normally associated with image processing, but other signal data such as hyperspectral and multispectral techniques can be used as well, as long as the information assists in discriminating among targets and non-targets. Since the image formation process can involve discarding information, there may be improved methods that deal directly with raw sensor data.[242]

4.1.3. Inverse Synthetic Aperture Radar (ISAR)

It is possible to achieve the same large synthetic aperture without moving the transmitter/receiver. If the target rotates by a small amount, it has the same effect as if the transmitter/receiver were to travel a distance equal to the arc length at the range R.

ISAR systems are typically used for long-range imaging and identification of possible targets. The ISAR platform may be fixed or moving. The best targets for ISAR are ships which tend to yaw periodically in the sea state.[243]

---

[242] Naval Studies Board, "Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st-Century Force, Volume 3: Information in Warfare", National Academy of Science, Washington, D.C., U.S.A., 1997, Available on site: http://www.nap.edu/html/tech_21st/iwindex.htm
[243] Federation of American Scientist Web Page, Ibid.

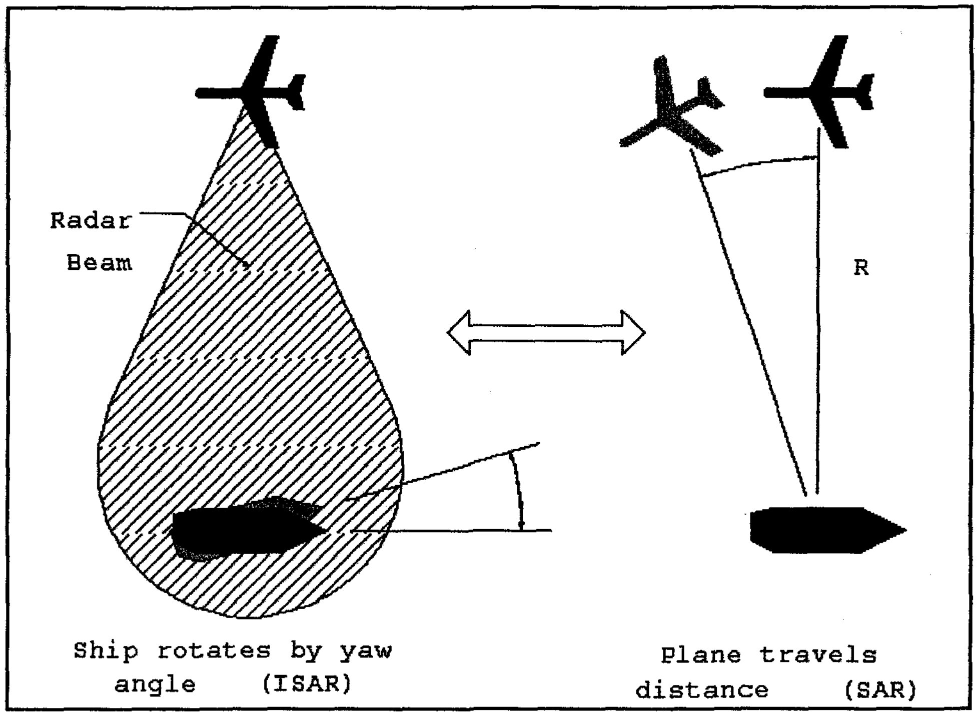


Figure 4.7: Equivalence of SAR and ISAR.

4.2. DIGITAL RADAR

After years of anticipation, a revolution is at hand in radar technology through the exploitation of a combination of modern digital techniques and fiber-optic communications. Not only will the next-generation radars be solid-state phased arrays, but they will also be almost entirely digital, confining the analog microwave portions to the extreme front end interface of the antenna with the outside world. Received signals will be digitized at the element after minimal analog processing (e.g., with an antialiasing fitler, a low-noise MMIC amplifier, and perhaps a single stage of up or down conversion) and transmitted in digital form over wideband fiber-optic links to convenient remote locations off the aperture for processing, e.g., digital beamforming, in-phase (I) and quadrative (Q) generation, pulse compression, clutter suppression, target extraction, multihypothesis tracking, and so on. Similarly, for transmit, digitally created waveforms will be generated off aperture and distributed via fiber optics to individual antenna elements where D/A conversion and MMIC power amplification will take place. With all signals in digital form, the phase shifting required by both transmit and receive functions can be implemented digitally by simply delaying the signals to or from individual antenna elements by different amounts. Coarse delays can be obtained by slipping clock cycles and fine delays by digital interpolation. This approach eliminates the need for analog phase shifters in the T/R modules and supplies, without effort, true time-delay digital beamsteering.[244]

4.3. IMAGING RADAR

Imaging radar works very like a flash camera in that it provides its own light to illuminate an area on the ground and take a snapshot picture, but at radio wavelengths. Radar uses an antenna and digital computer tapes to record its images. In a radar image, one can see only the light that was reflected back towards the radar antenna.

Typical radar (Radio Detection and Ranging) measures the strength and round-trip time of the microwave signals that are emitted by a radar antenna and reflected off a distant surface or object. For an imaging radar system, about 1500 high- power pulses per second are transmitted toward the target or imaging area, with each pulse having a pulse duration *(pulse width)* of typically 10-50 microseconds (us). The pulse normally covers a small band of frequencies, centered on the frequency selected for the radar. At the Earth's surface, the energy in the radar pulse is scattered in all directions, with some reflected back toward the antenna. This backscatter returns to the radar as a weaker radar echo and is received by the antenna in a specific polarization (horizontal or vertical, not necessarily the same as the transmitted pulse). These echoes are converted to digital data and passed to a data recorder for later processing and display as an image.[245]

In the case of imaging radar, the radar moves along a flight path and the area illuminated by the radar, or *footprint*, is moved along the surface in a swath, building the image as it does so.

The length of the radar antenna determines the resolution in the azimuth (along-track) direction of the image: the longer the antenna, the finer the resolution in this dimension. *Synthetic Aperture Radar (SAR)* refers to a technique used to synthesize a very long antenna by combining signals (echoes) received by the radar as it moves along its flight track. Aperture means the opening used to collect the reflected energy that is used to form

---

[244] National Academy of the Science Web Page, "4: Sensors", NAP, U.S.A. Available on site: http:www.nap.edu/html/tech_21st/t4.htm
[245] Freeman, Tony, "What is imaging Radar", Jet Propulsion Laboratory, Pasadena, CA, U.S.A., January 1996, Available on site: http://www.spaceimaging.com/products/radarsat/whatisradar.htm

an image. In the case of a camera, this would be the shutter opening; for radar it is the antenna. A *synthetic* aperture is constructed by moving a real aperture or antenna through a series of positions along the flight track.

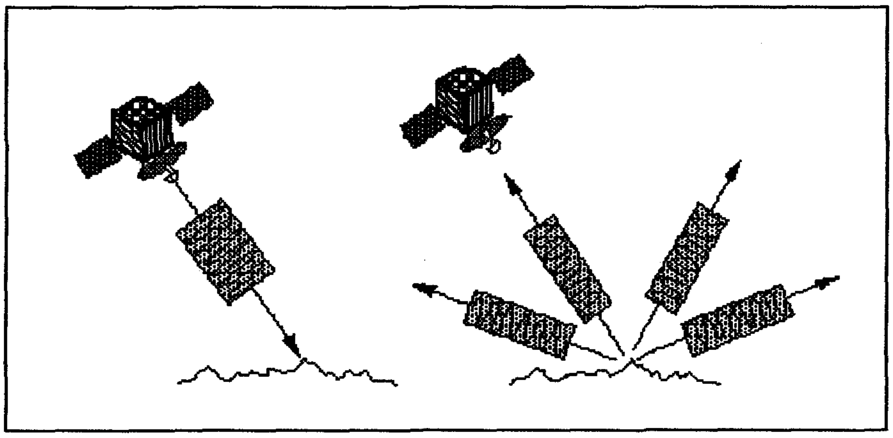


Figure 4.8: Radar transmits a pulse Measures reflected echo (backscatter)

As the radar moves, a pulse is transmitted at each position; the return echoes pass through the receiver and are recorded in an 'echo store.' Comparing the Doppler-shifted frequencies to a reference frequency allows many returned signals to be "focused" on a single point, effectively increasing the length of the antenna that is imaging that particular point. This focusing operation, commonly known as SAR processing, is now done digitally on fast computer systems. The trick in SAR processing is to correctly match the variation in Doppler frequency for each point in the image: this requires very precise knowledge of the relative motion between the platform and the imaged objects.[246]

Spaceborne Imaging Radar-C and X-band Synthetic Aperture Radar (SIR-C/X-SAR) is part of NASA's Mission to Planet Earth. The radars illuminate Earth with microwaves, allowing detailed observations at any time, regardless of weather or sunlight conditions. SIR-C/X-SAR uses three microwave wavelengths: L-band (24 cm), C-Band (6 cm) and X-Band (3 cm). The multi-frequency data will be used by the international scientific community to better understand the global environment and how it is changing. The SIR-C/X-SAR data, complemented by aircraft and ground studies, willgive scientists clearer insights into those environmental changeswhich are caused by nature and those changes which are induced by human activity. SIR-C was developed by NASA's Jet Propulsion

[246] Freeman, Tony, Ibid.

Laboratory. X-SAR was developed for the German space agency, and the Italian space agency.[247]

Parallel to the development of spaceborne imaging radars, NASA/JPL have built and operated a series of airborne imaging radar systems. NASA/JPL currently maintain and operate an airborne SAR system.[248]

4.4. SPACE BASED RADAR (SBR)

With the uncertain global political situation, there has been a shift in proposed space based radar applications. The former emphasis on global surveillance has changed to focus on theater support. One of the most important theater support missions is airborne target detection and tracking. Radar provides significant advantages for airborne detection because of its ability for day, night and all-weather operation. However, airborne target detection and tracking requires frequent data updates. Two distinct aspects of the constellation size problem are to assess constellation sizes as a function of orbit parameters, radar capabilities, and theater size. First, the number of satellites needed to provide a maximum and average revisit time was determined based on total satellite field-of-regard. This is a minimum number of satellites needed and is only a function of the altitude of the satellites. A second is to increased number of satellites required when realistic radar parameters are included.

For that case, the search rate of the radar determines what part of the instantaneous field-of-regard can be actually covered by a satellite while it is over a theater of interest.[249]

Space Based Radar will provide rapid Battlespace Dominance and Operational Decision Superiority through:[250]

- Day/night, near continuous surveillance with Ground Moving Target Indication (GMTI) and Synthetic Aperture Radar imaging from space.

---

[247] Photovault.com Web Page, "Spaceborne Imaging Radar-C/X-Band Synthetic Aperture Radar", 1995, Available on site: http://www.photovault.com/Link/Cities/Midwest/Louisiana.html

[248] Freeman, Tony, Ibid.

[249] Lapointe, Mike, "Future Spaced Based Radar", NSSA, U.S.A., July 1999, Available on site: http://www.fas.org/spp/military/program/nssrm/initiatives/sbr_dod.htm

[250] Air University, "Key Air Force Programs: Space", Air Force University, Maxwell, Alabama, U.S.A., 2003, Available on site: http://space.au.af.mil/space.pdf

- Deep-look, wide area surveillance of denied areas allowing for responsive, precision targeting for the warfighter.

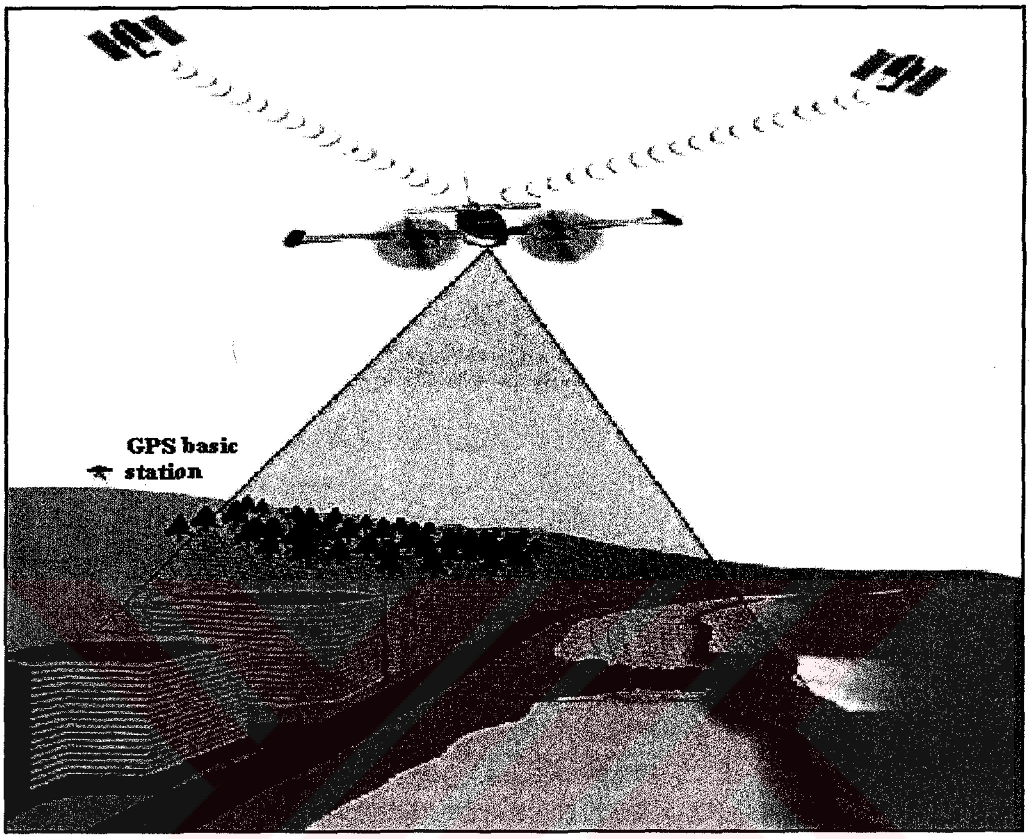


Figure 4.9: Future Space Based Radar (SBR)

In 1978, the United States launched a satellite known as Seasat, which had a resolution of about eighty-two feet. The satellite was in an orbit about a hundred miles above the earth. A traditional radar would have required an antenna about 1.2 miles wide, obviously impractical.[251] What made Seasat possible were two new innovations: phased-array and synthetic radar both combined into a single system on reconnaissance satellites.[252]

A space-based radar capability is needed to enable continuous (24-hour) full-global coverage. Benefits would include precision maps, detection and continuous tracking of sea,

[251] Richelson, Jeffrey, T., "America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program", Harper & Row Publications, New York, N.Y., U.S.A., 1990, p. 110.
[252] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 320.

ground and air moving targets, and accurate real-time determination of orders of battle (OOBs).[253]

4.5. SHIPBOARD ANTI-AIR-WARFARE (AAW) SYSTEMS, RADAR AND ELINT

A major issue for the future of reconnaissance and surveillance is the types of platforms in which the Services, and in particular the Navy, should invest. General categories are space-based, airborne, and shipboard, the latter including both surface and subsurface platforms. If an active radar sensor is required, the option of having satellites in synchronous orbit becomes prohibitive due to the R^4 dependence of radar signals on target range. Even a radar sensor in low orbit suffers from R^4 dependence, since practical considerations of orbital decay require significant satellite altitude, which maps into slant range requirements at least as severe as those of airborne radars, and typically worse.[254]

Radar technology development is likely to continue its evolutionary pace over the next several decades. Advances in solid-state transmit/receive (T/R) modules will include higher output power, greater direct-current-to-RF conversion efficiency, and increasing miniaturization. Even more importantly, costs will drop dramatically as production volumes increase, leading to extensive use of this technology in future systems. This will enable a variety of active array designs with two-dimensional electronic beam steering and dynamically reconfigurable apertures that will optimize multimode radar performance. Fighter radars will exploit T/R module technology to provide a variety of sophisticated air-to-air and air-to-ground modes, both detection and imaging. Higher average power achieved will enable fire control solutions at very long range against conventional targets, and will begin to have benefit against small-cross-section threats. Ship-based air defense radars will see a similar benefit in enhanced sensitivity as well as flexibility in the prosecution of multiple simultaneous fire control solutions.[255]

For modern shipboard anti-air-warfare (AAW) systems, the most critical performance requirement is the ability to successfully counter saturation attacks. Such attacks may

---

[253] Department of Defense, "Space Technology Guide-FY 2000-01", Office of the Secretary of Defense, Washington, U.S.A., 2002, Available on site: http://www.defenselink.mil/myer.pdf
[254] Naval Studies Board, "Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st-Century Force, Volume 3: Information in Warfare", National Academy of Science, Washington, U.S.A., 1997, p. 51-52, Available on site: http://www.nap.edu/html/tech_21st/iwindex.htm
[255] Naval Studies Board, Ibid, p. 55-56.

include numerous aircraft and particularly anti-ship missiles converging from multiple directions in close coordination, with the clear intention of overwhelming the defenses. The successful engagement of each of these targets by the AAW system(s) requires precise tracking so that useful fire-control data can be supplied to the ship's overall combat system. Conventional mechanically scanned 2-D or 3-D radars achieve this tracking by correlating successive radar echoes for each target. This function is often referred to as "track-while-scan" (TWS) and is usually performed on multiple targets at the same time, the system's computational power permitting. Obviously, the higher the sweep rate of the radar, the finer-grained the tracking information is going to be for each air target. In mechanically scanned radars, the rotation speed of the radar antenna and the update rate of target information (often referred to as "data rate") are obviously identical.

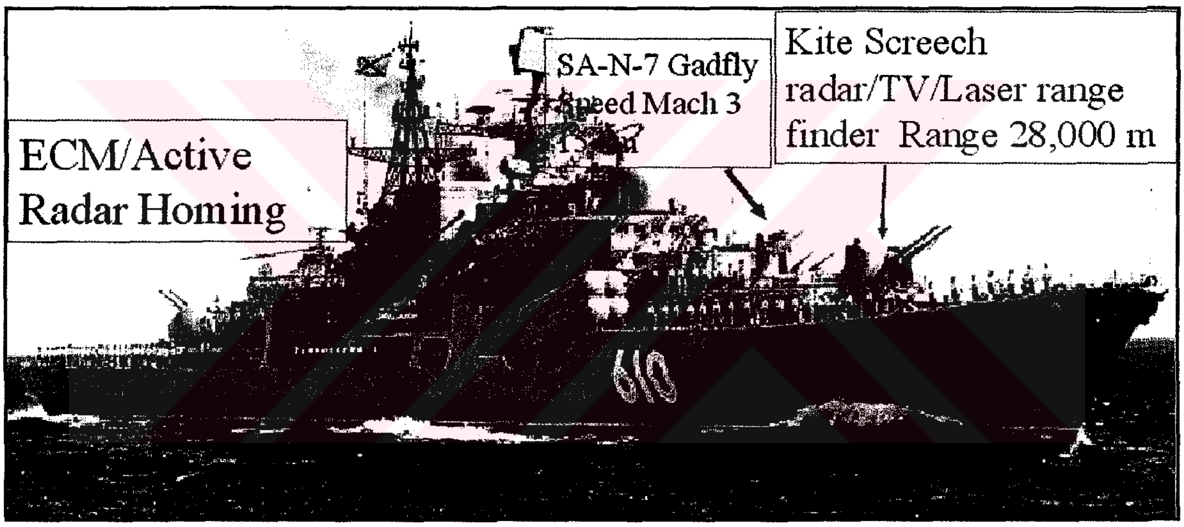


Figure 4.10: Shipboard AAW & Electronic Warfare Systems

For most current warships to provide separate radars dedicated to the target-tracking function creates a clear separation of duties: the surveillance radar performs the initial target detection and low-quality tracking and then passes this data to the tracking radar, which performs the high-quality tracking and fire-control operation (frequently providing illumination for radar-guided weapons).

The need for a high data rate means that the radar beam has to jump between widely separated targets almost instantaneously in order to quickly provide updates on their status, something impossible for a mechanical antenna. On the contrary, this is possible if the management of the radar beam is, instead, handled electronically by antennas formed by multiple independent transmitters, spaced at predefined regular intervals.[256]

4.6. FUTURE AIRCRAFT RADAR SYSTEMS

The Sentinel X-band mobile radar system is another sensor used in concert with the Army's Forward Area Air Defense Command, Control and Intelligence (FAADC2I) system. Using both electronically scanned phased array and mechanical scan technologies, this three-dimensional pencil-beam radar automatically detects, tracks, classifies, identifies, and reports multiple targets out to a range of 30 kilometers (18 miles). The sensor system reports targets such as cruise missiles, unmanned aerial vehicles, helicopters, and fixed-wing targets to forward area air defense systems for rapid engagement. Sentinel also links with the Air Force/Boeing E-3 Airborne Warning and Control System (AWACS) aircraft and to the Navy's Aegis radar and missile systems on cruisers and destroyers at sea, the general added.[257]

The use of off-board ELINT sensors and data links to pass high-fidelity data to strike aircraft is an established concept. It is valuable when considered as an adjunct to the striker's own sensor array but dangerous if considered as a substitute. An analogy can be drawn with the F-15C in its air-to-air role. That aircraft is capable of independent detection, identification (ID), and weapons employment. Data link from off-board ELINT sensors merely enhances those abilities. Any suggestion that an F-15 pilot could rely on data-linked information from airborne warning and control systems (AWACS) aircraft, to the exclusion of its own radar, would be inaccurate and unwelcome.

Similar limitations exist with other sensors. Electronic surveillance (ES-ELINT) sensors removed from the immediate battlefield have serious physical limitations; they are not generally in the radar's main beam and are often unable to see weak signals. Air-breathing

[256] Dranidis, Dimitris V., "Backboards of the Fleet: Shipboard Phased-Array Radars", Journal of Electronic Defense, U.S.A., May 2003. Available on site: http://www.jedonline.com
[257] Robinson, Clarence A., "The Electronic Battlefield", Faircount.com Web Page, Available on site: http://www.faircount.com/web04/yid/articles/electron.html

sensors may be blocked by terrain and the curvature of Earth. All of these factors combine to make a distant sensor's picture incomplete.[258]

Ground Based Common Sensor/Advanced Quick Fix is vehicle-mounted signals intercept and precision emitter location systems. The sensors identify enemy command, control, communications, and intelligence systems and radar, while providing electronic countermeasures against hostile communications. The GBCS/AQF core capabilities expand frequency and area coverage and add new classes of signals. The GBCS/AQF enhances the ground commander's ability to outmaneuver and destroy an enemy by locating or jamming threat command and control, fire control, and air defense centers.[259]

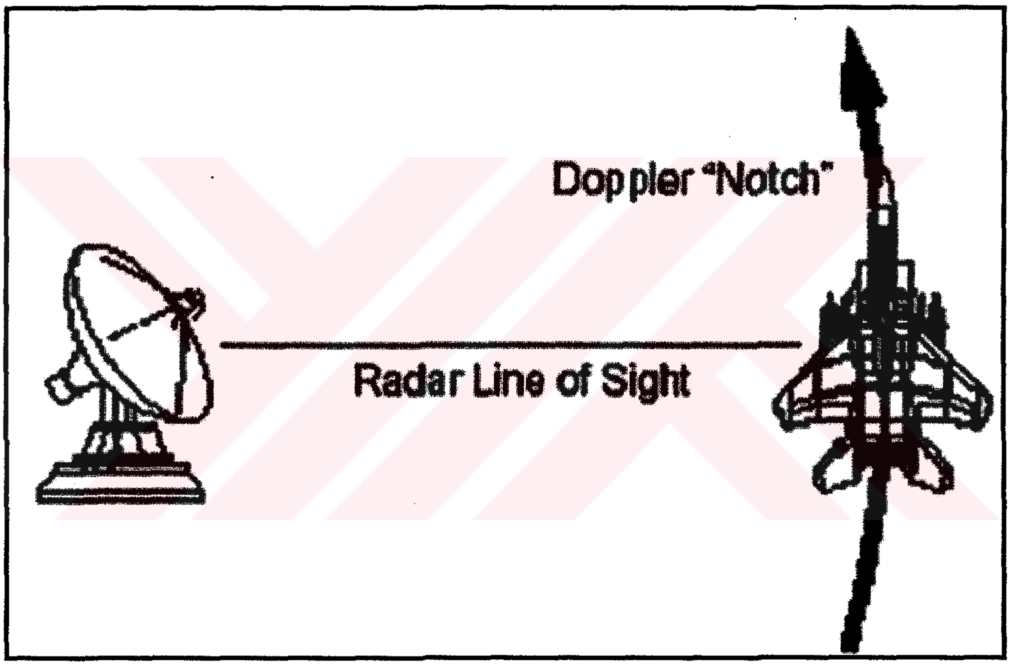


Figure 4.11: Doppler-Notch Diagram.

Low-power signals are particularly difficult for intelligence (ELINT), surveillance, and reconnaissance (ISR) sensors to pick out at long range. The distant collector often has to detect the low-signal-strength sidelobes or backlobes, rather than the main beam. Additionally, the strength of a signal is further attenuated by distance and atmospheric and weather effects.

258 Pietrucha, Maj Michael, "Needles in the Haystack: Hunting Mobile Electronic Targets", Air & Space Power Journal Magazine, U.S.A., Spring 2003.
259 Robinson, Clarence A., "The Electronic Battlefield", Faircount.com Web Page, Available on site: http://www.faircount.com/web04/yid/articles/electron.html

Data links need not reach across the battlefield. A flight of four aircraft could exchange information between nearby strike aircraft via a low-power data link that need not even use a radio frequency. A link can be designed for jam resistance and low probability of intercept.[260]

The ability of an RWR to accurately locate a modern SAM system is critical to the survival of the aircraft. A pulse-Doppler (PD) radar operator detects an aircraft by noting a difference in the frequency of the transmitted and reflected energy. That frequency (Doppler) shift is caused by the component of the aircraft's velocity that is directed toward or away from the radar. Pilots in a detected aircraft may try to break the enemy radar's tracking by turning and placing the radar at 90 degrees to their own vector. That change in direction reduces the velocity component toward or away from the radar site to near zero which results in a near-zero-Doppler shift. A reduced Doppler shift also enhances the effectiveness of chaff and decoys, which should allow the aircraft to break lock and hide in ground clutter. Most Doppler radar systems use a filter to reduce clutter by eliminating all returns below a certain velocity. To make the aircraft appear to have a velocity less than the filter velocity, or stay "in the notch," the pilot of a strike aircraft flying at 540 knots must hold a heading (plus or minus three degrees) that is perpendicular to the direction from the aircraft to the radar (Figure 4.9).

If one pictures a string connecting the aircraft to the radar, the aircraft must put the string at 90 degrees to the nose (directly off the left or right wing), which results in a curved flight path with the radar at the center. This means that the aircraft is not changing its distance from the radar, has no apparent velocity to the radar, and so is much harder to break out of clutter. To do that, pilots must know the location of the threat radar precisely if they are to survive and attack the target.

If the strike aircraft can locate the emitter to within a 2,000-foot-radius circle, it can cue other ELINT sensors. The F-15E, F-18, B-1, and B-2 can use high-resolution synthetic aperture radar (SAR) maps to precisely locate the target cues by onboard ES, thus bridging the gap from the circle provided by ES to Global Positioning System (GPS) quality

[260] Pietrucha, Maj Michael, Ibid.

coordinates provided by the SAR. Most importantly, this precise location is done rapidly, entirely within the cockpit of a strike aircraft capable of conducting an immediate attack.

The ISR data collected by larger, standoff systems, the strike aircraft also become *providers* of critical ELINT sensor data to other assets. Their positioning in the battlespace makes them an ideal collector. They stimulate the air defenses, becoming the reason that the radars turn on in the first place. They are the closest to an air threat. An array of onboard ELINT sensors, infrared (IR), radar, and electro-optics can be used to gather information, record it, and download it after the mission. Information gathered by the strike aircraft is transmitted to an ISR platform on a simple, line-of-sight link. The UAV (in the above example) then transmits the data beyond line of sight, using its own dedicated data links and removing the need to have a complex (and expensive) communications array aboard the strike aircraft. Electronic intelligence (ELINT) information, for example, can be used to update threat databases, characterize enemy radars, and analyze enemy tactics. The ability to bring back recorded data and conduct a postflight download will provide additional and essential intelligence, remembering that not everything of value is needed in real or near-real time.[261]

[261] Pietrucha, Maj Michael, Ibid.

5. SPACE, SATALLETIES AND ELINT

As war and intelligence operations become more sophisticated, they rely more heavily on space-relay links from military command centers to battlefield and, further, to outposts near the front lines of operation. More data, more electronic maps, more commands from top brass, even 3-D visualizations of enemy territory.[262] The reconnaissance and electronic intelligence (ELINT) that is received from space that helps watching the whole war area, the night vision systems, reflect the radical changes. Even though the Micro-electronics Evolution has enabled the weight and the size of the electronic elements to be small, it improved the performance.[263]

As the fourth dimension, space involves dominating the *high ground* of space to deny its advantages to the adversary and to use it to implement one's own command, control, communications, navigation, reconnaissance, air defense, missile defense, warning, and weather forecasting.[264] Space has been integrated ever more fully into military systems, from targeting to communications to intelligence. The infrastructure of military is utterly dependent on the space-based component. Like video clips jamming the Internet, the military's technological sophistication grows to fill the bandwidth.[265] Space assets can become a key to the future digitalization of the battlefield where some of the fog and friction of war is removed for the side domination space.[266] Ground troops, Special Forces and fighter pilots in the newly proclaimed war on terrorism will likely move more bits of data than ever before as they are forced to new levels of creativity to locate a terrorist leader who does not wish to be found and who has proven extremely elusive. It's possible that this operation might exhaust some of satellite capabilities in the region.[267]

Military operations rely heavily upon information lines of communication to, in, through, and from space. Space assets integrate and deliver command, control, communications,

---

[262] Britt, Robert Roy, "War on Terrorism Could Clog Military's Space Airwaves", U.S.A., 08 October 2001, Available on site: http://www.space.com/news/

[263] Caşın, M. Hakkı, "Digital Revolution for the Military: The Effects of the Electronics Revolution in the 21st Century on the International Security Strategy", Armed Forces Communications and Electronics Association, AFCEA, Ankara, September 1995, p. 6.

[264] Blackwell, J., "Battlefield of the Future: New Era Warfare? A Revolution in Military Affairs?", Air Force Press, Maxwell, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles/battle/ov-2.html

[265] Britt, Robert Roy, Ibid.

[266] Blackwell, J., Ibid.

[267] Britt, Robert Roy, Ibid.

computers, intelligence, surveillance, and reconnaissance (C^4ISR) capabilities; navigation; and weather so forces can deny such to an adversary, and enable combatant commanders and operational forces to synthesize information, dictate the timing and tempo of operations, and counter an adversary's ability to exercise command and control.[268] During the military operations in order to feed the troops' voracious appetite for electronic intelligence (ELINT) information, more than a dozen different American, British, French and Russian satellites gathered intelligence via photography, infrared and radar imaging, and radio and television intercepts; measured and reported weather conditions; communicated command and control (C^2) messages and data; and pinpointed targets and located people on the ground.[269]

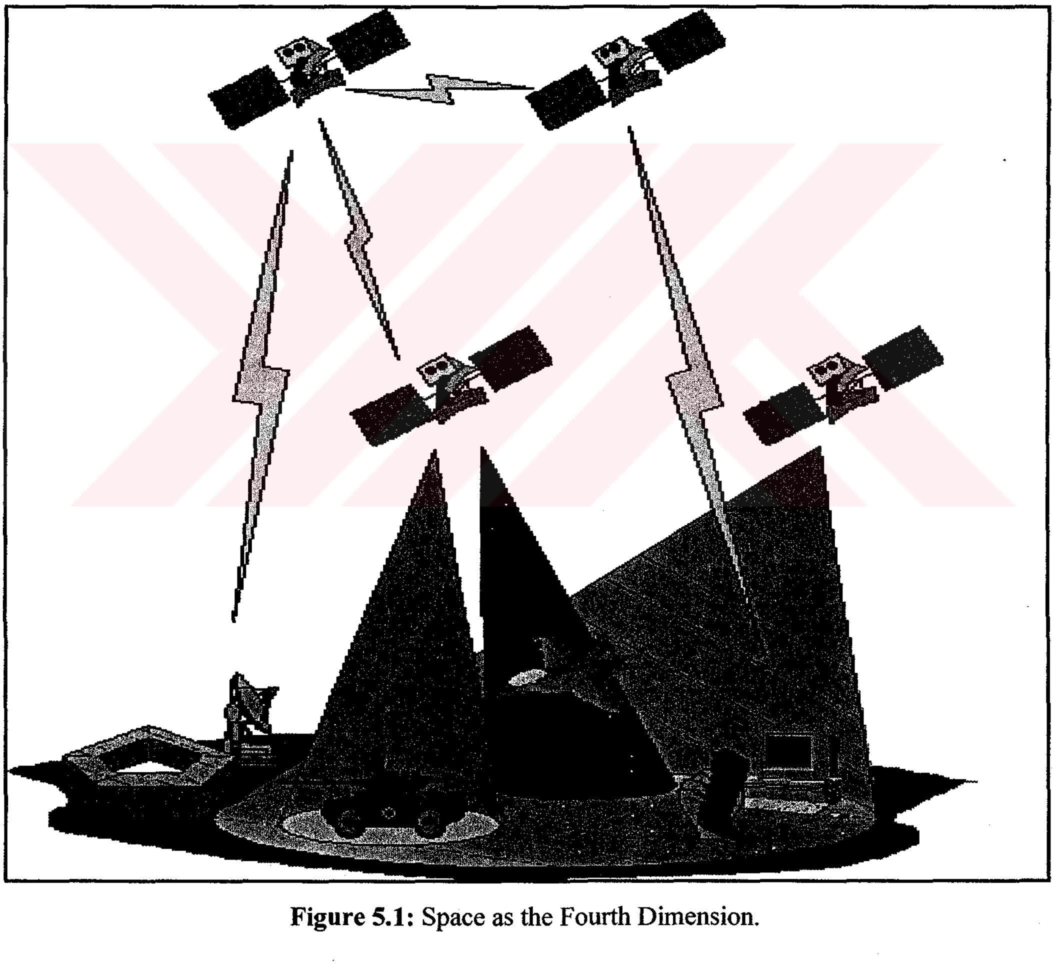


Figure 5.1: Space as the Fourth Dimension.

---

[268] Cohen, William S., "Annual Report to the President and the Congress – Information Superiority and Space", Secretary of Defense, DoD, U.S.A., 1999. Available on site: http://www.defenselink.mil/execsec/adr99.htm

[269] Anthony, R., "Space Today Online-The Satellite Wars- Afghanistan and Yugoslavia", U.S.A., 2001, Available on site: http://www.spacetoday.org/Satellites/YugoWarSats.html

Space is defined by SPACECOM as everything above 100 miles. Earth's atmosphere grows thinner with altitude in a gradual way, however. There is no clear edge. Pilots zooming above 50 miles are awarded astronaut wings, for example.

Most satellites, however, are at least 100 miles up with some ranging more than 22,000 miles above the surface. And military experts say the Armed Forces are relying more and more on these orbiting data and command posts to root out the enemy or to blow up targets with pinpoint accuracy from safe distances. So outer space increasingly becomes military space.

From 22,300 miles up, a satellite can see half the planet. That's where most missile-warning and communications satellites operate in what are called geosynchronous orbits; perches that remain fixed over a given part of the planet by orbiting Earth once every 24 hours.[270]

Weather satellites share this lofty region of space. Able to see half the globe, the GOES satellites of the National Oceanic & Atmospheric Administration feed constant data about cloud cover and moisture into weather forecasting programs. This information is also used by the military. Some television satellites also operate at this altitude. Their fixed location in the sky, relative to Earth, explains the fixed position of home satellite TV receiver dishes.

Various types of military communication satellites also traverse this high ground. More critical at this extreme altitude are a handful of Defense Support Program (DSP) satellites, first deployed in 1970. They are a key part of the military's early warning systems, using infrared sensors to detect heat from missiles or rockets. Though the operation of these DSP satellites is kept secret, the Federation of American Scientists says three are in operation and two are in space and available as backups.

[270] Britt, Robert Roy, Ibid.

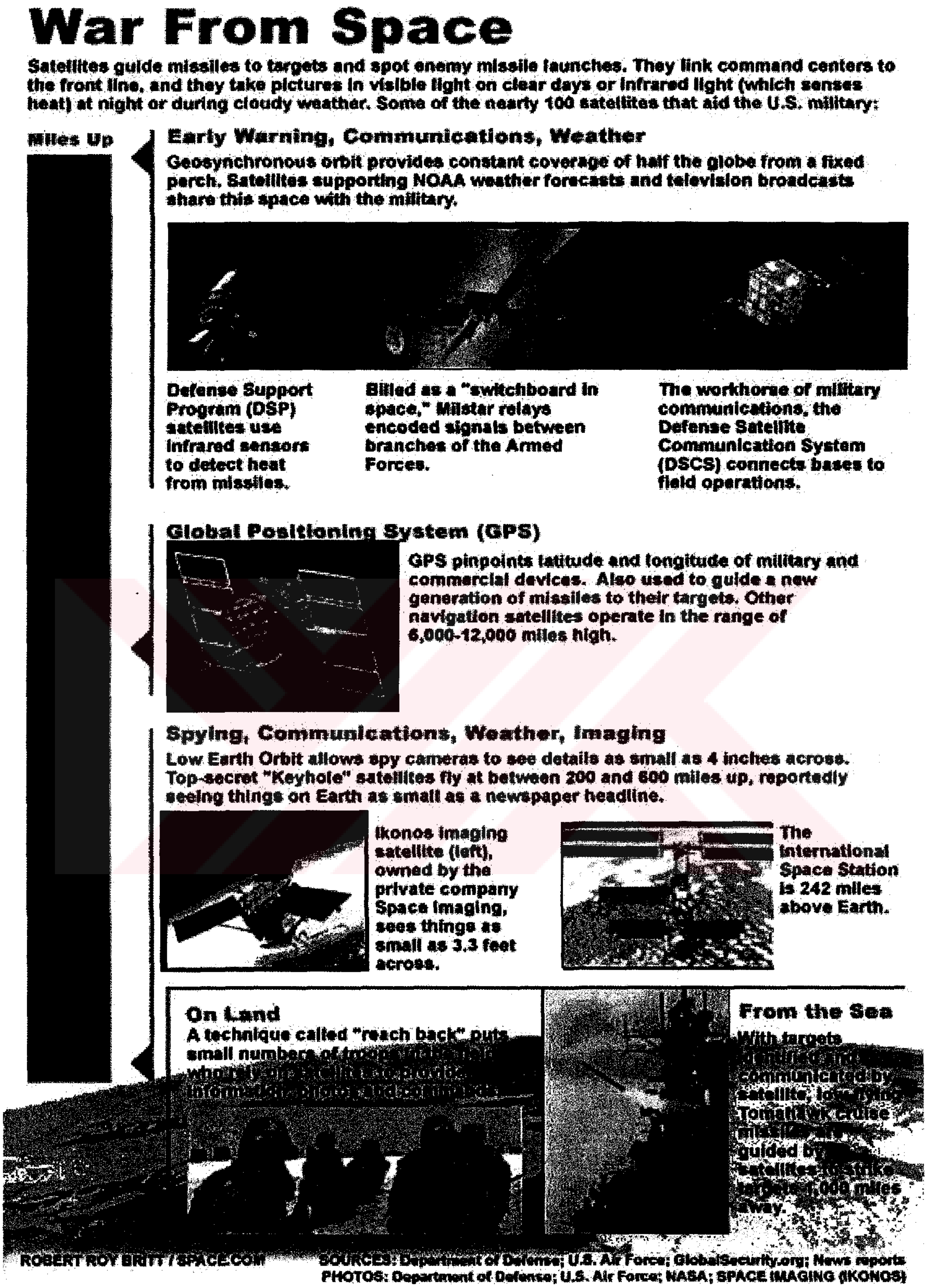


Figure 5.2: There Are Illustrated the US Satellites That How Many Miles Are above the Earth.

The military claims it can spot any missile launch over 90 percent of the Earth's surface. But there is a trade-off for the wide view offered from 22,300 miles up in space: an inability to see anything with high resolution. A host of other satellites, therefore, operate much closer to the planet. Lower, around 10,900 miles above the surface, are 24 satellites that comprise the Global Positioning System, or GPS. Each satellite circles the planet once every 12 hours, and they combine to give near-total coverage of the globe. GPS is absolutely critical to U.S. military operations. The GPS satellites emit constant signals, which when picked up by receivers in the air or on the ground can calculate time to within a billionth of a second, velocity within a fraction of a mile per hour and location to within a few feet, according to the Air Force.[271]

Five ground stations and four ground antennas, located around the world, coordinate the satellites and their signals. GPS has allowed for dramatic improvement over previous attempts, such as in Desert Storm, to target missiles and bombs remotely. One new bomb, called Joint Direct Attack Munition, or JDAM, has a GPS receiver installed inside it and can be programmed to hit a target based on longitude and latitude. Since the JDAM finds the target, the crew doesn't have to, allowing them to fly at higher and safer altitudes. The Department of Defense has not discussed whether JDAM has been used in Afghanistan.

A host of other satellites, providing intelligence imagery and weather data, are put into what's called Low Earth Orbit, typically between 100 and 300 miles up but as low as 80 miles and as high as 1,200 miles. Space shuttles and the International Space Station operate in Low Earth Orbit.

Several military spy satellites work in the 600-1,200 mile range. They're acronyms reflect the type of data they collect: electronic intelligence (ELINT); signal intelligence (SIGINT); and radar intelligence (RADINT).

Spy satellites orbit at some 25 times the speed of sound, typically passing over a given location twice a day. This routine is useful for spotting the movements of entire encampments, single vehicles and groups of people. Spy satellites are to see features as small as 4 or 5 inches across. They can identify people, but not faces. They can spot a

[271] Britt, Robert Roy, "Satellites Play Crucial Roles in Air and Ground Battles", Space News, U.S.A., 09 October 2001, Available on site: http://www.space.com/news/

license plate on a car, but they can't read it. Though highly classified, one type of spy satellite known as keyhole-class, is thought to see objects as small as a newspaper headline. Three of these satellites range over Earth's polar region. They resemble giant digital cameras, somewhat like the Hubble Space Telescope.[272] U.S. spy satellites played critical role during previous war and they are expected to today by military planners. U.S. intelligence agencies focused all available spy satellite resources on suspected targets in Afghanistan and Iraq.[273] Spy satellites include these general types:[274]

- Radar imaging satellites that uses microwave signals to peer through cloud cover and scan Earth surface.
- Optical satellites that use a large mirror to gather light for photography.
- Combo radar and optical satellites that see wider areas of Earth's surface with more detail.
- Signals intercepts and detection satellites that tune in on radio, telephone and data transmissions.
- Ocean observation satellites used to locate and determine the intent of ships.

Military analysts say keyhole-class use an elliptical orbit to take them as close as 200 miles and as far as 600 miles from the planet's surface. This odd orbit allows the satellites, as a group, to photograph nearly the entire planet several times a day.

No one knows exactly how many satellites the U.S. Military has in orbit. It is estimated the total number of orbiting spacecraft that support military activity directly or indirectly approaches 100. Included are roughly two dozen devoted to intelligence, two dozen that provide navigation, and another two dozen that handle communications. However, that along with other intelligence information, satellites enable special operations units to locate terrorists, plan forays into enemy territory, and then go in knowing what weapons have been disabled.

---

[272] Britt, Robert Roy, Ibid.
[273] Krane, J., "Sign on San Diego Military-In Terror War, High-Tech Military Tools could be Used to Hunt Low-Tech Foes", San Diego, U.S.A., 2001, Available on site: http://www.uniontrib.com/news/military/20010923-1313-attacks-high.html
[274] Anthony, R., "Space Today Online-The Satellite Wars- Afghanistan and Yugoslavia", U.S.A., 2001, Available on site: http://www.spacetoday.org/Satellites/YugoWarSats.html

Space-based battle support was tested in the Gulf War in 1991. Satellite imagery was used to find targets and assess the effects of bombing. Missile-warning sensors detected enemy Scud launches, information that was relayed -often by satellite- to commanders on the ground who controlled anti-missile batteries.[275] Space forces contribute to the overall effectiveness of military forces if deterrence fails by acting as a force multiplier that enhances combat power. The capability to control space will contribute to achieving information superiority and battlespace dominance.[276]

5.1. BATTLESPACE DOMINANCE

The use of space parallels the use of air. The first use of the air was to provide reconnaissance information for ground-based weapons. The second purpose was to destroy enemy reconnaissance aircraft. The third was the defense of reconnaissance aircraft, by arming them, increasing their agility, and creating a class of aircraft dedicated to fighting other aircraft. The fourth and most important use was to merge the reconnaissance platform with the weapons system by placing explosives on the aircraft. From that point on, control of the air was understood to be a means to dominate the land and sea, both militarily and politically. This same process is now unfolding in space.[277] Space is a medium like the land, sea, and air where military activities are conducted. Space forces are global in nature, support a forward presence, are necessary to maintain military readiness, and enable implementation of enhanced operational concepts. Space power is as important to the nation as land, sea, and air power. Space forces support military operations by providing information lines of communication enabling information superiority, contributing to deterrence, increasing force effectiveness, and ensuring the freedom of space.[278]

Space Command is a dominate force behind the U.S. military satellite systems. This is a look at each system. It operates an amazing array of satellites, both in technological capabilities and sheer numbers. This network of man-made constellations link commanders from the staff level in Washington to the squad leader on the ground in a far-flung country. They can communicate and exchange information and in many cases see what the other is

---

[275] Britt, Robert Roy, Ibid.
[276] Cohen, William S., Ibid.
[277] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 331.
[278] Cohen, William S., Ibid.

seeing. This ability is not by chance, but by careful design with satellites providing the eyes, ears and links for it all to come together.[279] Given that information dominance will be the key enabler in 21st century operations, the information provided by space-based assets is critical to the Army's success.[280]

Figure 5.3: Space as a Dominate Force.

From the first days of the space age through the Cold War bilateral strategic stability, crisis management, and arms control all rested on the capabilities created by space systems. While probably less critical, and certainly less well known, space forces also played a significant role in American theater capabilities as early as the Vietnam War. By the late 1960s, U.S. air commanders relied on satellite-based meteorological systems to plan their air operations and on geosynchronous communications satellites for connection with the national leadership.[281]

---

[279] McKaughan, Jeffrey D., "Eyes in the Sky", Volume: 2, Issue: 1, U.S.A., 02 February 2003. Available on site: http://www.mat-kmi.com/archive_article.cfm?DocID=90

[280] Army Science Board, "Final Report - Priotirizing Army Space Needs", Department of the Army, Washigton, D.C., July 1999, p. 20.

[281] Peebles, Curtis, "High Frontier: The U.S. Air Force and the Military Space Program", Government Printing Office (DoD), Washington, DC, U.S.A., 1997, p. 44-57.

On the whole, though, strategic and national users were the primary customers of space forces through this period. This changed with the end of the Cold War and, more visibly, with the Gulf War in 1991. Suddenly, the contributions of space forces to theater operations became manifest to all, from the tank columns maneuvering across the desert, to the fighter pilots' reliance on space forces for mission planning and weather data, to Special Forces' use of space-based communications. But as this potential and this reliance became clear, so, too, did the distance remaining to be traveled before space capabilities could be considered truly integrated with U.S. theater forces.[282]

As effective as space-based support to *Desert Storm* operations proved, this support was largely a result of heroic ad hoc adjustments, provided on the run as new requirements and opportunities appeared.[283] Overall, this was a classic and near-perfect trigger event, displaying for all the utility of these systems and the work that remained to take full advantage of what they could do. That recognition established the work program that has guided space forces over the past decade.

The process has proven to be much more difficult and time-consuming than first estimated. While progress has been steady, and improvements have been evident from operation to operation since 1991, every after action report throughout this period has identified issues with the integration of space and theater forces that still demand improvement. Even as results are still forthcoming from the current operations, early reports indicate that this will be the case once again. This pattern represents a combination of causes: the inherent challenges of the task, the continuing expansion in expectations of theater users, and the initial underestimation of the challenge being the most dominant.

From an operational perspective, the reorientation of space forces has demanded a series of collateral improvements in those forces. These include fusion, timeliness, coverage, integration, dissemination, command and control, and survivability.[284]

---

[282] Randolph, Stephen P., "Transforming America's Military - Controlling Space", Ed. Hans Binnedijk, , National Defense University Press, U.S.A., June 2002.
[283] Spires, David, "Beyond Horizons: A Half Century of Air Force Space Leadership", Government Printing Office (DoD), Washington, DC, U.S.A., 1998, p. 243-269.
[284] Randolph, Stephen P., Ibid.

5.2. SPACE SURVEILLANCE, INTELLIGENCE, AND TARGET ACQUISITION

Throughout most of the later half of the 21st century and into the 22nd century surveillance satellites have orbited the earth providing strategic intelligence and warning information. Surveillance satellites have complicated the balance of warfare by enabling countries to monitor each other's activities from outer space in real-time and with impressive clarity.[285] Space surveillance provides information on what is orbiting Earth. This information includes each object's orbital parameters, size and shape, and other data useful for determining its purpose. Space surveillance provides essential information to the operators of space systems, helps to determine the capabilities of potential adversaries, predicts the orbits of objects in space to include warning of potential collisions, and predicts space object reentry impact points. In addition, messages are sent to tactical commanders to warn them when they can be observed by a potential adversary's space systems.[286]

An additional broad category of surveillance satellite includes electronic intelligence (ELINT) satellites. ELINT satellites record the transmission of all electronic signals including radar, radio, and enemy telemetry signals.[287] Space based ELINT sensors on satellites have the advantage of unrestricted access over battlefields and areas that are otherwise difficult to gain access to for political or military reasons. Satellites can be used to verify compliance with treaties, determine the deployment and status of land, sea and air forces, and monitor activities in specific areas. If hostilities are initiated, space systems can provide attack warning, targeting intelligence, technical intelligence on enemy capabilities, and bomb damage assessment after strikes on the enemy.[288]

All component commanders need continuous communications, ISR and weather. These capabilities shape the battlespace. Blue forces can capitalize on precision target location data, employ precision weapons, and conduct BDA, thereby maximizing munition effectiveness. Precision navigation is necessary to both targeting and avoidance of fratricide. A critically important aspect is the stated need for **continuous** ISR, **continuous**

---

[285] Feeney, Christopher, "A Star Wars Non-Fictional Technical Commentary", University of Southern California Personal Web Page, U.S.A., Available on site: http://www-scf.usc.edu/-recker/swreal.htm
[286] The U.S. Army Web Page, "Reconnaissance, Surveillance and Target Acquisition", Fort Monroc, Virginia, U.S.A., 2002, http://www-tradoc.army.mil/dcscd/spaceweb/chap07d.htm
[287] Feeney, Christopher, Ibid.
[288] The U.S. Army Web Page, Ibid.

communications, **continuous** WTEM, precision navigation and precision targeting, which implies **continuous** surveillance on a mobile battlefield.[289] When information derived from space based reconnaissance, surveillance and target acquisition (RSTA) sensors is merged with information from other ground, sea and airborne systems, a more complete Intelligence Preparation of the Battlefield (IPB) is attained.

The United States has national satellite systems which are capable of performing worldwide reconnaissance and surveillance. Many of the systems have been designed to support strategic requirements. They are, however, capable of providing useful information to tactical commanders if the information can be provided in a timely manner.[290] The distinction between tactical and strategic intelligence is at the root of the problem. Satellite reconnaissance was developed for strategic purposes; to aid in a nuclear war. The most important function of SIGINT and ELINT satellites was monitoring telemetry from missile tests and emissions from radars and other electronic systems associated with the operation of nuclear warfare systems.[291]

The Electronic Processing and Dissemination System (EPDS) receives and processes electronic intelligence (ELINT) and other information to generate integrated products. The EPDS consists of a single 30 foot van that incorporates communications, processing, and analysis functions.[292] The improvements in ISR that will evolve over the next decade will be substantial with respect to coverage, revisit times, integrated asset management, and product dissemination to the field. Still, these will be evolved capabilities, not the revolutionary capabilities that will be available beyond the 2010 timeframe. None of the advanced new ISR systems that are currently in the planning stage (e.g., Discoverer II, IOSA) will be operational by that time. However, many of the new processing and dissemination initiatives will be in place to provide better support to military units.[293]

The U.S. Space Surveillance Network (SSN) is a collection of radar and optical sensors used to detect, track and identify objects in space. Although referred to as a network, the

---

[289] Army Science Board, "Final Report - Prioritizing Army Space Needs", Department of the Army, Washington, D.C., U.S.A., July 1999, p. 20-21.
[290] The U.S. Army Web Page, "Reconnaissance, Surveillance and Target Acquisition", Fort Monroc, Virginia, U.S.A., 2002, http://www-tradoc.army.mil/dcscd/spaceweb/chap07d.htm.
[291] Friedman, George & Meredith, Ibid, p. 325.
[292] The U.S. Army Web Page, Ibid.
[293] Army Science Board, Ibid, p. 32.

Space Surveillance Network was not originally planned as such. As various sensors became available, their particular capabilities were used to contribute to the space surveillance mission. The Space Surveillance Network cannot continuously track all satellites; therefore the Space Surveillance Center prepares a prioritized list of satellites to track. Generally, satellites with high interest missions or unstable orbits (objects about to deorbit) will have higher priority data collection requirements than other satellites.[294]

5.3. SPACE SURVEILLANCE NETWORK SENSORS

The U.S. Space Surveillance Network is organized into three categories of sensors:

- Dedicated Government owned sensors with a primary mission of space surveillance.
- Collateral Government owned sensors with a primary mission other than space surveillance.
- Contributing Owned and operated by other agencies but which provide surveillance data when not performing their primary mission.

5.3.1. Dedicated Sensors: Optical

Optical sensors are basically telescopes, gathering light reflected off an object in space. Like all telescopes, they have limitations; for example, they cannot track objects in Earth's shadow unless they are emitting light. Cloud cover, fog, atmospheric pollution, light glow from cities or a full moon degrade or prevent observations. The size of the object to be tracked and its distance from Earth are also limiting factors.[295]

Baker Nunn Camera: The BakerNunn camera is a large telescope with a camera attached. Imagery is recorded on film. Two to four hours are required for on site film processing and image analysis after which data is transmitted to the Space Surveillance Center. The system can image satellites ranging in altitude from 3,000 miles to 22,300 miles (geostationary) and somewhat beyond. The position a space object in the photo is determined by analyzing the star background. BakerNunn cameras are in operation in San

---

[294] The U.S. Army Web Page, Ibid.
[295] The U.S. Army Web Page, Ibid.

Vito, Italy and in Saint Margarets, Newfoundland (operated by Canada). Many other BakerNunn cameras have been replaced by GEODSS.

Ground Based Electro-Optical Deep Space Surveillance System (GEODSS): GEODSS is an electronically enhanced telescope that uses low light level television cameras and a computer instead of film. Sensor data are stored on magnetic media for analysis locally or the data are transmitted in near real time to the Space Surveillance Center for analysis, if required. The GEODSS sensors are more sensitive than the BakerNunn cameras, therefore they can detect, image and track smaller and dimmer objects. The system can image objects in space with an altitude of more than 22,000 miles. The GEODSS sensors provide vary accurate data which make them excellent for providing data to maintain the space object catalog. The sensors only operate at night. Weather conditions and a full moon restrict viewing opportunities. Each GEODSS site has three telescopes, each facing a different section of the sky. There are four GEODSS sites:

- Cicero, New Mexico
- Choe Jong San (near Taegu), Korea
- Maui, Hawaii
- Diego Garcia, Indian Ocean

A fifth GEODSS site in Portugal has been proposed. It would replace the two remaining BakerNunn sites.

Maui Optical Tracking and Identification Facility (MOTIF): MOTIF is an optical sensor similar to the GEODSS with an added Long Wave Infrared (LWIR) detection system. It performs near Earth and deep space surveillance and Space Object Identification. The range is similar to that of the GEODSS. The sensor is only operated at night. Clouds, high winds, high humidity and a full moon restrict viewing opportunities. MOTIF is collocated with the GEODSS site in Maui, Hawaii.[296]

[296] The U.S. Army Web Page, Ibid.

5.3.2. Dedicated Sensors: Radar

Navy Space Surveillance (NAVSPASUR) System: The NAVSPASUR system consists of three transmitters and six receivers located along the 33d parallel in the U.S. The transmitters emit a vertical continuous beam which forms an electronic fence. When an object passes through one of the transmitter's waves in space and two or more geographically separated receivers detect the reflected energy, the object's location can be determined by triangulation derived by interferometric techniques. This is essentially the same process that bistatic radars use. Once the object's location and general direction of movement are determined, NAVSPASUR operators notify the Space Surveillance Center, which can then notify a tracking radar to make more precise determinations of the object's characteristics. The range of this fence is 5,000 miles in length and can detect objects up to 15,000 miles out in space. The space object in orbit must have an inclination of greater than 33 degrees in order to pass through the electronic fence. It does not track, it only detects. More than one million detections are made every month.

Transmitters: Transmitters are located at Gila River, Arizona; Lake Kickapoo, Texas; and Jordan Lake, Alabama. Receivers are located at Fort Stewart, Georgia; Hawkinsville, Georgia; Silver Lake, Mississippi; Red River, Arkansas; Elephant Butte, New Mexico; and San Diego, California. NAVSPASUR headquarters is at Dahlgren, Virginia. The headquarters is also the Alternate Space Defense Operations Center and the Alternate Space Surveillance Center.

AN/FPS-85, Phased Array Radar: The AN/FPS85 Phased Array Radar is located at Eglin AFB, Florida. The radar is housed in a wedge shaped building that is 318 feet long. The transmitter side has 5,928 elements and is 126 feet tall. The receiver side has 19,500 elements and is 192 feet tall. The radar was originally built to detect Sea Launched Ballistic Missiles (SLBM). It became a dedicated space sensor in 1988, when the PAVE PAWS radar at Warner Robins AFB, Georgia became operational. The radar has the capability to track near Earth and deep space objects simultaneously. Approximately 95% of objects in low Earth orbit pass through this radar's coverage.

Saipan Space Surveillance Station: The Saipan Space Surveillance Station, on the Pacific island of Saipan, is well suited to monitor launches from China and the central Asian land mass. It transmits a single radar beam toward its target in space. From the reflected energy the systems is able to calculate the size, orientation, altitude, speed and direction of movement. The system is not suitable for searching the sky for satellites. The radar must first be queued so that it is pointed in the correct position. The radar can track an object in space with high precision, but it can only track one object at a time.

Deep Space Tracking System: The Deep Space Tracking System uses sensitive, highly accurate, 60foot dish antennas to detect and track Sband radio signals transmitted by radio beacons on most satellites. There are DSTS receivers located at Griffiss Air Force Base, New York; RAF Feltwell, Great Britain; and Misawa Air Base, Japan. These sites are expected to become operational in 1993 and 1994. The signals transmitted by most satellites are not significantly affected by weather and can operate during the day and at night. The system is capable of tracking many satellites in a short amount of time. This will allow the other optical and radar sensors to detect and track other unidentified objects in space. Since they rely on transmissions from the satellites, they cannot detect or track space debris or totally inactive satellites.[297]

5.3.3. Collateral Sensors

Ballistic Missile Early Warning System (BMEWS): The primary mission of BMEWS is to provide early warning and attack assessment of missile attacks launched against CONUS and southern Canada from the Asian land mass that pass over or near the North Pole. The system also serves to provide SLBM and ICBM warning/attack assessment for the United Kingdom and Europe. The radars are capable of tracking multiple space objects, however the capability is limited to relatively large objects in low Earth orbit.[298]

BMEWS sites are located at:

- Thule, Greenland (Site 1). A phased array radar, installed in 1987, provides 240 degree coverage against large objects such as ICBMs or SLBMs.
- Clear AFB, Alaska (Site 2). This site is equipped with 1961 vintage radars. They have proven to be very reliable, with a historical 99% availability rate.

---

[297] The U.S. Army Web Page, Ibid.
[298] The U.S. Army Web Page, Ibid.

- Royal Air Force Station, Flyingdales, Great Britain (Site 3). The site was initially built in 1964. It has three phased array radars which provide 360 degree coverage for warning/attack assessment of ICBM and SLBM attacks.

PAVE PAWS: PAVE PAWS is a system of radar complexes with a primary mission to provide warning/attack assessment of SLBM attack against CONUS and southern Canada. Each site operates a dual-faced phased array radar. The two northern sites (Cape Cod and Beale) can also provide warning/attack assessment of an ICBM attack from the Asian land mass. Each site can also provide satellite tracking data for space surveillance. The sensitivity of the radar limits detection and tracking to low Earth orbits of relatively large objects. Sites are located at:

- Cape Cod AFS, Massachusetts
- Beale AFB, California
- Robins AFB, Georgia
- Eldorado AFS, Texas

Due to a reduced threat, the PAVE PAWS system does not operate at all times.

AN/FSP-108, CPBRA DANE: COBRA DANE is the project name for a singlefaced phased array radar located at Shemya AFB, Alaska. Its primary mission is intelligence, with secondary emphasis being space surveillance. It can also perform warning/attack assessment for missile attacks. The radar operates in the Lband which provides better accuracy and sensitivity than Pave Paws. Due to its position, COBRA DANE provides important information on new foreign launches.

AN/FSP-79, Pirinclik, Turkey: The AN/FSP79 radar, located at Pirinclik, Turkey, has the same general mission as COBRA DANE. This system has two detection radars and a tracking radar. Two objects can be tracked simultaneously. It is the only 24hour a day deep space sensor in the eastern hemisphere.

AN/FPQ-16, Perimeter Acquisition Radar Attack Characterization System (PARCS): PARCS is a leftover from the Safeguard AntiBallistic Missile system at Cavalier AFB, North Dakota. Following the deactivation of Safeguard, the Army transferred PARCS to the Air Force. The Air Force assigned the radar a primary mission of warning/attack assessment of SLBM and ICBM attack against CONUS and southern Canada. Its singlefaced phased array radar is pointed northward over the Hudson Bay. It can provide valuable surveillance, tracking, reporting, and Space Object Identification data for the Space Surveillance Network. In June 1992, the Air Force deactivated the site and placed it in extended storage.[299]

5.3.4. Contributing Sensors

Millstone Hill Radar and Haystack Long Range Imaging Radar: These two radars, commonly referred to as the Millstone/Haystack Complex, are located in Lexington, Massachusetts. They are owned and operated by Lincoln Laboratories of the Massachusetts Institute of Technology (MIT). Millstone is a deep space radar that contributes 80 hours per week to tracking for the Space Surveillance Center. Haystack is a deep space imaging radar that provides wideband Space Object Identification data to the Space Surveillance Center about once every six weeks. In addition to the scheduled use of Haystack, USSPACECOM has the option to call on it two additional times in a year.

Antigua: A tracking radar is installed on Antigua, British West Indies off the coast of Venezuela. This radar is part of the Eastern Test Range which supports launches from the Eastern Space and Missile Center (Cape Kennedy and Cape Canaveral, Florida). The radar is very accurate, but has a limited search capability.

Ascension Island: A tracking radar, similar to the one on Antigua, is installed on this island located off the coast of Africa near the Equator. It also is part of the Eastern Test Range.

ALTAIR and ALCOR: The Advanced Research Project Agency (ARPA) LongRange Tracking and Identification Radar (ALTAIR) and the ARPA Lincoln CBand Observable Radar (ALCOR) are on the island of Kwajalein in the western Pacific. Operated by the Army, they are primarily used for ABM testing in support of the Western Space and Missile Center (WSMC). They support space surveillance missions when possible. ALCOR is a near Earth tracking radar, and is the only other radar besides Haystack that can provide wideband Space Object Identification. ALTAIR is a near earth and deep space

---

[299] The U.S. Army Web Page, Ibid.

tracking radar. Because of its nearness to the equator, ALTAIR alone can track one-third of the objects in the geosynchronous belt.

Kaena Point: Kaena Point is a tracking radar located on Oahu, Hawaii. It is part of the Western Test Range and reports to the Western Space and Missile Center. When not being used for test support, it supports the Space Surveillance Center with very accurate satellite tracking data.

Advance Research Program Agency (ARPA) Maui Optical Station (AMOS): AMOS is a similar to the GEODSS type optical sensor except that it has a deformable mirror to compensate for atmospheric disturbance, thereby creating clearer, sharper imagery. Operation is limited to nighttime only. Clouds and bright lights further restrict viewing opportunities. It is collocated with the GEODSS and MOTIF sensors on Maui.[300]

5.4. THE UNITED STATES' SIGINT, COMINT AND ELINT SATELLITES

Signals intelligence satellites are designed to detect transmissions from broadcast communications systems such as radios, as well as radars and other electronic systems. The interception of such transmissions can provide information on the type and location of even low power transmitters, such as hand-held radios. However, these satellites are not capable of intercepting communications carried over land lines, such as under-sea fiber optic cables (nor can they detect non-electronic communications, such as the spoken word).

Signals intelligence (SIGINT) consists of several categories. Communications intelligence (COMINT) is directed at the analysis of the source and content of message traffic. While most military communications are protected by encryption techniques, computer processing can be used to decrypt some traffic, and additional intelligence can be derived from analysis of patterns of transmissions over time. Electronic intelligence (ELINT) is devoted analysis of non-communications electronic transmissions. This would include telemetry from missile tests (TELINT), or radar transmitters (RADINT).[301]

---

[300] The U.S. Army Web Page, Ibid.
[301] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 302.

The United States had begun thinking about space-based reconnaissance and electronic intelligence (ELINT) soon after World War II.[302] In 1947, the Rand Corporation published a study on satellites, which stated that "by installing television equipment combined with one or more Schmidt-type telescopes in a satellite, an observation and reconnaissance tool without parallel could be established."[303]

Three countries have space-based SIGINT systems, though only the US possesses geostationary SIGINT satellites able to intercept terrestrial VHF and microwave communications and missile telemetry.[304] The United States operates four constellations of signals intelligence satellites in geostationary, elliptical and low Earth orbits.[305] The geostationary SIGINT constellation consists of three or four satellites. The first generation of GEO-ELINT satellites, known as Rhyolite, was launched in the early 1970s, and had a receiving antenna with a diameter of over ten meters. The next generation of these satellites, known as Chalet or Vortex, was first orbited in the late 1970's, and had an antenna with diameter of several tens of meters. The most recent models, known as Magnum, were first launched in the mid-1980s, and have a very large deployable antenna with a diameter of approximately 100 meters. Satellites with an even larger antenna are currently under development. Increasing the diameter of the antennae of these satellites makes it possible to detect lower power transmissions, as well as to determine the position of a transmitter with increased precision.[306] The current US geostationary satellites, called Advanced Orion, which are controlled from Pine Gap in central Australia and can intercept signals emanating from designated points on or near the earth's surface from about 40°E to about 180°E, are much more advanced than their predecessors. The two satellites launched so far (14 May 1995 and 8 May 1998)[307] not only have a much larger primary signals

[302] Friedman, George & Meredith, Ibid, p. 302.
[303] Richelson, Jeffrey, T., "America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program", Harper & Row Publications, New York, N.Y., U.S.A., 1990, p. 3-4.
[304] Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm
[305] Pike, John, "SIGINT Overview", Global Security Web Page, Washington, U.S.A., 8 October 2002, www.globalsecurity.org/space/systems/SIGINT
[306] Pike, John, "SIGINT Overview", Global Security Web Page, Washington, U.S.A., 8 October 2002, www.globalsecurity.org/space/systems/SIGINT
[307] Richelson, Jeffrey, "Despite Management/Budget Woes, NRO Launches Continue", Defense Week Magazine, U.S.A., 12 August 1996, p.16; Covault, Craig, "Eavesdropping Satellite Parked Over Crisis Zone", Aviation Week & Space Technology Magazine, U.S.A., 18 May 1998, p.30; and Covault, Craig, and

interception antenna array (the diameter of the primary parabloid reflector antenna on the previous Magnum/Orion satellites was about 100 meters), but also carry a log-periodic antenna forest and a variety of other secondary antennas for more specialized interception missions (including interception of mobile telephone conversations from fast-moving passenger aircraft).[308] The Pine Gap facility, which had 876 staff (428 US and 448 Australian) and 26 satellite antennas (14 in radomes) as at March 2002, is the largest SIGINT satellite ground control and data processing station in the world.

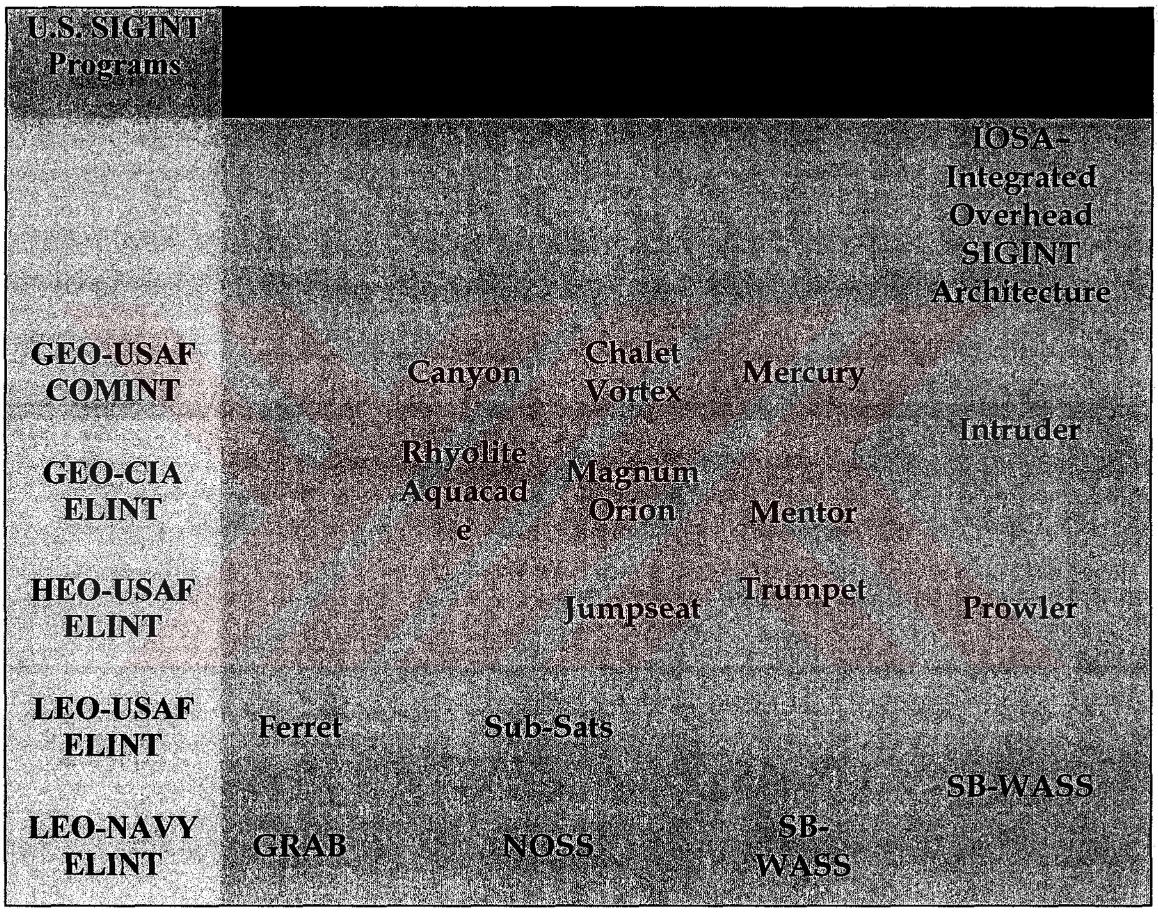


Figure 5.4: The United States' SIGINT, ELINT and COMINT Programs.

The notional geostationary SIGINT constellation consists of three or four satellites. The National Reconnaissance Office and National Security Agency launched a third Magnum signals intelligence satellite on the Space Shuttle on 14 November 1990. This spacecraft

Joseph C. Anselmo, "Titan Explosion Destroys Secret 'Mercury' SIGINT [Satellite]", Aviation Week & Space Technology Magazine, U.S.A., 17 August 1998, p.29.

308 Ball, Desmond, "The US-Australian Alliance: The Strategic Essence", Australian Journal of International Affairs, Vol. 55, No. 2, Australia, July 2001, p.239-240.

joined the Chalet (also known as Vortex) launched on 10 May 1989, and the second Magnum launched on 23 November 1989. In addition to these 1989 launches the constellation also includes the first Magnum, launched on the Shuttle in 1985. The older Chalet launched in 1981 has probably left service, having long surpassed its five year design life.[309]

In addition to these geostationary SIGINT satellites, two Jumpseat SIGINT satellites, launched in 1985 and 1987, remained in service throughout the end of the 1980s.[310] These satellites, in highly elliptical Molniya-type orbits, provide specialized coverage of the far Northern regions of the Soviet Union.

Signals intelligence provided one of the first warnings that the Iraqi invasion of Kuwait was likely, when a Soviet-built TALL KING radar resumed operation 29 July 1990. The 350 mile range radar had been out of service for a number of months prior to the invasion.[311] By early October US electronic intelligence had some success in monitoring Iraqi military communications, but the Iraqi army was also using underground cables to communicate, making it difficult to determine Iraqi military intentions.[312]

5.4.1. World's First ELINT Satellite (GRAB)

The Galactic Radiation Background Experiment (GRAB) was a US Navy electronic intelligence (ELINT) satellite system that became operational in July 1960 and was operated until August 1962. GRAB was officially declassified in June 1998. GRAB obtained information on Soviet air defense radars that could not be observed by Air Force and Navy aircraft flying ELINT missions along accessible borders in Europe and the western Pacific. From 500 miles above earth, safe from surface-to-air missiles, the GRAB satellite's simple, circular orbit passed it through the energy beams from Soviet radar whose pulses traveled straight and far beyond the horizon into space.[313] The system is

---

[309] Pike, John, "SIGINT Overview", Global Security Web Page, Washington, U.S.A., 8 October 2002, www.globalsecurity.org/space/systems/SIGINT

[310] Richelson, J., "The U.S. Intelligence Community", Ballinger, Cambridge, MA, U.S.A., 1985, p. 122.

[311] Aviation Week Editor, "Invasion Tip", Aviation Week & Space Technology, 6 August 1990, p. 15.

[312] Gertz, Bill, "US Breathes Easier as it Spots Iraq's Jamming Gear", The Washington Times, Washington, D.C., U.S.A., 9 October 1990, p. A8.

[313] Pike, John, "Project Tattletale: Galactic Radiation Background Experiment (GRAB)", Washington, D.C., U.S.A., October 2002, Available on site: http://www.globalsecurity.org/Space/GRAB%20Galactic%20Radiation%20Experiment.htm

described as being a transponder that picked up the radar signals from two Soviet radar systems, Gage and Token, and rebroadcast these directly to the ground.[314]

In the evolving atomic era, U.S. quest for technical intelligence about Soviet military capabilities inspired NRL scientists and technologists to seek the high ground of space. From 500 miles above earth, safe from surface-to-air missiles, the GRAB satellite's simple, circular orbit passed it through the energy beams from Soviet radar whose pulses traveled straight and far beyond the horizon into space.

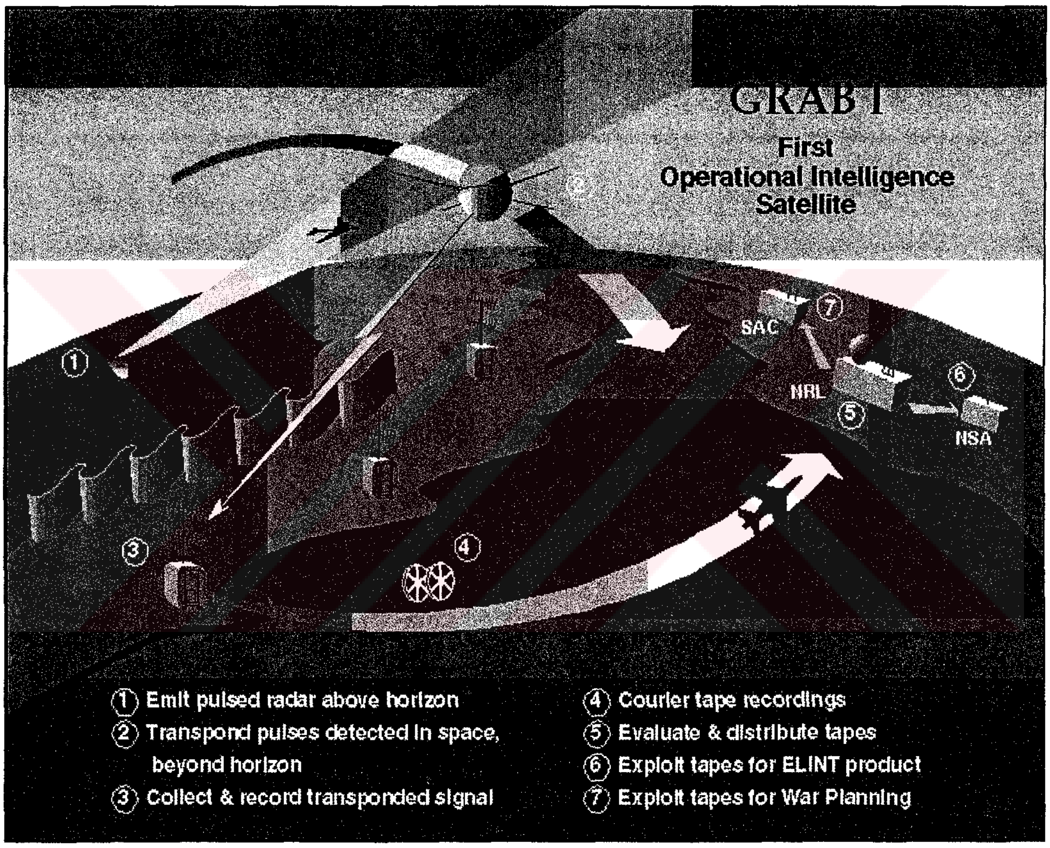


Figure 5.5: GRAB I First Operational Intelligence Satellite.

GRAB's task was to receive each pulse of a radar signal in a certain bandwidth, as sensed by its tiny antennas, and transpond a corresponding signal to collection huts at ground sites within GRAB's field of view.[315]

---

[314] Grahn, Sven, "An Analysis of the Design of GRAB, the First ELINT Satellite", Available on site: http://www.svengrahn.pp.se/radioind/GRABELINT/GRABELINT.html

The ELINT satellite system was proposed by the Naval Research Laboratory in the spring of 1958. In parallel with exploratory development by the NRL, the Office of Naval Intelligence obtained endorsements of Project Tattletale from elements of the executive and legislative branches. After NRL completed development of the GRAB satellite and a network of overseas ground collection sites, a first launch was approved by Eisenhower on 5 May 1960, just four days after a CIA U-2 aircraft was lost on a reconnaissance mission over Soviet territory. The GRAB satellite got a free ride into space on 22 June 1960 with the Navy's third Transit navigation satellite. GRAB carried two electronic payloads, the classified ELINT package and instrumentation to measure solar radiation (SolRad). The SolRad experiment was publicly disclosed in DoD press releases on this and subsequent launches. Four more launches were attempted, and one was successful on 29 June 1961.

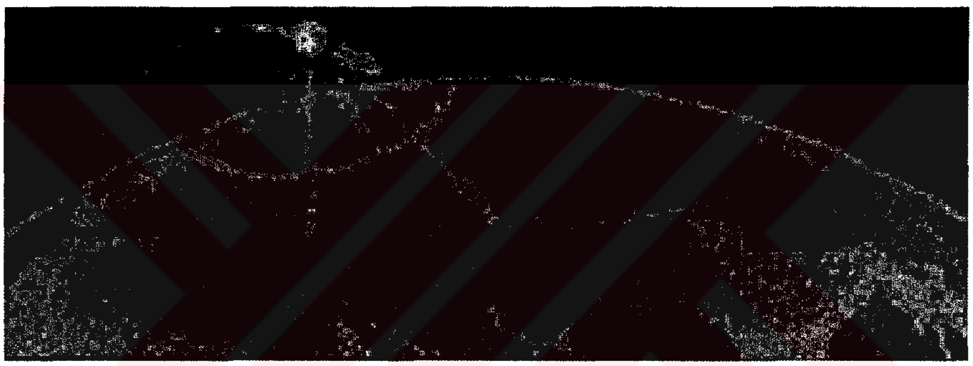


Figure 5.6: The ELINT Information to Be Derived By Processing the Satellite Downlink.

The Director of Naval Intelligence exercised overall control. Data recorded on magnetic tape were couriered back to the NRL, then evaluated, duplicated, and forwarded to the NSA at Army Fort Meade, Maryland, and the Strategic Air Command at Offut Air Force Base Omaha, Nebraska, for analysis and processing. SAC's processing was aimed at defining the characteristics and location of air defense equipment to support building the SIOP (single integrated operations plan), a responsibility of the Joint Strategic Targeting Staff at Offut AFB. In searching the tapes for new and unusual signals, NSA found that the

---

315 Naval Research Laboratory, "G R A B, Galactic Radiation and Background, World's First Reconnaissance Satellites", Naval Research Laboratory, Washington, D.C., U.S.A., 2002, Available on site: http://www.nrl.navy.mil/

Soviets were already operating radar that supported a capability to destroy ballistic missiles.[316]

5.4.2. The Fifth Generations (2000+) US ELINT Satellites

PROWLER: The PROWLER geosynchronous SIGINT geolocation platform was initially intended to help locate strategic relocatable targets. The design of this spacecraft is said to include low-observable features.

It was an antecedent of the Precision SIGINT Targeting System (PSTS) Advanced Concept Technology Demonstration [ACTD]. Apart from the Army RC-12 Guardrail's Communications High-Accuracy Location System (CHALS) and Quicklook ES systems use of time-difference-of-arrival direction-finding, few existing SIGINT systems provide targetable geolocation accuracies against communications or radar emitters. PSTS is a Joint Service and Defense Agency effort to develop and demonstrate a near-real-time, precision targeting, sensor-to-shooter capability using existing national [including overhead] and tactical systems. PSTS will provide tactical users with targeting that is one order of magnitude improvement over what can be accomplished by any of the single candidate systems operating alone.[317]

INTRUDER: The INTRUDER geosynchronous SIGINT spacecraft represents a consolidation of previously discrete COMINT and ELINT collection programs into a single collection platform under the Integrated Overhead SIGINT Architecture [IOSA]. When NRO presented its five-year program to Congress in the fall of 1995, the new satellites under development -- including the INTRUDER signals intelligence satellite -was estimated to cost roughly a billion dollars apiece. IOSA will improve SIGINT performance and avoid costs by consolidating systems, utilizing medium lift launch vehicles wherever possible, and using new satellite and data processing technologies. At the urging of Congress, NRO initiated the study phase for the follow-on architecture, IOSA-2. These

---

[316] Naval Research Laboratory, Ibid.
[317] Pike, John, "Signal Intelligence", Washington, D.C., U.S.A., October 2002, Available on site: http://www.globalsecurity.org/space/systems/SIGINT

systems are intended to be increasingly responsive to operational needs and the military is an integral partner and participant in NRO space missions.[318]

INTEGRATED OVERHEAD SIGINT ARCHITECTURE (IOSA): The NRO is developing the collection architectures of the future that will ensure US Information Superiority as called for in Joint Vision 2010. In the area of Signals Intelligence (SIGINT), NRO is introducing an Integrated Overhead SIGINT Architecture (IOSA) that will improve SIGINT performance and avoid costs by consolidating systems, utilizing medium lift launch vehicles wherever possible, and using new satellite and data processing technologies. At the urging of Congress, NRO has initiated the study phase for the follow-on architecture, IOSA-2. These systems are intended to be increasingly responsive to operational needs and the military is an integral partner and participant in NRO space missions. As the NRO begins this revolutionary research and development (R&D) program and new acquisition efforts for SIGINT, military partners are helping shape the next generation of satellites.

IOSA-2 studies focused on whether a a new space-based SIGINT architecture could significantly improve collection from space of the numbers and types of signals expected to be critical to military and intelligence users in 2010 and beyond. Plans for IOSA-2 called for a move away from large [5-ton or heavier] spacecraft in favor of a larger number of smaller spacecraft. While the NRO anticipated retaining at least a few large SIGINT satellites, much of the collection effort was going to be offloaded to smaller satellites. In late 2000 the NRO and NSA decided not to invest in a new generation of SIGINT satellites, and instead continue with the current spacecraft configurations. The SIGINT community will consequently continue to operate within the bounds of the current Integrated Overhead Sigint Architecture (IOSA-1). Continuation of IOSA-1 benefits Boeing, which bought the Hughes' satellite manufacturing business where most SIGINT spacecraft are built. Moving to a new IOSA-2 architecture could have allowed another company to compete in this market.[319]

---

[318] Pike, John, "Intruder", Washington, D.C., U.S.A., October 2002, available on site: http://www.globalsecurity.org /Space/INTRUDER.htm

[319] Pike, John, "Integrated Overhead SIGINT Architecture", Washington, D.C., U.S.A., November 2002, Available on site: http://www.globalsecurity.org/Space/Integrated_Overhead_SIGINT_Architecture.htm

SB-WASS: The US Navy and Air Force have had a variety of ELINT satellite programs for intercepting and recording ground- and ship-based radar transmissions and locating the positions of the transmitters. These ELINT satellites provide intelligence about the ranges and signal characteristics (such as operating frequencies, pulse repetition rates, antenna rotation speeds, etc.) of radar systems, which is used to map air defense networks and shipping movements for targeting purposes.[320] The newest national space satellite system will consolidate the missions, facilities and infrastructure of two existing satellites. This will facilitate the closure of six ground stations and consolidate operations at one site, eliminating significant facility expenses. The "two existing satellites" referred to are almost certainly (95 % confidence) low altitude broad area surveillance signals intelligence systems.[321]

The US Navy, for example, developed the Naval Ocean Surveillance System (NOSS), which involves a triplet of sub-satellites, is able to detect, identify, precisely locate (through triangulation) and track surface ships and relay this information in real-time to US and Allied naval command centers and weapons platforms. This system was evidently incorporated during the 1990s into a joint US Navy-Air Force program called the Space Based Wide Area Surveillance System (SB-WASS), which can locate both land- and ship-based radar and radio transmissions. The first of these satellites was reportedly launched on 8 September 2001.[322] Three of the US Navy's five Classic Wizard ground stations for controlling the NOSS satellites, and processing and disseminating the ELINT, have been closed (i.e., the stations at Edzell in Scotland, Adak in Alaska and Winter Harbor in Maine), leaving Guam in the Pacific and Diego Garcia in the Indian Ocean. These remaining stations are jointly maintained by US Army and Air Force SIGINT personnel as well as Navy counterparts, indicating that the new program collects ELINT from both land-based and ship-based emitters.[323]

---

[320] Cereijo, Manuel, Ibid.

[321] Marietta, Martin, "SB-WASS - Consolidated Program", US Air Force Laboratuary, Washington, D.C., U.S.A., 1995, Available on site: http://www.afbmd.laafb.af.mil/XRT/xrte/recon/index.html

[322] Guillemette, Roger, "Trio of NRO Spy Satellites to be Launched During Next Two Months", Space.com Web Page, U.S.A., 6 September 2001, Available on site: http://www.space.com/missionlaunches/nro preview 01906.html; and Bourne, Jim, "New Spy Satellite Arrives in Orbit Riding Atlas", Space.com Web Page, 11 September 2001, Available on site: http://www.space.com/missionlaunches/atlas launch 010908.html.

[323] Richelson, Jeffrey T., "The U.S Intelligence Community", 4th Edition, Westview Press, Boulder, Colorado, U.S.A., 1999, p.186-187.

Requirements for this program are apparently part of the responsibilities of the Air Force Intelligence, Surveillance and Reconnaissance Development Plan, (Space Portion), a product of SMC/XRT, the Concept Development and Technical Planning Office (XRT) of the Space and Missile Systems Center (SMC), located at Los Angeles Air Force Base, California. The requirements identified as Space Based Radar (AWACS-B) are apparently part of this program.

As of mid-2003 the Request For Proposal for the new Space-Based Radar program will not be issued until future customers of the space-based mobile ground target tracking system form a consensus on an operational concept. That concept of operations will dictate how much the system will cost and how contractors choose to bid on the effort.[324]

5.5. RUSSIAN AND CHINESE ELINT SATELLITES

The Russian Federation is the only member of the European space community known to operate ELINT satellite systems. Russia still maintains two ELINT satellite programs, but the level of activity has declined greatly since the demise of the Soviet Union. More than 200 ELINT satellites were launched from 1967 to 1991, or about nine a year, whereas it has averaged just 2.5 launches a year since 1992.[325] Additional spacecraft may have carried ELINT packages as secondary payloads. During 1993-1994, a total of 11 Russian ELINT spacecraft, representing three classes of vehicles, were launched, although one satellite failed to reach orbit due to a booster malfunction. At the beginning of 1995 the integrated Russian ELINT constellation consisted of 11 primary spacecraft.

Two of the three ELINT networks established and maintained by the USSR/CIS are believed to be global in nature, i.e., they are designed to detect land-based as well as sea based electronic signals. The principal mode of operations is for each satellite to record the type of signal received and to determine the direction of the transmitter from the satellite's position. These data are then stored and forwarded to special receiving stations or are relayed in near real-time via data relay satellites. Analysts on the ground can then combine

---

[324] Marietta, Martin, Ibid.

[325] Clark, Phillip, "The Decline of Russia's ELINT Satellite Programmes", Jane's Intelligence Review, U.S.A., November 2000, p.18-20; and Federation of American Scientists (FAS), Intelligence Resource Program, "Signals Intelligence Programs and Activities – Russia", 26 November 1997, Available on site: http://www.fas.org/irp/world/russia/program/sigint.htm.

the data from seven satellites to pinpoint the location of the receiver and to determine the type of the emitter. For mobile targets, the frequency of ELINT over-flights is crucial to maintaining an accurate knowledge of the target's position.[326]

Historically, ELINT systems have played a major role in Soviet military doctrine. With the dramatic increase of radio and radar emitters on the battlefield during the past 30 years, the value of ELINT satellites has also risen. In the former Soviet Union, the Chief Intelligence Directorate of the Soviet General Staff (GRU) was tasked with the primary responsibility for global ELINT satellite systems. Collection activities were managed by the Satellite Intelligence Directorate, while the data analysis function was performed by the Decrypting Service.[327]

At the end of 1994 the Russian global ELINT satellite capability was distributed between a second-generation, store/dump system nearing the end of a long (15 year) service record and a more advanced model which will probably remain the principal intelligence gathering system for the remainder of this decade. The former has apparently been reduced to a constellation of three or less spacecraft, known as Tselina D, placed in orbital planes 30 degrees apart at altitudes of 635-665 km, while the latter is now represented by four spacecraft, known as Tslenia 2, in orbital planes 40 degrees apart at altitudes of 850 km.[328]

- Tselina D
- Tselina 2
- EORSAT
- RORSAT

The Russian military intelligence service (GRU) runs the Tselina (virgin lands) -2 radar-monitoring system, which involves two operational satellites (in circular orbits with altitudes of about 850 km), the most recent of which, Kosmos 2369, was launched on 3

[326] Johnson, Nicholas, and David Rodvold, "Europe and Asia in Space 1993-1994", Kaman Sciences, Air Force Phillips Laboratory, U.S.A., 1996, Available on site: http://www.plk.af.mil/
[327] Andrew, C., and O. Gordievsky, "KGB, The Inside Story", Harper Collins Publisher, New York, NY, U.S.A., 1990, p. 609; Ball, D., "Soviet Signals Intelligence (SIGINT)", Canberra Papers on Strategy and Defence No. 47, Strategic and Defence Studies Centre, The Australian National University, Canberra, Australia, 1989.
[328] Johnson, Nicholas, and David Rodvold, Ibid.

February 2000.[329] The Tselina-2 satellites operate in a near real-time mode, downlinking their data via Geyser geostationary communications relay satellites, and can probably locate emitters to an accuracy of 4-5 km.[330] The Russian Navy maintains an ELINT Ocean Reconnaissance Satellite (EORSAT) program, which became operational in 1979, but which was also hit by the cutbacks in Russian military space programs in the 1990s. Indeed, for five weeks in November-December 1999, and for four weeks in November-December 2001, Russia had no operating EORSAT.[331] The most recent EORSAT launch occurred on 21 December 2001 (Kosmos 2383). The EORSATs are able to detect, identify and track surface ships, to provide targeting data of about 2km accuracy, and to relay this data in near real-time to anti-ship missile platforms (such as other ships, helicopters, etc.).[332]

China has evinced a limited interest in development of an ELINT satellite capability, and has experimented with several systems, although it still does not have an operational system. A 1,108 kg ELINT satellite was launched from the Shuang Cheng Tzu Missile Range (SCTMR) in the Gobi Desert on 30 August 1976. It decayed from orbit on 25 November 1978.[333] On 19 September 1981, three SJ-2 satellites were launched on a single booster from the SCTMR, providing a capability for determining the location of radio and electronic emitters as well as for recording the emissions.[334] The doublet DQ-1 launched on 3 September 1990 could have involved ELINT applications.[335] It is also likely that ELINT packages of various sorts have been launched aboard subsequent Chinese photographic intelligence (PHOTINT) and/or communications satellites. In 1999, the

[329] Clark, Phillip, "Worldwide Spacecraft Launches, February 2000", Jane's Intelligence Review, U.S.A., April 2000, p.56.
[330] Federation of American Scientists (FAS), Space Policy Project, "Tselina 2", U.S.A., 2002, Available on site: http://222.fas.org/spp/guide/russia/military/sigint/tselina2.htm.
[331] Clark, Phillip, Ibid., p.20; and David, Leonard, "Space Junk and ISS: A Threatening Problem", Space.com Web Page, U.S.A., 7 January 2002, Available on site: http://space.com/missionlaunches/junk_iss_020107.html.
[332] Anderson, Jack, "There's Nothing New About Military Satellites in Space", Long Island Newsday, U.S.A., 11 February 1985.
[333] Sherman, Madeline W., (ed.), "TRW Space Log, 1957-1982", Electronics and Defense Sector, TRW, Redondo Beach, California, U.S.A., 1983, p.92.
[334] Federation of American Scientists (FAS), "SJ-2", FAS Space Policy Project, World Space Guide, U.S.A., 30 June 1998, Available on site: http://www.fas.org/spp/guide/china/military/sigint/sj-2.htm; and Morris, William R., "The Role of China's Space Program in Its National Development Strategy", Maxwell Paper No. 24, Air War College, Maxwell Air Force Base, Alabama, August 2001, p.10.
[335] Federation of American Scientists (FAS), "DQ-1", FAS Space Policy Project, World Space Guide, U.S.A., 30 June 1998, at http://www.fas.org/spp/guide/china/military/sigint/dq-1.htm.

Heritage Foundation reported that China has an "advanced electronic intelligence (ELINT) satellite program" in the development stage.[336]

5.6. SATELLITE COMMUNICATIONS SYSTEM

The Satellite Communications System provides both secure voice and high data rate transmissions in the Super High Frequency (SHF) band. It provides unique and vital national security communications for global command and control, crisis management, intelligence (ELINT etc.) and early warning data relay, treaty monitoring and surveillance information, and diplomatic traffic.

Ground mobile forces (GMF) use DSCS spacecraft to fulfill multichannel SHF initial system worldwide operational requirements. The US Defence Satellite Communications System-DSCS II and III satellites are positioned in geostationary orbits and are continuously available for use by earth terminals located within 5,000 nautical miles of their subsatellite points.[337]

Many countries now have the ability to monitor selected foreign communications satellites (COMSATs). The US maintains the most extensive SATCOM SIGINT capabilities in the Asia-Pacific region. The first US station established to intercept international satellite communications in the region in the early 1970s for intercepting communications passing through the INTELSAT COMSAT stationed over the Pacific Ocean.[338] The US DSCS system originated in Department of Defense's Initial Defense Communications Satellite Program, which was inaugurated in 1966. After launching 26 of these spacecraft, the Air Force renamed the program in 1971 and launched the first of 16 DSCS Phase II satellites.[339] In 1995, it had five dish antennas, three facing westwards, one of which 'appears to be the UKUSA site for monitoring the Inmarsat-2 satellite that provides mobile satellite communications in the Pacific Ocean area'.[340] The Yakima station was one of the

---

[336] Fisher, Richard D., Jr., "Heritage Report on China's 1998 Zhuhai Air Show", The Heritage Foundation Web Page, U.S.A., 1998, Available on site: http://www.heritage.org/exclusive/zhuhai/part1.html.
[337] McKaughan, Jeffrey D., "Eyes in the Sky", Military Aerospace Technology Magazine, Volume: 2, Issue: 1, U.S.A., 02 February 2003. Available on site: http://www.mat-kmi.com/archive_article
[338] Hager, Nicky, "Secret Power: New Zealand's Role in the International Spy Network", Craig Potton, Nelson, New Zealand, 1996, p.30-31.
[339] McKaughan, Jeffrey D., Ibid.
[340] Hager, Nicky, Ibid, p. 31.

original stations in the Echelon system, the global system organized by the UKUSA countries for monitoring the non-military telecommunications of other governments, businesses and private organizations.[341] Phase II satellites have two transponders, each having a bandwidth constrained by the nominal 2009 MHz bandwidth of the total usable bandwidth of 410 MHz. Each transponder is subdivided by filters to provide two operational channels; for example, four operational channels for each satellite. Four antennas are mounted on the despun platform. Two of them are Earth coverage horn (ECH) antennas, one for uplink and one for downlink. The remaining two are parabolic dish type antennas. A single biconical horn is used to support the dedicated S-band telemetry and control link and was mounted on the lower end of the spinning section.

The on-orbit DSCS constellation is comprised of five DSCS III satellites in geosynchronous or geostationary (these terms have slightly different definitions) orbit at an altitude of about 22,300 miles. B11 (DSCS III SLEP), launched in October 2000 and now operating in the Eastern Atlantic, is the newest DSCS satellite on orbit. Fourteen DSCS III satellites have been built, with 12 on orbit and two yet to launch. The MILSATCOM Joint Program Office of Space and Missile Systems Center (SMC), Los Angeles Air Force Base, CA, is responsible for development, acquisition and sustainment of the DSCS Space Segment. The last two DSCS satellites are scheduled for launch in 2003 and will utilize the Evolved Expendable Launch Vehicle (EELV) whereas previous launches all took place using the Atlas Centaur booster.[342]

Russia has a Big Ear SATCOM SIGINT station at Andreyevka, near Vladivostok, for monitoring satellite communications in northeast Asia. The Japanese Chobetsu/DIH maintains a SATCOM SIGINT station for intercepting transmissions from Russia's communications satellites.[343]

China has also developed SATCOM SIGINT capabilities for monitoring international satellite communications. China had established 'a ground station for intercepting signals transmitted through the US and Russian communication satellite. A second SATCOM

---

[341] Campbell, Duncan, "Inside Echelon", Global Policy Web Page, 25 July 2000, Available on site: http://www.globalpolicy.org/globaliz/law/infotech/echelon.htm.
[342] McKaughan, Jeffrey D., Ibid.
[343] Richelson, Jeffrey T., "Foreign Intelligence Organizations", Ballinger, Cambridge, Massachusetts, U.S.A., 1988, p.257.

SIGINT station is located outside Beijing. A third station is located for monitoring satellite communications in central Asia.[344] China has also established a SATCOM SIGINT station to intercept US satellite communications.[345] A satellite tracking and control station which sits astride the equator in the central Pacific, is also capable of intercepting selected (S-band) satellite communications in the mid-Pacific.[346]

Taiwan is able to intercept Chinese satellite communications. In India, the Research and Analysis Wing (RAW) of the Cabinet Secretariat maintains a number of SATCOM SIGINT stations.[347]

Australia has the most extensive SATCOM SIGINT capabilities in the Southeast Asian region. It became operational in 1993, and monitors a wide range of the communications satellites stationed in geostationary orbits over the Indian Ocean and Southeast Asia.[348] The station intercepts both regional geostationary satellites (such as Russian, Chinese, Japanese, Indian and Pakistani communications satellites) and international communications satellites (including INTELSAT COMSATs and INMARSAT maritime COMSATs). New Zealand has a SATCOM SIGINT station which became operational in 1990, and which focuses on satellite communications in the southwest Pacific area, working in close cooperation with the NSA.[349]

In Southeast Asia, Singapore is the only country with a functioning foreign SATCOM SIGINT facility. It intercepts the down-links of both regional and international COMSATs, including INMARSATs.

In addition to intercepting foreign/international satellite communications for intelligence purposes, some countries have acquired capabilities for jamming selected satellite

---

[344] Gertz, Bill, and Rowan Scarborough, "Inside the Ring: China Eavesdropping", The Washington Times, Washington, U.S,A., 5 May 2000, p.A10.
[345] Timperlake, Edward, and William C. Triplett, "Red Dragon Rising: Communist China's Military Threat to America", Regnery, Washington, D.C., U.S.A., 1999, p.128.
[346] Gilley, Bruce, "Pacific Outpost: China's Satellite Station in Kiribati has Military Purposes", Far Eastern Economic Review, Australia, 30 April 1998, p.26-27
[347] Ball, Desmond, "Signals Intelligence (SIGINT) in South Asia: India, Pakistan and Sri Lanka (Ceylon)", Canberra Papers on Strategy and Defense No. 117, Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, 1996, p.19.
[348] Ball, Desmond, "Over and Out: Signals Intelligence (SIGINT) in Hong Kong", Intelligence and National Security, Vol. 11, No. 3, Australia, July 1996, p.485-492.
[349] Hager, Nicky, Ibid, chapter 10.

broadcasts and down-links. Both the US and the Soviet Union developed SATCOM jamming capabilities during the Cold War. China has also developed limited SATCOM jamming capabilities.[350] India has constructed a station 'to monitor and possibly screen out foreign [satellite television] broadcasts'.[351] Indonesia (according to the commander of the US Space Command) has 'relatively primitive' anti-satellite jammers, involving 'basic radio-frequency transmitters', which it has used on several occasions since 1996 to interfere with the COMSATs of commercial rivals or to jam politically or ideologically objectionable transmissions.[352] In 1996, Indonesia jammed a (C-band) communications satellite following a commercially-inspired dispute with Tonga over claimed satellite orbital positions.[353] In May 2001, Secretary of Defense Donald Rumsfeld said that there has been 'instances' where Indonesia had jammed a Chinese satellite which was evidently broadcasting information to Muslim fundamentalists and which it found objectionable.[354] Some non-State organizations, such as the Falun Gong movement in China, have also demonstrated the ability to jam (and even hijack) satellite transmissions.[355] There has also been a growing appreciation that some forms of SATCOM transmissions, including those involving sat-phones and GSM cell phones, can be used for targeting purposes – as demonstrated in April 1996 when Russian authorities killed the president of Chechnya with an air-to-surface missile while he was talking on a sat-phone via the INMARSAT network, and in August 1998 when the US used Osama bin Laden's satphone transmissions to target cruise missiles in the attack against the al-Qaeda base at Khowst.[356]

Of course, every country has the ability to intercept (and sever or jam) international satellite communications entering national gateways. In some countries this is done by

---

[350] Broder, Jonathon, "The Threat Over the Horizon", MSNBC Web Page, U.S.A., 27 April 2001, Available on site: http://www.msnbc.com/news/561893.asp

[351] Crosette, Barbara, "India Foreign TV Monitor Sights: Alien Influences"", International Herald Tribune, U.K., 13 June 1991, p.7.

[352] Wall, Robet, "Intelligence Lacking on Satellite Threats", Aviation Week & Space Technology Magazine, U.S.A., 1 March 1999, p.54-55.

[353] Hyten, John E., "A Sea of Peace or a Theater of War: Dealing with the Inevitable Conflict in Space", Air & Space Power Chronicles, U.S.A., 4 January 2001, Available on site: http://www.airpower.maxwell.af.mil/airchronicles/cc/Hyten.html

[354] Kitfield, James, "The Permanent Frontier", The National Journal, U.S.A., 17 March 2001, Available on site: http://www.globalsecurity.org/org/news/2001/010317-nj.htm.

[355] Pan, Philip P., "Banned Falun Gong Movement Jammed Chinese Satellite Signal", Washington Post Web Page, U.S.A., 9 July 2002, at http://www.washingtonpost/com/wp-dyn/articles/A41297-2002Jul$.html

[356] Ball, Desmond, "Desperately Seeking bin Laden: The Intelligence Dimension of the War against Terrorism", Ed. Ken Booth and Tim Dunne, Palgrave/St Martins, London and New York, 2002, p.63-64.

SIGINT/cyber cells co-located with the national gateway stations, or utilizing the facilities at national SATCOM ground control stations.

The US DSCS III satellites support globally national security users. The final four satellites, such as B11, have been upgraded with Service Life Enhancement Program (SLEP) modifications. These provide substantial capacity improvements through higher power amplifiers, more sensitive receivers and additional antenna connectivity options. The DSCS III communications payload includes six independent SHF transponder channels that cover a 500 MHz bandwidth. Three receive and five transmit antennas provide selectable options for Earth coverage, area coverage and/or spot beam coverage. A special purpose (AFSATCOM) single-channel transponder is also on board. DSCS III also carries a single-channel transponder used for disseminating emergency action and force direction messages to nuclear-capable forces.

Modulation techniques include time division multiple access (TDMA), frequency division multiple access (FDMA) and spread spectrum multiple access (SSMA). Future modulation techniques will include demand assigned multiple access (DAMA). The DSCS radio frequency portions are undergoing various upgrades to support its mission well into the 21st century.[357]

Some of the upgrades include:

- Heavy/Medium Terminal Modification: This upgrade affects the AN/FSC-78 and AN/GSC-39 terminals. These terminals' RF components will be replaced with solid state devices for the transmitters and receive amplifiers. Included will be computer monitor, test and measurement, and control of the terminal functions.
- Super High Frequency Tri-band Range Extension Terminal (STAR-T): This developmental terminal will replace AN/TSC-85B/93B terminals at echelons above corps (EAC). The terminal will be mounted on a HMMWV. Its primary mission is to provide multiband communications and interface with commercial and military assets (dial central and satellite); DGM; TRI-TAC terminals at EAC; and with MSE terminals and ECB.

---

[357] McKaughan, Jeffrey D., Ibid.

The DSCS Operational Control System (DOCS) controls all DSCS user terminals operating on DSCS spacecraft. This system also is undergoing upgrades that will allow higher control capability using less equipment and manpower resources.

A secondary payload is a U.S. Air Force SATCOM UHF single transponder used to transmit emergency action messages between military command posts (CPs) and force elements. The communications system is supported by one receive multibeam antenna (MBA), two receive ECH antennas, two transmit MBAs, two transmit ECH antennae, and a gimballed dish antenna (GDA). Each of the six independent repeaters operates in the SHF region to relay telephone, data, wideband imagery and secure digital voice signals.[358]

5.7. METEOROLOGICAL SATELLITE PROGRAM

Weather and Environmental Monitoring are essential to optimizing force operations. Weather impacts a variety of combat elements. For example, inaccuracies in wind data can significantly affect the number of artillery rounds required to neutralize a target. Visibility and wind data are also important in planning and executing helicopter operations. A third area in which wind data are vital is in predicting chemical/biological agent dispersion. Cloud bottom data are important to Air Force delivery of smart munitions and affects close air support operations. Cloud bottom data can also affect helicopter route planning. Moisture content in the soil affects its trafficability and thus the maneuver options and timing.[359]

Operational commanders require timely, quality weather information to effectively employ weapon systems and protect their resources. The Defense Meteorological Satellite Program (DMSP) is Department of Defense's most important and often the only source of global weather data to support U.S. military operations. It provides visible and infrared cloud cover imagery and other meteorological, oceanographic, land surface and space environmental data.[360] Communication links exist to the ground segment for the Defense Meteorological Satellite Program (DMSP). Through this system, cloud cover data are available with 4-hour latency from the time of the satellite pass.

---

[358] McKaughan, Jeffrey D., Ibid.
[359] Army Science Board, "Final Report - Prioritizing Army Space Needs", Department of the Army, Washington, D.C., July 1999, p. 34.
[360] McKaughan, Jeffrey D., Ibid.

DMSP, originally known as the Defense System Applications Program (DSAP) and the Defense Acquisition and Processing Program (DAPP), is a long-term Air Force effort in space to monitor the meteorological, oceanographic and solar-geophysical environment of the Earth in support of US operations. The first DMSP satellite, F-8, was launched on June 18, 1987. All spacecraft launched have a tactical (direct readout) and a strategic (stored data) capacity. The USAF also maintains an operational constellation of two near-polar, sun-synchronous satellites.

While managed at the Space and Missile Systems Center, DMSP command and control is provided by a joint operational team at the National Oceanic and Atmospheric Administration, DMSP satellites provide meteorological data in real time to Air Force, Army, Navy and Marine Corps tactical ground stations and Navy ships worldwide. This data is also stored in recorders on the satellites for later transmission to one of four ground stations.

5.8. MILSTAR: A JOINT SERVICE PROGRAM

Milstar is a joint service program to provide extremely high frequency (EHF) satellites; a satellite mission control segment; and new or modified Army, Navy, and Air Force communication terminals for survivable, jam-resistant, worldwide, secure communications to strategic and tactical war fighters. A key feature of the Milstar system is the interoperable terminals used by U.S. warfighters. For example, sea-based terminals can be used to upload new data onto cruise missiles carried aboard submarines and guided missile destroyers in real time. Land-based terminals, such as the Several Channel Anti-Jam Man-Portable (SCAMP) and the Secure Mobile Anti-Jam Reliable Tactical Terminal (SMART-T), provide communications and data exchange for the mobile, ground-based warfighter.[361] This program's mission statement is to provide the President, Secretary of Defense, and Combatant Commanders with assured, worldwide command and control (C^2) for tactical and strategic forces.[362]

---

[361] McKaughan, Jeffrey D., Ibid.

[362] Air University, "Key Air Force Programs: Space", Air Force University, Maxwell, Alabama, U.S.A., 2003, Available on site: http://space.au.af.mil/space.pdf

Figure 5.7: Milstar spacecraft that provide strategic tactical relay.

The MILSTAR Joint Terminal Program Office (JTPO) is coordinating and directing the development of interoperable medium data rate (MDR) protocols, as well as updating and reissuing the joint ILS plan to accommodate the reduced number of low data rate (LDR) terminals and new terminal initiatives for MDR terminals. It is also conducting interoperability testing in support of an Army production decision, developing and LDR/MDR terminal specification for MILSTAR II satellites, evaluating engineering changes to ensure tri-service interoperability, and providing technical assistance in the areas of requirements as well as enhancing the MILSTAR Information Exchange System.[363]

Milstar had a rough beginning as there were concerns over the high cost estimates and uncertainty over the requirements as the Cold War drew to a close. The satellite constellation was originally planned to consist of four active (and one spare) satellites in geosynchronous equatorial orbit, as well as three active (and one spare) satellites in geosynchronous polar orbit, with a tenth spacecraft procured as a ground spare in

[363] Mathews, Tom, "The Secret History of the War", Newsweek Magazine, New York, NY, U.S.A., 18 March 1991, p. 28-39.

anticipation of a launch failure. Plans were revised calling for six satellites in a mixture of low- and high-inclination orbits. A low-inclination orbit would place the satellites in positions to cover the Atlantic, Pacific, and Indian Oceans as well as North and South America. Satellites in the high-inclination orbit would cover the Polar Regions, Europe, Africa and Western Asia. The first launch of a first-generation Milstar Block I satellite was on February 7, 1994, with a second launch in November 1995.[364]

Milstar objectives for 2010-2025 are:[365]

- Provide the right communications to the right user at the right time by being information services driven
- Be fully integrated with the Defense Information Systems Network (DISN)
- Reduce the satellite communications 'footprint' of terminals, radios, antennas, RF signature, people, etc.
- Be user friendly and interoperable

Milstar has been specifically designed to overcome shortfall characteristics of existing satellite communications systems. Concepts for survivability in a hostile space environment (Cold War-era thinking) had shaped the design of this military communication system, especially with the first two Milstar satellites. As part of the program restructuring, requirements for a classified payload were deleted from the Block 2 satellites as were "heroic" survivability features, such as hardening against nuclear shock.

Milstar Block 2 satellites 3 through 6 have both Low Data Rate and Medium Data Rate (MDR) payloads with increased tactical capabilities, including two nulling spot antennae that can identify and pinpoint the location of a jammer and electronically isolate its signal, allowing Milstar users to operate normally and at full capacity with no loss in signal quality or speed, despite any attempt by hostile forces to jam or intercept its signal.

Satellite 3, the first Block 2 satellite, did not reach its proper orbit and the satellite was placed in its final non-interference "parking" orbit and shutdown in April 1999. Milstar

---

364 McKaughan, Jeffrey D., Ibid.
365 Pike, John, "Military Communications", Global Security Web Page, Washington, D.C., U.S.A., October 2002, Available on site: http://www.globalsecurity.org/Space/Military.htm

satellite 4 was launched successfully February 27, 2001, and satellite 5 was launched successfully on January 15, 2002. Milstar satellite 6 was planned to launch in 2003.[366]

5.9. NAVSTAR: GLOBAL POSITIONING SYSTEM (GPS)

Navstar Global Positioning System (GPS) is a space-based radio positioning, navigation and time distribution system. GPS User Equipment (UE) consists of standardized receivers, antennae, antenna electronics, etc., grouped together in sets to derive navigation and time information transmitted from GPS satellites. The Navstar Global Positioning System (GPS) is a constellation of 27 orbiting satellites in an 11,000-mile circular orbit that provides navigation data to military and civilian users all over the world.[367] The GPS continues to mature into a worldwide positioning, navigation, and timing information resource. The military utility of GPS–enabled precision munitions was illustrated in the conflict in the Balkans. Consequently, integration of GPS into all levels of combat forces remains a high priority.[368] This exceeds the operational requirement of 24 satellites and provides robustness and overlapping capability should any one satellite fail. The system is operated and controlled by the Air Force.

GPS satellites orbit Earth every 12 hours, emitting continuous navigation signals. With the proper equipment, users can receive these signals to calculate time, location and velocity. The signals are so accurate, time can be figured to within one millionth of a second, velocity within a fraction of a mile per hour and location to within 100 feet.[369]

With the growing importance of GPS to military operations and the need to maintain this advantage for friendly forces, the Department's navigation warfare (Navwar) initiative continued on course, and operational requirements for Navwar were formally validated. Navwar efforts, including the recently completed Navwar ACTD, are focused on selecting the most effective solutions for assuring uninterrupted DoD and allied use of GPS, denying access to an adversary, and maintaining GPS service for peaceful purposes outside the theater of operations. US is evaluating alternatives and developing a roadmap for

---

[366] McKaughan, Jeffrey D., Ibid.
[367] McKaughan, Jeffrey D., Ibid.
[368] Cohen, William S., "Annual Report to the President and the Congress – Information Superiority and Space", Secretary of Defense, DoD, U.S.A., 1999. Available on site: http://www.defenselink.mil/execsec/adr99.htm
[369] McKaughan, Jeffrey D., Ibid.

modernizing the system to satisfy more demanding military and civil requirements to ensure the continued utility of the system well into the 21st century.

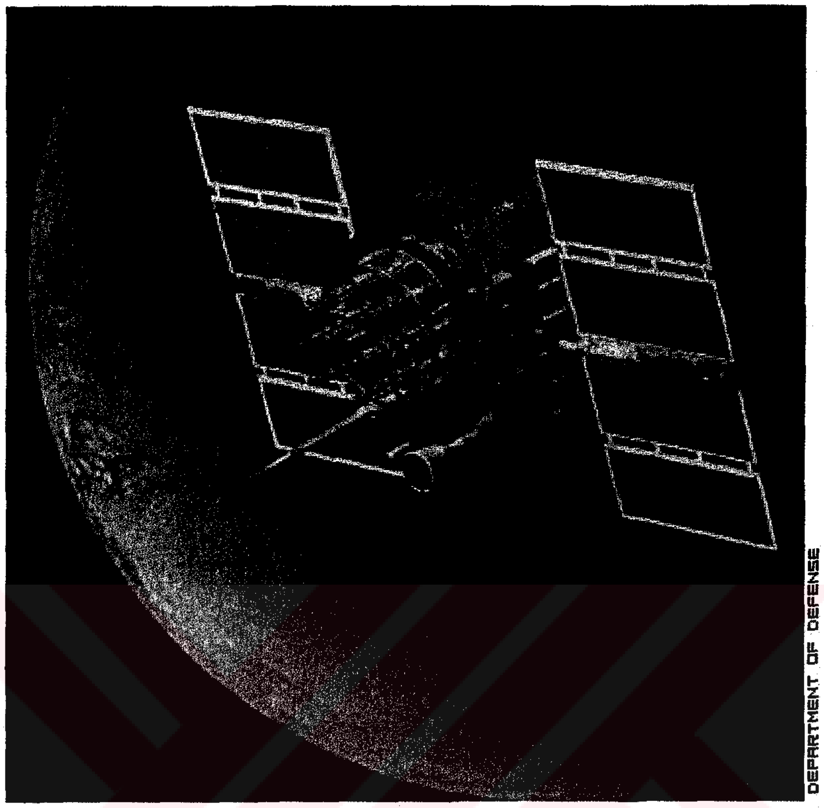


Figure 5.8: The network of Global Positioning System (GPS) satellites.

An Interagency GPS Executive Board provided proactive management and oversight of the dual–use aspects of the system. Two new civil signals will be added to future GPS satellites to provide civil users with increased accuracy and robustness and to permit an even broader spectrum of GPS applications.[370]

The satellites transmit on two L-band frequencies with three pseudo-random noise (PRN) ranging codes. The coarse/acquisition (C/A) code has a 1.023 MHz chip rate, a period of 1 millisecond (ms) and is used primarily to acquire the P-code. The precision (P) code has a 10.23 MHz rate, a period of 7 days and is the principal navigation ranging code. The Y-code is used in place of the P-code whenever the anti-spoofing (A-S) mode of operation is activated.

---

[370] Cohen, William S., Ibid.

The C/A code is available on the L1 frequency and the P-code is available on both L1 and L2. The various satellites all transmit on the same frequencies, L1 and L2, but with individual code assignments. Due to the spread spectrum characteristic of the signals, the system provides a large margin of resistance to interference.

The first GPS satellite was launched in 1978. The first 10 satellites were developmental satellites, called Block I. Twenty-one of the original 27 Block II and Block IIA satellites launched between 1989 and 1996 are still operational, which is remarkable considering their estimated life space was 7 1/2 years.

There are seven Block IIR satellites on-orbit with six operational. There are three launches planned in 2003 with the first Block IIR-M scheduled for July 2004. Expectations are for 21 Block IIR total. Between 12 and 16 Block IIF satellites are planned (there are currently none in orbit). Satellites 1 through 6 are being modernized to carry additional civil signals (L2C and L5), a civil-only safety-of-life signal and an M-Code military-only signal. Satellites 7 through 9 will be procured in 2005 and the last three in 2006. The GPS Block III program is currently under review.[371]

Also China and Europe Union have made great amount of investment in satellite technology and they are in effort to establish their own GPS systems. And Russia launches several communication satellites one after another for its own GPS system.[372]

5.10. DEFENSE SUPPORT PROGRAM

Air Force Space Command-operated Defense Support Program (DSP) satellites are a key part of North America's early warning systems. In their 22,000 miles-plus geosynchronous orbits, DSP satellites help protect the United States and its allies by detecting missile launches, space launches and nuclear detonations. The number of satellites in the DSP constellation is classified.[373]

---

[371] McKaughan, Jeffrey D., Ibid.
[372] Can, S., "Uzayda Trafik Yoğun", Ulusal Strateji Dergisi, Yıl:3, Sayı:17, CNR, İstanbul, 2001, p.10.
[373] McKaughan, Jeffrey D., Ibid.

DSP was the world's first *real-time* satellite reconnaissance and ELINT program. It could detect the launch of missiles and report the launch almost simultaneously.[374] The first satellite was the launching of the Defense Support Program in 1970. Its neutral-sounding name notwithstanding, the DSP was America's first line of defense against nuclear attack.[375] Since that time, DSP satellites have provided an uninterrupted space-based early warning capability. The original DSP satellite weighed 2,000 pounds and had 400 watts of power, 2,000 detectors and a design life of one and one-quarter years. Throughout the life of the program, the satellite has undergone numerous improvements to enhance reliability and capability. The weight grew to 5,250 pounds, the power to 1,275 watts, the number of detectors increased three-fold to 6,000 and the design life has been increased to a goal of five years.

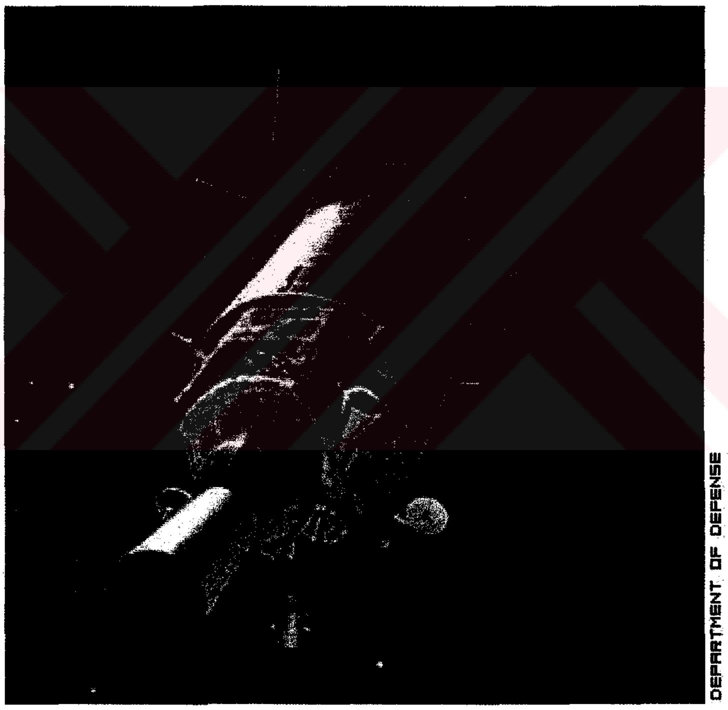


Figure 5.9: US Air Force Defense Support Program (DSP) satellites.

DSP satellites use an infrared sensor to detect heat from missile and booster plumes against the Earth's background. In 1995, technological advancements were made to ground

[374] Richelson, Jeffrey, T., "America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program", Harper & Row Publications, New York, N.Y., U.S.A., 1990, p. 68.
[375] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 311.

processing systems, enhancing detection capability of smaller missiles to provide improved warning of attack by short-range missiles against U.S. and allied forces overseas.

Numerous improvement projects have enabled DSP to provide accurate, reliable data in the face of evolving missile threats. On-station sensor reliability has provided uninterrupted service well past their design lifetime. Recent technological improvements in sensor design include above-the-horizon capability for full hemispheric coverage and improved resolution. Increased on-board signal-processing capability improves clutter rejection. Enhanced reliability and survivability improvements were also incorporated.[376]

DSP's effectiveness was proven during Desert Storm, when DSP detected the launch of Iraqi Scud missiles and provided warning to civilian populations and coalition forces in Israel and Saudi Arabia.[377] They had ofcourse, been much improved since 1970. there were more sensitive sensors, three times as many infrared detectors, a much more powerful telescope, and superior data-transmission capabilities. This allowed DSPs to detect the plumes of fighter planes and to provide enough warning of SCUD launches for Patriot missile crews.[378] Although the number of satellites in the constellation is classified, DSP-23, the last funded satellite is scheduled for launch in 2003.

The launch of Flight 22 (out of a total of 23) is scheduled for October of 2003. As the SBIRS High program is/was envisioned as the follow-on program, performing those missions of DSP plus others, Flight 23 is scheduled as the last launch for DSP.[379]

5.11. ON LAND SATELLITES "REACHING BACK" (Above 200-500 miles above Earth)

A technique called "reach back" puts small numbers of troops in the field who rely on satellites to provide information, photos, electronic intelligence (ELINT), and command. (See Figure 5.2)

As they try to root out terrorists in forbidding, mountainous country, U.S. and ally forces will depend heavily on reach-back. It involves leaving much of the administrative

[376] McKaughan, Jeffrey D., Ibid.
[377] McKaughan, Jeffrey D., Ibid.
[378] Covault, Craig, "Recon Satellites Lead Allied Intelligence Effort", Aviation Week and Space Technology Magazine, U.S.A., 4 February 1991, p. 25
[379] McKaughan, Jeffrey D., Ibid.

personnel and details behind in order to streamline a unit of troops, who then rely on a wide communications pipe to get data and orders from military command centers.

Soldiers in the field could, for example, speak directly with an expert on mines and download photos and illustrated instructions for how to defuse or detonate them. The Navy is experimenting with animated 3-D visualizations of enemy territory. The military continually ratchets up its use of reach-back as satellite capabilities improve. Curiously, almost no fighter jets rely on satellite communications. The receiving units are simply too large to stuff into an F-16. They're just beginning to scratch the surface of bringing real-time info into the cockpit via satellite as the size of receiver units shrinks.

In all, nearly 100 satellites contribute directly or indirectly to operation Enduring Freedom. But the operation as planned will be just one-tenth the size of Desert Storm. It would have to go seriously wrong in order to require the kind of satellite support that might clog the system.[380]

5.12. MICRO AND NANO ELINT SATELLITES

Miniaturization techniques have already been used for years to reduce spacecraft component size and weight and also costs. After three years of work, the world's smallest self-propelled satellite was delivered by University of Washington to the Air Force and NASA for launch. The nanosatellite, dubbed "Dawgstar" and was launched from the Space Shuttle in early 2003, took samples from the Earth's ionosphere and conducted experiments in formation flying with two other satellites, an ability scientists say is vital for the next generation of space endeavors.

Dawgstar resembles a small six-sided box, measuring 18 inches across and 12 inches high, and weighing less than 40 pounds. It will fly with companion satellites from Utah State

[380] Britt, Robert Roy, "War on Terrorism Could Clog Military's Space Airwaves", U.S.A., 08 October 2001, Available on site: http://www.space.com/news/

University and Virginia Tech. Dawgstar, with the aid of eight tiny plasma thrusters, is the primary craft capable of maneuvering itself. The mission's two main objectives are:[381]

- Conducting a scientific study of disturbances in the Earth's ionosphere. Such disturbances can cause significant disruption in communications among networked satellites and with sites on the ground. A better understanding of ionospheric disturbances will be essential in managing groups of nanosatellites in Earth orbit and operating space-based radar systems.
- Performing experiments in precision formation flying with the satellites from Utah State and Virginia Tech. The satellites will fly about one to three miles apart and will attempt to maneuver in concert to tolerances of 33 feet or less. The ability of small satellites to fly in precise formation could make possible a wide array of new applications, including a next-generation Internet, space-based radar and ultra-powerful space telescopes.

Most of the miniaturization benefits achieved have been for existing satellites, but, as current technology miniaturization trends continue, it has become popular to predict the operational deployment of microsats, nanosats, and even picosats. For the future, the utility of microsats per se and the new operational concepts they may enable will depend on a series of technology experiments to progressively establish their feasibility and utility. A summary assessment of such factors is depicted below.

More specifically and over the longer term, microsats of appropriate mass, size and capability are being considered to:[382]

- Augment existing constellations during contingency or theater operations
- Perform special-purpose or limited-scope "niche" missions, such as nuclear detonation (NUDET) detection
- Operate as distributed or multifunctional platforms in the performance of several space missions

[381] Harrill, Rob, "World's Smallest Self-Propelled Satellite Nearly Ready for Air Force, NASA", Space Daily Newsletter Online Edition, Seattle, U.S.A., 2 November 2001, Available on site: http://www.spacedaily.com/nanosats.html
[382] Department of Defense, "Space Technology Guide-FY 2000-01", Office of the Secretary of Defense, Washington, U.S.A., 2002, Available on site: http://www.defenselink.mil/myer.pdf

- Support Space Control concepts by providing additional platforms for Defensive or Offensive Counterspace options
- In conjunction with the foregoing, provide unique capabilities to enable new, innovative operational concepts.

Israel's military space goal is to launched constellation of small, low-Earth orbit satellites carrying a range of sensors, including synthetic aperture radar (SAR) with a resolution of well under a meter for day/night, bad-weather observations. They consider such observations critical for keeping track of potential foes, such as Iran and Libya, which have long-range ballistic missile programs.[383]

A bit further off is the development of very small nano-satellites that could be used to disable satellites. The thought is that someday a Middle Eastern power (some analysts suggest that the effort could be supported by North Korea's space program) might launch a satellite that could gather intelligence on other countries, try to intercept data gathered by its space constellation or even attack individual satellites. There is an open, wide band of information that is vulnerable. Piracy or guerrilla warfare in space has to be considered seriously.

In 2005, Israel will have a SAR demonstrator in the 650-lb. class. It will need lots of processing capability, but that's not a big challenge. The challenge will be to enhance and distribute the data just the same as electro-optical imagery. Electro-optical and SAR imagery payloads also are expected to be supplemented with communications and electronic intelligence-gathering (ELINT) packages. With next-generation technology, they will be able to put a 1-meter-class SAR in a 220-lb. micro-satellite for a little cost.

Dedicated SAR sensors will offer intelligence analysts the ability to locate evidence of underground structures such as tunnels. Tunnels have been the bane of Israeli military operations, particularly in Gaza. They are used to smuggle people, weapons and explosive across the border from Egypt. Tunnels are also used to house mobile missiles, weapons manufacturing and production facilities for chemical and biological weapons. For example, foreign weapons experts here and in the U.S. say Syria has an underground assembly line

---

[383] Fulghum, David A., "Micro and Nano Sats.", Aviation Week & Space Technology Magazine, Volume 158, Issue 24, Tel Aviv, Israel, 16 June 2003, p.140.

for 700-km. (435-mi.) range, two-stage Scud-Ds in operation northwest of Damascus. Israeli officials also want to introduce hyper-spectral sensors that will make it harder to camouflage or hide targets from satellite observation.[384]

Israeli leaders initially rejected the idea of a space program because of the expense and complications of launching missiles to the east over nations with hostile regimes. They invested instead in the development of unmanned aircraft for gathering crucial intelligence from high-threat areas. However, as nations in the region began to develop ballistic missiles and nonconventional weapons, defense planners decided to focus on the rapid development of a line of micro- and mini-satellites and small high-resolution sensors.

The Israeli defense ministry is working on a strategy to make micro- and mini-satellites - and eventually even smaller nano-satellites- more capable. One promising option is to split a large payload among several satellites. The satellites' arrangement or formation would depend on the task. COMINT, SIGINT and ELINT satellites would likely be arranged in long lines to quickly triangulate the position of transmitters of interest. Satellites would be flown in a cluster circular, chevrons or a square to create a single, large virtual aperture of much greater resolution.[385]

5.13. WIDEBAND GAPFILLER AND ADVANCED EXTREME HIGH FREQUENCY

The Wideband Gapfiller Satellites (WGS) will provide near-term continuation and augmentation of the services currently provided by the DSCS and the Global Broadcast Service (GBS). WGS will complement the DSCS III Service Life Enhancement Program (SLEP) and GBS payloads, and offset the eventual decline in DSCS III capability. Together these assets will provide wideband services during the transition period between today's systems and the advent of the Objective X/Ka wideband system or Advanced Wideband System (AWS) in 2008.

This combination of the Wideband Gapfiller Satellites, DSCS satellites, GBS payloads, wideband payload and platform control assets, and earth terminals operating with them has been referred to as the Interim Wideband System (IWS). WGS will support wideband

[384] Fulghum, David A., Ibid, p.140.
[385] Fulghum, David A., Ibid, p.140.

military satellite communications services beginning around 2004. The Gapfiller System will support continuous 24 hour per day wideband satellite services to tactical users and some fixed infrastructure users. Limited protected services will be provided under conditions of stress to selected users employing terrestrial modems capable of providing protection against jamming. The combined wideband satellite communications system consists of space vehicles of multiple types, control terminals and facilities and user terminals.[386]

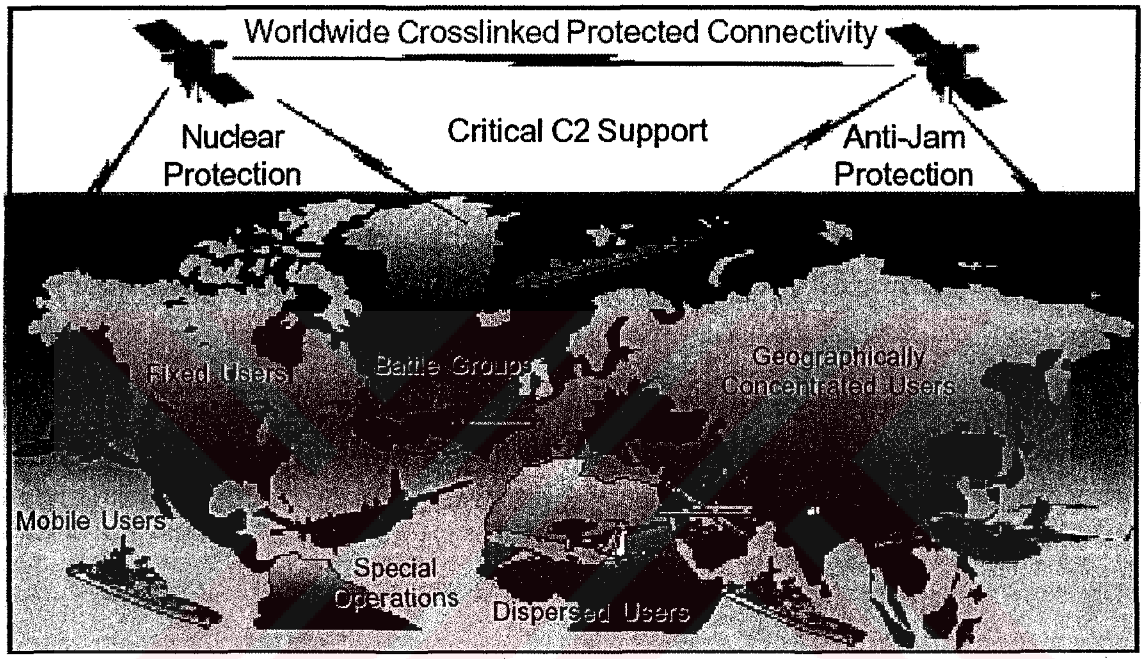


Figure 5.10: Advanced Extremely High Frequency (AEHF) System Concept[387]

The space segment will support communication services in two military frequency bands:[388] X-band and Ka-band. The WGS payload will be capable of supporting at least 1.2 Gbps aggregate simplex throughput. The Gapfiller satellites will operate in X-band (8 steerable/shapable) and in WGS Broadcast Ka-band (10 steerable), similar to the Phase II GBS in service today. This capability will ensure interoperability with existing and new X-band and GBS terminals. The Gapfiller satellites will also provide a new two-way military

[386] McKaughan, Jeffrey D., Ibid.
[387] Department of Defense, "Space Technology Guide-FY 2000-01", Office of the Secretary of Defense, Washington, U.S.A., 2002, Available on site: http://www.defenselink.mil/myer.pdf
[388] Air University, "Key Air Force Programs: Space", Air Force University, Maxwell, Alabama, U.S.A., 2003, Available on site: http://space.au.af.mil/space.pdf

Ka-band capability to support the expected military mobile/tactical two-way Ka-terminal population with greatly increased system capacity.[389]

The Advanced Extreme High Frequency (AEHF) satellite, also known as the Advanced Wideband Satellite (AWS), program is the next generation of highly secure, high capacity, survivable communications to the U.S. warfighters during all levels of conflict, and will become the protected backbone of DoD's military satellite communications architecture.[390]

Wideband communications services rapidly move large quantities of C^4I information including intelligence products (ELINT), video, imagery, and data. US's wideband strategy is to launch the four remaining Defense Satellite Communications System satellites supplemented by Global Broadcast Service payloads on Ultra–High Frequency Follow–on (UFO) satellites. Three Wideband Gapfillers will be launched starting in 2004 to reduce the growing gap between tactical wideband requirements and capabilities. A more capable commercial–like Advanced Wideband System is envisioned starting in 2008.[391]

AEHF satellites will replenish the existing EHF system (Milstar) at much higher capacity and data rate capability with decreased launch costs. The AEHF system will give warfighters the first-ever capability to set up command and control networks and allow commanders real-time control of their own network resources. The capability of the software both on the satellite and the associated ground Mission Control System is ten times greater than current capabilities providing up to 4,000 simultaneous networks and up to 6,000 users per satellite. Other technology highlights are the Phased Array uplink and downlink antennae and the Ion Propulsion System used to take the satellite to its final orbit after insertion into its initial orbit from the launch vehicle.

This program focuses on utilizing commercial technology to the maximum extent possible and will ensure technology development is sufficient for a medium launch lift vehicle. A four-satellite constellation would be required to meet current system requirements of

---

[389] McKaughan, Jeffrey D., Ibid.
[390] McKaughan, Jeffrey D., Ibid.
[391] Cohen, William S., "Annual Report to the President and the Congress – Information Superiority and Space", Secretary of Defense, DoD, U.S.A., 1999. Available on site: http://www.defenselink.mil/execsec/adr99.htm

worldwide coverage. An ongoing transformational communications satellite study will determine whether satellites there will be further procurement under this program.[392]

The strategy for protecting communications calls for launching four Milstar II satellites by 2002 as planned, followed by the first launch of a more capable Advanced Extremely–High Frequency system in 2006. Narrowband communications services provide networked multi–party and point–to–point narrowband links to tens of thousands of rapidly moving warfighters. US launched its last UFO satellite in 1999 and plan to supplement the constellation with a satellite in 2003 to maintain the system through 2007. In 2008, the US plans to launch a UFO replacement system known as the Advanced Narrowband System.[393] AEHF is a cooperative program Memorandums of Understanding (MoU) signed with Canada and the Netherlands. An MoU with the U.K. is expected in the near future.[394]

5.14. WEAPONS IN SPACE, SPACE-BASED INFRARED AND LASER SYSTEMS

Satellites are the most common space assets, but especially U.S., is in an effort to use the space for different purposes.[395] Some of these space systems are seen in figure 5.11.

The Space-Based Infrared System (SBIRS) program was envisioned as an integrated system that would provide the nation with critical missile defense and warning capability. It is designed to incrementally upgrade and eventually replace the DSP and with that, provide a greatly enhanced detection, identification and tracking capability.[396] An infrared capability called false color, which gave it the ability to see through haze and darkness, substantially increasing its effectiveness. Just as important was the development of a fully multispectral sensing system.[397]

[392] McKaughan, Jeffrey D., Ibid.
[393] Cohen, William S., Ibid.
[394] McKaughan, Jeffrey D., Ibid.
[395] Kenyon, R., "Air/Space Based Platforms", Highfrontier Web Page, U.S.A., 2000, Available on site: http://www.highfrontier.org/hf_spacebased.html
[396] McKaughan, Jeffrey D., Ibid.
[397] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 316.

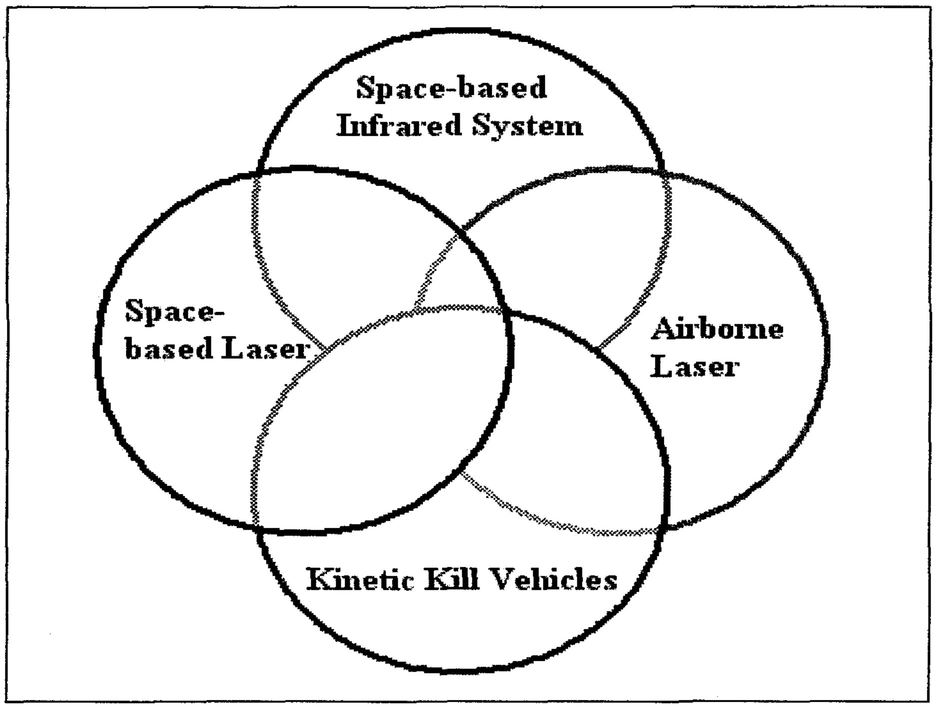


Figure 5.11: Some Space Systems

SBIRS Low's primary mission is to provide a missile-tracking program. Funding and responsibility for this effort was transferred to Missile Defense Agency (MDA) in 2002. It seems most likely that alternatives to SBIRS Low will gain more favor, as there were technology and cost factors that worked against the program. A combined sea, land and aircraft based sensing system is considered a reasonable alternative and will probably be proposed to the U.S. Senate in March 2003.[398]

Space-based laser system is still in the early stages of development. It is designed to culminate in a demonstration intercept in the space of a boostphase ballistic missile target. The target number of satellites for the space-based laser in the current plan is 20, and it is estimated that kill times per missile range from 1 to 15 seconds, depending on the range to the target.[399]

As the strategic environment evolves, military requirements change, and technology advances, space-based weaponry considerations will inevitably be readdressed.[400] Planners envision three mission areas in which space-based weaponry might provide necessary

[398] McKaughan, Jeffrey D., Ibid.
[399] Kenyon, R., Ibid.
[400] Randolph, Stephen P., "Transforming America's Military - Controlling Space", Ed. Hans Binnedijk, , National Defense University Press, U.S.A., June 2002.

capabilities: terrestrial attack, antisatellite missions, and missile defense. From a technical perspective, three broad approaches have undergone study: kinetic weapons, delivery of conventional precision weapons, and directed energy weapons (most often radio frequency or laser).[401]

Kinetic weapons are generally studied in the form of tungsten or titanium rods to be released from orbit in clusters and directed against large fixed targets or for missile defense. If used for terrestrial attack, these would be limited to a vertical attack profile and so would be most suited for use against tall buildings, missile silos, hardened aircraft shelters, and the like.[402]

Directed energy weapons would be capable of light-speed attack for either destructive or disruptive effects. This category offers the greatest technical challenges, most urgently in the areas of generating and directing the power necessary to achieve required effects within a spacecraft weight budget low enough for launch. The Air Force's Space-Based Laser (SBL) program has continued work since the mid-1980s on these technologies and had been working toward a test mission launching in 2012. Recent reports indicate that the program is now undergoing a complete restructure and will return to component development with no plan for a flight test.[403]

The fate of the SBL program illustrates a long-term hurdle for the development of space-based weaponry. In the absence of a catastrophic trigger event, consensus behind the strategic utility and military requirement for space-based weapons will be very difficult to sustain through the extended development periods and the expense necessary to field these capabilities. Depending on orbital geometry and the basing mode, space-based weapons could provide a very rapid response capability and an attack option that precludes effective defense. Against a highly capable adversary, these weapons might provide a leading-edge

---

[401] Preston, Bob, "Space Weapons Earth Wars" RAND Publications, Santa Monica, CA, U.S.A, 2001.
[402] Iannota, Ben, "Explaining X-planes", Aerospace America Magazine 39, No. 11, U.S.A., November 2001, p.30.
[403] Martel, William, ed., "The Technological Arsenal: Emerging Defense Capabilities", Smithsonian Institution, Washington, DC, U.S.A., 2001.

attack option to blunt the effectiveness of defending forces. They might provide the only effective counter to an opposing directed-energy weapon.[404]

The diplomatic and political costs of these capabilities would depend on the circumstances surrounding their deployment, and in particular whether they are viewed as a justifiable response to valid threats.[405] This range of options for exploitation of space 20 years hence changes fundamentally if there is a breakthrough in launch technology. If launch costs can be reduced and responsiveness improved, the possibilities for human exploitation of space expand beyond any horizon now envisioned.

5.15. KEY ENABLERS OF SPACE TECHNOLOGY

Control of space will mean the ability to command and control (C^2) the complex systems that allow space-based fleets to see, to shoot, and to communicate, command and control will rest with the men and women in space, whose intelligence is necessary to mange these complex fleets spread over trillions of cubic miles. Defending manned platforms will allow continued use of space. Thus, these invaluable assets will themselves become defensive fortresses, fast, agile, heavily armed, each command center linked to the rest by highly secure links such as laser-based communications.[406]

Space capabilities and assets have a proven track record of enhancing situational awareness and providing robust communications that are timely and accurate. Space is a key enabler for information operations.[407] Just a few years ago, knowledgeable observers looked forward to the day, expected to arrive soon, when U.S. military space capabilities would be fueled by developments in the commercial market. Military space was expected to ride a wave of commercial technology and capabilities in a partnership of equals with the commercial sector. The communications, navigation, ISR and WTEM data become key building blocks for Information Dominance.[408]

---

[404] Randolph, Stephen P., Ibid.

[405] Logsdon, John, "Just Say Wait to Space Power," Science and Technology Magazine, U.S.A., Spring 2001, Available on site: www.nap.edu/issues/17.3/p_logsdon.htm.

[406] Friedman, George & Meredith, Ibid, p. 374.

[407] Army Science Board, "Final Report - Priotirizing Army Space Needs", Department of the Army, Washigton, D.C., July 1999, p. 18-19.

[408] Army Science Board, Ibid, p. 19.

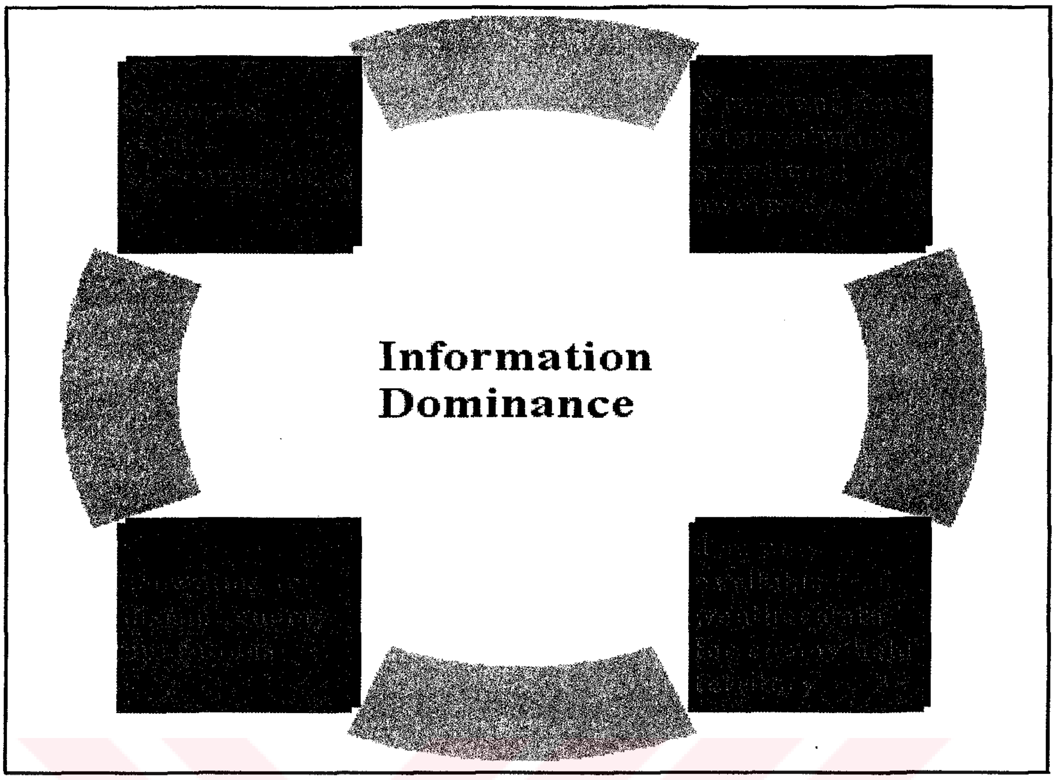


Figure 5.12: Building Blocks for Information Dominance.

Global coverage from satellite and "nonspace" means allows the commander to manage the battlespace. Wireless communications and access to direct downlinks support strategic, operational and tactical missions. Through remote sensing and national assets, continuous overwatch and blue-force tracking are feasible and attainable. Evolving doctrine to develop sensor-to-shooter links puts threat forces in harm's way.

These conditions demand attention if the United States is to preserve its capabilities in this sector and to sustain its ability to meet future requirements. Three related components must be addressed: adequate R&D funding; people with the expertise and energy to move the bounds of the possible still further; and the overall structure and capability of the industrial base.[409]

[409] Randolph, Stephen P., Ibid.

5.16. AREAS FOR FUTURE PROGRESS

The aim of integration is a transparent employment of space forces and manned and unmanned sensors, all feeding into a command system able to use the information for real-time decision-making and targeting.[410] The role of space forces in that construct, in providing sensor data, connectivity, and precision navigation and timing, will be critical.

Already the integration of GPS data into weapons guidance has transformed the U.S. military into an all-weather precision strike force, creating unparalleled capabilities that have proven themselves in Afghanistan. More broadly, reports indicate that in ongoing operations, imagery has been piped directly to Special Forces units for tactical decision-making in real time. If accurate, this report marks the progress that has occurred in a relatively short time in transcending old organizational, doctrinal, and technical barriers. As recently as 1999, informed observers estimated that space force contributions to theater operations reached only 10 to 15 percent of their potential.[411] It appears that space-based contributions across the range of theater operations have now gone far beyond that estimate.

Various antisatellite (ASAT) programs are reportedly in progress in the People's Republic of China, fed both by old Soviet technology and indigenous developments. These reports have included everything from old co-orbital ASAT systems, to laser blinders, to parasitic microsatellites. All of these are technically feasible, and they represent only a portion of the range of options open to an adversary seeking to cut the chain of data derived and transmitted through space. Given the importance of space systems to the national information infrastructure, their protection is far more than a strictly military requirement.

With a few exceptions, notably the Milstar communications satellite, the United States has historically paid little attention to the survivability of its space systems. The need to do so

---

[410] Cebrowski, Arthur K., and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, U.S.A., January 1998, Available on site: www.usni.org/Proceedings/Articles98/PROcebrowski.htm

[411] Watts, Barry, "The Military Use of Space: A Diagnostic Assessment", Center for Strategic and Budgetary Analysis, Washington, DC, U.S.A., February 2001.

now reflects the growing importance within the theater command structure and the proliferation of technology around the world.[412]

A better understanding of the threat environment will strengthen America's ability to protect its space capabilities. From a mission perspective, the links and ground stations are more accessible to attack and probably an easier target than space systems. As with any military capability, there exists a broad menu of options that could be used to protect American space capabilities; these will be dependent on their role, orbital regime, and technological composition. Generalizations are impossible here, except to note that more attention must be given to survivability of these systems if they are to continue in their central role in U.S. theater capabilities. Too often in the past, survivability measures have been traded off for competing performance or cost considerations.

The virtues of constant surveillance, or persistence, have become clear to all and are at the heart of the drive toward more responsive targeting. In the Afghanistan campaign, with a permissive air-defense environment, UAVs and manned aircraft have provided the persistent surveillance necessary to meet theater requirements. Over the long run, though, a space-based system would provide both global capabilities beyond the reach of any practical force of air-breathing systems and coverage in a denied-access situation. It is unlikely that any space-based system could fully replace air-breathing platforms, but a constellation of satellites might relieve some of the operational tempo burden now placed on manned ISR aircraft. A space-based surveillance force would provide full-time coverage of selected areas, through the spectrum of peacetime, crisis management, and operational employment. Among the lessons being repeated in Afghanistan is that preconflict preparation is the key to effective battlefield intelligence; a space-based system would provide exactly that capability. It would also avoid the complications of basing rights and overflight requests for ISR assets and provide surveillance unobtrusively for any region necessary to meet national or theater requirements. Naval forces would find a space-based radar (SBR) system especially valuable, extending their standoff range and increasing targeting flexibility.[413]

---

412 Randolph, Stephen P., Ibid.
413 Friedman, Norman, "Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare", Naval Institute Press, Annapolis, MD, U.S.A., 2000.

It may be that the real challenges for SBR will lie more in TPED than in the space component of the system. The quantities of data available through this system will be staggering. They will make extremely heavy demands on bandwidth and on the terrestrial information infrastructure. The organizational issues may prove as difficult as the technical. This movement toward a generation of low-flying, taskable systems will also move the world of military space to a whole new level of operational and technical complexity that will place heavy demands on planners and operators alike. Defining the operational and technical linkages among SBR, other sensors, and theater forces will also require careful thought.[414]

The generation beyond this may see the operational advent of clustered systems: small satellites flying in formation, cooperating to perform the functions of a large "virtual satellite." In principle, these could provide a flexible mix of passive and active sensors, reconfigurable while on orbit to meet new operational demands. They could provide the opportunity to field sparse-aperture systems that could provide staring electro-optical surveillance from geosynchronous distances. Alternatively, clustered microsats could provide a GMTI capability comparable to SBR.[415]

Coordinating the interactions of clustered satellites will demand a focused development effort. The U.S. military is just beginning to address these capabilities with the TechSat 21 cluster of three satellites scheduled for launch in 2003. Both DOD and NASA are exploring these technologies for applications, such as surveillance, passive radiometry, terrain mapping, navigation, and communications; certainly this would be an opportunity for cooperative development between these two agencies. These technologies will demand government-led development since commercial applications lie far in the future.

---

[414] Randolph, Stephen P., Ibid.

[415] Das, Alok, "Choreographing Affordable, Next-Generation Space Missions Using Satellite Clusters," Technology Horizons Magazine, No:3, U.S.A., September 2000, p. 15-16.

6. UAV AND ELINT

An opportunity exists to exploit planned advances in intelligence, surveillance, reconnaissance, and the development of unmanned aerial vehicles (UAV) to address future military needs. Through all-source, coordinated intelligence fusion, it will be possible to supply the war fighter with all-weather, day or night, near-perfect battlespace awareness. This information will be of precision targeting quality and takes advantage of multiple sources to create a multidimensional view of potential targets. Early in the twenty-first century, reconnaissance UAVs will mature to the extent that reliable, long-endurance, high-altitude flight will be routine, and multiple, secure command and control communications links to them will have been developed.[416] Not only are UAVs much cheaper to operate and maintain than manned aircraft, but they have improved enormously in terms of reliability, endurance, payload capacity, and operational versatility. They are also relatively expendable, and can be used on technical intelligence collection missions that would be too dangerous for manned systems to undertake.[417]

"UAVs play a key role in the run for battlespace information dominance and will be increasingly present in future conflicts," notes Shai Shammai, Research Analyst at Frost & Sullivan.[418] Until the time frame of the Gulf conflict, basically two types of assets provided reconnaissance: manned airborne platforms and satellites. Both of these classes of collectors have positive and negative aspects. Manned platforms (U-2, SR-71, JSTARS, AWACS, Guardrail, ES-3, ATARS on F-16 and F/A-18 aircraft, etc.) provide high resolution data, are extremely flexible at adapting to multiple mission scenarios, and can loiter (with air refueling) within the conflict region up to the limitations of the crew (about eight hours). Crew limitations also limit their ability to react quickly to global conflicts. Additionally, manned platforms have extra costs and weight allowances associated with crew requirements. But the most significant limitation of manned platforms is the risk to

---

[416] Carmichael, Bruce W., Troy E. DeVine, Robert J. Kaufman, Patrick E. Pence, and Richard S. Wilcox, "Strikestar 2025", A Research Paper Presented To Air Force *2025, U.S.A.,* August 1996, Available on site: http://www.au.af.mil/au/2025/volume3

[417] Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm

[418] Space Daily Web Page, "Both Civil and Military Needs Driving European UAV Market", San Jose, 07 January 2004, Available on site: http://www.spacedaily.com/news/uav-04a.html

the crew. The American populous and government leaders are becoming increasingly sensitive to loss of life scenarios.[419]

Satellite reconnaissance, because of the principles of orbital mechanics, can see virtually anywhere in the world every day. They also collect information across wide areas and at no risk to human life. Orbital mechanics also limit a satellite's coverage of a conflict area to about 20 minutes each orbit pass, with only about three to four passes a day, depending on target latitude. Continuous coverage of a conflict region from space would require a large satellite constellation (similar to the Global Positioning System constellation) costing billions of dollars. Also, satellite orbits are constant, enabling an enemy to easily predict when the satellites will observe the region and, therefore, conceal activities and forces. Satellites also tend to be expensive and considered "national assets", primarily used by the national decision makers on strategic and operational issues. Dissemination of satellite-derived intelligence to the tactical battlefield commander was a major fault of the national systems during the Gulf conflict.

UAVs have demonstrated their ability to fill the gap between manned airborne and satellite reconnaissance platforms. UAVs provide complimentary capabilities to the commander by conducting day or night reconnaissance, surveillance, and target acquisition (RSTA), rapid battle damage assessment (BDA), and battlefield management in highthreat or heavily defended areas where the loss of a high-value, manned system is likely but near-real-time information is required. As mentioned earlier, the Pioneer UAV system did provide critical support to coalition forces during the Gulf conflict. But significant gaps still existed among all the reconnaissance platforms. Theater commanders perceived an intelligence shortfall during the Persian Gulf conflict. A memorandum from the Under Secretary of Defense (Acquisition and Technology) (USD (A&T)) outlined the need and characteristics for a system to fill this need.[420]

UAVs break down into two major categories as a function of the payload that they carry. Intelligence, surveillance and reconnaissance (ISR) payloads include various sensors to

---

[419] Jones, Christopher A., Maj., "Unmanned Aerial Vehicles (UAVS) An Assessment of Historical Operations and Future Possibilities", US Air Command and Staff College, U.S.A., March 2003, p. 23, Available on site: www.fas.org/irp/program/collect/docs/97-0230D

[420] Jones, Christopher A., Maj., Ibid., p. 24.

collect data ranging from EO/IR (electro-optical, typically streaming NTSC video/infrared), synthetic aperture radar (SAR), to various signal intelligence sensor suites. Think of this type of UAV as a modern day U-2 that can monitor enemy troop movements, assess battle damage, and even direct smart munitions to targets without putting humans in harm's way.

Also included in this category of UAV are platforms that may ultimately perform electronic jamming and countermeasures functions. Again in the case of the Navy, this shipboard capability would eliminate the need for the forwardly deployed EA-6B Prowler piloted aircraft that performs this function today. It's also conceivable that with even more intelligent capabilities, UAVs can supplement and reduce operator workload in airborne control centers like JSTARS or AWACS.[421]

Most UAV deployments are expected to be intelligence, surveillance and reconnaissance (ISR) applications. The challenge for manufacturers would be to introduce downgraded, cheaper military applications. The growing focus on homeland security solutions is the main revenue driver as the European Union expands and new ISR needs emerge.[422] UAVs could provide earlier detection and tracking of low-flying aircraft traversing ridges, keeping the E-3 updated via datalink. In a signals-ELINT role, UAVs could triangulate faster, and in a search-and-rescue or optical-collection role, they could use real-time video imaging and spot cameras to help the JSTARS get a closer look at troop advancements, downed airmen, enemy vehicles, or bunkers. Real-time battlefield identification could become more accurate and expedient, giving field commanders an added tool on the battlefield. The objective here is to create a highly adaptable system that would help minimize line-of-sight and orbit restrictions—the possibilities are virtually endless.[423] And their role is expanding beyond just surveillance and RECON, with more autonomy, on-board intelligence and lethality.[424]

[421] Ciufo, Chris A., "UAVs: New Tools for the Military Toolbox", COTS Journal, U.S.A., June 2003, p. 68-69.
[422] Space Daily Web Page, "Both Civil and Military Needs Driving European UAV Market", San Jose, 07 January 2004, Available on site: http://www.spacedaily.com/news/uav-04a.html
[423] Ortiz, David, "A New Role for Today's UAVs", Aerospace Power Journal, Oklahoma, U.S.A., Fall 2000.
[424] Ciufo, Chris A., Ibid, p.67.

Although UAVs were successful in providing critical information during the Gulf conflict, they could not provide high resolution data covering large areas. The Pioneer system was basically a video camera flying about 5,000 feet above the battlefield. But the true success of the Pioneer system was not in the quality of intelligence it provided to the battlefield commander, rather its greatest success was that of changing opinions and attitudes of military officials about the role of UAVs in future reconnaissance architectures. UAVs are a critical element of the U.S. forces' ability to obtain and retain dominant battlefield awareness (DBA), crucial aspects of supporting Joint Vision 2010 and the Air Force's concept of Global Engagement.[425]

The obvious extension of these developments is to expand UAV use to include lethal missions. In 2025, a stealthy UAV, is refered to as "StrikeStar," will be able to loiter over an area of operations for 24 hours at a range of 3,700 miles from launch base while carrying a payload of all-weather, precision weapons capable of various effects. Holding a target area at continuous risk from attack could result in the possibility of "air occupation." Alternatively, by reducing loiter time, targets within 8,500 miles of the launch and recovery base could be struck, thus minimizing overseas basing needs.

A concept of operations for this UAV will include various operation modes using the information derived from multiple sources to strike designated targets. In developing and fielding this type of a weapon system, a major consideration will be carrying weapons aboard unmanned vehicles. However, the StrikeStar UAV concept has the potential to add new dimensions to aerial warfare by introducing a way to economically and continuously hold the enemy at risk from precision air attack.[426]

The need for technologies is nearly limitless, and making UAVs a growth industry. Examples of funded program initiatives include improved sensors, signal processing and reconfigurable computing subsystems, streaming video and audio compression techniques, multi-modal sensors (EO/IR, SAR, SIGINT/ELINT) that eliminate the need to swap

[425] Jones, Christopher A., Maj., Ibid, p. 25.
[426] Carmichael, Bruce W., et al., Ibid.

payload packages with each mission, fuel cells for endurance and stealth, compact avionics and robotics, lighter weight weapons, and on-platform communications buses.[427]

Certainly UCAVs would demand more autonomy in order to successfully deliver ordnance. But this raises the stakes for higher performance technology that can on one hand fulfill the mission role, while on the other make the platform even safer for friendlies. Understandably, the Army and Marines are a bit apprehensive over intelligent weapons flying overhead, spotting targets, and killing them. Moreover, most UAVs may at some point be flying in civilian airspace either en route to a mission location or as part of the mission itself. This raises the stakes for collision avoidance technology that works passively and stealthily (without emitting radar pulses), but doesn't add much weight to the payload or reduce the *on-station* capability.

Planning Task Force for Acquisition, Technology and Logistics recently outlined mission areas that have critical deficiencies and must be solved. One area cited is airborne electronic attack, both the ability to protect the UAV from being jammed (and hence either failing to perform its mission, or worse, causing it to crash), as well as to provide offensive electronic attack capability.[428]

One of the most promising future possibilities is the increased use of unmanned aerial vehicles (UAV) to perform tasks previously accomplished by manned aircraft. Unmanned aircraft have the potential to significantly lower acquisition costs in comparison with manned alternatives. Unmanned aircraft can also be tasked to fly missions deemed unduly risky for humans, both in an environmental sense (i.e., extremely high-altitude or ultra long-duration flight) as well as from the combat loss standpoint.

6.1. UAVs' HISTORICAL DEVELOPMENT

UAVs are not new; they have a long history in aviation. Pilotless aircraft, whether as aerial targets or for more belligerent purposes, have a history stretching back to the First World War.[429] UAV employment has supported military reconnaissance needs since the First

[427] Ciufo, Chris A., Ibid, p. 70.
[428] Ciufo, Chris A., Ibid, p. 70-71.
[429] Munson, Kenneth, "Jane's Unmanned Aerial Vehicles and Targets", Jane's Information Group Limited, Surrey, UK, 1996.

World War. Historically, most UAVs have been very small, some even hand-launched like toy radio-controlled airplanes, and mostly confined to the reconnaissance role.

The German uses of the V-1 in World War II showed that unmanned aircraft could be launched against targets and create a destructive effect.[430] Unfortunately, the V-1 was a "use and lose" weapon. Once launched, it was designed to destroy itself as well as the target. The Japanese tried a similar ploy late in World War II. They launched balloon bombs laden with incendiary and other explosives. The United States also tried a type of UAV during World War II called Operation Aphrodite. There were some rudimentary attempts to use manned aircraft in an unmanned role. The technology was not enough to launch these systems on their own and control them.[431]

6.1.1. UAV and ELINT During Cold War

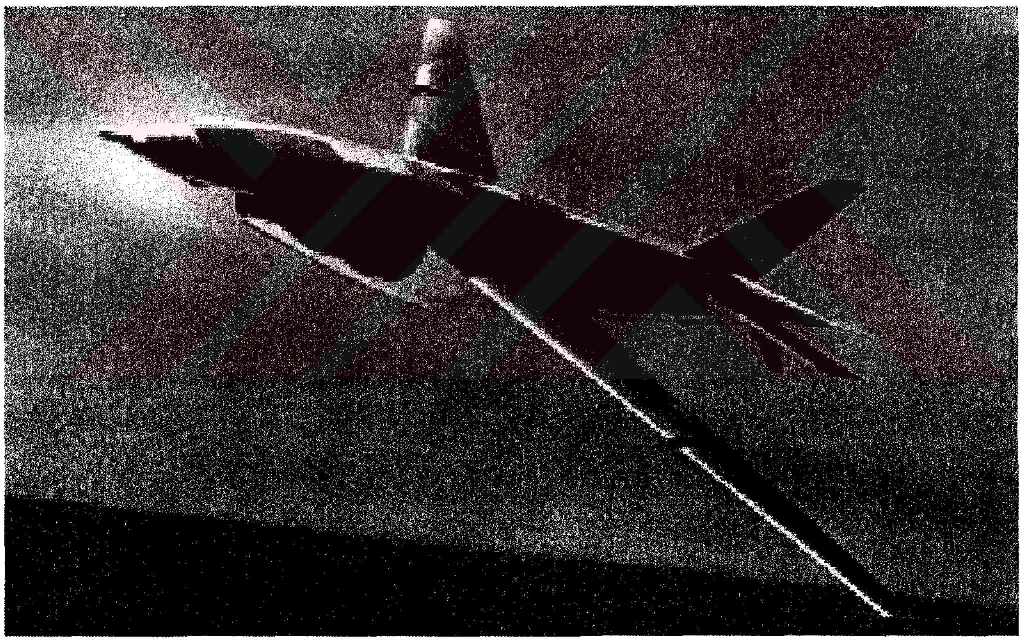


Figure 6.1: AQM-34 Lightning Bug

During this intense time of the Cold War, U.S. policy centered on to stay abreast of the Soviet's strategic nuclear posture. US did not want to experience a nuclear "Pearl Harbor."

[430] Gorn, Dr Michael H., "Prophecy Fulfilled: Toward New Horizons and Its Legacy", Air Force History and Museums Publications, U.S.A., 1994, p.28-35.
[431] Garamone, Jim, "From the U.S. Civil War To Afghanistan: A Short History of UAVs", American Forces Press Service, Washington, U.S.A., April 2002, Available on site: http://www.defendamerica.mil/articles/apr2002/a041702a.html

Of greatest concern was the Soviet intercontinental ballistic missile (ICBM) program under development in the heart of the Soviet Union.[432] In the 1950s, the US developed an unmanned intercontinental-range aircraft, the Snark. Designed to supplement Strategic Air Command's manned bombers in nuclear attacks against the Soviet Union, this unmanned aircraft also destroyed itself as it destroyed the target. In effect, these were precursors of today's cruise missile.

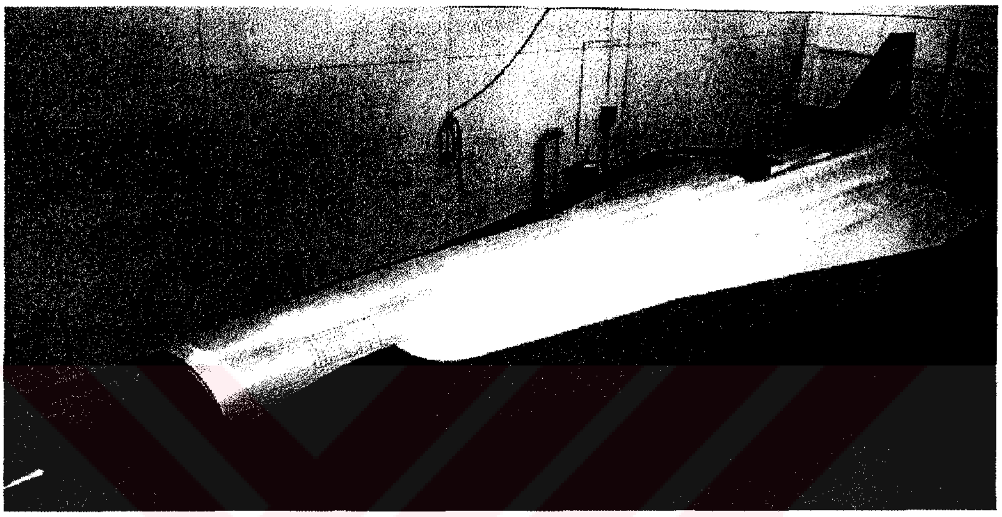


Figure 6.2: D-21 Tagboard

In the United States, the UAV has normally been associated with the reconnaissance mission and designed to be a recoverable asset for multiple flight operations. The remotely piloted vehicles (RPV) of the early 1960s were developed in response to the perceived vulnerability of the U-2 reconnaissance aircraft, which had been downed over the Soviet Union in 1960 and again over Cuba in 1962.[433] "Red Wagon" was the code name for a 1960 project by Ryan Aeronautical Company to demonstrate how its drones could be used for unmanned, remotely guided photographic reconnaissance missions.[434] The Air Force's development of a new UAV reconnaissance system evolved from a target drone airframe

[432] Jones, Christopher A., Maj., Ibid, p. 1.
[433] Crickmore, Paul F., "Lockheed SR-71 - The Secret Missions Exposed", Osprey Aerospace, London, UK, 1993, p. 9-16.
[434] Wagner, William, "Lightning Bugs and Other Reconnaissance Drones", Aero Publishers, Inc., Fallbrook, California, U.S.A., 1982, p. 15.

(the BQM-34). As early as 1965, modified Ryan Firebee drones were used to overfly China with some losses experienced.[435]

The Cuban situation vividly demonstrated the need for quick intelligence gathering while also demonstrating the political sensitivity with using manned collection platforms. As U.S. involvement in the Vietnam War broadened, the Air Force fielded this country's first operational photo-reconnaissance unmanned aircraft, the AQM-34 Ryan Aeronautical "Lightning Bug."

In 1962, US began development of the D-21 supersonic reconnaissance drone (Figure 6.2). The D-21 (code-named "Tagboard") was designed to be launched from either the back of a two-seat A-12 (designated M-12 for this project) or from under the wing of a B-52H.[436] The drone could fly at speeds greater than Mach 3.3, at altitudes above 90,000 feet, and had a range of 3,000 miles.[437] At the end of the D-21's mission, the reconnaissance and navigation equipment as well as the exposed camera film could be parachuted away from the airframe and be recovered by a specially equipped aircraft.[438]

Figure 6.3: BQM-34 UAV with Stubby Hobo

[435] Wagner, William, Ibid, p. 115.
[436] Miller, Jay, "Lockheed's Skunk Works: The First Fifty Years", Aerofax, Inc., Arlington, Texas, U.S.A., 1993, p.134-135; Rich, Ben R., "Skunk Works", Little, Brown and Co., New York U.S.A., 1994, p.267.
[437] Miller, Jay, Ibid, p. 141.
[438] Crickmore, Paul F., Ibid, p. 38.

The best known United States UAV operations were those conducted by the United States Air Force during the Vietnam War. Ryan BQM-34 (Ryan designation: Type 147) "Lightning Bug" drones were deployed to the theater in 1964.[439]

In addition to the reconnaissance role, in 1971 and 1972, drones were armed with Maverick missiles or electro-optically guided bombs (Stubby Hobo) in an attempt to develop an unmanned defense suppression aircraft to be flown in conjunction with manned strike aircraft (Figure 6.3).[440]

6.1.2. Vietnam War and UAV & ELINT

Reconnaissance drones were first developed by the US for spying on Vietnam, China and North Korea in the 1960s and early 1970s.[441] During the Vietnam War, technology started to make UAVs more effective. They were used fairly extensively and were called drones. Large numbers of modified Firebee drones overflew North Vietnam. Lightning Bug capabilities evolved to not only support photographic missions, but subsequent modifications also supported other missions: night photo, real-time video, electronic intelligence (ELINT) that increased the safety of manned aircraft flying over hostile areas, electronic counter measures (ECM), real-time communications intelligence (COMINT), PSYOPS leaflet dropping and surface-to-air missile (SAM) radar detection, location and identification.[442] Some UAV missions, conducted at very low altitudes, provided critical battle damage assessments (BDA) to confirm that strike aircraft had hit their assigned targets.

The Strategic Air Command (SAC) 100th Strategic Reconnaissance Wing (SRW) operated these drones, mostly employing them in Southeast Asia. Most missions involved photography and real-time video, electronic intelligence (ELINT), and communications intelligence (COMINT). Some UAV missions, conducted at very low altitudes necessitated by poor weather conditions, provided battle damage assessments (BDA) to confirm that

---

[439] Longino, Dana A., Lt Col, "Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios", Air University Press, Maxwell AFB, Alabama, U.S.A., December 1994, p. 3; Wagner, Ibid, p. 52.
[440] Wagner, William, Ibid, p. 185.
[441] Wagner, William, Ibid, p.54-58, 65, 74; and Aaart, Dick van der, "Aerial Espionage: Secret Intelligence Flights by East and West", Arco/Prentice Hall, New York, U.S.A. 1985, p.72-73.
[442] Weatherington, Dyke, "Unmanned Aerial Vehicle Roadmap Report", Technology and Logistics Magazine, U.S.A., 18 March 2003.

U.S. strike aircraft had hit their assigned targets.[443] Flights over Communist China started in 1964, proceeding on to sorties over North Vietnam, Loas and Cambodia. With aircraft flying initially from Bien Hoa AB, South Vietnam, and later from U-Tapao, the program was a huge success. Not only did the UAVs provide photographs and ELINT on crucial enemy MiG and SAM defenses, they also acted as "clay pigeons" to determine the precise command codes used to detonate the enemy SAMs' warheads. This intelligence kept U.S. strike and bomber aircraft safe from all but the worst ravages of the Soviet-supplied SAMs, affording U.S. aircraft the ability to jam the incoming missiles at opportune moments.[444]

In August-October 1964, following the Gulf of Tonkin incident and in the context of US preparations for large-scale military intervention in Vietnam, the US began to use Ryan Model 147 drones, called Lightning Bugs, for reconnaissance flights over southeastern China. The Lightning Bugs, together with DC-130 Hercules 'mother aircraft', were based at Kadena on Okinawa. The typical mission involved launch of the drones from airspace near Hainan Island, after which they would climb to some 60,000 feet and fly over Hainan, Guandong and Fujian, and land at Taoyuan air base in Taiwan, mapping Chinese intelligence and air defense facilities in these areas. Some flights were accompanied by US ELINT aircraft, which would record and analyze the electronic activity generated by Chinese air defense systems attempting (often successfully) to shoot down the drones.[445]

The first SIGINT flights began in October 1965, using Model 147E Lightning Bugs, flown from Bien Hoa Air Force Base in South Vietnam. A particularly memorable flight took place on 13 February 1966, when a 147E drone was able to 'sniff' the emissions associated with the proximity fuse on SA-2 surface-to-air missiles, and to relay the vital information before being destroyed.[446] After a US Navy EC-121 SIGINT aircraft was shot down by North Korean fighters in April 1969, another version of the Lightning Bug, called the Model 147TE or Combat Dawn, was developed for SIGINT operations against North Korea. A larger model, the 147TF, with an 8-hour time-on-station and 'improved SIGINT

---

443 Jones, Christopher A., Maj., Ibid, p. 9.
444 Thornborough, Anthony M., "Sky Spies: Three Decades of Airborne Reconnaissance", Arms and Armor Press, London, England, 1993, p. 35.
445 Wagner, William, Ibid, p.54-58, 65, 74; and Aaart, Dick van der, Ibid, p.72-73.
446 Bamford, James, "Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World", Century, London, U.K., 2001, p.321-322.

gear', became operational in 1973. These UAVs flew almost 500 missions from 1970 to 1975.[447]

The intelligence community tasked the Lightning Bug under a classified operations order code-named Buffalo Hunter. The first operational flight for the Lightning Bug in Southeast Asia was 20 August 1964; the last flight was on 30 April 1975. In all, the 100th SRW flew 3,435 operational sorties in Southeast Asia. During the course of the war the Lightning Bug provided some invaluable results. Some accomplishments were:[448]

- Obtained the first photographic evidence of SA-2 missiles in North Vietnam.
- Took the first photographs of Soviet MiG-21D/E aircraft in North Vietnam.
- Obtained photographic evidence of Soviet helicopters in North Vietnam.
- Photographed an SA-2 missile detonation at close range (20 to 30 feet).
- Provided the only daily low altitude bomb damage assessment (BDA) of B-52 raids during "Linebacker II."

6.1.3. Arab-Israel Conflict and UAV & ELINT

In 1970, the Israeli government requested U.S. assistance in overcoming the Egyptian-Soviet air-defense system along the Suez Canal. Although the U.S. Air Force had purposely ignored drone weapons delivery, the Israeli dilemma highlighted a fact that NATO countries could face the same threat in Europe. In 1971 the Air Force received the "Have Lemon" program to demonstrate new approaches to accurately delivery stand-off weapons. Within a year of contract initiation, Air Force successfully demonstrated the launch of a Lightning Bug drone that subsequently launched an AGM-65 Maverick electro-optical seeking missile against a radar control van. The demonstration program also included the Lightning Bug dropping an electro-optical glide bomb, "Stubby Hobo," against a target. Although the demonstration program succeeded and was ready for deployment in early 1972, the drone weapon program never deployed operationally. In Vietnam, the enemy camouflaged their SAM sites very well, hindering the ability of the drone operator and the missile system to identify the targets. Even though the drone

---

[447] Vectorsite.net Web Page, "The Lightning Bug Reconnaissance Drones", 1 February 2002, Available on site: http://www.vectorsite.net/avuav3.html.
[448] Jones, Christopher A., Maj., Ibid, p. 10.

weapon delivery never deployed, the U.S. began realizing the utility of using a UAV attack system to go in on the first wave and soften up the target so that manned aircraft could go in and finish the job.[449]

The Israelis effectively used UAVs in 1973 and 1982. In the 1973 Yom Kippur War, the Israelis used UAVs as decoys to draw antiaircraft fire away from attacking manned aircraft. In 1982, UAVs were used to mark the locations of air defenses and gather electronic intelligence information in Lebanon and Syria. During the war, the Israelis used UAVs to continually monitor airfield activities and use the information that was gathered to alter strike plans.[450]

Several of the UAVs we know today owe much to Israel, which develops UAVs aggressively. The U.S. Hunter and Pioneer UAVs are direct derivatives of Israeli systems.[451]

6.1.4. The Gulf War, UAV and ELINT

During Operation Desert Storm, coalition commanders could see across the entire battlespace, understand infinite details of the enemy, and lead coalition forces to a new level of precision engagement never seen before. A wide spectrum of collection platforms; satellites, Joint STARS, AWACS, UAVs, and others collected electronic intelligence (ELINT). The U.S. Army, Navy, and Marine Corps capitalized on their use of UAVs to help accomplish the task of battlefield-intelligence (ELINT) gathering, sometimes referred to as intelligence preparation of the battlefield.[452]

The employment of UAVs clearly demonstrated their ability to complement other information systems, providing a total battlespace view to all commanders, from the tactical battlefield commander to the operational-level decision makers.[453] According to the interim DOD report to Congress on Desert Shield and Desert Storm, UAVs performed

---

449 Jones, Christopher A., Maj., Ibid, p. 12-13.
450 Wagner, William, Ibid, p.6.
451 Garamone, Jim, "From the U.S. Civil War To Afghanistan: A Short History of UAVs", American Forces Press Service, Washington, U.S.A., April 2002, Available on site: http://www.defendamerica.mil/articles/apr2002/a041702a.html
452 Jones, Christopher A., Maj., Ibid, p. 17-18.
453 Longino, Dana A., Lt.Col, "Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios", Air University Press, Maxwell AFB, Alabama, U.S.A., December 1994, p. 9.

"direct and indirect gunfire support, day and night surveillance, target acquisition, route and area reconnaissance and BDA". The Pioneer system "appears to have validated the operational employment of UAVs in combat".[454]

Figure 6.4: Pioneer on Sea Duty

The United States rediscovered the UAV in the Gulf War. The Pioneer UAV (Figure 6.4) was purchased by the Department of the Navy to provide inexpensive, unmanned, over-the-horizon targeting, reconnaissance, and battle damage assessment (BDA). The Army purchased the Pioneer for similar roles and six Pioneer systems (three Marine, two Navy, and one Army) were deployed to Southwest Asia to take part in Desert Storm. During the war, Pioneers flew 330 sorties and more than 1,000 flight hours.[455] Once, during Desert Storm, Iraqi troops actually surrendered to a Pioneer. At the time, the battleship USS Missouri used its Pioneer to spot for its 16-inch main guns and devastate the defenses of

[454] Jones, Christopher A., Maj., Ibid, p. 18.
[455] Longino, Dana A., Lt.Col, Ibid, p. 9.

Faylaka Island, which is off the Kuwaiti coast near Kuwait City. Shortly after, while still over the horizon and invisible to the defenders, the USS Wisconsin deliberately flew its Pioneer low over Faylaka Island. When the Iraqi defenders heard the sound of the UAV's two-cycle engine, they knew they were targeted for more naval shelling.[456]

In the aftermath of the Gulf War, the United States began to look more closely at the use of the reconnaissance UAV and its possible use to correct some of the reconnaissance shortfalls noted after the war. Space-based and manned airborne reconnaissance platforms alone could not satisfy the war fighter's desire for continuous, on-demand, situational awareness information.[457] As a result, in addition to tactical UAVs, the United States began to develop a family of endurance UAVs that added a unique aspect to the UAV program.[458] Three different aircraft comprise the endurance UAV family.

6.1.5. The Yugoslavian (Bosnia) Civil War, UAV and ELINT

Following the Gulf War, the US military officials recognized the worth of the unmanned systems. An international crisis brought the UAV back into the spotlight. This time the crisis was the civil war in the former Yugoslavian republics. The Predator started life as an Advanced Concept Technology Demonstration project. The program hurried the development of the Predator along, and it demonstrated its worth in the skies over the Balkans. The Predator operates between 15,000 and 25,000 feet. It carries three sensor systems: a color video camera and synthetic-aperture radar.[459] MajGen Kenneth Israel, director of the Pentagon's Defense Airborne Reconnaissance Office (DARO), recently stated that: "Predator has done a remarkable job. It helped the general impression about UAVs in the Services and in the Department in a very positive way. Because it's been so successful, I think there's been an awakening. It has sparked support for UAVs across the board and for our planned family of UAVs."[460]

The first deployment to the Balkans supporting NATO, UN and U.S. forces, from July through November 1995, involved three Predators with only EO/IR sensors and the LOS

[456] Garamone, Jim, Ibid.
[457] Longino, Dana A., Ibid, p. 7.
[458] Zaloga, Steven J., "Unmanned Aerial Vehicles", Aviation Week and Space Technology, U.S.A., 8 January 1996, p. 87.
[459] Garamone, Jim, Ibid.
[460] Jones, Christopher A., Maj., Ibid, p. 25-26.

and UHF SATCOM data links. The system operated from a base in Albania. The system's unique live video and dynamic retasking capabilities increased the commander's battlefield awareness and allowed him to focus his assets at the right place and time. Many credit the Predator with providing NATO commanders with the critical intelligence to begin a bombing campaign that, in turn, led to the Dayton Peace Accord signed in December 1995. Adverse weather was the principle limitation to system abilities. In-flight icing, high winds, precipitation and cloud cover limited Predator's ability to perform planned missions.

The Predator system deployed again to the Bosnian AOR in March 1996, this time based out of Hungary. This time the vehicles included a SAR sensor, the commercial SATCOM link, active de-icing capabilities for the wings, and an expanded information dissemination infrastructure.

During the operational deployments to the Balkans, the system successfully integrated into a complex C^4I architecture. However, the system operators experienced reluctance from airspace managers to integrate it with manned aircraft. The resulting restrictions on Predator employment hampered its ability to contribute to the intelligence collection missions. The procedures for the JFACC's airspace control authority (ACA) to control UAV operations, it is clear from all the Predator deployments that more effort is needed to familiarize the JFACC staff with UAV operations within controlled airspace.[461]

6.1.6. Operation Enduring Freedom in Afghanistan

The Predator unmanned aerial vehicle (UAV) has been used in combat, launching Hellfire missiles at targets in Afghanistan. This was represent the first use of the Predator as a weapons platform.

A demonstration of the "weaponization" of Predator is underway and being conducted in two phases. The first is the safe launching of Hellfire from Predator at low altitude. An earlier version of this laser designator was first fitted to unarmed Predators during Operation Allied Force to designate targets for other armed platforms over the former Yugoslavia. The second phase is engagement of targets "from an operationally significant

---

[461] Jones, Christopher A., Maj., Ibid, p. 32-33.

altitude". She did not define what altitude would be "operationally significant," although this would presumably be over 15,000 and likely over 16,000 feet, which according to informed sources is the standard deck of air operations.

The K-class, or Hellfire II, is the currently fielded version. Improvements for the K class, however, are largely internal - dual warheads for defeating reactive armor, hardened electro-optical countermeasures, semi-active laser seeker, and a programmable autopilot for trajectory shaping - while the physical characteristics of this version of the Hellfire (weight, length, etc.) remain the same as those of earlier variants. Thus, the successful demonstration of the firing of the C-class Hellfire would point to the feasibility of doing the same with the Hellfire II.

Figure 6.5: Hellfire missiles from a Predator UAV.

In a parallel development, NATO and Operation Enduring Freedom allies US and UK are working on ways to jointly operate Predators from an independent Tactical Control System (TCS). The TCS was originally envisioned as a common control system for all medium UAVs being considered for the US armed forces: the Air Force's Predator, the Army's Shadow, and the Navy's Fire Scout. NATO quickly signed on to the concept, issuing STANAG 4586 defining a requirement for a common UAV-control system. The TCS is widely regarded as a leading proposal. The UK has acquired a TCS system, and there are plans to demonstrate the capability for allied operators to hand control from one station to another. UK operators take command of a US Predator in flight in support of their own forces, receiving reconnaissance information and ELINT via datalink, and perhaps even launching Hellfire missiles.[462]

The Global Hawk is a jet-powered UAV taking to the skies over Afghanistan. Still under development, it is at the same stage the Predator was when it first flew over Bosnia. The Global Hawk operates around 60,000 feet and its suite of sensors is akin to what the U-2 reconnaissance plane carries. Global Hawk does not carry a very sophisticated signal intelligence system. But tests show the Global Hawk has great potential in this area and the Air Force continues to develop its full capability.[463]

In northeast Asia, China is the only country with an operational UAV capability, including ELINT and EW systems. The Chinese Air Force's primary long-range UAV is the WZ (Wu Zhen, or unmanned reconnaissance) -5, better known as the Chang Hong-1, based on US reconnaissance drones shot down over China in the 1960s. Production began in the late 1970s, and some were used in the Sino-Vietnam border conflict in 1979.[464] The latest version of the Chang Hong is a prospective ELINT platform.[465] In addition, according to a report by the US Department of Defense, 'China already has a number of short-range and longer-range UAVs in its inventory for reconnaissance, surveillance, and electronic warfare roles', and has 'several developmental UAV programs underway related to reconnaissance, surveillance, communications, and EW'.[466] In early 2000, for example, China Aviation Industry Corporation (AVIC) released a photograph of a 'concept stage' UAV configured for ELINT and EW missions.[467]

In Southeast Asia, Singapore was the first country to invest in a substantial UAV capability. In the 1980s, the Royal Singapore Air Force acquired a batch of Scout UAVs

---

[462] Rivers, Brendan P., with Michael Puttré, "Predator Unleashes Hellfire", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com
[463] Garamone, Jim, Ibid.
[464] Sinodefense.com Web Page, "WZ-5 Unmanned Reconnaissance Aerial Vehicle", Chinese Defense Today, Available on site: http://www.sinodefense.com/airforce/aircraft/uav/wz5.asp.
[465] Fisher, Richard D., Jr., "PLAAF Equipment Trends", National Defense University Conference on PLA and Chinese Society in Transition, U.S.A., 30 October 2001, p.7-8, Available on site: http://www.ndu.edu/inss/China_Center/RFischer.htm.
[466] US Department of Defense, "Annual Report on the Military Power of the People's Republic of China: Report to Congress Pursuant to the FY2000 National Defense Authorization Act", U.S.A., 12 July 2002, p.18, Available on site: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf.
[467] Fisher, Richard D., Jr., "Questions About the Air Battle Dimension of the PLA's Developing Information-Strike Combine", National Defense University Center for the Study of Chinese Military Affairs, U.S.A., 27 October 2000, p.6-7, Available on site: http://www.ndu.edu/inss/China_Centre/paper8.htm.

from Israel, and some 40 Searcher Mark II UAVs were acquired in 1995-1997. Although these are normally equipped with electro-optical (EO) and thermal imaging sensors, some of them have undoubtedly been re-equipped for SIGINT collection missions. Singapore has also been indigenously developing several types of UAVs, including larger vehicles such as the Firefly, which could carry SIGINT systems as well as other sensors. At the Asian Airospace 2002 show in Singapore in February 2002, another Israeli company, Elisra Electronic Systems, exhibited a UAV-mounted, 20 kg ELINT system, priced at just US$10 million, which can be fitted 'on any type of UAV the customer wants'; the President of Elisra said that 'negotiations had begun with Asian armies wishing to upgrade their intelligence capabilities with a fairly cheap system'.[468]

Indonesia has been negotiating with Israel for the procurement of ELINT-equipped surveillance drones since 2000.[469] The Malaysian Ministry of Defense has begun flight testing a locally-produced Eagle UAV system, complete with a ground control station and a remote receiving station, and with a 60 kg payload capacity for carrying various sensors or EW equipment.[470]

6.2. THE US DEFENSE AIRBORNE RECONNAISSANCE OFFICE

In 1994, USA created the DARO (Defense Airborne Reconnaissance Office) to unify airborne reconnaissance architectures and enhance the acquisition of manned and unmanned airborne assets and associated ground systems. Since its conception, the DARO built an Integrated Airborne Reconnaissance Strategy for a comprehensive defense-wide airborne reconnaissance capability that will work in concert with the National Reconnaissance Office (NRO) spacebased assets. The DARO oversees the Defense Airborne Reconnaissance Program, which consists of U-2, RC-135, and EP-3 aircraft programs, non-lethal tactical and endurance UAVs, the Distributed Common Ground System (DCGS), advanced reconnaissance technology and sensors, and the Common Data Link (CDL). DARO develops, demonstrates, and acquires improved airborne

[468] Monthly Economic News on Israel, "Elisra Offers Low-Cost Intelligence-Gathering by UAV in Asia", Embassy of Israel, Singapore, Singapore, 10 March 2002, Available on site: http://www.israelbiz.org.sg.
[469] Far Eastern Economic Review, "Indonesia Seeks Israeli Defense Help", Far Eastern Economic Review, U.S.A., 5 October 2000, p.10.
[470] Jane's Defense Weekly, "Ministry Will Test *Eagle* Scout Drone", Jane's Defense Weekly Magazine, U.S.A., 24 April 2002, p.13.

reconnaissance capabilities, and performs system-level tradeoffs for manned aircraft and UAVs, sensors, data links, data relays, and associated processing and dissemination systems. The DARO also establishes and enforces commonality and interoperability standards for airborne reconnaissance systems.[471]

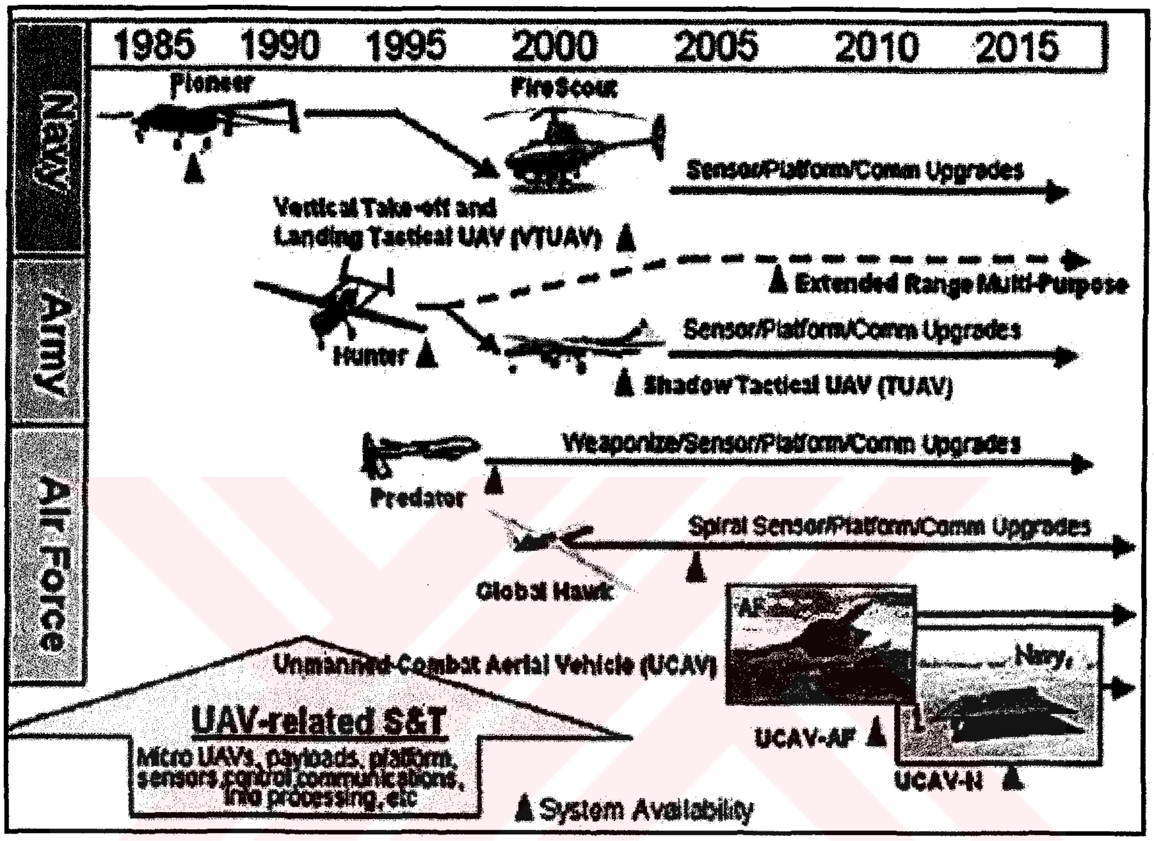


Figure 6.6: UAV evolution

Since 1964 the US has developed at least 11 different UAVs although only three entered production. The most well known is the Predator. Next, the Global Hawk is a high-altitude-endurance UAV intended for missions requiring long-range deployment and wide-area surveillance or long sensor dwell over the target area. The Hawk can fly around the world using GPS, satellite and ground communications. These aircraft are programmed to carry out missions, and like our Explorer spacecraft, are not constantly under direct control.[472]

[471] Jones, Christopher A., Maj., Ibid, p. 26.
[472] Gilleo, Ken, "The Real Warbots", Reed Electronic Group, U.S.A., 2002, Available on site: http://www.reed-electronics.com/semiconductor/index.asp

The DARO is utilizing the Advanced Concept Technology Demonstrations (ACTDs) process to demonstrate and evaluate promising UAV concepts through early user involvement in realistic operational scenarios. ACTDs started in 1994 for the Medium Altitude Endurance UAV (Tier II or Predator), the Conventional High Altitude Endurance (HAE) UAV (Global Hawk), and the Low Observable HAE UAV (DarkStar). In 1996 the DOD terminated the Hunter UAV program and initiated a Tactical UAV (TUAV or Outrider) ACTD.[473]

The DARO envisions that the future UAVs will consist of two classes -tactical and high-altitude endurance UAVs- with two systems in each class. The tactical class consists of the Outrider UAV and the Predator UAV. The UAV Joint Program Office (JPO), under the Navy Service Acquisition Executive, manages both programs. The two HAE UAVs are the Global Hawk (Tier II Plus) and the DarkStar (Tier III Minus). Both programs are being developed by the Defense Advanced Research Projects Agency (DARPA).

The HAE UAVs will be theater-level assets controlled predominately by the Joint Task Force Commander. The tactical UAVs will come under the control of lower echelons. The HAE UAVs will provide broad area surveillance over the battlefield, while the tactical UAVs will provide much more focused coverage. The HAE UAVs will provide high-resolution digital (still frame) imagery, while the tactical UAVs will provide predominately video. The HAE UAVs will provide extremely high bandwidth data; the tactical systems will provide data at much lower bandwidths. The HAE UAV systems, designed to be relocateable, will usually operate from fixed bases. The tactical systems will be fully deployable.[474]

6.3. THE PREDATOR MEDIUM ALTITUDE ENDURANCE UAV

The Predator UAV is an outgrowth of the Gnat 750 aircraft (Figure 6.7).[475] It is also known as the Tier II, or medium altitude endurance (MAE) UAV.[476] It is designed for an endurance of greater than 40 hours, giving it the capability to loiter for 24 hours over an

---

[473] Jones, Christopher A., Maj., Ibid, p. 26-27
[474] Jones, Christopher A., Maj., Ibid, p. 26.
[475] Zaloga, Steven J., "Unmanned Aerial Vehicles", Aviation Week and Space Technology, U.S.A., 8 January 1996, p. 87.
[476] Fulghum, David A., "International Market Eyes Endurance UAVs", Aviation Week and Space Technology, U.S.A., 10 July 1995, p. 40-43.

area 500 miles away from its launch and recovery base.[477] It is powered by a reciprocating engine giving it a cruise speed of 110 knots, loiter speed of 75 knots, ceiling of 25,000 feet, 450 pound payload, and a short takeoff and landing capability. The Predator carries an electro-optical (EO) and infrared (IR) sensor and was recently deployed with a synthetic aperture radar (SAR) in place of the EO/IR sensor. The Predator is also unique in its ability to collect full-rate video imagery and transmit that information in near real-time via satellite or line of sight (LOS) data link.[478]

The Predator UAV was solution to an intelligence collection shortfall that the warfighters encountered during the Persian Gulf conflict. The Commanders demanded an intelligence collection asset that could provide near real-time information, continuous coverage, and interoperability with C4I structures without endangering human life or sensitive technologies. Predator, also identified as the Medium Altitude Endurance (MAE) or Tier II UAV, is a derivative of the Gnat 750 (Tier I) UAV.[479]

Figure 6.7: The Predator UAV flew a reconnaissance mission over Afghanistan.

The Predator system has three parts: The air vehicle with its associated sensors and communications equipment, the ground control station (GCS), and the product or data

[477] Longino, Dana A., Lt.Col, Ibid, p. 27.
[478] Fulghum, David A., "Predator to Make Debut Over War-Torn Bosnia", Aviation Week and Space Technology, 10 July 1995, p. 48.
[479] Jones, Christopher A., Maj., Ibid, p. 29

dissemination system. The air vehicle carries EO (still frame and video), IR (still frame) and SAR (still frame) sensors which enable the system to acquire and pass imagery to ground stations for beyond-line-of-sight (BLOS) use by tactical commanders. The command link to the vehicle from the ground station allows the operator to dynamically retask the sensors and vehicle as requested by the field commander. Recent addition of de-icing equipment now allows transit and operation in adverse weather conditions. The "commercial off-the-shelf" (COTS) sensor hardware does not compromise sensitive technology if lost over enemy territory. The data provided is also unclassified, greatly easing releasability to coalition partners. The GCS consists of a pilot position, a payload operator position, and two data exploitation and communications positions.

Sensor data from the Predator vehicle integrates into the current theater-level C4I architectures through the TROJAN SPIRIT II (TS II) satellite communications (SATCOM) system. To provide near-real time broadcast of Predator video to numerous theater and national users simultaneously, the dissemination system uses either the Joint Broadcast System (JBS) or the TS II switch or both.[480]

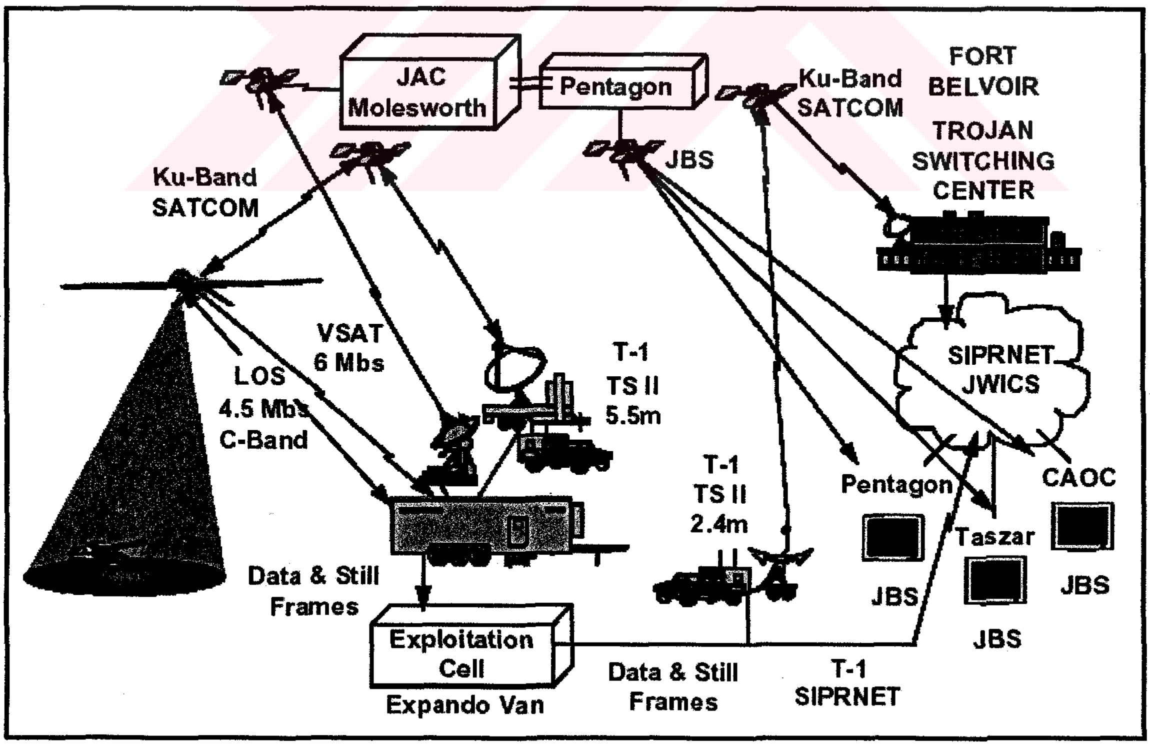


Figure 6.8: Predator EUCOM Deployment C^4I Architecture.

[480] Jones, Christopher A., Maj., Ibid, p. 30-32.

The Air Force's Predator UAV proved its military capability flying reconnaissance missions in Bosnia, and was credited with taking out one of Al-Qaeda's top lieutenants in Afghanistan with a Hellfire missile.[481] The Air Force has placed Hellfire missiles aboard the Predator. In the near future, the UAV might aim a laser at a target and attack it. The combat Predator can also mark targets with its laser for other aircraft or read targets marked by other sources. Predator is not an all-weather system, however. As a result of lessons learned in the Balkans, Predator employs a simple anti-icing system which allows it to exit the icing condition but will not allow it to conduct continuous operations in the condition. The new Predator B has a number of characteristics that will better allow it to deal with a wider range of environmental events including icing conditions.[482]

6.4. THE HIGH ALTITUDE ENDURANCE UAV (HAE UAV)

The DarkStar and Global Hawk air vehicles, with their Common Ground Segment (CGS), form the HAE UAV system. The two air vehicles are complementary: DarkStar will provide a capability to penetrate and survive in areas of highly defended, denied airspace, while Global Hawk's even greater range, endurance and multi-sensor payload will provide broad battlefield awareness to senior command echelons. The CGS will ensure interoperability between the air vehicles and transmission of their sensor products to the C^4I infrastructure, as well as provide common launch and recovery and mission control elements (LRE and MCE). Thus, the HAE UAV system will provide the joint warfighter with an unprecedented degree of broad reconnaissance-surveillance coverage and flexibility. The systems are being designated for pre- and post-strike, standoff and penetrating reconnaissance missions, cost-effectively complementing other reconnaissance assets.[483]

The US began a revolution in UAV reconnaissance by initiating the HAE UAV Program in 1994. The DARO designated the DARPA as the executive agent for the initial phases (Phases I and II) of these two ACTDs. After demonstration of acceptable flight and sensor performance, the Air Force became the executive agent for the final ACTD demonstration

[481] Sample, Doug, "Pentagon Plans Heavy Investment in UAV Development", American Forces Information Service, News Articles, Washington, USA, 18 March 2003. Available on site: http://www.dod.mil/news/Mar2003
[482] Garamone, Jim, Ibid.
[483] Jones, Christopher A., Maj., Ibid, p. 34.

(Phase III) and any follow-on acquisition activity (Phase IV). Currently, both programs plan to transition from Phase II to Phase III in January 1998.

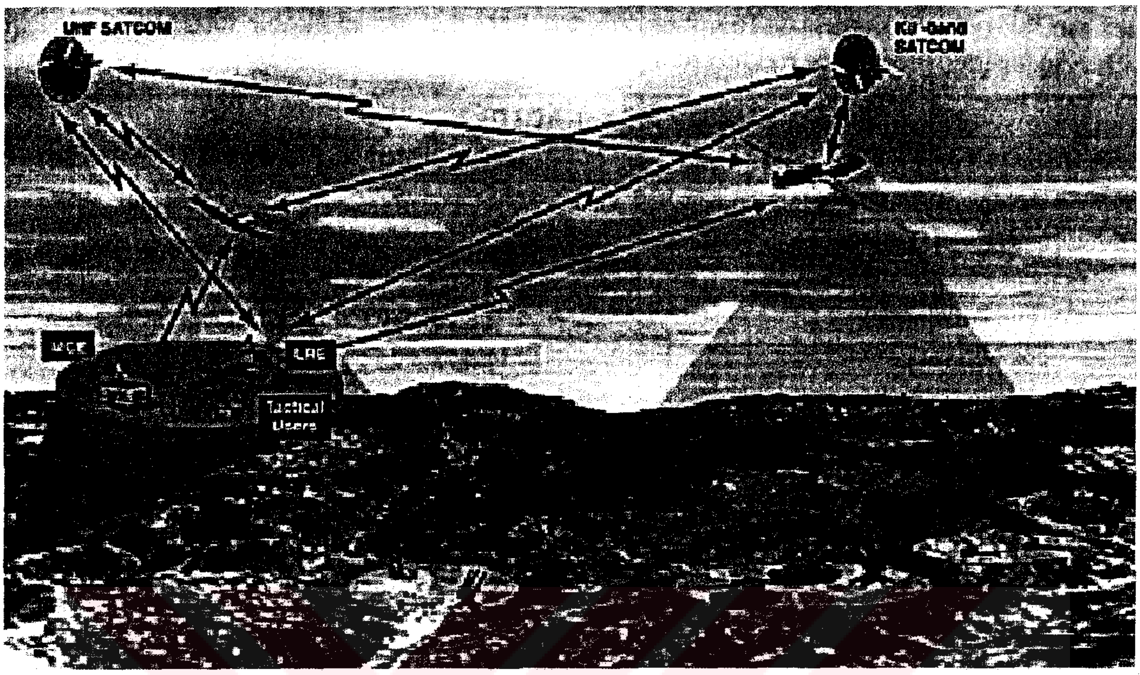


Figure 6.9: High Altitude Endurance UAV Concepts of Operations

The HAE UAV performance objectives come from three Mission Needs Statements (MNS):[484]

- Long Endurance Reconnaissance, Surveillance, and Target Acquisition (RSTA) Capability;
- Broad Area Coverage Imaging Capability;
- Assured Receipt of Imagery for Tactical Forces.

The ACTD program objectives include demonstrating military utility and developing a concept of operations (CONOPs) addressing operational control, airspace management, tasking, and data dissemination. The program management approach is revolutionary in that it allows the contractors the flexibility to adjust system specifications. Also implemented is the use of Integrated Process Teams (IPTs) that emphasize new and innovative ways of doing business. This management approach allows maximum user involvement from the outset. The users, led by USACOM, are refining program objectives

[484] Jones, Christopher A., Maj., Ibid, p. 35-36.

and assessing system operations and CONOPs. The users may identify recommendations or shortfalls that impact long-term system capabilities.[485]

6.5. THE GLOBAL HAWK HIGH ALTITUDE ENDURANCE UAV

The pre-eminent UAV is the high-altitude (above 60,000 feet), long-endurance (20 hours) Global Hawk, which was first used operationally in Operation Enduring Freedom in Afghanistan. The Global Hawk's 'baseline payload' consists of electro-optical (EO) and infra-red (IR) sensors and a synthetic aperture radar (SAR), but there are plans to produce a version with a 3,000 lb SIGINT payload by 2004-05.[486] A higher performance vehicle is the Aeronautical Conventional High Altitude Endurance (CHAE) UAV (Figure 6.10).[487] Global Hawk, also identified as the Conventional High Altitude Endurance (CONV HAE) or Tier II Plus UAV, will be the HAE UAV 'workhorse' for missions requiring long-range deployment and wide-area surveillance or long sensor dwell over the target area. The system is completely computer-operated and can be used for long-term surveillance. The high-flying Global Hawk currently carries photo reconnaissance equipment, but production versions of the system will carry electronic intelligence (ELINT) gathering materials.[488] To start with, a Global Hawk which flew to Australia from California in April 2001, the first non-stop flight across the Pacific Ocean by an autonomous aircraft, was equipped with an L-100 ELINT/ESM system to intercept ships' radio-frequency emissions and relay the approximate positional information of vessels to ground controllers, to aid the development of a future SIGINT system.[489]

It will be directly deployable from well outside the theater of operation, followed by extended on-station time in low- to moderate-risk environments. There, the system can look into high-threat areas with EO/IR and SAR sensors that provide both wide-area search and spot imagery. Because of Global Hawk's tremendous range capability, theater

---

485 Jones, Christopher A., Maj., Ibid, p. 35-36.

486 Fulghum, David A., "Long-Range UAV Exports Face Arms Control Hurdles", Aviation Week & Space Technology Magazine, U.S.A., 11 June 2001, p.64-65; Sirak, Michael, and Andrew Koch, "USAF, USN Consider New Missions for Global Hawk", Jane's Defense Weekly, U.S.A., 15 August 2001, p.5; and Wall, Robert, "Costs Spur Drive to Tweak Global Hawk", Aviation Week & Space Technology Magazine, U.S.A., 17 June 2002, p.28-30.

487 Fulghum, David A., "International Market Eyes Endurance UAVs", Aviation Week and Space Technology, U.S.A., 10 July 1995, p. 43.

488 Sample, Doug, Ibid.

489 Wall, Robert, "Global Hawk in Australia Auditions for New Role", Aviation Week & Space Technology Magazine, U.S.A., 30 April 2001, p.32-33.

coverage is available at H-hour (vice days to weeks for deployment and initiation of operations for tactical assets). The vehicle achieves a high degree of survivability by its very high operating altitude and self-defense measures.[490] It is designed to fulfill a post-Desert Storm requirement of performing high-resolution reconnaissance of a 40,000 square nautical mile area in 24 hours. The Global Hawk is designed to fly for more than 40 hours giving it a 24-hour loiter capability over an area 3,000 miles from its launch and recovery base.[491]

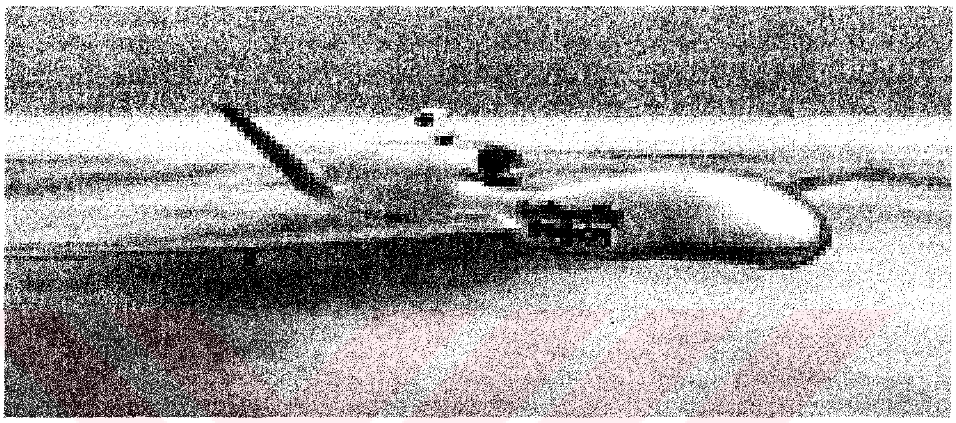


Figure 6.10: The Global Hawk UAV

US completed the final Global Hawk aircraft design review in May 1996. Full air vehicle assembly was completed in September 1996. Subsystem checkout is on-going as of this report. DARPA occurred for the first flight in the Fall 1997. After that the system will perform a series of aircraft flight and system tests and initial user demonstrations. The operational demonstrations of the full HAE UAV system began in mid-1998.

In light of Predator's successful wide dissemination of imagery via JBS satellites during its second Bosnia deployment, comparable scenarios are being examined for this longer-range UAV under a Global Hawk-Airborne Communications Node (ACN) system concept. The ACN concept envisions a communications node payload for the UAV to provide gateway

[490] Jones, Christopher A., Maj., Ibid, p. 39.
[491] Fulghum, David A., "International Market Eyes Endurance UAVs", Aviation Week and Space Technology, U.S.A., 10 July 1995, p. 43.

and relay services to surface and air forces. This capability would specifically enhance the commander's Dominate Battlefield Awareness (DBA) and Information Superiority.[492]

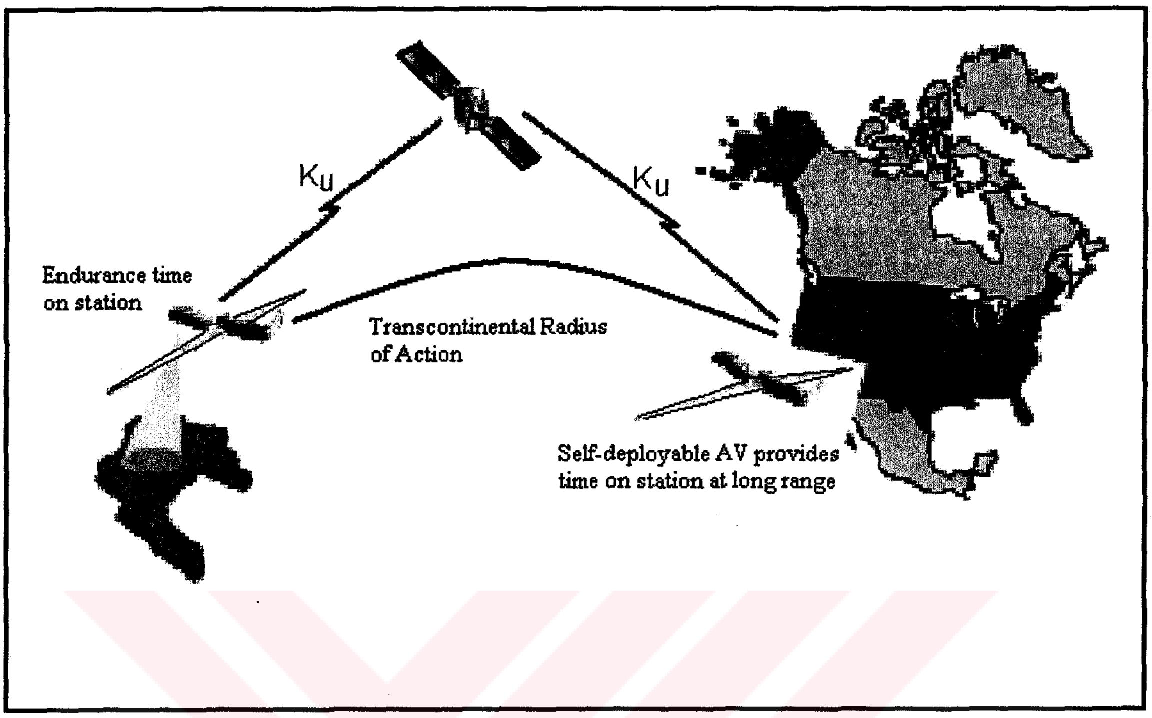


Figure 6.11: Global Hawk Employment Concept

Two flight tests have confirmed the first successful operation of a German electronic-intelligence (ELINT) sensor onboard the Global Hawk unmanned aerial vehicle (UAV) as part of ongoing risk-reduction efforts to prepare UAV for deployment to Germany. The tests were a first step toward possible future development of a German-owned and operated Global Hawk derivative -the Euro Hawk- considered as a potential replacement for Germany's aging Atlantic maritime-patrol aircraft. The sensor-produced in Germany and integrated by Global Hawk. It was able for the first time to detect radar transmissions from emitters.[493]

The Global Hawk is a jet-powered still under development. The Global Hawk operates around 60,000 feet and its suite of sensors is akin to what the U-2 reconnaissance plane carries. Tests show the Global Hawk has great capability to develop sophisticated

[492] Jones, Christopher A., Maj., Ibid, p. 40.

[493] Rivers, Brendan P., "Global Hawk Preps for German - European Report", Journal of Electronic Defense, U.S.A., January 2003. Available on site: http://www.jedonline.com

electronic intelligence (ELINT) system and the Air Force continues to develop its full capability.[494]

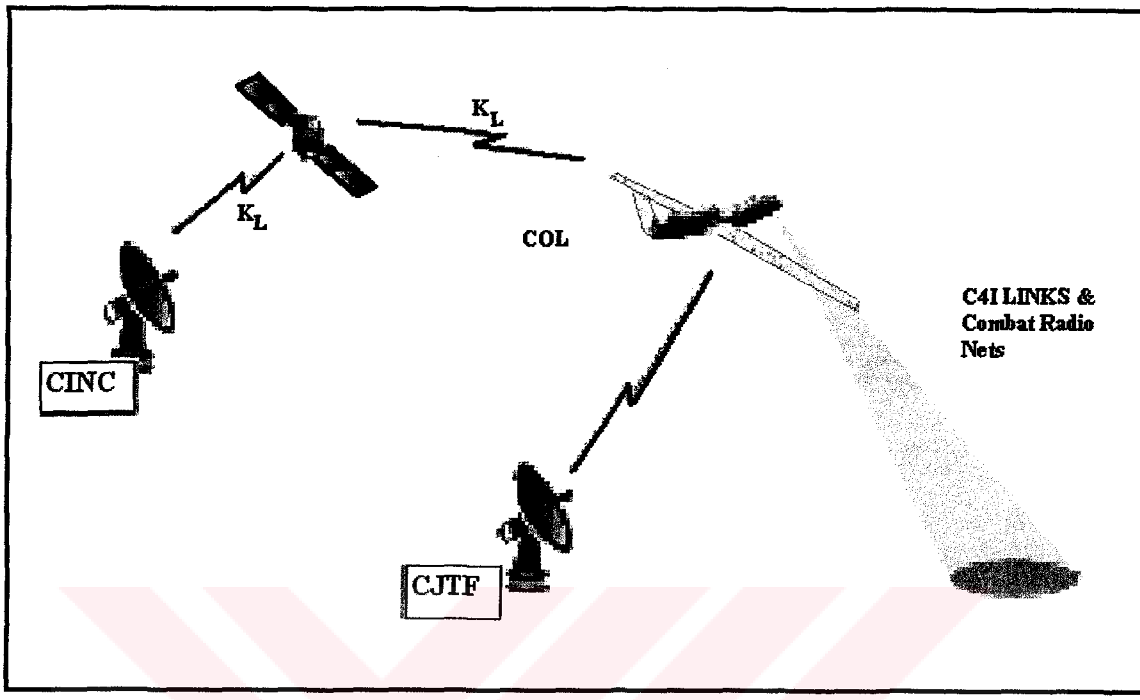


Figure 6.12: Global Hawk Airborne Communications Node Concept

Australia plans to acquire six Global Hawk UAVs in 2004 for broad-area surveillance purposes. Australian officials have said that they would like to include a SIGINT capability in this program.[495] Japan is also a likely customer for the Global Hawk system.[496]

6.6. THE DARKSTAR LOW OBSERVABLE HAE UAV

The low observable high altitude endurance (LOHAE) UAV (Tier III- or DarkStar) is the final member of the DARO family of endurance UAVs (Figure 6.13). DarkStar is designed to image well-protected, high-value targets with either SAR or EO sensors.[497] DarkStar will provide critical imagery intelligence (IMINT) and electronic intelligence (ELINT) from highly defended areas. The vehicle design trades performance and payload capacity for survivability features against air defenses, such as its use of low observable

---

[494] Garamone, Jim, Ibid.
[495] Garamone, Jim, Ibid.
[496] Vectorsite.net Web Page, "US Endurance UAVs", 1 February 2002, Available on site: http://www.vectorsite.net/avuava.html.
[497] Zaloga, Steven J., "Unmanned Aerial Vehicles", Aviation Week and Space Technology, U.S.A., 8 January 1996, p. 90-91.

technologies to minimize the air vehicle's radar return. The air vehicle will self-deploy over intermediate ranges and carry either a SAR or EO payload.[498]

It will be capable of loitering for eight hours at altitudes above 45,000 feet and a distance of 500 miles from its launch and recovery base.[499] DarkStar can be flown from runways shorter than 4,000 feet. DarkStar's first flight occurred in March 1996, the first fully autonomous flight was occurred using differential GPS.

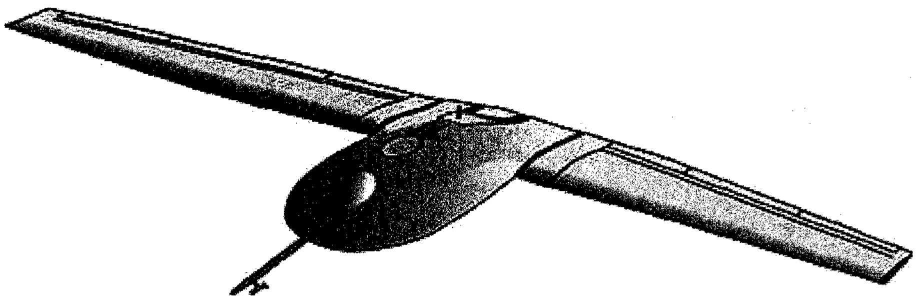


Figure 6.13: DarkStar UAV

Of significant interest to this UAV is its ability to radiate a SAR sensor but remain stealthy. The SAR sensor uses a low power, low probability of intercept (LPI) waveform and a low radar cross section, sidelobe suppression antenna. In the search mode, this SAR will provide strip images about 5.6 NM wide. Also, both the SAR and EO sensors only look-out the left side of the aircraft. [500]

US's new endurance UAVs, along with manned airborne reconnaissance aircraft, are designed to meet Joint Requirements Oversight Council (JROC) desires for the development of reconnaissance systems that are able to maintain near perfect real-time knowledge of the enemy and communicate that to all forces in near-real-time. US's goal is "extended reconnaissance", which is "the ability to supply responsive and sustained intelligence data from anywhere within enemy territory, day or night, regardless of weather, as the needs of the war fighter dictate".[501] The objective is to develop by the year

[498] Jones, Christopher A., Maj., Ibid, p. 41
[499] Zaloga, Steven J., Ibid, p. 1.
[500] Jones, Christopher A., Maj., Ibid, p. 41-42.
[501] Zaloga, Steven J., "Unmanned Aerial Vehicles", Aviation Week and Space Technology, U.S.A., 8 January 1996, p. 1.

2010, a reconnaissance architecture that will support the goal of "extended reconnaissance".

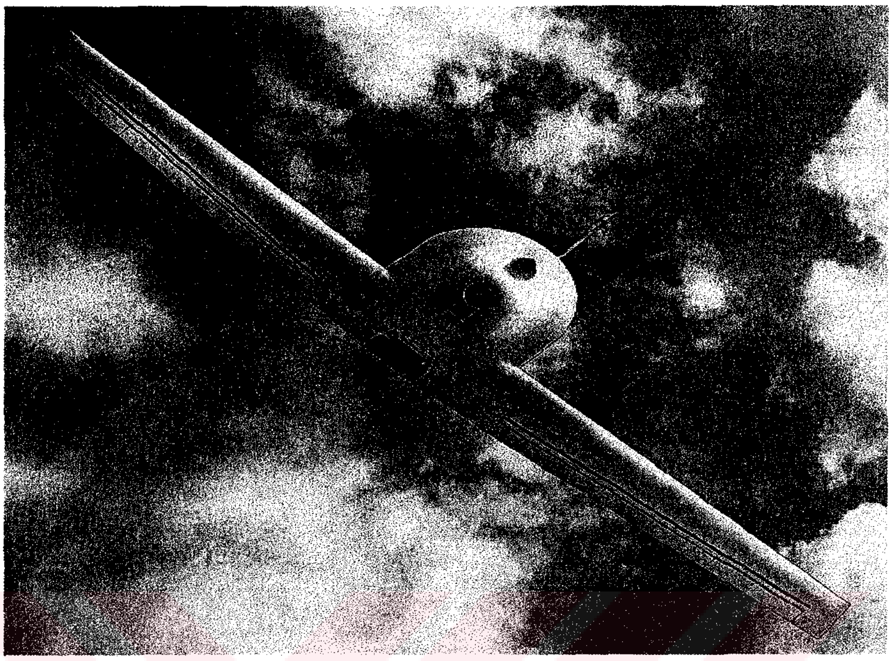


Figure 6.14: The DarkStar UAV

To do this, US will consolidate platforms, introduce endurance and tactical UAVs, emphasize all-weather sensors as well as multispectral optical sensors, improve information systems connectivity to the war fighter through robust line-of-sight and over-the-horizon communications systems, produce scaleable and common-use ground stations, and focus on the benefits of interdisciplinary sensor cueing.[502] In conjunction with spaceborne and other surveillance assets, this objective architecture will provide the war fighter and command elements with near-perfect battlespace awareness.

The seamless integration of airborne and spaceborne reconnaissance and surveillance assets, along with robust, on-demand communications links, coupled with the experience in long-endurance, high-altitude UAVs made possible by current DARO efforts, will lead to the next step in the development and employment of unmanned aerial vehicles-the long-endurance, lethal, stealthy UAV. A possible name for this new aircraft is "StrikeStar".

---

[502] Zaloga, Steven J., Ibid, p. 4.

6.7. ADVANCED CONCEPT TECHNOLOGY DEMONSTRATIONS (ACTD)

Except for the Pioneer and Hunter UAV programs, all recent UAV developments are (or have been) ACTDs. The Predator program was the first ACTD to transition to a formal acquisition program, and its lessons learned are being applied to the other UAV programs. ACTDs, an acquisition philosophy started in 1994, are intended to be quick-development programs designed to get mature technologies into the hands of users for early evaluation of operational utility. These programs should complete development and demonstrations within two to three years; compared to the routine ten equivalent years for the traditional acquisition program. ACTDs are unique in that they focus on demonstrating warfighter determined essential capabilities and mission potential.[503]

The UAV JPO is conducting proof-of-principle demonstrations of mature payloads to evaluate their suitability and utility for tactical UAV applications. Currently, the JPO is utilizing the Pioneer and Hunter UAVs to test several different payload reconnaissance sensor packages, as well as a few non-reconnaissance payloads. The potential missions that these payloads could support are: meteorological, nuclear/biological/chemical (NBC) detection, ELINT, COMINT, hyperspectral imaging, foliage penetration SAR imaging, mine detection, laser designator/rangefinder, and radar and radio/data link jamming. None of these demonstrations are outside the "box" of the traditional reconnaissance mission areas, for two reasons. First, its charter limits the DARO, that funds all these efforts, to the oversight of non-lethal tactical and endurance UAVs only. Secondly, employing lethal UAVs runs counter to current doctrine, attitude, and beliefs.[504]

The Air Force and Navy are designing and testing combat UAVs. The Army is developing a tactical UAV called Shadow 200. This will give leaders "over-the-hill" surveillance capabilities. [505] Meanwhile, the Marine Corps has developed Dragon Eye, a small, hand-launched UAV that can give leaders a snapshot of the battlefield, and it plans to make improvements to the Pioneer UAV developed by the Navy. The Pioneer was used in the Gulf War. The Army also has the Hunter UAV, and both are primary surveillance UAVs

---

[503] Jones, Christopher A., Maj., Ibid, p. 43-44.
[504] Jones, Christopher A., Maj., Ibid, p. 44.
[505] Weatherington, Dyke, "Unmanned Aerial Vehicle Roadmap Report", Technology and Logistics Magazine, U.S.A., 18 March 2003.

and relay video in real time. The Navy is developing Neptune, which can drop small payloads and the X-46/X-47, a large autonomous unmanned combat aerial vehicle that has a 11-meter wingspan. The system will be initially built for tactical surveillance, but the Navy envisions it one day becoming a strike system.[506] In the future it may be that a small UAV could fly into the window of a building, land at some innocuous location and observe activities.

UAVs have a great potential for the strategic and operational commander in the pursuit of national interests. To optimize that potential, the apparent pro-pilot bias that favors manned aircraft over UAVs must be overcome. In addition, leaders must finds ways to fund lethal UAV development and support the research and development of doctrine to support it. While doing so, leaders must also ensure that lethal UAVs and their concept of operations comply with the wishes of a public that demands safety and accountability.

UAVs offer a unique advantage for military leaders because they can conduct dangerous mission without the risk of human life. UAVs will soon have the capability for reconnaissance in areas possibly contaminated with biological or chemical agents or suppress enemy air defenses, or provide deep strike interdiction.[507]

6.8. STRIKESTAR UAV AND ELINT

The force multiplier required for 2025 conventional aerospace triad forces must be capable of exercising the airpower tenets of shock, surprise, and precision strike while reducing the OODA-loop time from observation to action to only seconds. Also, this force must possess the capabilities of stealth for survivability and reliability for a life span equivalent to that of manned aircraft. Many possibilities exist across the spectrum of conflict. StrikeStar could act as a force multiplier in a conventional aerospace triad one fourth the size of the force structure.

The StrikeStar UAV could add a new dimension to the war fighter's arsenal of weapons systems. StrikeStar must rely on a system of reconnaissance assets (ELINT, IMINT etc.) to provide the information needed for it to precisely and responsively deliver weapons on

[506] Sample, Doug, Ibid.
[507] Sample, Doug, Ibid.

demand. StrikeStar itself should have a minimal sensor load. The robust, expensive sensors will be on airborne and space reconnaissance vehicles, feeding the information to the UAV.

StrikeStar will give the war fighter a weapon with the capability to linger for 24 hours over a battlespace, and destroy or cause other desired effects over that space at will. Bomb damage assessment will occur nearly instantaneously and restrike will occur as quickly as the decision to strike can be made. StrikeStar could fly well above any weather and other conventional aircraft. It would fly high enough to avoid contrails and its navigation would not be complicated by jet stream wind effects. StrikeStar will allow continuous coverage of the desired battlespace with a variety of precision weapons of various effects which can result in "air occupation"-the ability of *aerospacepower* to continuously control the environment of the area into which it is projected. Such capabilities should easily be possible by 2025. By the year 2000, Tier II+ UAV have reached nearly the StrikeStar range/endurance and payload capabilities and the Tier III- have demonstrated stealth UAV value. The issue then revolves around the use of such an unmanned capability and how such a capability could add value to *aerospacepower* of the twenty-first century.[508]

As proved in Gulf War, the technology now exists to preprogram computerized combat missions with tremendous accuracy so that our stealth fighters could fly by computer program precisely to their targets over Iraq. A stealthy drone is clearly the next step, and it's anticipated that we are heading toward a future where combat aircraft will be pilotless drones. [509]

Precision engagement will consist of a system of systems that enables forces to locate the objective or target, provide responsive command and control, generate the desired effect, assess our level of success, and retain the level of flexibility to reengage with precision when required. Even from extended ranges, precision engagement will allow to shape the battlespace, enabling dominant maneuver and enhancing the protection of forces.[510]

---

[508] Carmichael, Bruce W., et al., Ibid.
[509] Rich, Ben R., "Skunk Works", Little, Brown and Company, New York, N.Y., U.S.A., 1994, p. 340.
[510] Carmichael, Bruce W., Troy E. DeVine, Robert J. Kaufman, Patrick E. Pence, Ibid.

6.8.1 Milestones of UAV

Currently, technology is being developed to accomplish this concept. While the technology will exist by the beginning of the twenty-first century, transferring this technology from the laboratory to the battlefield will require reaching new milestones in aerospace thinking.

First, military leaders must be willing to accept the concept of lethal UAVs as a force multiplier for conventional aerospace triad of 2025. They should not deny the opportunity for continued growth in this capability.[511] The issue revolves around the use of an unmanned capability and how such a capability could add value to *aerospacepower* of the twenty-first century.

Second, doctrinal and organizational changes need to be fully explored to ensure this new weapon system is optimally employed. In the context of a revolution in military affairs (RMA), developing a new weapon system is insufficient to ensure our continued prominence. We must also develop innovative operational concepts and organizational innovations to realize large gains in military effectiveness.[512]

6.8.2. Effect of Pro-pilot Bias on UAV Development

Unmanned aerial vehicles offer military leaders the ability to use *Global Awareness* to more accurately apply *Global Reach* and *Global Power* when and where needed. For years, UAVs have had the capability to push beyond the realm of observation, reconnaissance, and surveillance, and assume traditional tasks normally assigned to manned weapon systems.

There are three identifiable concerns that will be analyzed concerning "pro-pilot bias" and its effects on UAV development. First, there is a skepticism that current UAV technology provides the reliability, flexibility, and adaptability of a piloted aircraft.[513] Basically, this

---

[511] Cooper, Jeffrey, “Another View of Information Warfare: Conflict in the Information Age”, SAIC, Publication Draft for 2025 Study Group, U.S.A., 1996, p. 26.

[512] McKitrick, Jeffrey et al., “Battlefield of the Future: 21st Century Warfare Issues: The Revolution in Military Affairs”, Ed:Barry R. Schnieder and Lawrence E. Grinter, Air University Press, Maxwell AFB, Alabama, U.S.A., September 1995, p.71-75; Krepinevich, Andrew F., Jr., “The Military Technical Revolution: A Preliminary Assessment”, Air Command and Staff College, War Theory Course Book, Volume 3, Maxwell AFB, Alabama, U.S.A., September 1995, p.163.

[513] Longino, Dana A., Lt.Col, Ibid, p. 28.

perception implies that UAVs are incapable of performing the mission as well as equivalent manned aircraft since they are unable to respond to the combat environment's dynamic changes. This incorrectly assumes all UAVs operate autonomously as do cruise and ballistic missiles. These latter systems do lack flexibility and adaptability, and only do what they are programmed to do. Other UAVs, like the Predator, are remotely piloted vehicles, and are as flexible and adaptable as the operator flying them. The operator's ability to respond to the environment is dependent on external sensors to "see" and "hear" and on control links to provide inputs to and receive feedback from the UAV. Future UAVs using artificial intelligence will respond to stimuli in much the same way as a human, but will only be as flexible and adaptable as programmed constraints and sensor fusion capabilities allow.

In 2025, technology will enable near-real-time, sensor-shooter-sensor-assessor processes to occur in manned and unmanned aircraft operations. The question is not whether either of these systems is flexible and adaptive but whether it is more prudent to have a human fly an aircraft into a hostile or politically sensitive environment, or have an operator "fly" a UAV from the security of a secure site.

The UAV has been assigned a support role, primarily in reconnaissance. The UAV is following the same development path that the airplane took over 50 years ago when the Army culture relegated it to a reconnaissance and mission support role.[514]

6.8.3. Effect of Responsiveness on UAV Development

The StrikeStar system must be responsive to a dynamic environment and design must include flexible C^4I systems, C^2 operations, and UAV guidance and fire control systems. It is imperative that a lethal UAV be able to assess its environment and adapt to it accordingly. This requires real-time data and assessment, high-speed data transmission capability, flexible C^2 procedures, reliable controller capability, and a real-time reprogramming capability.

An advantage of a manned aircraft is that the pilot can make the last-second decision to deliver the weapon, abort the delivery, or change targets as the situation dictates. At the

[514] Carmichael, Bruce W., et al, Ibid.

last-second, a pilot can detect an unknown threat preventing him or her from reaching the target, and has the ability to change targets when the original target has moved. Simply, a pilot has the ability to assess and react to a environment characterized by fog and friction. Lethal UAVs (and/or their controllers) must have the same ability to adapt to an unanticipated or dynamic environment. They must be able to discern the environment, consider the threat (in cost-benefit terms), confirm the intended target, and have the ability to deliver, abort, or change to a new target. The consequences of not having this ability relegates the UAV to an autonomous system and raises accountability questions in the event of an unintentional or inadvertent delivery. Real-time information and control is essential to protecting our accountability in lethal UAVs. [515]

6.8.4. StrikeStar Technology

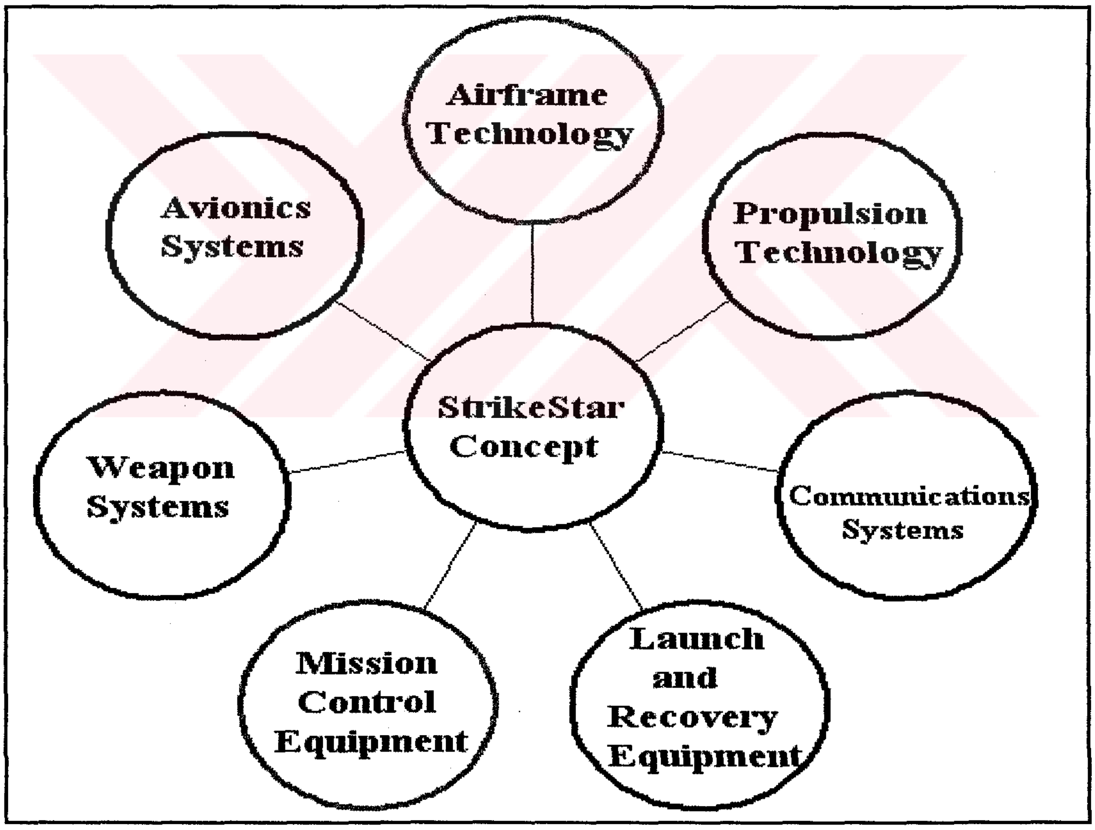


Figure 6.15: Some Technologies Support the StrikeStar Concept

The war machine described above is fiction, but the technology is within our grasp to make it a reality. In the past, UAV systems have been plagued with reliability problems or by

[515] Carmichael, Bruce W., et al, Ibid.

design flaws.[516] Current efforts are producing mature technology that improves overall reliability and functionality. The Global Hawk and DarkStar UAVs are excellent examples of how quickly UAV systems technology is advancing. Table 6.1 provides a summary of US UAV characteristics from a system capabilities perspective.[517]

This family of UAVs capitalized on past accomplishments and started the evolutionary process of adapting technologies proven in manned aircraft to UAV platforms.[518] Trends indicate a wide range of anticipated technologies will support the StrikeStar concept and provide platform robusting. Some include in figure 6.15.

Table 6.1: US UAVs, System Characteristics

Characteristic	Maneuver UAV	Interim Joint Tactical Pioneer	Joint Tactical Hunter	MAE Predator	CHAE UAV Global Hawk Tier II Plus	LOHAE UAV DarkStar Tier III Minus
Max Altitude (ft)	13000	15,000	25,000	25,000	>65,000	45,000
Endurance (hrs)	3	5	12	> 24	> 24	> 8
Rad. action (nm)	27	100	> 108	500	3000	> 500
Max Speed (kts)	TDB	110	106	129	> 345	> 250
Cruise Speed	<90	65	> 90	110	345	> 250
Loiter Speed	60-75	65	< 90	70-75	340	> 250
Payload Wgt(lbs)	50	100	196	450	2,140	1287
Max Wgt	200	429	1700	1873	24,000	8,600
Navigation	GPS	GPS	GPS	GPS/INS	GPS/INS	GPS/INS

Sensor technologies are not critical to the construction and design of StrikeStar, but are critical to its operation. We expect reconnaissance efforts for both manned and unmanned aircraft and space platforms will continue to advance. StrikeStar will rely on other platforms for target identification, but could have the capacity to carry reconnaissance sensors using modular payload approaches. This concept does not advocate combining expensive reconnaissance sensors on the same platform carrying a lethal payload, since separating sensors from the weapon platform lowers costs and lessens the risk of sensor loss.

---

[516] Longino, Dana A., Lt.Col, Ibid, p. 3-4.
[517] Carmichael, Bruce W., et al, Ibid.
[518] Cameron, K., "Unmanned Aerial Vehicle Technology", Defense Science and Technology Organization, Melbourne, Australia, February 1995.

The technologies noted above have to support the system characteristics shown in Table 6.2 to ascertain current capabilities and identify enabling technologies that support the StrikeStar concept. Adding stealth characteristics to a Global Hawk-size UAV reduces vulnerability and allows covert operation. Improved payload capacity allows the ability to carry both more and varied weapons.[519]

Table 6.2: StrikeStar System Characteristics

Characteristic	StrikeStar
Wingspan (ft)	105
Max Altitude (ft)	>80,000
Endurance (hrs)	> 40
Rad. action (nm)	3700 w/24 hr loiter
Max Speed (kts)	> 400
Cruise Speed (kts)	400
Loiter Speed (kts)	400
Payload Wgt (lbs)	4000
Max Wgt (lbs)	24,000
Navigation	GPS/INS

6.8.5. Communications Systems

A fused real-time, true representation of the Warrior's battle space-an ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute warrior's mission in that battle space. To provide continuous battlefield dominance, information dominance is critical for StrikeStar operations. Battlespace awareness as envisioned under the *C^4I for the Warrior Program* will provide the information infrastructure required for command and control (C^2) of the StrikeStar platforms. UAV communications systems function to provide a communications path, or data link, between the platform and the UAV control station, and to provide a path to pass sensor data. The goal of the C^4 system is to have the head of the pilot in the cockpit, but not his body.[520]

---

[519] Carmichael, Bruce W., et al, "Strikestar 2025", A Research Paper Presented To Air Force 2025, U.S.A., August 1996, Available on site: http://www.au.af.mil/au/2025/volume3
[520] Ackerman, Robert K., "Tactical Goals Encompass Sensors, Autonomous Arts", Signal Magazine, U.S.A., December 1995, p. 27.

StrikeStar communications would provide a reliable conduit for status information to be passed on a downlink and control data to be passed on the uplink in hostile electronic environments. The uplink and downlink data streams would be common datalinks interoperable with existing C^4 datalinks to maximize data exchange between sensors, platforms, and their users. Status and control information would be continually transferred between StrikeStar and its controller in all cases except during autonomous operation or implementing preprogrammed flight operations. The data link would need to be impervious to jamming, or even loss of control, to ensure weapon system integrity. User-selectable, spread spectrum, secure communications in all transmission ranges would provide redundancy, diversity, and low detection and intercept probability. Both beyond line-of-sight and line-of-sight communications methods would be supported to a variety of control stations operating from aerospace, land, and sea platforms.[521]

Command and control of UAVs via satellite links has been demonstrated to be highly reliable. The MILSTAR constellation or its follow-on could serve as the primary C^2 communications network for StrikeStar platforms. MILSTAR's narrow-beam antennas coupled with broad-band frequency hopping provides isolation from jammers and a very low probability of detection.[522] The Defense Satellite Communications System (DSCS) constellation and Global High-Frequency Network could provide alternate paths for connectivity and redundancy depending on mission profiles. The vast HF network provides nearly instantaneous coverage and redundancy under adverse environmental conditions. High-Frequency can provide commanders with useful, flexible, and responsive communications while reducing the demand on overburdened satellite systems.[523] The continued proliferation of commercial satellite networks may allow StrikeStar platforms to exploit these networks as viable communications paths as long as C^2 integrity of on-board weapons is assured.

StrikeStar would rely on other platforms, like Predator, DarkStar, Global Hawk or ground, airborne, or space reconnaissance, to detect and locate potential targets. The StrikeStar

---

[521] USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century", Summary volume, USAF Scientific Advisory Board, Washington, D.C., U.S.A., 15 December 1995, p.27.
[522] Busey, Adm James B., "MILSTAR Offers Tactical Information Dominance", Signal Magazine, U.S.A., July 1994, p. 11.
[523] Wallace, Michael A., "HF Radio in Southwest Asia", IEEE Communications Magazine, U.S.A., January 1992, p. 59-60.

could team with any or a combination of all these assets to produce a lethal hunter-killer team. Once geolocated, the target coordinates would be passed to StrikeStar along with necessary arming and release data to ensure successful weapon launch when operating in command-directed mode. In autonomous mode, StrikeStar would function like current cruise missiles, but allow for in-flight retargeting, mission abort, or restrike capabilities. Communications for cooperative engagements with other reconnaissance platforms require minimum bandwidth between StrikeStar and its control station since the targeting platforms already provide the large bandwidth necessary for sensor payloads.

As with any C^4 system, we anticipate StrikeStar's requirements would grow as mission capabilities and payloads mature. It is possible StrikeStar follow-ons could be required to integrate limited sensing and strike payloads into one platform, thus significantly increasing datalink requirements. In this event, wideband laser data links could be used to provide data rates greater than 1 gigabit per second.[524] In addition, a modular payload capability could allow StrikeStar platform to carry multimission payloads such as wideband communications relay equipment to provide vital C^4 links to projected forces.

6.8.6. Mission Control Equipment

As mentioned, StrikeStar will be controllable from a multitude of control stations through the common data link use. Control stations could be based on aerospace, ground, or sea platforms depending on the employment scenario. A control station hierarchy could be implemented depending on the employing force's composition and the number of StrikeStars under control. The StrikeStar C^2 hierarchy and control equipment would allow transfer of operator control to provide C^2 redundancy. Current efforts have established a common set of standards and design rules for ground stations. This same effort needs to be accomplished for aerospace and sea based control stations.

Significant efforts to miniaturize the control stations would be needed to allow quick deployment and minimum operator support through all conflict phases. Man-machine interfaces would be optimized to present StrikeStar operators the ability to sense and feel as if they were on the platforms performing the mission. Optimally, StrikeStar control

[524] Signal, "Optical Space Communications Cross Links Connect Satellites", Signal Magazine, U.S.A., April 1994, p. 38.

could be accomplished from a wide variety of locations ranging from mobile ground units to existing hardened facilities. The various control stations would be capable of selectively controlling StrikeStars based on apriori knowledge of platform C^2 and identification procedures.[525]

6.8.7. StrikeStar Concept of Operations

The purpose of the StrikeStar concept of operations is to define the operational application of the StrikeStar by highlighting system advantages, defining future roles and missions, and illustrating interrelationships between intelligence, command and control (C^2), the weapon, and the war fighter.

Aerospacepower roles and missions in future are difficult to predict, yet we know they will be tied to the nature of future conflict. Gulf War has been touted by many as the first modern war and a clear indicator of the nature of future conflict. Others believe that the conflict was not the beginning of a new era in warfare but the end of one, perhaps the last ancient war.[526] In terms of posing aerospace forces for the future, it is imperative we look for discontinuities in the nature of future war as well as commonalties to past conflicts. It is a fact that our future roles and mission will be a reflection of our technological capabilities and most significant centers of gravity as well as those of our enemies.[527] It is safe to say the missions that are the most challenging today will be the core requirements of aerospacepower tomorrow.

Revolutions in conventional warfare will be driven by rapidly developing technologies of information processing, stealth, and long-range precision strike weapons.[528] A StrikeStar's relative invulnerability, endurance, and lethality would force redefinition of roles and missions and revolutionary doctrinal innovation for airpower employment.

[525] Carmichael, Bruce W., et al., Ibid.
[526] McPeak, Gen Merrill A., "Selected Works 1990-1994", Air University Press, Maxwell AFB, Alabama, U.S.A., August 1995, p.230.
[527] Meilinger, Col Phillip S., "10 Propositions Regarding Air Power", Air Force History and Museums Program, Maxwell AFB, Alabama, U.S.A., 1995, p. 60.
[528] Fitzsimuonds James R. and Jan M. Vantol, "Revolution in Military Affairs", Joint Force Quarterly Magazine, U.S.A., Spring 1994, p. 27.

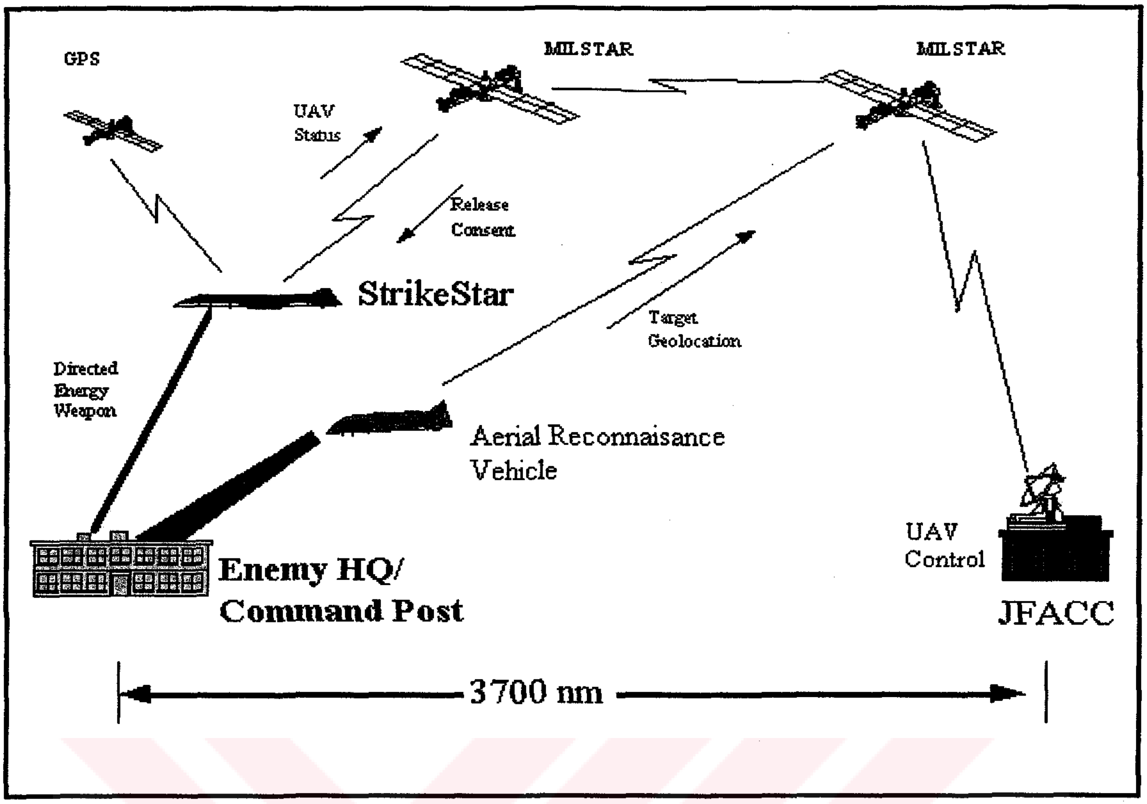


Figure 6.16: StrikeStar C^2 Architecture

The StrikeStar is inextricably linked to reconnaissance and command and control systems. The system architecture depicted in Figure 6.16 illustrates how a StrikeStar is tied and integrated into the larger battle space systems. Keep in mind that it is the entire architecture, or the system of systems, which enables mission accomplishment.[529] The StrikeStar is a relatively dumb system: it carries few sensors, and it is not designed for a great deal of human interface. The viability of the StrikeStar concept in 2025 depends on its ability to plug into the existing battlespace dominance and robust C^2.

Dominant battlespace awareness in 2025 must include near real-time situational awareness, precise knowledge of the enemy, and weapons available to affect the enemy.[530] This intelligence (ELINT) must be comprehensive, continuous, fused, and provide a detailed battlespace picture. The intelligence-gathering net will utilize all available inputs from

[529] Fulghum, David A., "DarkStar First Flight Possible in March", Aviation Week and Space Technology Magazine, U.S.A., 19 February 1996, p. 55.
[530] Warfighting Center, "Warfighting Vision: 2010 A Framework for Change", Joint War fighting Center, Ft Monroe Va., U.S.A., August 1995, p.10.

aerospace assets, both manned and unmanned sensors.[531] The StrikeStar would rely on this integrated information for employment, queuing, and targeting. A StrikeStar in this architecture adds value since it enables an aerospace platform to provide dominating maneuver with lethal and precise firepower in a previously unattainable continuum of time. A pictorial representation of this concept is presented in Figure 6.17.

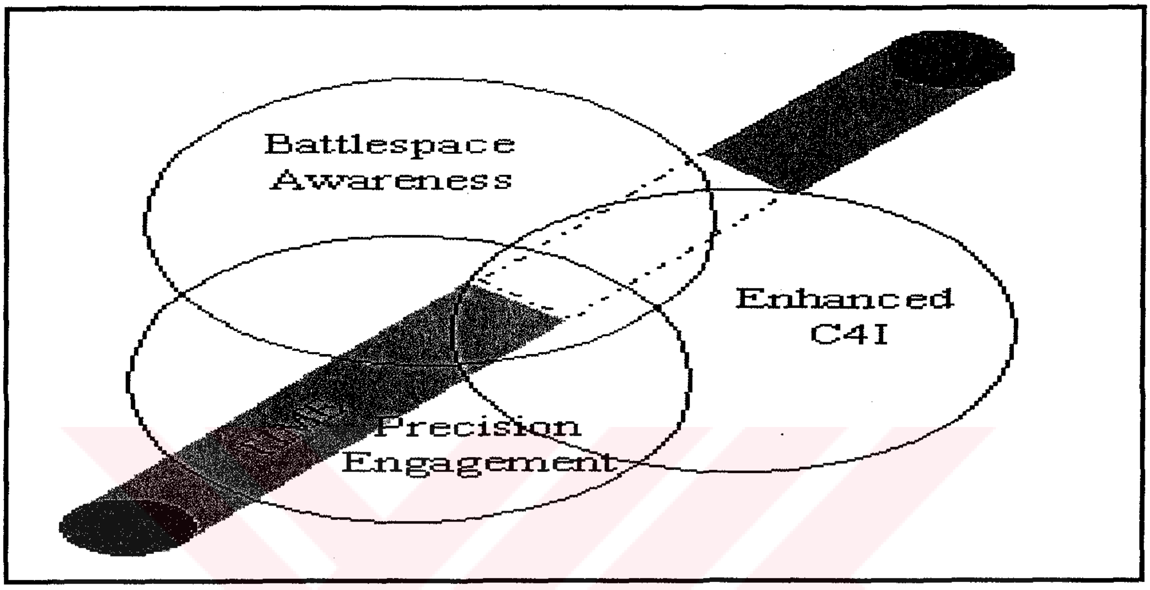


Figure 6.17: A System of Systems Over Time Continuum

Command and control capabilities in 2025 are the defining element in the StrikeStar concept. A StrikeStar would need to be fully integrated into a common C^2 element that manages all aspects of the air battle in 2025. A StrikeStar places several unique demands on the command and control element. C^2 personnel would employ a StrikeStar by nominating targets, pulling down required intelligence (ELINT), and selecting the platform and weapon to be used against them. The command element could then command weapons release or tie the StrikeStar directly to an AO sensor in an autonomous mode. In the autonomous mode intelligence is collected, sorted, and analyzed and then forwarded to a StrikeStar positioned to attack immediately a target by-passing the C^2 element (sensor-to-shooter). To reduce vulnerability of the command center and StrikeStar, data-link emissions should be held to a minimum.

[531] U.S. Air Force 2025 Concept, “Surveillance and Reconnaissance, Real-Time Integration”, 2025 concept briefing, Maxwell AFB, Alabama, U.S.A., 19 January 1996, Available on site: http://www.au.af.mil/au/2025/2025_concept

The type and location of the command center used in 2025 will depend on the nature of the conflict. Missions of the most sensitive nature, clandestine operations, or retaliatory strikes are best served by a short and secure chain of command. Therefore, these StrikeStar applications would be best served by a direct link to the platform from a command center located in the hub of political power. Similarly, if a StrikeStar is utilized in extremely hostile theaters, a command and control center located far from hostilities is most advantageous. In low-intensity conflicts, peace enforcement, or domestic urban applications, the C^2 center could be moved to the vicinity of the conflict as a mobile ground station, an airborne platform, or even a space-based station.

A StrikeStar would proceed to the target via the programmed flight path. Although stealthy technology and altitude reduces vulnerability, flight path programming should integrate intelligence (ELINT) preparation of the battlefield (IPB) to optimize this technology and avoid obvious threats. Once in the AO the StrikeStar would release its weapons or recognize its assigned sensor and establish a "kill box." The kill box is a block of space where the StrikeStar releases weapons on threats identified by coupled sensors. [532]

6.9. INTEGRATE SPACE-BASED SYSTEMS AND UAVs

Enemies will probably have the ability to target satellites in LEO and to affect an EMP burst in space (via a nuclear explosion). Satellites must already be hardened due to solar activity. This shielding could be intensified to negate EMP effects. However, this shielding would be required on all satellites for which military operations are dependent including civilian-owned communications satellites.

The ASAT threat depends on target orbit. Satellites in geosynchronous earth orbit (GEO) should remain relatively secure. During our planning period (2005-2015), it is improbable that any niche will have air-launched access to GEO. Putting an ASAT into GEO will require a powerful booster. For any niche, such boosters will require a fixed launch complex. Such a complex should not survive conflict initiation; the US would attack fixed space launch facilities on day one of the war.

---

[532] Hallion, Richard P., "Storm over Iraq Air Power and the Gulf War", Smithsonian Institution Press, Washington. D.C., U.S.A., 1992, p.155.

On the other hand, LEO satellites would be reachable by air-launched (e.g., the F-15/ASAT) or mobile ground-launched systems. Options for decreasing this vulnerability will be few. Targeting air-launched ASATs prior to launch is not likely; they'll be difficult to identify among the hundreds or thousands of similar type weapons. The most effective measure will probably involve two steps:

1. Maneuver the satellites.
2. Destroy the enemy's space-tracking capability.

Without solid data on satellite tracks, the niche would find targeting extremely difficult. Other defensive measures could include in-flight interception of the ASAT, stealthy satellites, and a rapid replacement capability.

What this means is that satellites would probably be targeted to varying degrees. Because communications satellites are primarily in GEO, they should survive (unless the enemy develops a mobile ASAT with GEO range). Reconnaissance satellites, however, operate primarily in LEO. Their survival in war with an enemy is less certain.

As a result, the US must augment space-based systems with atmospheric systems. Fortunately, UAVs, along the lines of Tier II+ and Tier III-, are well along in development. High altitude-long endurance UAVs, with loiter times of 48–72 hours, are probable in our planning time frame. They promise sufficient loiter times and survivability to accomplish the surveillance mission. While UAVs have capabilities that recommend them in their own right, they are also necessary to provide redundancy for space-based systems. Satellites in LEO with predictable trajectories are simply too vulnerable to interdiction.[533]

This technological solution brings with it an organizational challenge. The theater commander must integrate two fundamentally different architectures. The commander in chief (CINC) must integrate both space-based and atmospheric sensors and relays; total reliance on one or the other for critical tasks is not wise. One or the other may be unavailable to perform a specific job at a crucial time. It will be far more effective to integrate their tasks so that one type of system is not the sole source for any vital node. It

[533] Barnett, Jeffery R., "Future War - An Assessment of Aerospace Campaigns in 2010", Air University Press, Maxwell Air Force Base, Alabama, U.S.A., January 1996.

will also be far more efficient to integrate the data acquired by each system. Because space-based and atmospheric systems are presently controlled by separate commanders, this integration will require adjustments to current command relations.[534]

6.10. NEXT GENERATION OF UAVS

The Endurance models of unmanned aerial vehicles are the next generation of UAVs and have tremendous potential for future operations. Their purpose is to provide near real-time imagery to the Joint Task Force (JTF) Commander. If these aircraft can be properly designed and fielded at a reasonable cost, they will give the JTF Commander an expendable, long-dwell, tactical UAV systems with continuous, all-weather narrow area search capability. This class of UAV will remain on station at extended ranges for periods exceeding 24 hours. With this asset, the on-scene Commander can receive direct reconnaissance, surveillance, and target acquisition information over defended hostile areas without waiting for "national assets.[535]

The US Air Force Research Laboratory (AFRL) is developing the next generation of unmanned air vehicles (UAV) with an eye on enhancing the effectiveness and affordability of the systems. Engineers and scientists are concentrating their efforts on technologies for Strike unmanned air vehicles, directed energy integration and SensorCraft to enhance the warfighter's capabilities.

UAV lead for the directorate, researchers are homing in on the three areas to help focus the technology developments on conceptual vehicles and capabilities. Over the next several years, AFRL will combine the innovations into one or several platforms and perform flight tests on a prototype as early as 2011.

UAV missions are most often characterized as the "dull, dirty and dangerous. *Dull*; as in patrolling no-fly zones or very long electronic intelligence (ELINT), surveillance and reconnaissance (ISR) missions; the UAV is just as alert in the last hour of its patrol as it is in the first hour. *Dirty*; as in operations in airspace potentially contaminated with biological

---

[534] Barnett, Jeffery R., Ibid.

[535] Howard, Stephen P., "Special Operations Forces and Unmanned Aerial Vehicles: Sooner or Later", Air University, Maxwell AFB, Alabama, U.S.A., June 1995.

or chemical weapons. *Dangerous*; as in electronic attack missions, often performed early in a battle while the enemy's air defenses pose a serious threat.

The technology advancements AFRL scientists are exploring range from adding advanced sensors (ELINT etc.) to facilitate automatic collision avoidance, integrating the propulsion system with the airframe to reduce size, and developing mission control capabilities that will enable multiple UAVs to operate as a cooperative group. Along with these advancements, the directorate is developing on-vehicle control capabilities to enable UAVs to be as safe and effective as manned assets, but at a reduced size, weight and cost. Technologies in development include photonic vehicle management systems, intelligent reconfigurable control, prognostic health management, automatic collision avoidance and automatic air refueling.[536]

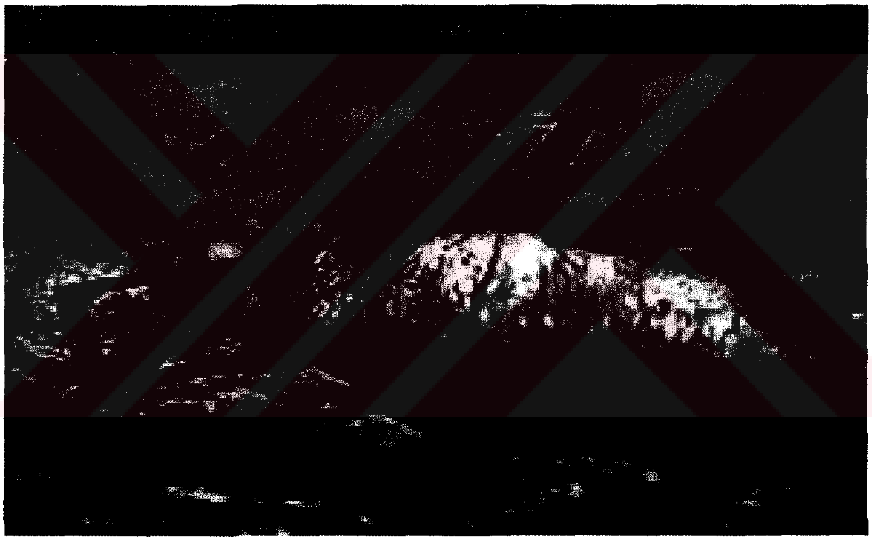


Figure 6.18: Next generation of UAVs

Focusing on the three development areas also guides scientists into designing UAVs that are capable of certain feats. These major enabling thrusts are preemptive and reactive suppression of enemy air defenses using strike UAVs; efficient and effective integration of directed energy weapons into tactical UAVs; and increased endurance permitting longer range and more complex ISR missions.[537]

[536] Barr, Larine, "Dull, Dirty and Dangerous", Military Aerospace Technology Online Edition, Volume 2, Issue 3, U.S.A., 10 July 2003. Available on site: http://www.mat-kmi.com/archive_article
[537] Barr, Larine, Ibid.

With antenna technology of this type, the Sensorcraft could use one or two of its four antenna segments to search for targets while using another for communications. The advanced antennas would also be compatible with bistatic and passive detection and tracking techniques.[538]

6.10.1. Breaking from Current Design Paradigms

In the realm of airframe concepts, researchers are breaking from current air vehicle design paradigms to structurally embed and integrate antennas, arrays and subsystems into the wings and fuselages of UAVs. This will enable researchers to design vehicles around the mission's sensor requirements rather than designing the sensors to fit the constraints of the vehicle. Towards that effort, AFRL researchers are exploring a concept for the warfighter, called SensorCraft, a futuristic ISR UAV. The SensorCraft integrates sensing devices, information technologies and new propulsion systems into an airframe capable of revolutionary ISR capabilities.

The directorate is investing considerable resources on adaptive structures, active flow control, and ultra-lightweight airframe concepts specific to high altitude airfoils to enhance aerodynamic efficiency of concepts such as the SensorCraft. This increase in endurance would allow the system to fly longer range, and more complex missions or loiter time, which could result in fewer vehicles needed to maintain a continuous presence over the battlefield. Though there are many technology hurdles to jump, a full-scale SensorCraft platform could be ready for flight tests in eight or nine years. Platforms with smaller subsets of technologies could be ready for tests as early as 2008.

In addition to SensorCraft, the Air Vehicles Directorate is exploring a concept that combines helicopter and plane-like characteristics. Called SkyTote, the craft has counter-rotating propellers and will be able to accomplish vertical take offs, landings and hovers. Once airborne, SkyTote can transition to wing-borne flight with its advantage of higher

---

[538] Sweetman, Bill, "HALE Storms to New Heights", Jane's International Defense Review, Vol.34, Essex, UK, March 2001, p. 55.

speed and increased range. The directorate is conducting flight tests on SkyTote this year.[539]

6.10.2. Superior ELINT, IMINT etc. Sensors

This aircraft will be equipped with a variety of multi-mission payloads including TV, FLIR, Radar, Electronic Countermeasures, Data Relay, and a Laser Designator.[540] These sensors would provide large area surveillance to dramatically increase combat identification capabilities for the warfighter.

The sensor spectrum for UAVs is very comprehensive, ranging across both electro-optical and radio frequency spectrums. A prevailing theme is size, weight and power reduction through advanced technologies, paving the road to more prolific incorporation of multifunction capabilities. A primary example of this is our structurally embedded low frequency antenna technologies to enable respectable performance in areas of foliage penetration and airborne target tracking.[541] When the next generation UAV is fully operational it can orbit at 20-25,000 feet for 24 hours at a time, and send, via satellite communications, high resolution real/near real time electro-optical, infrared, and synthetic aperture radar imagery to a ground control station near the Joint Force Commander's headquarters.[542]

6.10.3. Integrating Propulsion Systems

In addition to exploring new platforms and sensors, US AFRL researchers are striving to integrate the propulsion system with the airframe of UAVs, which can have enormous payoff in vehicle size, weight, and cost.

UAVs are sized to three things: mission requirements (speed, range, etc.), payload (weapons systems, etc.) and a propulsion flow path length. The flow path must be sufficiently long to give good flow quality to the engine but twisting and turning to get around items installed in the fuselage. If it can be made the highly offset inlet more

---

[539] Barr, Larine, Ibid.
[540] Howard, Stephen P., "Special Operations Forces and Unmanned Aerial Vehicles: Sooner or Later", Air University, Maxwell AFB, Alabama, U.S.A., June 1995.
[541] Barr, Larine, Ibid.
[542] Howard, Stephen P., Ibid.

compact, that sizing (especially length) requirement is cut proportionally. If air vehicle weight is proportional to the CUBE of the length scale—imagine the payoff. Additionally, vehicle cost is proportional to weight, so it will be got a smaller, lighter and less expensive air vehicle.

According to Addington, the technology will reduce the length and diameter ratios of current ducts (F/A-22 and F-35 are both about 5) to about 2.5, but with flow quality (pressure recovery and circumferential distortion) equivalent to the fighters or better.[543]

6.10.4. Improved Safety and Effectiveness

Another goal pursued by AFRL researchers is to develop technologies to increase safety and effectiveness of UAVs. On a practical level, inventors are working on programs like the automatic air collision avoidance system and automated aerial refueling in which the vehicles, whether manned or UAVs, must talk to each other to formulate plans and intentions. This could be done via data links or other methods, but they still must communicate. Autonomous UAVs must communicate and work with other UAVs and manned aircraft as an integrated team.

The UAVs of the future will not just be passing knowledge, pictures per se, but they will use knowledge to think about what the pictures mean. If we trust the capability of the UAVs to generate and disseminate knowledge, then we reduce the need for pictures, videos, and the like and we can ultimately reduce our communication bandwidth requirements.

In concert with these advances, the directorate is pursuing a new generation of more unitized structures for UAVs that will reduce manufacturing costs and increase system readiness without weight or supportability penalties. The approach is to identify, develop and transition new structural design concepts and manufacturing methods for both metals and composites that place emphasis on reducing part count and the number of structural joints and fasteners.[544]

---

[543] Barr, Larine, Ibid.
[544] Barr, Larine, Ibid.

6.11. UNINHABITED COMBAT AERIAL VEHICLES (UCAVS)

Uninhabited Combat Aerial Vehicles (UCAVs) are remotely operated aircrafts used by the military in the SEAD mission. The objective of SEAD is to destroy, neutralize, or temporarily degrade enemy air defenses in a specific area by physical attack or electrical warfare. The goal of the lethal suppression is to prevent systems from radiating, either through physical damage or by intimidation. The mission requires detection, location, identification, and destruction of important elements of enemy air defenses.[545]

The "unmanned" aircraft of the present have particular advantages, such as cost or endurance, but are either cruise missiles or reconnaissance vehicles. The "uninhabited" combat aircraft (UCAV) will be high performance aircraft that are more effective for particular missions than their inhabited counterparts. The enabler for viable UCAV employment is the constantly evolving information technologies, allowing the use of new aircraft and weapons' technologies unavailable for use in inhabited aircraft.[546]

Figure 6.19: UCAV Attacking Air & Land Targets with High Power Laser

The Suppression of Enemy Air Defenses (SEAD) mission involves the active stimulation of the enemy radar patrols. This entails fighter pilots flying into enemy territory in the hope

[545] Gallimore, Jennie J., "Uninhabited Combat Aerial Vehicles in the Military SEAD Mission", Wright State University, Dayton, OH, U.S.A., 14 March 2000.
[546] Jones, Christopher A., Maj., "Unmanned Aerial Vehicles (UAVS) An Assessment of Historical Operations and Future Possibilities", US Air Command and Staff College, U.S.A., March 2003, p. 49-52, Available on site: www.fas.org/irp/program/collect/docs/97-0230D

that enemy ground patrols turn on their local radar tracking devices to pinpoint the fighter pilots exact locations for destruction. When the enemy turns on their radar the fighter pilots are able to pinpoint the enemy radar locations on the ground. At this point it is only a matter of who can fire first and who can avoid the oncoming missiles. The fighter pilots have the advantage of high speeds and 3 dimensional movements, whereas the radar patrols are nearly immobile.[547]

It is the improvements in sensors, processors, and information networks that make the UCAV possible. Information, critical to today's precision weapon systems, are increasingly derived from sensors outside the air vehicle itself. Current concepts call for transmitting information derived from many sources over a satellite or ground-based datalink to the pilot of a high performance combat aircraft. The amount of information available for display in the cockpit is enormous, quickly saturating the human pilot with more data than can be effectively absorbed. The extremely low observability of the UCAV will also result in the reduction of standoff distance at the weapon release point; meaning the UCAV can be closer to the target at weapons release. This will, in turn, allow employment of less expensive PGMs with less sophisticated weapon sensors and guidance systems and lower propulsion costs than longer range stand-off weapons. An effective UCAV will be possible in the next century as the result of the simultaneous optimization of information flow, aircraft performance, and mission effectiveness. The UCAV will not completely replace inhabited aircraft for decades, but the presence, or absence, of a pilot is now an available design trade. The advances in weapons systems, particularly the Air Force's Airborne Laser Program, could add completely new dimensions for employing UCAVs.[548]

Obviously the SEAD mission is a very dangerous mission for the fighter pilots and it is a goal of the military to take the pilot out of the combat vehicle. Uninhabited combat aerial vehicles (UCAVs) will make significant contributions to the warfighting capability of operational forces. Timeliness of battlefield information is greatly improved while reducing the risk of capture or loss of manned assets.[549]

---

[547] Gallimore, Jennie J., Ibid.
[548] Jones, Christopher A., Maj., Ibid, p. 49-52.
[549] Gallimore, Jennie J.,Ibid.

6.12. MICRO UNMANNED AERIAL VEHICLES (MicroUAV)

U.S. is also investigating the viability of Micro Unmanned Aerial Vehicles (MicroUAV). The development of the MicroUAV would be a technological feat so radical that it would push the state of the art in flight control, navigation, communications and propulsion. These tiny drones, no more than 15 cm in span or length, could scout inside buildings, for example, collect biological-chemical samples, or attach themselves to structures or equipment and act as listening and/or video posts. No specific application has drawn engineers to the project, but it is confident that technologies, like micro-sensors and micro-electro-mechanical systems, being developed for other programs will provide the necessary capabilities to make a small-scale aircraft fly.[550]

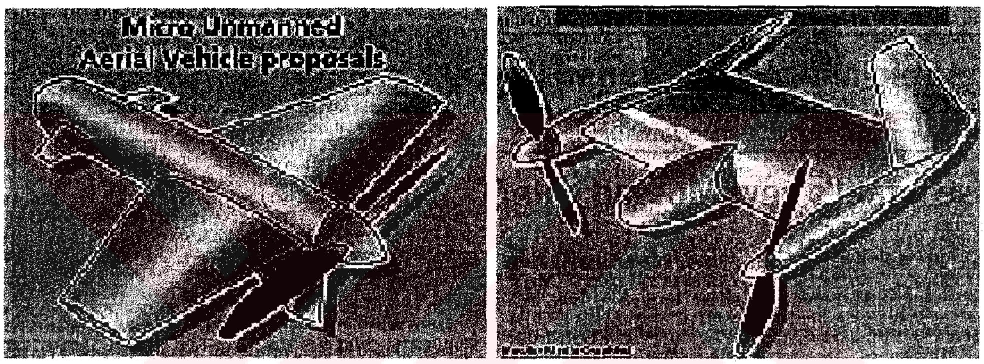


Figure 6.20: MicroUAVs

Technologies of interest include new approaches for flight stability and control; lightweight approaches to propulsion and power; lo-power, lightweight navigation, communications and onboard processing; advanced structures and packaging, and MAV-tailored payload technologies, including imaging or other sensors.[551] True "micro" air vehicles (MAV) must integrate smart materials, micro electromechanical systems (MEMS) sensor and actuator elements, energy sources, power converters, as well as miniaturised computing and communication circuits to achieve intelligent navigation, self-stability, and propulsion in a palm-sized automaton.[552]

---

[550] Evers, Stacey, "ARPA Pursues Pocket-Sized Pilotless Vehicles", Jane's Defence Weekly Magazine, Vol.26, No.12, UK, 20 March 1996, p. 3.
[551] Evers, Stacey, "US Research on Micro Air Vehicles Design Takes off", Jane's Defence Weekly Magazine, Vol.27, No.23, UK, 11 June 1997, p. 14.
[552] Möller, Ralf, "Wings", Artificial Intelligence Lab, University of Zurich, Available on site: http://www.cis.plym.ac.uk/cis/InsectRobotics/Wings.htm

If this effort comes to fruition, MicroUAV employment could vary widely, but possible uses could be for surveillance, clogging aircraft engine inlets, jamming artillery and AAA gun barrels, dislodging the tracks on mechanized vehicles, and others. MicroUAV technology could also further reduce the possibility of collateral damage, since the weapon is only six inches across. Reducing collateral damage, even to enemy forces, is another trend of our society.[553] Micro Air Vehicles (MAV), of this size or smaller (15cm-85gr) offer the chance for the soldier, in the not too distant future, to significantly enhance their fighting capability. MAVs fitted with miniature cameras and other sensors will enable a soldier to have instant information about their immediate battlefield environment. There will be no place for enemy forces to hide.

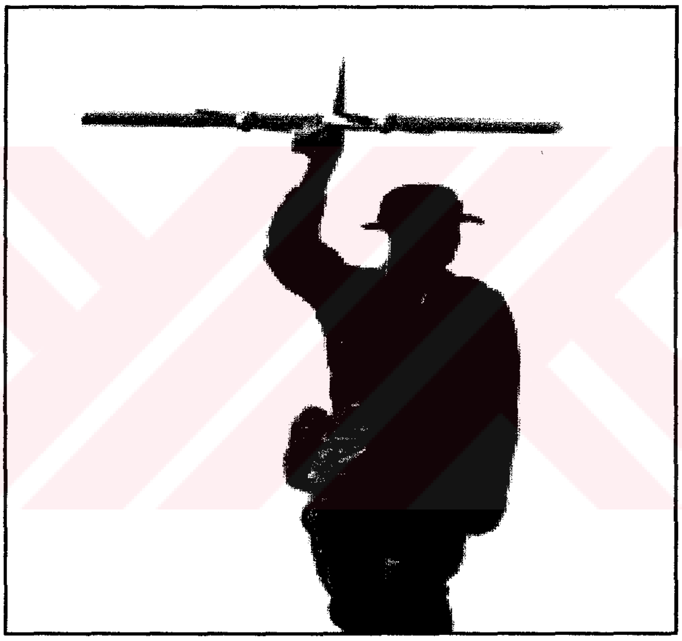


Figure 6.21: MicroUAV enhance soldiers capacity.

There are two main roles that the developers of MAVs have envisioned. First is a swarm of MAVs, literally like a flock of birds, that would be directed toward enemy forces and provide real time surveillance. MAVs used in this fashion could augment more conventional methods of surveillance with unique advantages derived from their size. MAVs are inherently stealthy, their small size, and quiet operation, enable very close surveillance of enemy forces that have no idea that they are being watched. A swarm of

[553] Evers, Stacey, "ARPA…", Ibid, p. 3.

MAVs would be particularly effective in wooded areas, if they could land or hover amongst the foliage that is traditionally a hiding place from conventional surveillance.

Second, they could be employed individually by troops on the battlefield using them as an extra, and highly maneuverable, pair of eyes. An urban foot soldier suspecting that enemy troops are ensconced in the basement of a building could launch an MAV to investigate. After releasing a tiny aircraft, which could easily be carried in his backpack, he could direct it to fly into the building and search for enemy personnel and munitions.

The traditional balance of urban warfare would be upset. The patrolling soldier now knows the precise location and disposition of his adversary hiding in the building, who in turn is unaware that they are being observed. Other suggestions for military uses for MAVs have included sniffing for chemical and biological gents, mine detection, jamming radar and communications, and employing them as assassins armed with micro weapons.[554]

[554] Möller, Ralf, Ibid.

7. AIR FORCE AND ELINT

Effective command and control systems magnify the unique characteristics of air and space power: flexibility, speed, range, responsiveness, precision, and observation. To quick observe, analyze, and predict will reveal an enemy's weakness and possible intent.

The virtual integrated planning and execution resource system provides commanders at the strategic, operational, and tactical levels an integrated “system of systems” that achieves information supremacy, allowing dominance of the battlespace. It provides commanders the ability to plan collaboratively with combat and support forces. Parallel planning permits simulation of alternate courses of action using war gaming and advanced decision support the systems to evaluate congruence of objectives, potential risks, and vulnerabilities. This capability improves upon and hardens the users' observe-orient-decide-act (OODA) loop, reducing “fog and friction” in executing operations. It provides commanders a real-time bird's-eye view of the battlespace during execution. This perspective results in visibility of all logistics from factory to foxhole and improved combat identification. The information is displayed using a three-dimensional holographic projection with natural human-machine interface during planning and execution. It tailors information from the strategic to the tactical level.[555]

The survivability and effective conduct of air operations require timely collection, processing, analysis, production, and dissemination of reliable and accurate intelligence. Continuous information from air-, surface-, and space-based sensors is needed to provide warning and attack assessment. Intelligence, surveillance, and reconnaissance (ISR) information is also needed to identify and exploit enemy centers of gravity; to help formulate objectives; to detect, identify, characterize, and monitor air threats; and to support all combat forces. Collection requirements are tailored to support the targeting cycle and threat environment. Target development, weapon selection, mission planning, and combat assessments depend on well-integrated collection and analysis.[556]

---

[555] Miller, Lt Col Gregory J., et al, “Virtual Integrated Planning And Execution Resource System (VIPERS): The High Ground Of 2025”, A Research Paper Presented to Air Force, Washington, U.S.A., August 1996
[556] US Air Force, “Air Force Doctrine Document 2–1.1 - Counterair Operations”, Secretary of the Air Force, U.S.A., 6 May 1998. Available on site: www.fas.org/man/dod-101/usaf/docs/afdd/afdd2-1-1

Both active and passive defensive air operations need highly granular order of battle data bases on enemy air defense (and offense) forces, well-founded tactics estimates, and precise specifications and signature data on enemy weapons. Intelligence preparation of the battlespace (IPB) can determine where a theater missile may or may not be located, thus narrowing down the area for surveillance and reconnaissance assets and TBM combat air patrols.[557] European coalition aerial task force could, in theory, be assembled from existing assets, with various national permutations: electronic surveillance and intelligence by Britain and France; airborne early-warning and control also by Britain and France; electronic counter measures by Germany; air control and extended surface attack by any combination of F16s, together with Tornados from Italy, Germany or the UK and Gripens from Sweden; all-weather reconnaissance by the UK, France or Germany, supported by clear-weather assets from other partner.[558] Almost every advanced attack aircraft carries equipment designed to foil enemy sensors. For example, the AN/ALE-45 electronic countermeasure ejection system used on the F-15 is nothing more than an updated version of the old World War II metallic chaff that used to be dumped out the door of B-17s.[559]

In adapting to a dramatically different conflict environment, the Air Force will need to undertake a substantial, and perhaps radical, transformation of its capital stock inventory, doctrine, and organizational structure. The Air Force has a dominant position in the existing military regime and a commanding lead in the early period of the transition to a new one. The Air Force will, however, have to take steps to foster greater innovation if it is to retain its current advantages in military effectiveness over its competitors in the future.[560]

Future theater air operations will likely be characterized by an increasing emphasis on long-range precision strikes (LRPS), stealth, UAVs and weaponized UAVs, electronic and information strikes, and operations conducted as part of the systems architecture described

[557] US Air Force, Ibid.
[558] Mason, Tony, "The Role of European Ground and Air Forces After the Cold War: Roles, Missions and Means for the Specific Use of Aerial Forces", Ed. Gert de Nooy, Netherlands Institute of International Relations 'Clingendael', Netherlands, 1997, p. 157.
[559] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 290.
[560] Krepinevich, Andrew, "Air Force of 2016", CSBA Publications, October 1996, Available on site: http:www.csbaonline.org/4Publications/Archive/Air_Force_of_2016.htm

above. Strikes conducted by individual, manned platforms will probably decline in relative importance.

In adjusting its strategic focus to undertake this transformation, the Air Force should emphasize:[561]

1. Building core competencies. A core competency is a complex combination of technology, manufacturing base, skilled manpower, training, organizational agility, doctrine and operational experience that allows the Air Force to do something of strategic importance extremely well.
2. Stealthy long-range unmanned aerial vehicles (UAVs) and weaponized UAVs.
3. Stealthy long-range cargo aircraft and long-range unmanned aerial cargo vehicles with precision airdrop capability.
4. Small satellites and a rapid satellite launch capability.
5. Active and passive methods for achieving control of space.
6. Improved information-based capabilities for use on a variety of platforms to include: enhanced stealth, deception, concealment/cloaking capabilities, enhanced electronic strike and electronic defense capabilities, and other related capabilities.
7. The integration of military ISR, C^4I, and LRPS systems into systems architectures.
8. Advanced precision-guided munitions.
9. Adopting a "hedging" approach to the Air Force capital stock inventory.

7.1. C^4ISR ROSOURCES AND REQUIREMENTS

Effective air operations require a reliable command, control, communications, computers, intelligence, surveillance, and reconnaissance (C^4ISR) capability that includes space-based assets. C^4ISR assets should be capable of exchanging information rapidly; interfacing with other Services, components, and coalition partners; and displaying information of common concern while employing guard technologies that allow the secure interchange of data. The information flow supports the chain of command and should be as complete, secure, and near real time as possible. The system should be flexible enough to redirect selected forces, even when they are airborne.

[561] Krepinevich, Andrew, Ibid.

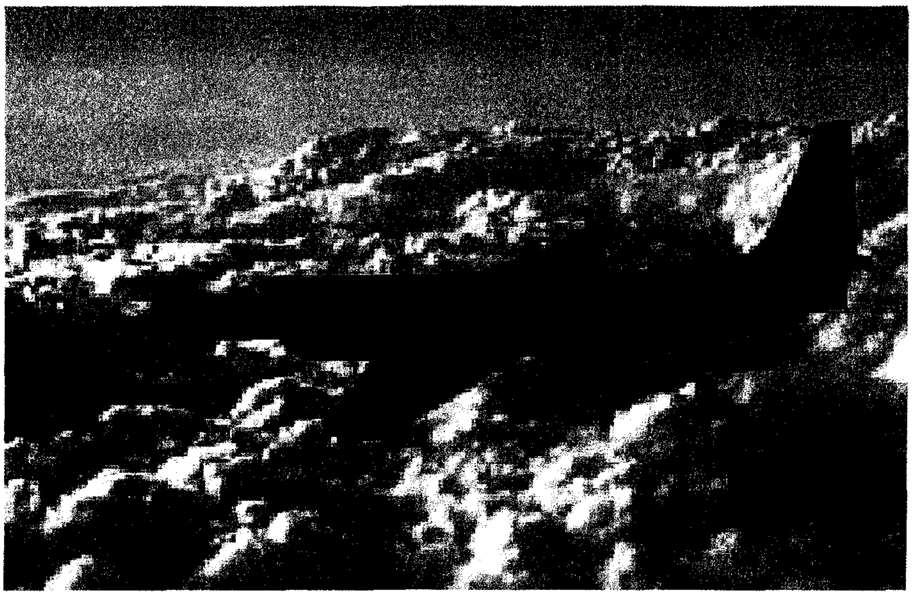


Figure 7.1: Intelligence, surveillance and reconnaissance platforms such as the U–2 increase battlespace awareness.

The information exchange between different Services and components and between all levels of command should be survivable, interoperable, and flexible, even if an intermediate level is disabled. This is achieved with the Global Command and Control System (GCCS.) GCCS provides a common operational picture (COP) of the battlespace to the warfighter, within a modern C4 system capable of providing effective support well into the 21st century. The JFACC uses the following C4I resources to conduct air operations.[562]

European reconnaissance, surveillance and electronic intelligence (ELINT) capabilities have recently been enhanced by the French and British E3 AWACs aircraft and by the British and German reconnaissance variants of the Tornado. Electronic intelligence assets, however, are scanty, and reconnaissance squadrons elsewhere are obsolescent and only clear-weather capable. There is no European real-time reconnaissance acquisition and distribution system. The greatest European weakness, however, is dependence on US C^3I systems. Without such facilities, European aerial forces would be operating out of area in circumstances at least a generation behind those of Desert Storm and Deliberate Force.[563]

[562] US Air Force, Ibid.
[563] Mason, Tony, Ibid, p. 157.

7.2. THEATER AIR CONTROL SYSTEM

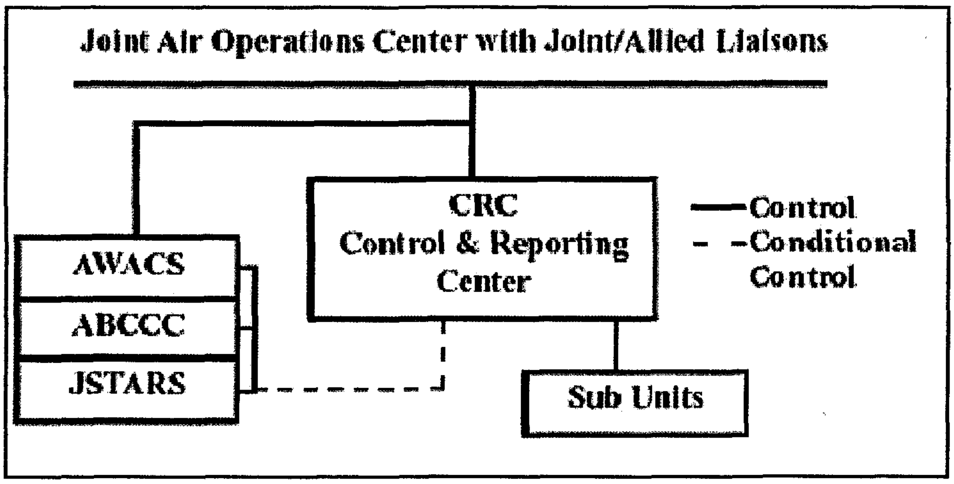


Figure 7.2: Theater Air Control System.

The Theater Air Control System (TACS) povides an overarching means of controlling air functions. It includes the personnel, procedures, and equipment necessary to plan, direct, and control air operations and to coordinate air operations with other components. It is composed of control agencies and communications-electronic (ELINT) facilities to provide centralized control and decentralized execution of air operations.[564] The TACS is a hierarchy of organizations and C2 systems to plan, direct, and control theater air operations and coordinate air operations with other Services and allied forces. The TACS airspace control role is to be the executor of the ACP and ACO. The following elements of the TACS coordinate, integrate, and regulate airspace activities within the Air Force.[565] The radar-equipped C^2 elements of the TACS provide mobility and communication information interface, as well as automation. TACS ground elements use the Modular Control System (MCS). Airborne elements include the Airborne Warning and Control System (AWACS), airborne battlefield command and control center (ABCCC), and the joint surveillance, target attack radar system (JSTARS).[566] Figure 7.3 shows the kinds of communication links used in current theater air operations. Some of the critical links are vulnerable to cheap, mobile, low-power jammers that would be easy for an enemy to obtain.[567]

---

564 US Air Force, Ibid.
565 Keys, Ronald E., "Airspace Control in the Combat Zone", Air Force Doctrine Document 2-1.7, Air Force Doctrine Center, U.S.A., 4 June 1998, p. 32.
566 US Air Force, Ibid.
567 Buchan, Glenn C., "Strategic Appraisal: The Changing Role of Information in Warfare - Implications of Information Vulnerabilities for Military Operations", Chapter 10, RAND Publications, MR1016, Santa Monica, California, U.S.A., 1998.

Aerial warfare has, during the postwar ear, seen a decline in the number of aircraft engaged in combat and the increasing importance of each aircraft. As this has occurred, the ability to submerge the tactical within the strategic has declined. At the same time, the quality of C^3I for aerial warfare has soared. During Desert storm, the combination of airborne sensor and data-management systems, such as AWACS, with computerized mission-planning systems permitted theater air commanders to combine campaign strategy with mission execution. The quantity and quality of data made it possible to respond rapidly to changing circumstances.[568]

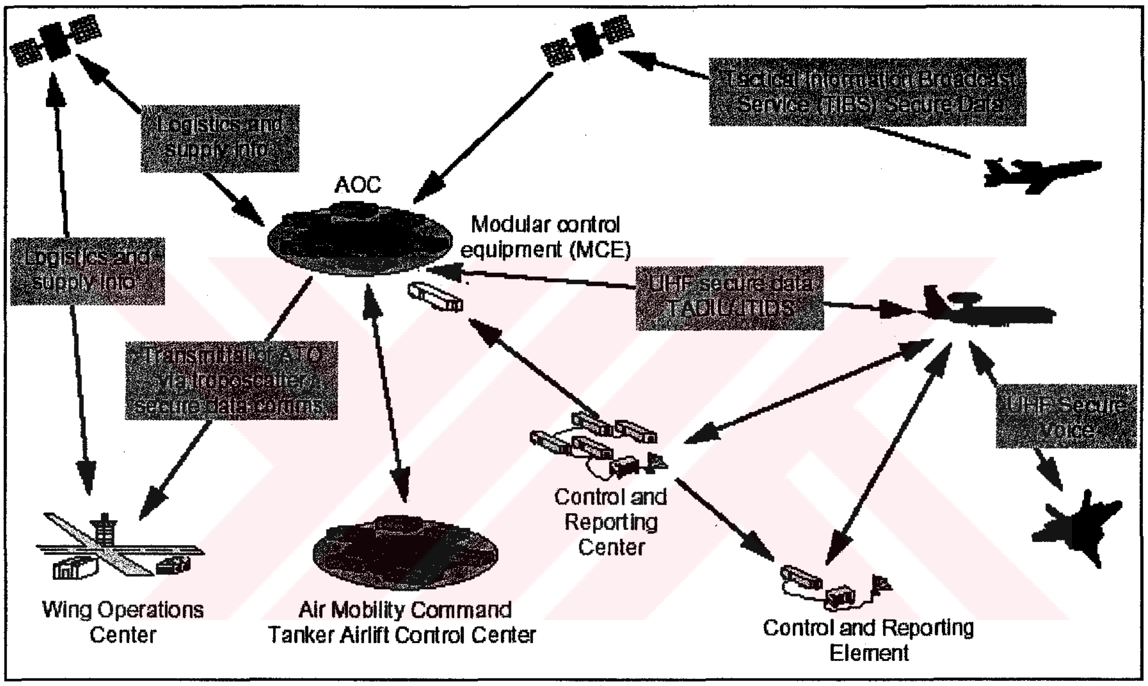


Figure 7.3: Typical theater air communication links

7.3. AIR OPERATIONS CENTER

The Air Operations Center (AOC) is the principal air operations installation from which aircraft and air warning functions of combat air operations are directed, controlled, and executed.[569] It provides centralized planning, direction, control, and coordination of air operations. Within the AOC, the airspace management and control team coordinates and integrates the use of airspace in a combat area. Integrated into both the combat plans division and the combat operations division within the AOC, the airspace management and

[568] Friedman, George & Meredith, Ibid, p. 370.
[569] US Air Force, Ibid.

control team accomplishes combat airspace planning and execution.[570] The AOC includes the equipment and personnel necessary to accomplish the planning, directing, controlling, and coordinating of theaterwide air operations. It has the capacity to display the current air and surface situation, using data from many sources. The AOC plans mission requirements and uses the ACP to deconflict missions and targets.[571] Two major sets of systems and processes are central to the Air Force's ability to conduct operations. The first includes all the systems that actually collect the basic intelligence data necessary to support operations, plan the operations, and execute them.

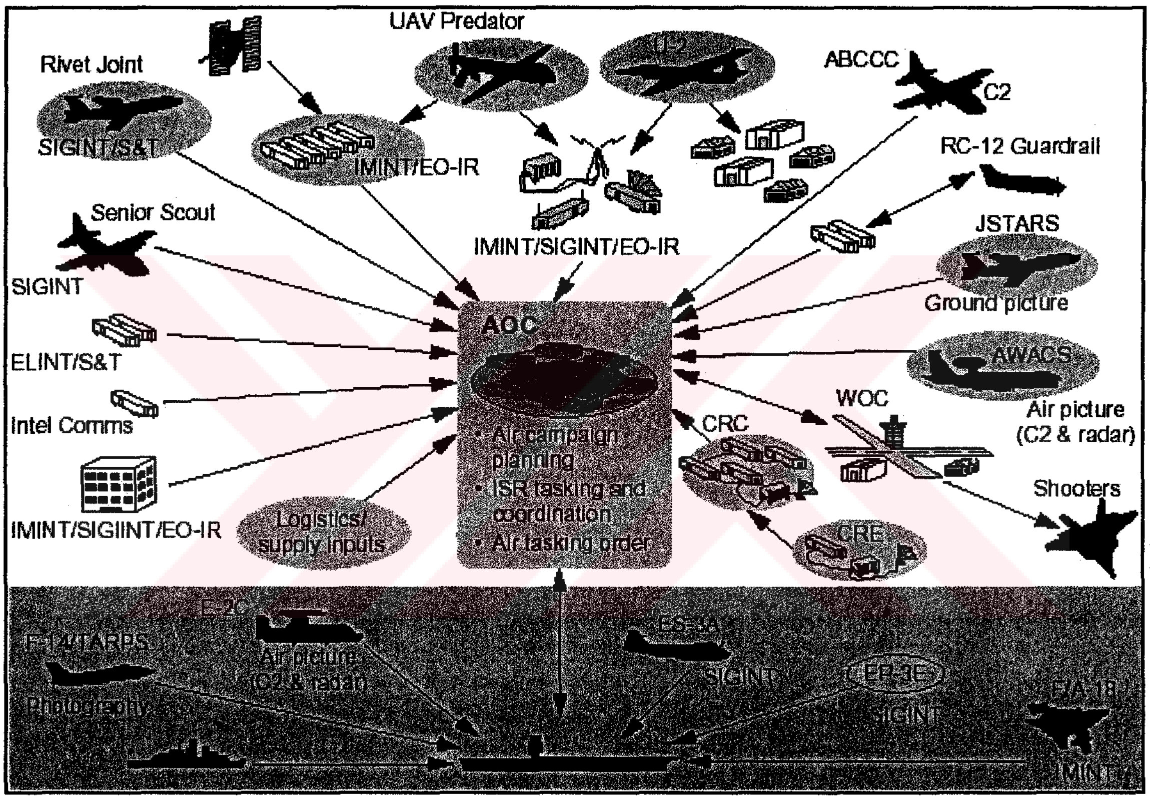


Figure 7.4: Air Force Combat Operations

Figure 7.4 shows some of the critical systems that the Air Force currently relies on and how they are wired together. The most important elements include the following:[572]

1. The whole array of intelligence-collection sensors, platforms, processors, and analysts that collect and analyze the information necessary to provide planners a

---

[570] Keys, Ronald E., Ibid, p. 32.
[571] US Air Force, Ibid.
[572] Buchan, Glenn C.,Ibid.

sense of what is going on, warn them of attacks, allow them to target weapons or otherwise conduct operations, and allow them to assess the effects of earlier operations

2. The planning and command center(s) where information is integrated, plans are constructed, orders are given, and progress of operations is monitored.
3. The forces that execute the operations.
4. The communications systems that wire all of the critical systems together.
5. Systems that provide other critical information to planners and operators.

7.4. CONTROL AND REPORTING CENTER

The control and reporting center (CRC) is directly subordinate to the AOC and is the senior TACS radar element responsible and implements theater mission control through employment of C^2 elements for the decentralized execution of air defense and airspace control. It also serves as the primary command, control, and surveillance facility within the TACS.[573]

The CRC's primary mission is to provide airspace management and airspace control to include: air traffic detection, tracking and identification, scramble or airborne orders, data link management, and management of air defense activities within its AO. Additionally, it establishes C^2 liaison, mission control, navigational air rescue assistance, aircraft threat warning, and coordination with artillery warning control centers and the friendly artillery warning service. The CRC may further delegate control and surveillance areas to other radar units or AWACS within its AO for optimum radar and radio coverage and management of air operations. These areas will normally remain static unless mission requirements or equipment status dictate adjustment.

In a TACS environment, the CRC communicates up to the AOC, down to subordinate units, and laterally to other TACS/joint/allied units. It provides management of air operations, weapons control, air surveillance and identification functions, and also directs the region or sector air defense. The CRC relays instructions and information from the AOC to subordinate or lateral units, determines ground rules, and coordinates assignment

[573] Keys, Ronald E., "Airspace Control in the Combat Zone", Air Force Doctrine Document 2-1.7, Air Force Doctrine Center, U.S.A., 4 June 1998, p. 34.

of targets to ensure defensive assets of all components are employed in mutually supporting roles within its assigned AO. The CRC also detects, identifies, collects, and reports all air activity within its assigned AO and provides the digital data link interface between Air Force, Army, Navy, and Marine Corps joint tactical air operations systems, as well as those of allied nations. The CRC performs the airspace control function within the AO.[574]

The CRC battle staff directs fighter aircraft and air defense artillery assets necessary to defend its assigned area. The CRC battle commander normally establishes ground rules for initial assignment of airborne targets to air defense artillery. All air defense elements coordinate continuously with air defense artillery fire coordination units to eliminate duplication of efforts and to ensure adequate commitment of assigned weapons against hostile threats. The authority to exercise TACON of weapon systems may be delegated to the CRC. The authority to declare a hostile in the area of surveillance and identification may also be delegated.[575]

7.5. AIRBORNE WARNING AND CONTROL SYSTEM

The primary role of the Airborne Battlefield Command and Control Center (ABCCC) is to provide C^2 of air assets that support the land component commander. It can also act temporarily as an extension of the AOC for battle management and execution of the daily ATO in the close battle. The ABCCC can be employed in the absence of ground-based TACS elements unilaterally or with other airborne elements of the TACS. The ABCCC provides procedural (i.e., nonradar) aircraft control. It can also function in a limited role as a backup ASOC to assign or divert sorties to more lucrative targets, coordinating with the AOC and Army command and control centers.[576]

The Airborne Warning and Control System (AWACS) provides the TACS with a flexible and capable airborne radar platform. It provides an initial battle management function and command and control capability and should be among the first systems to arrive in any new theater of operations. It provides early warning, radar surveillance, management of air

---

[574] US Air Force, Ibid.
[575] US Air Force, Ibid.
[576] Keys, Ronald E., Ibid, p. 36.

operations, and weapons control functions. The AWACS allows detection of low-flying aircraft and missiles and provides control of aircraft beyond the coverage of ground-based radar. AWACS can detect and identify hostile airborne threats and assign weapon systems to engage enemy targets.[577]

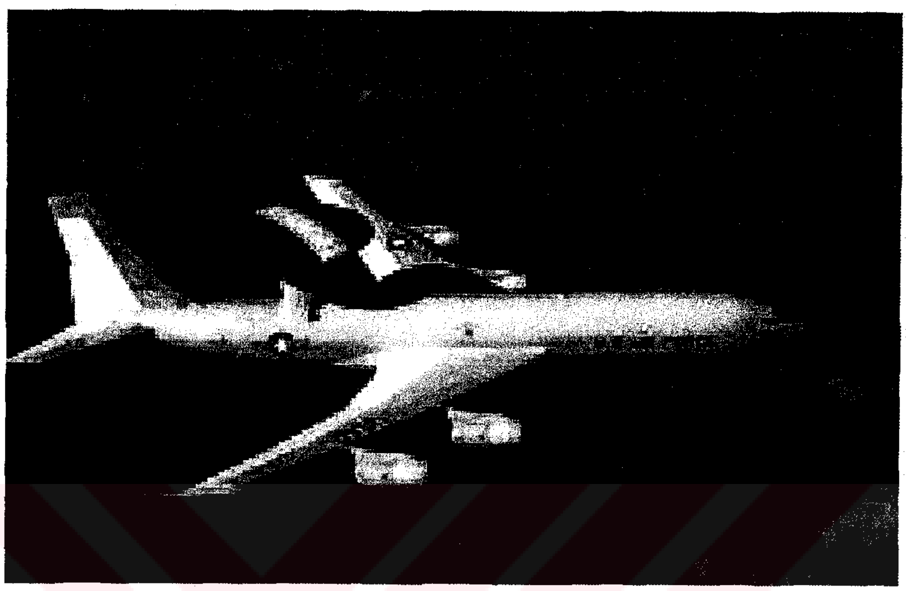


Figure 7.5: E–3 Airborne Warning and Control System (AWACS) aircraft are a key element of C2.

The extent, variety and sophistication of airborne SIGINT operations have increased markedly in Asia over the past decade. Russian SIGINT flights around Japan have been greatly reduced. But US airborne activities in the western Pacific have been upgraded, while eight regional countries have been acquiring their own capabilities –viz.: Japan, South Korea, China, Taiwan, Australia, Singapore, Thailand and India. Airborne systems are very expensive to operate and maintain, but they provide the only cost-effective means for regular, real-time surveillance of the electromagnetic emissions in important parts of the spectrum that are undetectable from ground sites.[578]

The primary airborne collection mission is electronic intelligence (ELINT), involving 'ferret' flights designed to intercept and record the emissions of radars and other radio/electronic systems –garnering data about the signal sources, strengths and characteristics (such as operating frequencies, pulse repetition rates, antenna rotation

[577] US Air Force, Ibid.

[578] Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm

speeds, etc.), to map air defense networks, airfields and missile batteries for target planning purposes. These flights are sometimes deliberately provocative, intending to generate programmed responses. Others are equipped for interception of naval radars and emitters, enabling them to locate, identify and track (and plan electronic or missile attacks against) surface ships. For many countries in Asia, airborne ELINT systems provide the primary means of ocean surveillance. Some aircraft carry both passive ELINT and active EW systems, such as jammers and electronic counter-measures (ECM) equipment, allowing them to monitor and record some signals for intelligence purposes while jamming or manipulating and deceiving other electronic systems. Others are configured for COMINT, loitering for hours in favorable radio reception areas to intercept HF and VHF radio communications. More specialized aircraft focus on the interception of the telemetry and associated signal traffic generated during foreign missile tests, or on special types of communications.[579]

The most modern US systems are able to intercept e-mail and computer-to-computer data traffic, as well as cell phone traffic, serving cyber-warfare tasks rather than more conventional SIGINT collection missions. Special receivers have been installed on at least one US Air Force SIGINT aircraft, and were reportedly also carried by the Navy EP-3 involved in the incident off Hainan on 1 April 2001, which intercept the proforma data codes used in computer-to-computer data exchanges. The proforma include the dial tones of protocols and link-ups that determine the signaling method (such as data transfer multiplexers and private branch exchanges) and the paths and speeds of data transmission. The airborne cyber-warriors are reportedly able to 'conduct intrusions of foreign computer systems', and hence manipulate, deceive or disable them.[580]

The US continues to operate by far the largest and most active, as well as the most advanced, fleet of SIGINT aircraft in the Asia-Pacific region. More than 30, US aircraft are engaged, several of them on a daily basis, in collecting SIGINT of some sort or another around East Asia and the western Pacific. The US now flies more than 400 reconnaissance

[579] Cereijo, Manuel, Ibid.
[580] Fulghum, David A., "China May Sell EP-3 Secrets", Aviation Week & Space Technology Magazine, U.S.A., 16 April 2001, p.37-38; and Arkin, William, and Robert Windrem, "The U.S.-China Information War: Machine-to-Machine, Battles a Backdrop to EP-3 Incident", MSNBC Web Page, U.S.A., 19 August 2001, Available on site: http://www.msnbc.com/news

missions a year along the periphery of China, or an average of more than one per day,[581] mostly for SIGINT purposes, and mostly with flights originating from bases in Japan. The US Air Force has a base for RC-135V/W Rivet Joint SIGINT aircraft in Japan. These aircraft, which carry a SIGINT crew of some 21-27 radio and radar intercept officers, linguists and maintenance technicians, as well as three pilots and two navigators, and which can stay aloft (with aerial refueling) for 10-30 hours, are used for intercepting both communications and electronic signals. The US Navy has a squadron (VQ-1) of six EP-3E ARIES (Advanced Reconnaissance Integrated Electronics System) II SIGINT aircraft, based in Washington, but with a permanent detachment of 1-2 aircraft in Japan. Another eight ES-3A Shadow aircraft are used for carrier-based SIGINT operations, with six home-based at the North Island Naval Air Station in San Diego, California, and two at Japan.

Table 7.1: SIGINT aircraft in Asian countries

Country	Aircraft	Number	Range (km)	Comments
Japan	YS-11E EP-3 EC-1	10 5 1	2,320-2,670 7,760 3,000	Equipped with J/ARL-1 J/ARL-2 SIGINT system.
China	Tu-154M	4	3,700-5,200	
Taiwan	EC-130 S-70C(M)	1 2	3,360 600	
S. Korea	Hawker 800	4	3,620	
Singapore	EC-130H Fokker F50 Maritime Enforcer	2 6	3,750 1,400-2,000	Equipped with the ARGO Systems AR-7000 Black Crow ELINT system. Five others (Nos. 714-718) carry Israeli-supplied ELINT and COMINT systems.
Thailand	IAI Arava	3	1,300	
Australia	EP-3C EC-130H King Air 200 Learjet	2 1 1 1	5,000-7,000 3,750 3,650 3,900	Two P-3C Orion LRMP aircraft configured for SIGINT; One C-130H Hercules aircraft configured for SIGINT

Japan now has about 16 dedicated SIGINT-collection aircraft, half a dozen electronic warfare (EW) training aircraft with some ELINT capabilities, and 13 E-2C Hawkeye and four E-767 airborne early warning and control (AEW&C) aircraft with substantial

[581] Cossa, Ralph A., "U.S.-China Relations: The Crew's Home; Now What?", PacNet 15A, CSIS, U.S.A., 16 April 2000, Available on site: http://www.csis.org/pacfor/pac0115A.htm.

secondary ELINT capabilities.[582] In 2000-01, South Korea acquired four specially-equipped Hawker 800 SIGINT aircraft, containing both COMINT and ELINT sub-systems (with coverage of up to 40 GHz), together with an associated ground station for data processing.[583]

The Chinese Air Force operates four Tu-154M long-range transport aircraft modified for SIGINT collection.[584] Another Tu-154M SIGINT aircraft is operated by China United Airlines (CUA), the commercial arm of the Air Force; it uses civil markings (CUA B-4138), but was equipped in 1995 with a synthetic aperture radar (SAR) as well as COMINT and ELINT equipment for covert SIGINT operations.[585] Taiwan has a SIGINT-equipped C-130H Hercules aircraft, and two S-70C(M) Thunderhawk helicopters.[586]

In Southeast Asia, Singapore acquired modest but sophisticated airborne SIGINT capabilities in the early 1990s. Two of the Air Force's C-130H Hercules aircraft have been equipped with extensive suites of Israeli-supplied COMINT, ELINT and EW systems for strategic, operational and tactical SIGINT mission.[587] Singapore also has six Fokker F-50 Maritime Enforcer Mark-2 maritime patrol aircraft, which are equipped with modern SIGINT systems, and which operate around Southeast Asian waters from the Andaman Sea to the South China Sea.[588] Since early 2001, Singapore has also been examining possible aircraft 'for an emerging requirement for a high-altitude ELINT/SIGINT platform'.[589]

---

582 Ball, Desmond, and Euan Graham, "Japanese Airborne SIGINT Capabilities", Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, December 2000.
583 Streetly, Martin, "Asia Pacific Boosts Airborne Surveillance", Jane's Defense Weekly, U.S.A., 13 February 2002, p. 27-28.
584 Streetly, Martin, Ibid, p. 27.
585 Smith, Charles R., "Chinese Airlines Serve PLA Military", Newsmax.com Web Page, 16 April 2002, Available on site: http://www.newsmax.com/archives/articles/2002/4/15/172400.shtml; and Sinodefense Web Page, "Chinese Defense Today: Tu-154 Jet Transport", Available on site: http://www.sinodefense.com/airforce/aircraft/transport/tu154.asp.
586 Ball, Desmond, "Signals Intelligence in Taiwan", Jane's Intelligence Review, Australia, November 1995, p. 508.
587 Ball, Desmond, "Developments in Signals Intelligence and Electronic Warfare in Southeast Asia", Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, December 1995, p. 16-17.
588 Streetly, Martin, Ibid, p. 28.
589 Angelfire Web Page, "Singapore Looking for a SIGINT Aircraft", Gulfstream News, Available on site: http://www.angelfire.com/biz6/gulfstream/gulfnews.html.

In 1995-98, the Royal Australian Air Force acquired two EP-3C Orion aircraft which had been specially configured for SIGINT operations,[590] which were used extensively around Timor in 1999-2000, and which were more recently used in the Persian Gulf in support of Operation Enduring Freedom.[591] The RAAF reportedly also operates a SIGINT-configured C-130H Hercules aircraft; the Australian Army has a King Air 200 fitted for ELINT operations; and the Navy has a Learjet specially equipped for ELINT and electronic warfare activities.[592]

7.6. AIRBORNE BATTLEFIELD COMMAND AND CONTROL CENTER

The Airborne Battlefield Command and Control Center (ABCCC) is an integral part of the airborne elements of the TACS. It is a specialized airborne command, control, and communications (C^3) center equipped with extensive communications systems providing the capability to perform both the AOC and air support operations center (ASOC) functions. ABCCC's primary function is battle management of tactical air operations - directing air support to ground operations in the forward area. As an extension of the AOC, ABCCC can scramble or divert assets as mission requirements dictate, while assisting the ASOC by providing C^2 services in the forward area beyond the ASOC's communications range.[593]

The EC-130E is a modified C-130 'Hercules' aircraft designed to carry the ABCCC capsules. While functioning as an extension of ground-based command and control authorities, the primary mission is providing flexibility in the overall control of tactical air resources. In addition to maintaining control of air operations, ABCCC can provide communications to higher headquarters, including national command authorities, in both peace and wartime environments. The ABCCC system is a high-tech automated airborne command and control facility featuring computer generated color displays, digitally controlled communications, and rapid data retrieval. The platform's 23 fully securable

590 Barker, Geoffrey, "RAAF Spy Planes Secretly Watch Indonesia", Australian Financial Review, Australia, 11 May 2000, p. 1,10.
591 Ball, Desmond, "Silent Witness: Australian Intelligence and East Timor", The Pacific Review, Vol.14, No.1, Australia, 2001, p.41, 45-46.
592 Ricketts, Peter, "Special Mission Aircraft: Same Result, Lower Cost", Asia-Pacific Defense Reporter, Australia, March/April 2002, p.44-45.
593 US Air Force, Ibid.

radios, secure teletype, and 15 automatic fully computerized consoles, allow the battlestaff to analyze current combat situations and direct offensive air support.[594]

Figure 7.6: Airborne Battlefield Command and Control Center (ABCCC) provides critical C^3 functions in the Theater Air Control System.

The success of the air campaign during Desert Storm depended on the allies' ability to suppress the Iraqi air defense system; that is, to prevent the launching of both surface-to-air and air-to-air missiles. If that failed, the allies had to confuse the missiles' sensors; and if all else failed, they had to have aircraft sufficiently agile to evade the missiles.

The Iraqi air defenses consisted of radar installations linked into a command and control (C^2) system capable of activating ground-based air defenses and aircraft. The United States had excellent intelligence on the system, from the French, who designed it, and from the Soviets, who supplied many of the surface-to-air missiles used. The United States also knew a great deal about it from signals and electronic intelligence (ELINT).[595]

Constant communications with most air and ground agencies in the TACS keeps the ABCCC battlestaff abreast of developing air and ground situations and maintains higher headquarters coordination for positive control of air assets. Although not radar equipped, ABCCC's computerized tactical battle management system (TBMS) is linked with the

---

[594] Special Operations.Com Web Page, "EC-130E Airborne Battlefield Command and Control Center", 2002, Available on site: http://www.specialoperations.com/Aviation/EC_130/ABCCC/default.htm

[595] Friedman, George & Meredith, Ibid, p. 286.

joint tactical information distribution system (JTIDS) and other intelligence, surveillance, and information fusion systems providing capability for improved situation awareness. The ABCCC can deploy in an initial response to world events and to provide C^2 services as the theater situation matures. ABCCC is also well suited to support combat search and rescue (CSAR) and air theater missile operations.[596]

7.7. AIR FORCE RADAR (ELINT) SYSTEM AND JSTARS

The EP-3E Aries 2 aircraft is equipped with the APS-134 frequency agile search radar, located in a ventral dome just forward of the wing. Data collected by the aircraft are processed by the AYK-14 computer and given form by the ASA-66 tactical display. Other specialized electronic systems include the ARR-81 for communications intercept and analysis, the ALR-76 for automatic location and identification of radars, and the ALR-82 as an aide in intercepting and classifying electronic signals.

The main target of ELINT is radars. The three broad categories of radars are target acquisition (the classic, long-range circular scan), target tracker (a sector search with pinpoint accuracy) and weapons guidance, which is actually on the air defense missile. What crews don't know without collateral intelligence is whether the missile is still on the launching rail or already in flight. Communications intelligence can sometimes fill in that blank by listening to the chatter between missile crews and their area directors. The primary tool of the ELINT operators is the direction-finding antennas that dot the EP-3.[597]

During Desert Storm, the United States deployed an experimental aircraft with real-time information sensing equipment, joint surveillance and target-attack radar system (JSTARS), which was a resounding success.[598] JSTARS is not just an aircraft. It's really two systems: the Air Force E-8 aircraft and the Army ground-station modules. JSTARSs first deployed to support Operation Joint Endeavor in Bosnia from 14 December 1995 to 27 March 1996.[599] JSTARS is similar to AWACS (airborne warning and control systems), except that where AWACS is designed to manage the air battle, JSTARS is designed to

---

[596] US Air Force, Ibid.
[597] Fulghum, David A., "Flexibility, Endurance Are Valued EP-3 Assets", Aviation Week & Space Technology Magazine, U.S.A., April 2001.
[598] Friedman, George & Meredith, Ibid, p. 148.
[599] Wentz, Larry K., "Bosnia: Intelligence Operations", DDOCCRP Web Page, Chapter IV, U.S.A., Available on site: http://www.ddoccrp.org/bosend.htm

manage the ground battle. The aircraft is a Boeing 707 with a twenty-six-foot-long radar housing underneath the fuselage. JSTARS currently carries a multimode radar system. One of these modes, the wide-area surveillance/moving-target indicator (WAS/MTI), is a Doppler radar that detects the motion of objects. In the WAS mode, the movement of larger armored formations can be detected, while in the MTI mode, individual vehicles can be seen and tracked vehicles distinguished from wheeled vehicles.[600] The Joint Surveillance, Target Attack Radar System (JSTARS) is a long-range, airborne sensor system which provides real time radar surveillance information on moving and stationary surface targets, via secure data links to air and surface commanders. Although JSTARS was not "officially" operational during DESERT STORM, it identified and targeted SCUD missiles and launchers, convoys, trucks, tanks, SAM sites, and artillery pieces. JSTARS information builds situational awareness for the JFC and JFACC to manage air operations, to update target information, and to provide real time targeting.[601]

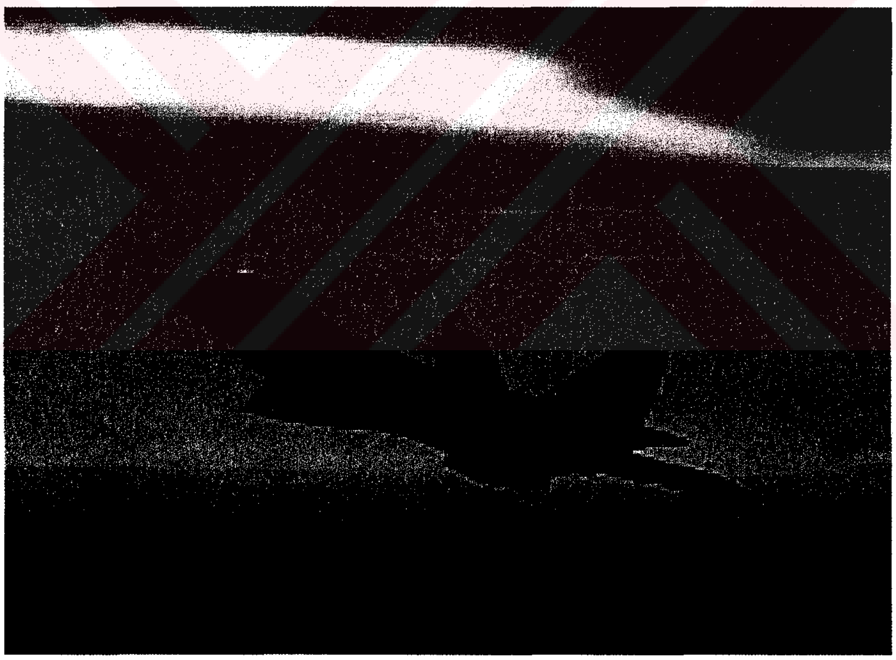


Figure 7.7: The radar being developed for the F-35 Joint Strike Fighter will also be fitted onboard the F/A 22 Raptor.

The second mode on JSTARS board is synthetic aperture radar (SAR). SAR permits JSTARS to produce maps of target areas, or photograph-like images of particular installations. In addition to mapping any stationary target; bridge, aircraft on the ground,

[600] Friedman, George & Meredith, Ibid, p. 148.
[601] US Air Force, Ibid.

tanks standing still, it can also map metallic structures buried beneath the surface. The depth that it can reach is classified.[602] As munitions buried beneath the surface become more important, and mine warfare was certainly a critical part of Desert Storm, this ability will be crucial. JSTARS was able to map the Iraqi minefields in southern Kuwait.

In its WAS-MTI mode, JSTARS can cover a fifty-thousand-square-kilometer region. This meant that during Desert Storm, a single JSTARS aircraft was able to provide complete coverage of Kuwait. It can also focus down to a twelve-by-twenty-mile segment, where it can distinguish individual vehicles. A fleet of JSTARS can provide coverage of any size battle area.[603]

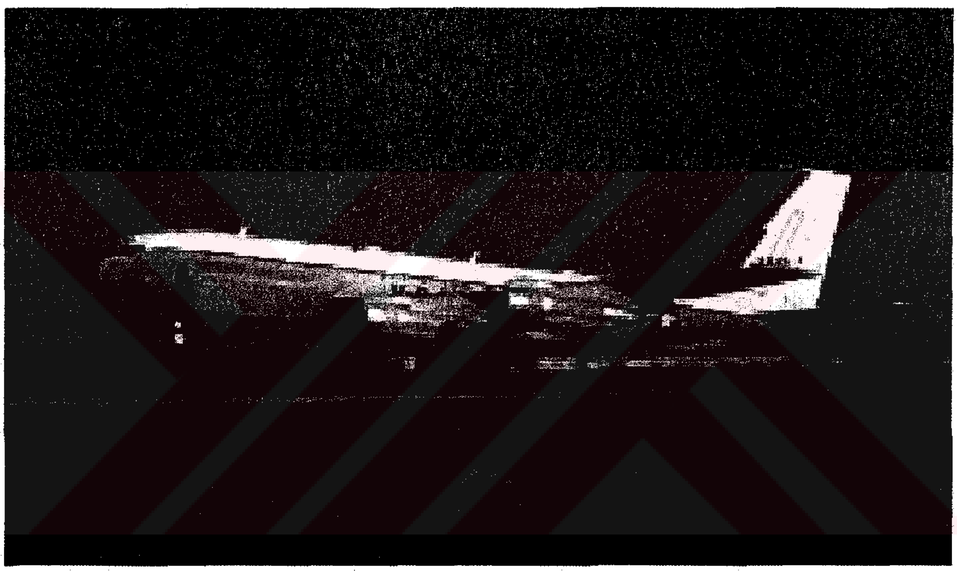


Figure 7.8: RC–135 Rivet Joint Provides Battlespace Assessment.

Advances in technology make today's F/A-22 Raptor very different from the first planned. Technological advancements in the fire-control radar and integrated avionics, combined with the advent of smaller, very precise munitions, create a far more powerful air-to-ground strike system. One change will be the insertion of the new, evolved radar being developed for the F-35 Joint Strike Fighter. This sensor has an air-to-ground mode not available in the AN/APG-77(V) that is currently being installed in the new fighters. The new radar will be smaller and lighter that the current system. These changes will also be

602 Grier, Peter, "Joint STARS Does Its Stuff", Air Force Magazine, U.S.A., June 1991, p. 40-41.
603 Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 148-149.

needed to accommodate the new, small-diameter bomb. There are also some inherent ELINT and SIGINT capabilities in the F-35's sensors which may be carried over into the Raptor.[604]

RIVET JOINT is an airborne signals intelligence (SIGINT) collection and reporting platform. Working in conjunction with the AWACS and JSTARS aircraft, RIVET JOINT provides near-real-time assessment of hostile airborne-, land-, and sea-based electronic emitters via secure communications. RIVET JOINT capabilities "round out" the radar tracking information provided by the AWACS and JSTARS by correlating location, emitter type, and mode of intercepting signals.[605]

U.S. Air Force wants to replace its E-3 AWACS air-surveillance, E-8 Joint-STARS ground surveillance and RC-135 Rivet Joint electronic intelligence-gathering (ELINT) fleets with the new, multi-sensor command and control aircraft (MC2A). They put many advanced radar antennas on a single aircraft without creating electronic interference between the radars or with other electronic intelligence (ELINT) sensors. Designers deal with how the combination of antennas will not affect the aircraft's flying characteristics. To identify and resolve potential problems, Air Force planners are looking at a four-phase approach to refining the new Boeing 767-based design. In phase one, they would put a ground moving target indicator (GMTI) radar on the green aircraft. This mission now belongs to Joint-STARS. Phase two would add a battle management, communications and intelligence capability in the aft section of the aircraft. The Air Force wants to transfer the Rivet Joint capability to a 767 as part of the total recapitalization of the intelligence, surveillance and reconnaissance (ISR) fleet and to enable it to carry out more missions from a single aircraft type. Phase three would largely complete the baseline aircraft by putting on an air moving target indicator (AMTI) radar. This is currently the AWACS mission. The capability would likely involve attaching a top-hat or a circular dome antenna to the top of the aircraft aft of the wings. A final phase of the program would involve a separate modification of some MC2A aircraft for passive operations (few electronic emissions) as signals and communications intelligence-gathering platforms, a role now performed by the Rivet Joint.

[604] Chaisson, Kernan, "New Radar for Raptor's New Mission", Journal of Electronic Defense, U.S.A., November 2002. Available on site: http://www.jedonline.com
[605] US Air Force, Ibid.

The wave of the future is netting and integrating as many types of radar as it can be to accomplish a variety of missions. It's common sense that they would need to be looking into detecting stealthy targets. But the current focus is to get Astor deployed as quickly as possible to do its baseline ground surveillance mission.

The U.S. Air Force has developed and intensively tested the "Paul Revere" testbed aircraft in August 2002. The system has already been deployed to South Korea as part of a ground station and teamed with a UAV control system, will likely next be demonstrated on Paul Revere. It's a resource management tool with a machine-to-machine control program that runs at two levels. First, it monitors all the resources and sensors on board the aircraft. The program also looks at all the resources available on the network. It determines where the assets and sensors are, as well as their capabilities and fields of view. When the request for a piece of data about a certain location comes in, the resource manager determines who's in the best position to capture the data, and it automatically allocates the resources.[606]

7.8. AIRSPACE CONTROL AND INTEGRATION WITH AIR OPERATIONS

Theater airspace control can become very complex since all military components, and possibly civilian traffic, can execute operations in the same airspace. The timely exchange of information over reliable, interoperable means of communication is required to effectively coordinate, integrate, and deconflict the airspace used for friendly air operations. The ACA develops and implements an ACP based on the JFC's guidance. Execution of the plan is accomplished through ACOs which provide specific airspace control procedures applicable for defined periods of time. The main goals are deconfliction of all airspace users and their air assets, enhancement of combat operations, and protection of friendly forces from enemy air and missile attacks.

Standardized procedures and close coordination help to facilitate common understanding, reduce the possibility of confusion, and contribute to the overall effectiveness of air operations. The JFC establishes the geographic boundaries within which airspace control is to be exercised and also provides priorities and restrictions regarding the use of the airspace. Airspace control is normally one of the primary functions of the Air Force TACS.

[606] Fulghum, David A., "Key Decisions Remain For New Intel Aircraft (cover story)", Aviation Week & Space Technology, Vol.157, Issue 4, Washington, U.S.A., 22 July 2002, pp.178.

The Air Force's C^2 system is structured to conduct airspace control, OCA and DCA operations, and other air operations to minimize the risk of harm to friendly forces. Since different components have OPCON of specific air assets, the C^2 structure is designed to integrate with other components to provide responsive and timely support. Integration with hostnation airspace and air defense control structures is also essential.[607]

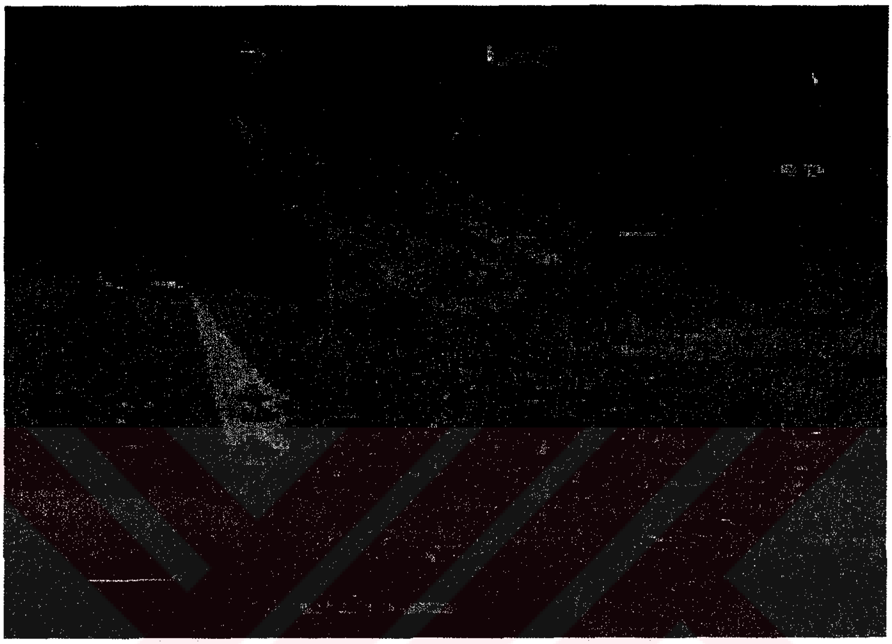


Figure 7.9: The Theater Air Control System plans, directs, and controls air operations.

Unity of command is imperative to employ forces effectively. Because of the integrated relationships and responsibilities between airspace control and OCA and DCA operations, the ACA and AADC duties should normally be performed by the JFACC. These functions often rely on the same resources and are frequently executed simultaneously in the same airspace. Assigning responsibility and authority to coordinate and integrate airspace control and air operations to one air commander greatly enhances the effort to gain and maintain control of the air environment. The ACP is tied to all other air operations plans. These operations are closely coordinated and integrated with each other, as well as with other operations in the air, on land, and at sea. Centralized control of these operations

[607] US Air Force, Ibid.

provides unity of command, optimizes weapon systems and target pairings, and minimizes the possibility of fratricide.[608]

7.9. FRIENDLY AND ENEMY COMBAT IDENTIFICATION

Combat Identification (CID) is the process of attaining an accurate characterization of entities in a combatant's area of responsibility to the extent that high-confidence, real-time application of tactical options and weapon resources can occur. The objective of CID is to maximize combat/mission effectiveness while reducing total casualties (due to enemy action and fratricide).[609] Combat Identification requires the assured, reliable identification of friendly versus adversary forces, thus enabling the engagement of targets at weapon range rather than at visual identification range. Air Force Combat Identification uses interrogation/response for aircraft targets, and it maintains compatibility with the current MK-12 and systems used by commercial aviation.[610] The objective of combat identification (CID) is to maximize mission effectiveness by providing high confidence, positive identification of friend or foe. Accurate and timely identification (ID) enhances real time tactical decisions and optimizes weapons employment, allowing timely engagement of enemy aircraft and missiles, conserving resources, and reducing risk to friendly forces.[611]

CID information may be obtained from onboard or off board surface, air, and space systems, and through airspace control measures documented in the ACP or ACO. To avoid a single point of failure, no one node will act as an exclusive conduit of all CID information. ELINT methods, which provide the most rapid and reliable means of identification, are normally used when available.

Airspace control requires an effective combination of positive and procedural ID. Both are intended to effectively provide safe and flexible use of the airspace. Positive identification relies on a high confidence ID derived from visual observation, radar observation of point

---

608 US Air Force, Ibid.
609 Cabasso, Jacqueline, "Joint Warfighting Science and Technology Plan: Combat Identification-Chapter IV", Western States Legal Foundation, Oakland, California, 2003, Available on site: www.wslfweb.org/docs/dstp2000/jwstppdf/08-CID
610 US Department of Defense, "Science and Technology-Chapter 17", U.S.A., 1996, Available on site: http:// www.defenselink.mil/execsec/adr96/chapt_17.html
611 US Air Force, Ibid.

of origin, and/or electronic means by an authorized control facility. Procedural control relies on a combination of airspace control measures documented in the ACP or ACO. For most scenarios, a combination of positive and procedural ID techniques is used to identify friendlies, neutrals, and foes.[612] The Army Combat Identification program uses a millimeter wave interrogation/response system to identify friendly systems on the battlefield and is exploring the advancements offered by improved situational awareness derived from battlefield digitization. Other Air Force and Navy combat identification efforts focus on noncooperative target recognition technologies, including inverse synthetic aperture radar imaging, jet engine modulation, and unintentional modulation on pulse-based specific emitters, as well as improved waveforms for the Mk 12. Success in all three areas -cooperative systems for ground targets, cooperative systems for air targets, and noncooperative systems -is needed to achieve an adequate combat identification capability.[613]

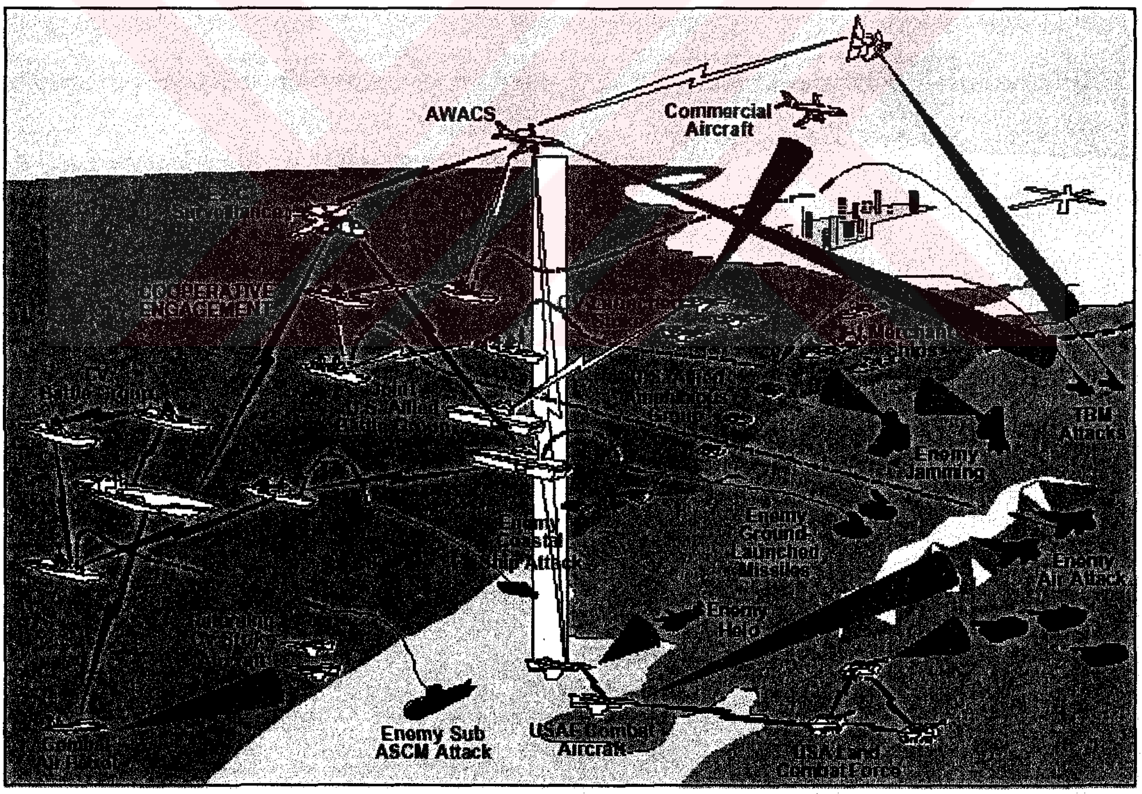


Figure 7.10: Combat Identification Concepts

[612] US Air Force, Ibid.
[613] US Department of Defense, Ibid.

The primary objective for CID is to correlate and assign a foe, friend, or neutral identification label to a "target". The identification label can be assigned at any time from initial detection of the potential target to weapon employment. To be useful for a direct-fire engagement, the correct target label must be correlated to a sensor return that is in a "weapon sight" (e.g., radar, laser, or thermal sight). Indirect-fire weapons or supporting-fire weapons operate from a different perspective as they cannot "see" the target. The identification is made and sent to the weapon by the fire requester or a surveillance/reconnaissance platform; the weapon is correlated to the specified target position. There are two classes of materiel solutions:[614]

- *Sensors:* the target is characterized either noncooperatively (e.g., radar signal modulation, high-range resolution radar, or electronic support measures [ELINT]) or cooperatively.
- *C3 (particularly digital datalinks and radios):* the target declares (either periodically or when queried) its identification and position in a reference frame that the "shooter" can correlate with its own weapon and sensor system Additionally, C3 systems are a medium for passing ID information from other sensors or sources.

7.10. OPERATION IRAQI FREEDOM AND DEVELOPMENT OF AIR FORCE ELINT

Since 1996, the US Air Force has used it to deploy thousands of tactical ELINT and SIGINT sensors worldwide, which rely on a variety of technologies ranging from state-of-the-art microwave, magnetic, passive and active infrared to old-fashioned trip wires. However, sensors that both detect and assess are now available. The Integrated Base Defense Security Systems (IBDSS) will integrate, upgrade and expand existing Tactical Automated Security System (TASS) systems, including electronic detection, alarm assessment, access control and communications. Unmanned aerial vehicle (UAV)

[614] Cabasso, Jacqueline, "Joint Warfighting Science and Technology Plan: Combat Identification-Chapter IV", Western States Legal Foundation, Oakland, California, 2003, Available on site: www.wslfweb.org/docs/dstp2000/jwstppdf/08-CID

integrated with ELINT and SIGINT sensors, cameras and other equipment are completely known as the Force Protection Airborne Surveillance System (FPASS).[615]

The US Air Force delivered the first FPASS in 2002 to support Operation Enduring Freedom. FPASS is partially portable. It is can be transported by vehicle in a large suitcase, but it is not small enough to be transported by backpack. Its mission is to provide real-time overhead video imagery for the detection and assessment of weapons threats and battle damage. Each FPASS system contains a ground control station with workstations, laptops, displays, recorder and communications equipment, six UAVs, a remote imagery viewing terminal and interchangeable payloads of color cameras with thermal imagers for day and night time imagery, as well as transportation cases and launch equipment.

UAVs integrated with thermal imagers for night vision, closed circuit television (CCTV), 360-degree turning cameras, radars and sensors (ELINT etc.) are into one system. For portable systems that can't rely on fiber and CCTV, is utilized digital video with RF as the transmission methodology. UAVs send video back to the command center via analog, converting it to digital there. However, some video can be converted to digital right at the camera. Cameras with wide-angle lens are used for area surveillance and assessment, earmarked to automatically cover sensors placed in their field of view.

UAVs can be integrated with the Global Positioning System (GPS), a variety of sensors and Remotely Operated Weapons System (ROWS). With UAVs integrated with GPS, it can be looked in the control room at what is intruding with the exact GPS coordinates of the target. Remote control software and a fiber-optic network system controls four guns in ROWS and 16 video displays. Integrated into ROWS are four cameras. One is a sighting camera showing the potential target. Next to it is a camera with a wide-angle lens to center the view of the potential target. The third is a thermal camera for night vision. There are three cameras mounted on guns, which are protected by a cover referred to as a clamshell. However, when the guns are covered, they are unusable. So a fourth camera checks what's going on before opening the clamshell lid of the other camera.

---

[615] Clarke, Patrick E., "Sun Never Sets on NETCOM Operations", Volume: 7, Issue: 8, U.S.A., 13 October 2003. Available on site: http://www.mit-kmi.com/archive_article

Battlefield intelligence sensors (ELINT, IMINT etc.) are also offered on Integrated Base Defense Security Systems (IBDSS), such as smart seismic sensors. Since they only cover a 75-meter radius, it is necessary to use many of them, placing them that distance apart. Another example is the short- and long-range anti-personnel radar sensors. A short range sensor can detect individuals who are walking or running within 300 meters, and those who are crawling within 150 meters. When a sensor detects something, it sends a radio signal to the command center, which then launches a camera-equipped UAV to get a view of what's there.

The sensors are slated to be used as well for the protection of nuclear sites, in smart gates with entry control and biometric identification, such as fingerprint, eyeball or face recognition. They are also used for weapons-storage and flight-line security.

The TASS sensors with battlefield intelligence sensors, electronic intelligence (ELINT) thermal imagers, CCTV cameras, UAV's, short- and long-range radar and a gun console are integrated. All of this is done with one PC and an XML-based interface, integrated with IP addressability to work on the Internet. IBDSS will provide upgraded sensors and enhancements of TASS equipment including handheld monitors, notebook and desktop computers, software, communications systems and handheld as well as long range thermal imagers. It will also expand the amount of equipment that will be available, incorporating more detection and assessment devices.[616]

[616] Clarke, Patrick E., Ibid.

8. NAVY AND ELINT

Information technologies will so profoundly influence future naval forces and missions that the pursuit of *information superiority* will become a paramount goal in force planning, acquisition, training, and operations. Commercial interests have been the primary cause for the dramatic improvement in and rapid growth of the capabilities of information systems and this trend is expected to continue. The Navy can leverage these technologies to attain military superiority through information superiority by applying them not only to battle management but also to preparation, planning, and logistics.

Information technology will be central to future naval operations and will provide tactical advantages to naval forces. The advantages accrue from development and application of several key technology areas associated with the collection, processing, display, interpretation, and distribution of significant information. Advanced technologies will enhance future naval information capabilities. All naval platforms within a battle group or amphibious-ready group, along with attached and supporting sensors and information transfer systems, will be enhanced in capability as a result of advances in these technologies.[617] Sensor technology is critical to the success of all naval force operational tasks or missions are obvious. Whenever information is required, sensors are utilized to make the physical measurements from which the desired information is extracted. Radar, optics, ELINT, and sonar sensors, through the active or passive exploitation of the physics of wave propagation, give information about distant objects that is useful for general surveillance and situation awareness as well as for more specific purposes, such as real-time target location and weapon guidance. Other sensors, such as position-sensing devices or inertial sensors, produce useful real-time local measurements that can be used to control all kinds of platforms, including whole ships, steerable radar or communication antennas, and gun mounts on ships, or even individual missiles in flight, depending on just where the sensors are located.[618]

---

[617] Naval Studies Board, "Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st-Century Force, Volume 3: Information in Warfare", National Academy of Science, Washington, D.C., U.S.A., 1997, Available on site: http://www.nap.edu/html/tech_21st/iwindex.htm

[618] National Academy of the Science Web Page, "4: Sensors", NAP, U.S.A. Available on site: http:www.nap.edu/html/tech_21st/t4.htm

Continuing exponential reductions in the size and power consumption of computers will increase their role in naval systems. Computers will be used to process raw ELINT and other sensor data into information, transform and transmit that information where it is needed, support combat simulations and rehearsals, store and recall data on operational objective areas, launch information warfare attacks, and assess battle damage, among many other potential, and yet-to-be imagined applications.[619]

Command and control (C^2) is the "exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of his mission." At the center of this system is a complete, accurate, and timely information set on which the commander and his staff base their decisions.

The availability of timely, accurate, and complete information on all aspects of the projected battle space is a key element in the success of the commander's mission. Information, then, can be considered to be a critical driver of warfare and will significantly influence how warfare will be conducted. The concepts of C^3 and IW are complementary but separate and distinct. C^3 develops and uses tactical information to execute missions; IW protects friendly information while offering tactical advantage by attacking and/or exploiting the enemy's information systems. Four key operational concepts embody improved intelligence and command and control:[620]

- Dominant maneuver
- Precision engagement
- Full-dimensional protection
- Focused logistics

8.1. IMPORTANCE OF INFORMATION NETWORKS

Information distribution and control systems in the 2035 time frame will provide a completely transparent and seamless medium for transfer of information to users. Improved connectivity and capacity will facilitate transfer of video, voice, and data to the mobile or disadvantaged user. The military will use channels embedded in the global

[619] Naval Studies Board, Ibid.
[620] Naval Studies Board, Ibid.

information infrastructure built to support commercial and personal uses. Fiber-optic cable-based backbone networks will provide long-haul virtual circuit or datagram services to local networks at permanent camps, bases, stations, and piers. These same networks will also serve satellite ground stations or other remote injection sites. Commercial systems with military special-purpose adjuncts will provide long-haul trunking connection to mobile platforms in all ocean areas around the globe. Surface action groups, amphibious ready groups, and carrier battle groups will coordinate operations by communicating over radio networks using high-frequency (HF), ultrahigh-frequency (UHF) line-of-sight (LOS) packet switched technologies based on asynchronous transfer mode or its derivatives. These backbones along with satellite links will be interconnected with platform-based local area networks (LANs) that support all applications in use on the platform. ELINT and other sensor systems will also transport raw and processed sensor data over these communications channels.

Links to shore-based networks will be available through RF LOS, geosynchronous satellite, or surrogate satellite links. Personal communications system (PCS) links will be available through terrestrial base stations or low Earth orbit (LEO) satellite systems. Figure 8.1 illustrates the composite commercial and unique military network architecture and its global extent. The panel envisions that in 2035, problems associated with the availability of connectivity, capacity, and coverage will be largely solved; however, the potential vulnerability of these systems will require special attention. Commercial network infrastructure will provide interconnectivity to the naval forces, and access will be obtained through lease or outsource arrangements.[621]

It is expected that future tactical communications for each platform will have a scaled version of a family of intelligent programmable digital radios. The radios will utilize multiband, multifrequency antennas, coupled to signal conditioning electronics and converters and selectable software to realize a choice of waveform, link protocols, modulation type, and codes. The computing engine will host the software as necessary to perform missions. The associated processor of these radios will also be used for other applications, such as operator training, link testing, and network management and control.

---

[621] Naval Studies Board, Ibid.

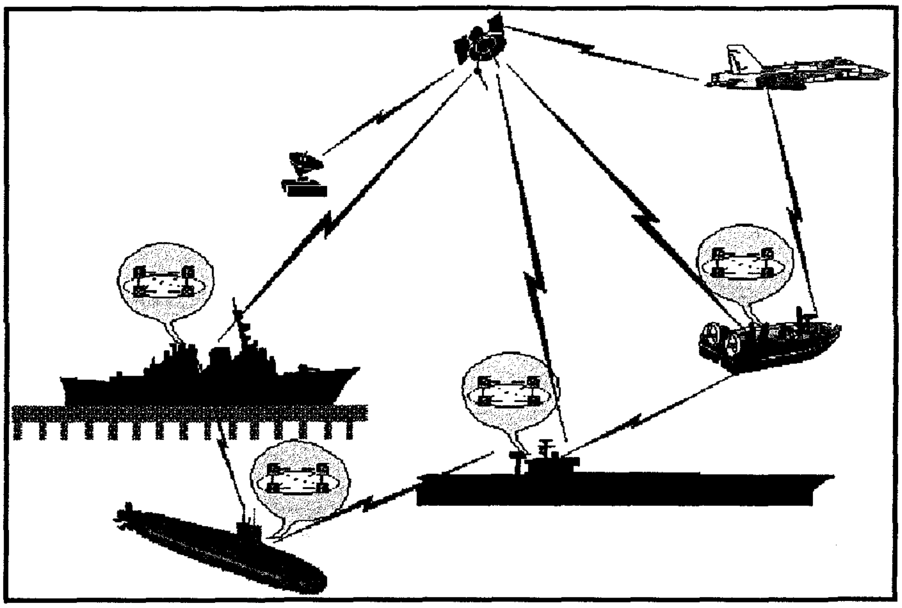


Figure 8.1: Networked Systems on Every Platform.

These technologies will help provide a force that has battle-space dominance. Weapons will be delivered precisely from platforms at sea to targets hundreds of miles away with precision and lethality in support of mission objectives. Unmanned ELINT and other sensor systems will be launched and recovered from naval platforms at sea to provide near-real-time multispectral surveillance products fused into a common operational picture. This picture will be used by commanders throughout the joint task force to monitor the tactical situation, redirect forces and ELINT and other sensor systems, and provide battle damage and kill assessments.

New information systems will be in place to provide worldwide knowledge of weather, as well as a global surveillance and reconnaissance capability. These capabilities will be supported by the ability to correlate data rapidly and automatically from the various sources. The combination of the Global Positioning System (GPS) and a common geo-referencing system will create a synergy among ELINT and other sensor and attack systems. A common data or information model will have been adopted to enable the interoperability of the data that are gathered by the various ELINT and other sensors. There will be a coherent, consistent set of data within the system to provide separate nonredundant tracks on targets of interest. The resolution of multiple tracks on the same object into a single track will be enabled by a world grid referencing system and the ability to provide highly accurate positioning data via the GPS or its derivatives. Through multisensor fusion of tracks and a common information model, databases of tracks will be synchronized and a common operational picture will be available to naval forces worldwide.

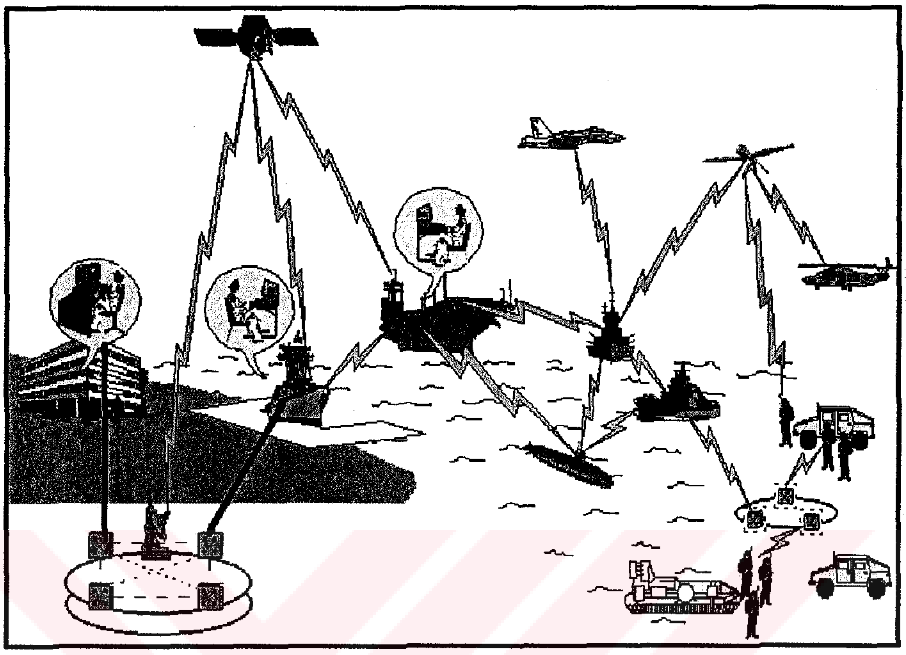


Figure 8.2: Ubiquitous Wide-Band Communications.

Information networked capabilities may result in flattened, more effective and more flexible command organizations, better coordination, and improved reaction time. Simply put, information technologies will allow naval forces to fight smarter and dominate the battle space more rapidly than ever before.

Success in modern warfare hinges on information superiority not only in surveillance and intelligence, but also in weapons targeting and guidance, navigation, force management, and logistics.[622]

8.2. FUNDAMENTALS IN NAVAL ELECTRONIC WARFARE

The importance of naval EW is increasing enormously. Modern battlespace scenarios above the water require EW as the key element to protect own naval forces from attack and to detect the hostile use of the radio-frequency spectrum. In recent years, most navies kept their highly sensitive EW techniques in full secrecy because EW is likely a continuing

[622] Naval Studies Board, Ibid.

battle between active systems that attack and defensive systems which protect. As EW covers the full scale of the electromagnetic spectrum, it can be categorized into passive Electronic Support Measures (ESM) and both actively operated Electronic Countermeasures (ECM) and Electronic Counter-Countermeasures (ECCM). Nevertheless, both ECM (involving jammers and a diversity of flares and decoys) and ECCM become relatively in naval use in recent years. A typical above-water mission is often subdivided into a passive phase involving the interception, localization, and identification of the hostile electromagnetic emissions and an active phase which is usually directed at jamming and deception techniques to deny their use by an enemy. Consequently, above-water ESM and ECM operations will be increasingly supported by a range of other assets which include land-based mobile or static EW systems and both Unmanned Aerial Vehicles (UAVs) and maritime patrol aircraft in the surveillance and information-gathering role.[623]

8.2.1. Electronic Support Measures

In the Anti-Ship Missile Defence (ASMD) role, Electronic Support Measures (ESM) also includes elements and tactics to support defensive threat warning and over-the-horizon targeting (OTHT). In recent trials, very high-sensitive microwave ESM has been also used to primarily detect signals from surface search radars at great distances. ESM can be broadly subdivided into Electronic Intelligence (ELINT) and Communications Intelligence (COMINT). ELINT activities are primarily conducted to intercept and analyze emissions from surveillance, fire-control and missile guidance radars. Modern shipboard COMINT equipment fully depends on digital computers (as does ELINT equipment) to automatically intercept, localize, analyze, and determine hostile transmissions and detect mobile or stationary radar systems is used by enemy. When combined, both ELINT and COMINT form Signal Intelligence (SIGINT) activities. They are an integral part of today's shipborne EW assets.[624]

[623] Nitschke, Stefan, "The Role of Electronic Warfare in Naval Warfare", Naval Forces Magazine, No.IV/2002, Vol.XXIII, Bonn, Germany, 2002, p. 16-17.
[624] Nitschke, Stefan, Ibid, p. 17.

8.2.2. Electronic Counter Measures

The use of Electronic Counter Measures (ECM) enables naval forces to disrupt enemy surveillance systems and communications networks. It is also being used to counter the effect of electromagnetic, IR, and laser systems deployed by an enemy for the purpose of missile guidance. The threat posed by enemy for the purpose of missile guidance. The threat posed by many new-generation missile systems in the anti-shipping role could be most critical due to the continually increasing proliferation of long-range, passive electro-optical (EO) forward-looking IR (FLIR) sensors and FLIR precision guided munitions seekers. For any of these reasons, ECM as the active element of naval EW will become relatively more critical in the future.[625]

8.2.3. Electronic Counter-Counter Measures

In naval architecture, Electronic Counter-Counter Measures (ECCM) systems are deployed to overcome ECM systems. The main method to counter ECM systems such as jamming equipment is frequently agility. Low-Probability of Intercept (LPI) radars can herein represent a severe problem for ECM systems due to their ability to become more agile in pulse repetition intervals (PRI) and frequency over a large frequency range. Such frequency-agile radars also perform different power management techniques which have been shown to be little vulnerable to jamming activity.[626]

8.3. NETWORKED SPECIFIC EMITTER IDENTIFICATION

Specific Emitter Identification (SEI) technology developed by the Tactical Electronic Warfare Division provided a significant capability to participants.[627] Typically, SEI receivers are able to identify navigation radars by the unique characteristics of their magnetron transmitters. If it was known what platform was carrying that particular radar, then it was possible to identify specific platforms - from long range and in poor weather. This technology has been vital to establishing maritime databases and is gradually being

[625] Nitschke, Stefan, Ibid, p. 17-18.
[626] Nitschke, Stefan, Ibid, p. 18.
[627] Terry, I., Terry, I., "Networked Specific Emitter Identification in Fleet Battle Experiment Juliet", U.S. Navy Tactical Electronic Warfare Division, San Diego, California, U.S.A., 2003, Available on site: http://www.nrl.navy.mil

extended to other EW areas.[628] SEI provides a reliable, long-range, all-weather positive target identification capability against seaborne platforms and land-based systems that emit radar signals. A network of geographically separated SEI-equipped aircraft, ship, and land-based platforms operating in a networked environment provided time-critical, tactically relevant Electronic Intelligence (ELINT) that contributed to early Indications and Warning (I&W) of suspected hostile vessels, enhanced the commander's situational awareness, and assisted him in forming courses-of-action during the exercise.

Specific Emitter Identification (SEI) technology enables passive identification of platforms emitting radio frequency signals, thus enhancing ocean surveillance and combat ID capabilities. The warfighter has a highly reliable method of passively identifying emitters and hence knows the identity of each individual ship and aircraft. This capability allows for the correct identification and surgical removal of threat systems. At present, both coastal and open ocean surveillance operations are being conducted using prototype SEI equipment, including monitoring maritime shipping in support of embargo enforcement and tracking the movement of military assets.[629]

Naval operations in the littorals often occur in regions with high shipping densities. Interdiction operations and strikes against seaborne platforms under restrictive rules of engagement (ROE) scenarios require the capability to positively identify surface contacts, thereby reducing the ambiguities in the commander's overall target picture. Traditional surveillance methods fall short in the rapid establishment of the surface tactical picture when operating in such conditions. For FBE-J and MC-02, NRL installed UYX-4 SEI sensor systems onboard the destroyer USS Benfold, the command ship USS Coronado, a P-3 aircraft, and a mobile and fixed land-base site. These systems demonstrated the ability for one platform to acquire a target of interest, inject that target's SEI information into a network, and have a different platform miles away receive that contact's information in near real time. Of significance was the ability to identify and consistently re-identify

[628] Royal New Zealand Navy Web Page, "Defence Technology Agency Earns International Awards", New Zealand, March 2003, Available on site: http://www.navy.mil.nz/rnzn/article.cfm
[629] Federation of American Scientist Web Page, "Joint Warfighter DTOs Combat Identification", 1997, Available on site: http://www.fas.org/spp/military/docops/defense/97_dtos

shipboard, land-based, and airborne radars on different days, using SEI systems on different platforms, operated by different operators.[630]

8.3.1. Rapid dissemination of information

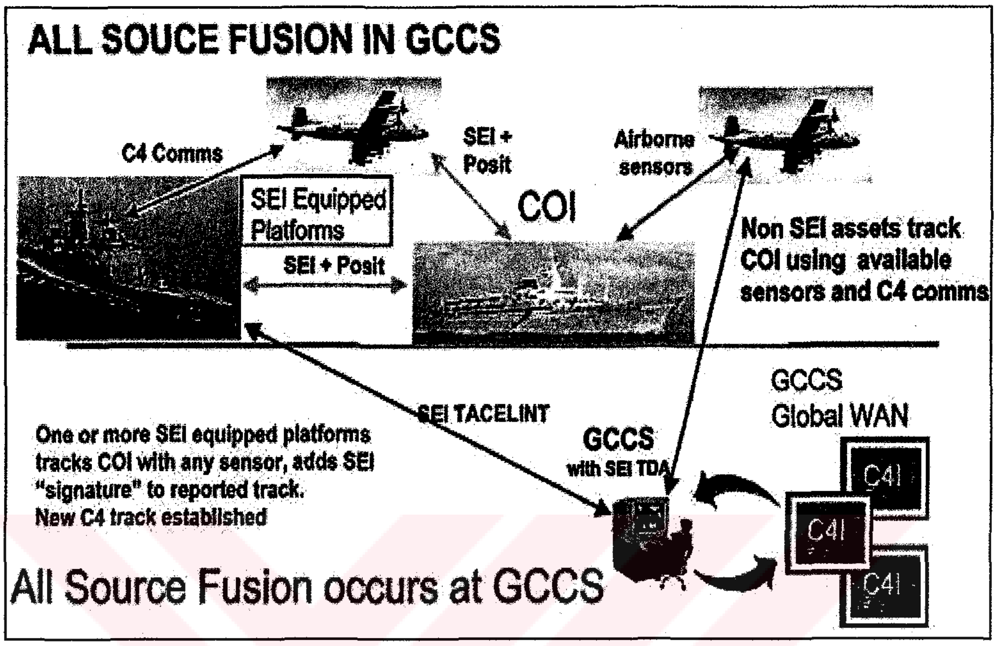


Figure 8.3: SEI TACELINT Message Carries SEI Signature from SEI Capable Units.

In the past, Tactical Electronic Intelligence (ELINT) messages containing SEI signature data were sent to theater commanders, national agencies, and other SEI sensor platforms, generally arriving 24-48 hours after the event occurred. During FBE-J, ELINT messages sent from an SEI sensor over the command network to another SEI sensor or to a command entity were observed with latency 10-15 seconds under normal network operating conditions. This ability to rapidly acquire and disseminate target information allowed the commander to make quick decisions in determining courses of action during the exercise.[631]

8.3.2. Development of Electronic Order of Battle

SEI-equipped units developed an SEI Ground Truth Data Base of Opposing Forces (OPFOR), potentially hostile, friendly, and background emitters over a period of 2 months

[630] Terry, I., Ibid.
[631] Terry, I., Ibid.

prior to exercise, forming the basis for threat emitter identification/re-identification during FBE-J/MC-02 execution.

Tactical usage of electronic order of battle: Using the ground truth database, the SEI-equipped P-3 aircraft, ships, and coastal site provided vital support in identifying/re-identifying emitters of interest. The information injected into the sensor grid provided real-time situational awareness by amplifying and de-conflicting the naval tactical picture with the SEI signature information.[632]

8.3.3. Networking achievements

NRL demonstrated that tactical ELINT messages produced and sent by the SEI sensor systems could be introduced into the GCCS-M 3.x command net as ELINT contact reports via a JOTS 1 Master TDBM, and further distributed to other GCCS-M workstations over the network using Common Operational Picture (COP) Sync Tools (CST). This was done using existing network TCP/IP communications, and the capabilities built into a GCCS-M 3.x JOTS 1 workstation, including auto-forward communications, track attribute correlation, track processing, generation, plotting, display and archiving.

Fleet Demand for NRL Technology: Leveraging on the successes and lessons learned from FBE:

1. Commander in Chief, Pacific Fleet made a direct request for the SEI system on USS Benfold to be cross-decked to another DDG to support real-world operations.
2. At the request of Commander, Naval Forces Europe, NRL is currently involved in the implementation of a Networked SEI Sensor Grid in the U.S. Sixth Fleet operational theater to support national defense objectives.
3. The Office of Naval Research (ONR) has funded the development and installation of an Integrated Sensor Suite, including an UYX-4 SEI system onboard the Navy's High Speed Vessel Joint Venture follow-on, HSV-X2.
4. ONR is also funding the Battle Group Distributed SEI Experiment (BGDSE) to equip an entire deploying carrier battle group with a Networked SEI capability.

[632] Terry, I., Ibid.

Fleet Battle Experiment Juliet demonstrated the value and power of SEI's capability to uniquely identify and consistently re-identify radar signals. SEI provides a significant contribution to solving the deconfliction problem between hostile radars from friendly radars in dense, complex emitter environments. NRL's research in Networked SEI is expected to continue to bring a significant capability to operational commanders for a variety of tactical missions around the world.[633]

8.4. AUTOMATIC TARGET RECOGNITION

Automatic target recognition (ATR) is usually associated with the development or implementation of cooperative and noncooperative sensor systems for surface targets. The need for ATR systems stems from the increased complexity of tactical and strategic battlespaces, the unprecedented amount of raw information produced by modern sensor systems, and the effectiveness of C^3 systems.[634] As the volume of sensor-provided data increases and the operational time of advanced weapon systems decreases, automatic target recognition (ATR) becomes mandatory, no human can provide the necessary decisions fast enough. Although certainly challenging, ATR has acquired a reputation for impossibility that does not reflect the facts. It is the case that, given two- and three-dimensional image data visually displayed, and enough time, a trained human is unbeatable in many recognition tasks. Considering for example, the task of finding a familiar face in the crowd without knowing in advance who it is going to be; a human can do this if the face is familiar to the observer; a computer cannot. But this does not mean that computer-based ATR is impossible. And it does not mean that ATR will not outperform the human in some circumstances.[635]

Collectively these can overwhelm the capability of human operators and decision makers. The magnitude and rate of information produced may exceed the operator's ability to absorb and process it in a timely fashion; performance declines with operator fatigue and varies with operator training. Consequently, ATR systems are being developed to provide

[633] Terry, I., Ibid.
[634] Cabasso, Jacqueline, "Joint Warfighting Science and Technology Plan: Combat Identification-Chapter IV", Western States Legal Foundation, Oakland, California, 2003, Available on site: www.wslfweb.org/docs/dstp2000/jwstppdf/08-CID
[635] National Academy of the Science Web Page, "4: Sensors", NAP, U.S.A. Available on site: http:www.nap.edu/html/tech_21st/t4.htm

an assortment of technological services that range from operator prompting (cueing) tools to fully automated recognition systems requiring no human operator intervention.[636] Research on automatic target recognition (ATR) is several decades old. This research involves four sensors: FLIR, LADAR, Polarimetric SAR (PSAR), and millimeter wave. These sensors complement each other well for fusion purposes, and unclassified data obtained by these sensors is beginning to become available. The general approach to ATR being pursued the study of sensor models; statistical models for characterizing background and clutter; geometric and radiometric models for targets; multisensor integration; and performance characterization.[637] The ability to distinguish between targets and nontargets automatically and noncooperatively is generally considered to be the province of automatic target recognition (ATR). Despite the fact that ATR technology is not yet mature, it is already clear that this technology will be an essential component of naval activity in the future. The Navy has a particularly high stake in the ability of ATR to effectively distinguish among target types, in order to provide accurate on-site intelligence in advance of conflicts and to properly, efficiently, and safely effect strike missions during conflicts.[638]

The first successful nonlinear concatenation of two specific optical processors has designed: a *synthetic aperture radar* (SAR) image generator and a *Vanderlugt* optical correlator. The image generator was a space-integrating decoupled tilted-plane design and provided nearly diffraction-limited processing of the input radar data from the SIR-A space shuttle mission with a resolution exceeding 3000 x 1000 pixels. Simulations of correlation operations involving SAR data from multiple flybys of a target object indicated that the key to successful pattern recognition on SAR images was the removal of phase information before correlation. With this system real-time target recognition and tracking of targets in SAR imagery was achieved with signal-to-peak-clutter values.[639]

---

[636] Cabasso, Jacqueline, Ibid.
[637] Cfar.umd.edu Web Page, "Automatic Target Recognition", 1996, Available on site: http://www.cfar.umd.edu/cvl/projects/automatic_target_recognition.html
[638] Naval Studies Board, Ibid.
[639] Weaver, Samuel, and Kelvin Wagner, "Real-time Optical SAR Image Generation, Speckle Reduction and Target Recognition", U.S.A., Available on site: http:// drip.colorado.edu/~samw/research/SAR-summary/SAR.project.summary2.htmlver.html

Automatic target recognition refers to the ability to recognize instances from a collection of models given sensor data and other information, and to be able to effect recognition despite viewpoint variations, occlusion, obscuration, camouflage, deception, model variability, and other confounding factors. The panel identified the following three application domains for ATR:[640]

- *Surveillance*. The goal is to locate and track targets from a distance, and the emphasis is on detection; there is typically a less urgent need for identification. Often, surveillance involves cueing a human operator.
- *Battlefield awareness*. The emphasis is on identification, particularly of friend, foe, or neutral, and integration of multiple sensor (ELINT etc) modalities and multiple data sources is highly desirable.
- *Precision guidance*. The emphasis is on accurate orientation and poses estimation in order to perform course correction and other functions related to positioning.

Naval forces in the future will make use of advanced technology in all three areas to support missions. Despite slow progress in fielding working ATR systems, it is likely that both continued progress and technology breakthroughs will lead to performance capabilities in all these areas that exceed human recognition capabilities and that can be executed at speeds that would have been unimaginable to image analysts a few decades ago. Progress in processors, memory, and sensors, as well as improved algorithmic techniques for processing signal data, image formation, and coherent combination of information (such as from moving targets), all point to major advances in a very few years.

8.5. ELINT & OTHER SENSORS AND AUTOMATIC TARGET RECOGNITION

Based on the technology trends and historical growth patterns described, the panel anticipates that future sensor technology will be characterized by the following:[641]

---

640 Naval Studies Board, Ibid.

641 National Academy of the Science Web Page, "4: Sensors", NAP, U.S.A. Available on site: http:www.nap.edu/html/tech_21st/t4.htm

- Ever-decreasing size and cost as microelectronics evolves into nanoelectronics within the limits and constraints implied by the physics of the interfaces.
- Migration of the analog-to-digital conversion to the front end of the sensor, leaving only those analog elements absolutely necessary for interfacing with the physical phenomenon to be sensed—e.g., microwave LNA, filters and power amplifiers, fiber-optic transducers, MEMS transducers, and the like.
- Ever-increasing application of computer processing as gigaflops grow to teraflops and then to petaflops.
- Development of monolithic smart sensors, combining sensing transduction, ADC, digital signal processing, communication input and output, and perhaps power conditioning on a single chip. This offers interesting possibilities for very small, very smart weapons such as affordable smart bullets.

Within Intelligence, Surveillance, and Reconnaissance (ISR), imagery from synthetic aperture radars, moving target indicator radars, and infrared cameras is to be fused to obtain a common picture of the battlespace. Automatic target recognition (ATR) algorithms enhance the immediate utilization of this imagery, and unmanned aerial vehicles carry the sensors to provide this imagery for all echelons of command.[642] Sensing systems grant an advantage over an adversary by providing an up-to-date picture of the battle space. The future use of unmanned aerial vehicles (UAVs), reconnaissance satellites, and remote air-dropped battlefield ELINT and other sensors will provide an all-weather, multisensor view of the battle space. Images with a resolution of 1 meter or better, accessible at a moment's notice, will be available for worldwide distribution. Remote sensors will pick up heat, sound, and motion in the area of operations. These will be immediately and stealthily forwarded for analysis and targeting. Updates of this battlefield picture could come in near-real time to support immediate retargeting and battle damage assessments (BDAs).[643] The US Navy's spaceborne electronic intelligence (ELINT) system, White Cloud, is based on SSU (Subsatellite Unit) satellites and is intended for

---

[642] US Department of Defense, "Science and Technology-Chapter 17", U.S.A., 1996, Available on site: http:// www.defenselink.mil/execsec/adr96/chapt_17.html
[643] Naval Studies Board, Ibid.

determining the location of warships of foreign states and following them by the method of taking bearings on the ships' onboard radioelectronic equipment from several positions.[644]

Within Command, Control, Communications, Computers, and Information (C^4I), communication and data links will utilize digital relay by satellite that will support joint and coalition operations over an entire theater, and will allow forces at all echelons to draw from remote databases the information most needed for their success. Direct connectivity from sensor to shooter will achieve nearly instant response to targets found by the ATR systems, giving a new ability to attack fleeting targets.[645]

Automatic target recognition can be thought of as a bandwidth enhancer. Given the need to transmit information about targets and threats to the commanders in as succinct and timely a manner as possible, ATR allows the naval forces to concentrate on the information that is explicitly required, dropping (preferably early in the transmission chain) what is irrelevant or redundant, such as distracting background and clutter.

Once transmission requirements are reduced, then the ATR products can be shipped everywhere, and knowledge of the battlefield, and indeed targets in the world, can be made accessible on demand everywhere. In much the same way that Internet capacity is providing wide access to information, increasing transmission capacity, provided by the global information infrastructure, will provide increased information access to warfighters. The panel envisions a world replete with ELINT and other sensors, in UAVs and satellites, the potential battlefield area, third-party sources, traffic lights, and even people's hats. These data will be widely accessible, but, in their totality, overwhelming.[646]

8.6. RADAR TECHNOLOGY ISSUES FOR FUTURE NAVAL WARFARE

Warfare in the future will become increasingly dependent on technological force multipliers as the numbers of personnel and equipment shrink in response to economic pressures, and as adversaries avail themselves of similar capabilities available in the open marketplace. Surveillance and reconnaissance are two military capabilities that will

[644] Thomson, Allen, "The U.S. Navy's 'White Cloud' Spaceborne ELINT System", (By:Maj.A.Andronov), Foreign Military Review, No.7, U.S.A., 1993, p. 57-60
[645] US Department of Defense, Ibid.
[646] Naval Studies Board, Ibid.

undergo dramatic growth in performance as a result of the explosion in information technology.

To fully appreciate the role of reconnaissance and surveillance on the future battlefield, it is also necessary to extend the several "system of systems" concepts that are emerging as part of the current revolution in military affairs. One such concept is the automatic fusion of real-time sensor and intelligence data in the context of various geographic and intelligence preparation-of-the-battlefield (IPB) databases to find and identify individual critical mobile targets.[647]

Radar, with its all-weather, long-range capabilities for detection and tracking, is the primary electromagnetic sensor in the Navy's tool box and promises to be useful throughout the time horizon of this study. Most of the common technology trends identified earlier are exhibited by radar technology and provide excellent guidance to the potential future capabilities and applications of this key sensor class.[648]

8.6.1. Types of Reconnaissance and Surveillance Platform

A major issue for the future of reconnaissance and surveillance is the types of platforms in which the Services, and in particular the Navy, should invest. General categories are space-based, airborne, and shipboard, the latter including both surface and subsurface platforms. A significant focus of this chapter is littoral operations, with particular emphasis on force projection ashore, whether for major regional contingencies, special operations, or operations other than war. Since most such operations will require deep look capability into hostile territory, the major platform competition in the future will be between spaceborne and airborne assets. Secondarily, there will be a competition in the airborne category between organic carrier-based assets and land-based assets within the inventory of the Navy or one of the other Services. Each of these surveillance platforms has its own set of advantages and disadvantages that must be fully understood and weighed against one another to arrive at a reasonable strategy for technology and system investment.[649]

---

[647] Naval Studies Board, Ibid.
[648] National Academy of the Science Web Page, Ibid.
[649] Naval Studies Board, Ibid.

The US Navy's surface fleet received the Advanced Integrated Electronic Warfare System (AIEWS). The Electronic Warfare Integrated System for Small Platforms (EWISSP) program will explore a number of technologies for potential integration aboard these LCAC and AAAV amphibians to protect them against missiles and other munitions employing radio-frequency (RF) and electro-optic/infrared (EO/IR) sensors for acquisition, surveillance, targeting, and tracking. To this end, four major subsystems are envisioned by the Office of Naval Research (ONR): electronic support, electronic attack, hybrid RF/IR sensors and countermeasures, and EO/IR sensors and countermeasures. Perhaps the biggest challenge will come in integrating all of these for fit aboard platforms with severe physical, weight, and environmental constraints.[650]

The list of components planned for each of these subsystems, moreover, is extensive. For electronic support, the ONR has specified millimeter-wave and microwave receiving antennas for signal detection and direction finding, as well as a variety of receivers for radar warning and other electronic support functions. In the electronic attack area, the ONR is calling for a slew of millimeter-wave and microwave transmitting antenna assemblies, along with the necessary converters and synthesizers to generate the electronic attack signals. In addition, techniques will be studied for modifying the radar cross-section of the EWISSP host platforms to appear as different platform types. The RF/IR sensors and countermeasures being looked at include IR threat warning, an IR obscurant and RF expendable-countermeasures system, an autonomous RF decoy platform (tethered, pole-mounted, or unmanned aerial vehicle), and an RF repeater decoy. EO/IR subsystems are expected to consist of laser and missile warners and a mid-IR laser-based countermeasures system.[651]

The primary alternatives to space-based surveillance systems are various categories of airborne platforms. Typical of today's land-based airborne surveillance systems are big platforms such as the P-3, the E-3, the E-8, Rivet Joint, and others. Other platforms include the carrier-based E-2C, as well as a variety of smaller signal intelligence (SIGINT) and other special-purpose platforms such as Guard Rail. A major issue to be considered for the

[650] Rivers, Brendan. P., "US Navy Looks to Protect Smaller Vessels", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com
[651] Journal of Electronic Defense, "US Navy Looks to Protect Smaller Vessels", November 2001. Available on site: http://www.jedonline.com

future is the place of carrier-based versus land-based surveillance. As the Navy transitions to a posture of littoral operations and force projection ashore, the case for organic platforms versus land-based support is weakened. Furthermore, the concept of joint warfighting argues that the surveillance assets of the other components will be available to support Navy and Marine Corps forces when required.

With future, perhaps larger versions of UAVs platforms, it should be possible to carry large surveillance payloads to the fleet from thousands of nautical miles away, loiter in the operating area for one or more days, and then return safely to the originating base when a relieving platform arrives on the scene. In the near term, land-based airborne surveillance will continue to be dominated by large manned platforms, and the Navy and Marine Corps should provide the appropriate data links and connectivity to these platforms so as to benefit from their presence in joint operations.[652]

8.6.2. Key Radar Technology Development for NAVY

Radar technology development is likely to continue its evolutionary pace over the next several decades. Advances in solid-state transmit/receive (T/R) modules will include higher output power, greater direct-current-to-RF conversion efficiency, and increasing miniaturization. Even more importantly, costs will drop dramatically as production volumes increase, leading to extensive use of this technology in future systems. This will enable a variety of active array designs with two-dimensional electronic beam steering and dynamically reconfigurable apertures that will optimize multimode radar performance. Multipolarization and multifrequency shared apertures will enhance the information gathering capabilities of future systems for such purposes as target classification, and will aid in the rejection of various sources of clutter. Large apertures processing wide instantaneous bandwidth signals at large-scan angles will be enabled by photonic manifold technology or by direct digital techniques. Fighter radars will exploit T/R module technology to provide a variety of sophisticated air-to-air and air-to-ground modes, both detection and imaging. Ship-based air defense radars will see a similar benefit in enhanced sensitivity as well as flexibility in the prosecution of multiple simultaneous fire control solutions.

---

[652] Naval Studies Board, Ibid.

The radar signal processor will be the most critical element in any sophisticated radar of the future. Several radar system concepts may reach maturity over the next several decades. Bistatic radar has held much promise but has been hindered by implementation difficulties and a lack of well-defined concepts of operation. Hybrid systems involving spaceborne radar illuminators and stealthy UAVs carrying bistatic receivers and signal processors may prove their military advantage in hostile environments. Similarly, the bistatic exploitation of existing signals in the environment may lead to practical low-cost radar detection or imaging equipment. AEW systems using the lower RF bands together with STAP processing will permit the detection and tracking of low-cross-section aircraft and missiles. In radar imaging, SAR image resolution will continue to improve within limits imposed by atmospheric distortion. Advances in autofocusing techniques will likely extend the ranges at which these higher resolutions can be achieved, and operational microwave SARs with several-inch resolution should be achievable.

The explosion in digital processing technology will provide great benefits in reducing the vulnerability of radars to electronic countermeasures (ECMs). Electronically scanned arrays together with sophisticated algorithms will be employed to sense the jamming or casual interference environment in time, space, frequency, and polarization dimensions, adapting the radar's operation in real time to changing conditions.[653]

From the earliest days of Navy involvement with space, the idea of putting a radar in space had seemed a good one. Shipbased radars had proved their worth as surveillance devices in World War II. Putting radars in aircraft had increased the surveillance horizon to 200 miles and more. The concept of putting surveillance radars in low orbiting satellites promised to increase the radar's horizon even more. Because satellites orbit the earth several times a day, it might even be possible for a low-orbiting, space-based radar to search daily entire oceans, unobstructed by cloud cover or the darkness of night.[654]

---

[653] Naval Studies Board, Ibid.
[654] Federici, Gary, "From the Sea to the Stars: A History of U.S. Navy Space and Space-Related Activities", Department of the Navy-Naval Historical Center, Washington, D.C., U.S.A., June 1997.

8.6.3. Sensor-to-Shooter Concept and ELINT

One of the weakest links in current sensor-to-shooter concepts is the capability to derive classification or identification information from sensor data. If lighting and weather conditions permit the collection of high-resolution optical imagery of a target complex, human operators and increasingly powerful machines can provide highly reliable classification of selected targets, but wide-area high-resolution imaging requires a high degree of automation. Electronic intelligence (ELINT) collectors can frequently provide precise classification of signal-emitting complexes based on the unique signatures observed. The most reliable long-range all-weather sensor is radar, however, and the state of the art in this realm is by no means complete. A great deal of investment has been made in automatic classification of targets seen in SAR imagery, and a certain degree of success has been achieved against certain targets in the clear. Much is left to be done to achieve robust classification at low false alarm rates for targets partially screened by foliage or other obstructions, and targets deliberately camouflaged by an enemy to defeat the classifier. As sensor resolutions improve, yielding more pixels on target and as processing technology continues to advance at its rapid pace, enabling more sophisticated algorithms to be employed, the performance of the classifiers will improve steadily, and should provide a very powerful capability over the next several decades.

The collection capability of future SAR systems will result in astronomical quantities of imagery at very high resolution. The fundamental limitations on SAR collectors today are not the sensors themselves, but the signal processors necessary to generate imagery and the data links necessary to disseminate it. Both of these limitations will all but disappear in the coming decades, resulting in collection systems that will be capable of imaging entire theaters of operations at very high resolution daily, or even several times a day. Human operators will be relegated to examining imagery that has been highly screened by automated techniques so as to reduce the bandwidth to that which is manageable by a finite number of interpreters. The ATR problem of finding and keeping track of mobile targets will be greatly assisted by the use of automatic change detection applied to SAR and other imagery, and three-dimensional interferometric processing of multipass SAR imagery will add height to targets, providing another dimension of information to enhance ATR performance. Dual polarization and multispectral SAR augmented by multispectral passive imaging under benign weather and cloud conditions will further increase the information content for each target on which the ATR system will operate. In response to this pervasive fixed target surveillance capability, future enemies will engage in ever more sophisticated CCD techniques to evade detection. This will drive sensor and ATR developers into seeking ever-increasing capabilities from their systems to identify partially obscured or disguised targets. It is not clear today which side will gain the upper hand in the long run, but economics will ultimately be the governing factor.

A relatively embryonic area of radar exploitation is in the area of moving ground targets. Virtually all airborne or spaceborne ground surveillance systems are either imaging systems, or systems that exploit a target's own emissions. Consequently, there is very little knowledge in the surveillance community about the potential benefits of moving target exploitation, and almost no prior body of knowledge on the subject. Moving target exploitation comes in several flavors, starting with the knowledge to be gained from the basic scan-to-scan detection picture obtained from a wide-area airborne ground surveillance system.[655]

8.7. ELECTRONIC BEAM STEERING AND LONG-RANGE LASER

Optical sensors are currently burdened with heavy, complex, and expensive gimbals. Electronic optical-phased array technology has the potential to provide lightweight, agile, and simple beam-steering subsystems that not only can rapidly and accurately point a single beam but also can point multiple simultaneous beams. Electronic steering of optical beams can be divided into two areas. One is the steering of narrowband (nearly monochromatic) light, such as with laser-based systems, and the other is the steering of wideband light as used in passive systems. Steering of monochromatic light is technologically easier since chromatic dispersive devices can be used directly and true time delay techniques are not required. It may be possible to design compact compensating optics that will allow useful wideband beam steering with intrinsically dispersive devices.

Military missions of the future will employ long-range laser designators to reduce casualties and increase weapon effectiveness. The system could include UAV or satellite-

[655] Naval Studies Board, Ibid.

based laser designators. These designators will receive target coordinate information from other off-board sensors and then be directed to maintain a laser spot on the target for the duration of the laser-guided munition flyout. These munitions are delivered by either artillery or fighter aircraft. A significant feature of a designator system is that they do not rely on the pilot and his platform to perform target identification, designation, or bomb damage assessment. The pilot flies near the target, releases the weapon, and then leaves the area, thus minimizing the risk of being hit by enemy fire.

Another advantage of long-range designation is that in times of military conflict, high-altitude targets would likely be equipped with GPS jamming equipment. This would make GPS-guided munitions less effective. A laser designation system, in contrast, would not be susceptible to GPS jamming. In contrast, this laser system is limited by the requirement for a clear line of sight (no clouds) to the target. [656]

8.8. US NAVY'S UAV PLAN AND ELINT

U.S. Navy may buy both manned and unmanned versions of the Gulfstream G550 as a replacement for the EP-3 electronic intelligence-gathering aircraft, as a candidate for the broad area maritime surveillance (BAMS) aircraft and as an unmanned aerial tanker for unmanned strike aircraft. The Gulfstream G550's features are:

- It can be turned a G550 into a true UAV carrying very heavy payloads.
- A Gulfstream G550 has a payload about 10 times that of the Global Hawk.
- The G550 could carry 10 tons of long-range ELINT and other sensors.
- The G550's current ceiling is 57,000 ft. The Navy's requirements for BAMS call for an operational ceiling in the low 50,000-ft. range.
- A G550 automatic takeoff, automatic landing and automatic air-to-air refueling with either a probe-and-drogue or boom system.
- In addition to refueling the G550, the Navy is very interested in putting buddy [refueling] pods onto the hard points and making it an air-refueling UAV. It can carry more than 40,000 lb. of fuel in the wings plus another fuel bladder in the

[656] Naval Studies Board, Ibid.

fuselage for a total of about 60,000 lb. With the retirement of the S-3, the Navy is relying on F/A-18E/Fs to refuel its strike aircraft.

Even though the business jet doesn't have the endurance of some unmanned aircraft, it still meets the service's coverage needs. One of the myths is that you need a UAV that can fly for 20-30 hr. to provide two orbits of persistent intelligence (ELINT), surveillance and reconnaissance anywhere in the world for 30 days. But General Dynamics researchers came up with a computer program to show they can meet the BAMS requirement. They placed G550s at five main P-3 bases around the world — Diego Garcia in the Indian Ocean, Okinawa, Hawaii, Sicily and Florida. The computer model then calculated that it would take only a dozen modified G550s (two of them used as trainers) to provide the necessary missions for two orbits anywhere in the world with aircraft flying 15-hr. BAMS missions.[657]

8.9. FUTURE DEVELOPMENTS AND TRENDS

As technology requirements grow after the 11 September 2001 terror attacks, navies will have a strong requirement for new techniques, new equipment, and advanced technologies in EW in order to cope with the increased complexity that evolves from the new asymmetrical threat and with today's capability-based planning. Anyway, this will also result in the inevitably centralizing influence of digitization and networked C^4ISR capabilities, naval combat, and other defensive aids for warships.[658] Leading manufacturers of naval surveillance radars forecast a future in which there is no longer a place for the traditional rotating radar antennas so dominant in post-1940 warships designs. The challenge is now to develop surveillance technology which can be combined in integrated mast structures with all other systems using the RF spectrum. The primary goal is to do this in such a way that future non-rotating radars can be applied not just on the high-end platforms, but also on smaller units such as frigates and corvettes.[659]

[657] Fulghum, David A., "Gulfstream Plans UAV", Aviation Week & Space Technology, Vol. 159, Issue 2, Washington, D.C., U.S.A., July 2003, p. 28.
[658] Nitschke, Stefan, Ibid, p. 23.
[659] Hewish, Mark, and Joris J. Lok, "Naval Surveillance Fixes Gaze on a New Breed of Radar", Jane's International Defense Review, Vol.31, Essex, UK, October 1998, p. 24.

Future naval warfare scenarios will increasingly include expeditionary operations able to maneuver in the open ocean and close to a potential hostile shore. The shift towards littoral operations means that shipboard defenses and sensor performances are complicated due to the fact that near-land environments typically feature phenomena such as extreme climatic and atmospheric anomalies.[660]

Littoral warfare is basically a C^4I problem. Providing for the effective operation of warships in the littoral region means extensive investment in command and control facilities. This involves both on-ship C^4I and the establishment of off-ship (either shore-based or on specialized command ships) C^4I facilities by which the activities of aircraft, warships, submarines, coastal defenses and land forces can be integrated. This requires extensive investment in datalinking, communications equipment, data fusion facilities and intelligence (ELINT) analysis. Surveillance and reconnaissance assets maintain their traditional importance.[661]

For naval missions conducted in such a complex environment, some potential of future shipborne communications-oriented EW systems (ESM-COM/ECM-COM) is likely seen in the suppression of hostile air defense control networks. Identifying and jamming land-based search and fire control radar sites, C^2 centers, air defense posts, and other equipment (such as GPS and sophisticated targeting and inertial navigation systems (INS) commonly used in homing heads of radar-guided missiles) could be also essential. However, missile threats evolving in heavy background clutter typical of near-land environments may increasingly have dual-mode (IR/EO, IR/radar) sensors that could be harder to defeat by today's shipborne ESM and hardkill/softkill defenses. Another problem for shipborne ESM equipment could be thermal image systems which give no emissions, EO devices, laser range-finders, and laser illuminators.

While the complexity of electromagnetic scenarios is continually increasing, there is indeed a tendency to increase the automation of the collection and analysis of the full spectrum of electromagnetic signals. If the next generation surface warship possesses new

---

[660] Nitschke, Stefan, Ibid, p. 23.
[661] Slade, Stuart L. "Littoral Warfare: Ships & Systems from the Sea to the Land", Produced by Forecast International/DMS, Available on site: http://www.defensedaily.com/reports/shipsys.htm

EW systems and C^{4}ISR, it will be able to achieve knowledge superiority over the future adversary.[662]

The aim must be to establish *battlespace dominance*, a phrase coined by the US Navy to cover attempts to dominate the surface, subsurface, air, land and space environments and to control the use of the electromagnetic spectrum. The extent to which this control is required is determined by whether the objectives of the operation are military, constabulary or benign. Battlespace dominance to the required degree will, however, remain essential if forces ashore are to maintain their freedom of action.[663]

[662] Nitschke, Stefan, Ibid, p. 23.
[663] Slade, Stuart L. Ibid.

9. ARMY AND ELINT

The Army is transforming into a more strategically responsive force, capable of dominating across the operational spectrum. It will depend on situational awareness for mission success as it trades armor for the ability to deploy faster, maneuver more quickly, engage targets beyond line of sight and dictate the time and circumstances under which it will accept engagement. The transformed Army's ability to accomplish this will rely on the systematic modernization of intelligence and electronic warfare (IEW) systems to enable near perfect situational awareness.[664] The needs of the future force drive the requirement for information superiority, the state of relative advantage over an opponent that is obtained by being able to get the right information to the right people at the right time, a key enabler for full spectrum force dominance.[665]

The fundamental mission for intelligence remains satisfying the commander's need for unambiguous, concise, accurate and timely threat information to support decision superiority. Army IEW systems, combined with the ability to leverage theater and national capabilities, will support decision superiority with instantaneous and complete, intuitive understanding of the battlespace within a 360-degree tactical infosphere.[666]

The wide array of sensors that were developed to locate targets for precision-guided munitions and cruise missiles allows for a vast and comprehensive sense of reality, providing an enhanced and extended sense of risks and targets. In addition, information from other sensor platforms, such as satellites, unmanned aerial vehicles (UAVs), manned aircraft, ground sensors, and so on, could be transmitted to the land forces, extending its vision even farther.[667]

Army intelligence in the Objective Force must operate within a national, joint and combined environment and will leverage the capabilities and expertise of the national intelligence community, friends and allies, academia, media and industry to contribute to

---

[664] Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, "Intelligence and Electronic Warfare System Modernization", Army Magazine, U.S.A., April 2002.
[665] Vane, Michael A., and Joseph M. Ozoroski, "Transforming the Doctrinal Development Process", Army Magazine, U.S.A., June 2003.
[666] Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.
[667] Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 380.

achieving dominant understanding at the point of decision. This knowledge will be presented using the collaborative, analytical and communications power of modern information technology.

For Army IEW, this mandates changes to current approach to providing intelligence. The existing architecture of multiple ground processing systems, each aligned with either a specific intelligence discipline or a specific sensor, is no longer operationally or economically viable. While each current system addresses a validated need, when viewed collectively, they are too heavy to deploy rapidly, do not achieve the requisite integrated solutions needed to achieve information dominance and do not constitute a true *mud to space* architecture.

IEW is focused on the migration of current systems toward an interoperable knowledge-centric construct with fewer, more capable ELINT and other sensors and processors. This reduction in the number of separate platforms will increase strategic deployability and tactical mobility while decreasing in-theater footprint. However, the fluid nature of ground combat mandates that some intelligence capabilities will always remain forward to provide dedicated near-real-time combat intelligence (COMINT, ELINT etc.) in the close fight.[668]

Ground stations of various types still account for the greatest volume of signals collection activities, although there have been enormous changes in the US and Russian dispositions in the region since the end of the Cold War, and numerous new complexes constructed by the regional countries themselves. The US is no longer interested in covering all HF radio transmissions around the world, but the HF band is still very important.[669]

During the 1990s, the US National Security Agency (NSA) closed down most of its world-wide HF radio interception and HF-DF network. The only countries in Asia which now host US SIGINT ground stations are Japan, South Korea and Thailand, although several other countries have SIGINT cooperation and exchange arrangements with the US –most notably Taiwan, Australia, New Zealand and Singapore.

---

[668] Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.

[669] Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm

The Soviet Union had built more than a dozen stations in Mongolia, North Korea, Cambodia and Vietnam, but these have now all been closed.[670] China maintains by far the most extensive SIGINT capabilities of all the countries in Asia, with several dozen ground stations deployed throughout the country, monitoring signals from Russia, the Central Asian states of the former Soviet Union, Japan, Taiwan, India, and Southeast Asia, as well as internal communications.[671] Many of them were expanded during the 1990s.

Japan has about 25 SIGINT ground stations of various sorts and capabilities, of which ten are large stations.[672] Taiwan has built, with NSA assistance, a large SIGINT facility just north of Taipei. US 'civilian contractors' continued to work jointly with their Taiwanese hosts.[673]

In Southeast Asia, several countries have substantial SIGINT organizations, although they are smaller and their capabilities more limited. In the 1960s and 1970s, Vietnam developed a remarkable SIGINT organization, with numerous ground stations (including covert interception and analysis facilities in the South), thousands of SIGINT personnel, and an ability to monitor and decrypt a large proportion of US and allied communications.[674] However, this capability has largely atrophied. Thailand now has the most extensive network of SIGINT ground stations, including numerous radio monitoring sites along the Burmese border which listen to the HF and VHF radio and walkie-talkie traffic of the Burmese Army and the various drug trafficking and ethnic insurgent groups in Burma. However, Thailand's SIGINT capabilities require modernization, while the Thai intelligence organization must be drastically reformed if the SIGINT is to better inform both policy-making in Bangkok and operations in the borderlands.

Singapore has the most advanced SIGINT capabilities in terms of technical and operational sophistication, complementing two ground facilities with modern airborne systems, and capable of comprehensively and systematically monitoring communications out to about

---

670 Cereijo, Manuel, Ibid.
671 Ball, Desmond, "Signals Intelligence in China", Jane's Intelligence Review, Vol.7, No.8, Australia, August 1995, p.365-370.
672 Richelson, Jeffrey T., "Foreign Intelligence Organizations", Ballinger, Cambridge, Massachusetts, 1988, p.256-258.
673 Minnick, Wendell, "Taiwan-USA Link Up on SIGINT", Jane's Defense Weekly, Australia, 24 January 2001, p.16.
674 Myer, Charles R., "Viet Cong SIGINT and U.S. Army COMSEC in Vietnam", Cryptologia, Vol.13, No.2, U.S.A., April 1989, p.145-146.

2,000 km around the island.[675] Australia maintains the largest and most capable SIGINT establishment in the Southeast Asian region. New investment has been directed mainly towards further enhancement of Defense Signals Directorate (DSD)'s SATCOM interception capabilities and the acquisition of new airborne collection systems.[676]

9.1. ARMY MODERNIZATION AND ELINT

Both the technological and operational environments within which the Army now operates have become far too dynamic to be supported by static, outdated development and publishing systems. The factors that affect today's military operations are so great that our soldiers and leaders require new and unique solutions to quickly prepare them to execute their new and unexpected missions in varying environments. The technological environment also changes rapidly.[677] Modernization plan is the result of a thorough examination of the threat, the nature and imperatives of the future battlefield, recognition of the need to reduce significantly the time required to develop and field advanced technology systems, and the recognition of time–constrained resources. The plan uses technology and systems that will make a significant contribution to the deterrent value of light forces or provide leap–ahead capabilities. The objective is to ensure that the Army light forces meet the future battlefield requirements of increased firepower, flexibility, mobility, survivability, and sustainability.[678]

The top priority for IEW modernization is the migration of our current "stove-piped" intelligence processors to the distributed common ground system-Army (DCGS-A), which is a modular and scaleable family of multi-intelligence processing and exploitation capabilities that will replace all current and future Army intelligence processing systems for national, joint and Army organic sensor data. Some of the current legacy systems (Tactical Exploitation System, Guardrail Common Sensor's Information Processing Facility, and the Common Ground Station) are destined to be sub-elements of DCGS-A and are scheduled to migrate to the objective system. DCGS-A is a system of systems and

---

[675] Cereijo, Manuel, Ibid.
[676] Australian Department of Defense, "Notice of Intention for the Relocation and Modernization of the Naval Communications Station Canberra", Canberra, Australia, October 1990, p.A-9, C-4.
[677] Vane, Michael A., and Joseph M. Ozoroski, "Transforming the Doctrinal Development Process", Army Magazine, U.S.A., June 2003.
[678] West, Togo D., "Army Science and Technology Plan: Close Combat Light", Secretary of the US Army, 1998, Available on site: http://www.fas.org/man/dod-101army/docs/astmp98/sec3h.htm

an integral component of the Army's knowledge-centric strategy. DCGS-A nodes located at each Army and joint echelon will task, process, exploit and provide users with Army, joint, national and coalition sensor data. Operating in a secure collaborative, networked environment, DCGS-A products will be available in near real-time via the all source analysis system (ASAS). The Joint DCGS architecture will ensure that other services will have access to Army sensor data and products.[679]

The next priority is the ASAS intelligence fusion system, which provides automated intelligence analysis, battlefield visualization, management of IEW resources, and production and dissemination of intelligence to warfighting commanders and staffs. ASAS is the IEW interface to the warfighting Army battle command system and to the joint global command and control system, and provides the ground force threat picture to the joint command operational picture. In the future, ASAS will become fully integrated with the emerging DCGS-A family of processors, providing Army intelligence with its first true knowledge-based architecture. ASAS will support the warfighter from theater to battalion, providing a timely, accurate, common and relevant enemy picture to commanders at all echelons.

The next IEW modernization priority is the aerial common sensor (ACS) (ELINT and other), the Army's next-generation airborne collection platform. ACS is being designed to bring global relevance with tactical responsiveness to the Objective Force, ground component and joint task force commanders, primarily through the distributed common ground system-Army architecture. Now in the early stages of component advanced development, ACS will be the only Department of Defense real-time signals intelligence precision targeting system. As a truly multi-intelligence collection system providing targetable intelligence against both stationary and moving targets, ACS will provide a larger area of coverage to support Objective Force operational geometrics and the greater lethality range of new weapon systems including Army tactical missile system Block 2 and Comanche.

Sensor payloads will include communications intelligence, electronic intelligence (ELINT), imagery intelligence (IMINT) and measurement and signature intelligence

[679] Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.

(MASINT and SIGINT), such as electro-optic (EO), infrared (IR), synthetic aperture radar (SAR), moving target indicator (MTI), multi- and hyper-spectral imagery sensors. ACS will be organic to the unit of employment and will merge the capabilities of guardrail common sensor and airborne reconnaissance-low into a single, multifunction platform, providing the requisite networked situational awareness/joint web-centric and deep strike precision targeting for the Objective Force, land component and joint task force commanders.[680]

Another priority for aerial IEW systems is the Army's tactical unmanned aerial vehicle (TUAV) program. In addition to the current TUAV program, the Army has plans to expand unmanned reconnaissance capabilities by fielding extended range (ERUAV) and small (SUAV) variants. The current TUAV, the Shadow 200, is the ground maneuver commander's primary day/night reconnaissance (ELINT, IMINT etc.), surveillance and target acquisition system. It provides the commander with enhanced situational awareness, target acquisition, battle damage assessment and enhanced battle management capabilities. The Shadow 200 consists of three air vehicles, two ground control stations (GCS), one portable GCS, and four remote video terminals that can provide near real-time video to commanders on the ground. The threshold range is 50 km with an objective range of 200 km and on-station endurance of four hours. The threshold payload is 60 pounds with an objective capacity of 100 pounds.

The extended range (ER) variant will use existing Shadow 200 ground control equipment and is expected to consist of up to six air vehicles and associated Shadow 200 ground control equipment. It will carry multiple payloads greater than 200 pounds. Threshold payloads will include advanced EO/IR, SAR/MTI, and communications relay. Objective payloads will include LIDAR, HSI, and signals intelligence/electronic warfare (SIGINT, ELINT). The ER threshold range is 200 km with an objective range of 300 km and an on-station endurance of eight hours. The SUAV is still in concept development, but it will provide a man pack capability to light and mounted troops that will be critical in urban or restricted terrain.

680 Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.

Prophet is the Army's all weather, "24/7" ground signals intelligence and MASINT sensor system with an electronic attack (ELINT) capability. Prophet will replace four currently fielded legacy systems, while significantly reducing manpower and logistics requirements. The objective system will provide enhanced situational awareness, battlespace visualization, target development and enhanced force protection in the brigade- and armored cavalry regiment-level areas of operation. Prophet gives the commander a near-real-time multi-intelligence (ELINT, IMINT etc.) picture of the brigade/armored cavalry regiment battlespace including the capability to detect, identify and electronically attack selected emitters.[681]

Prophet will support on-the-move and dismounted operations and will operate in close support to highly mobile combat maneuver forces throughout the spectrum of operations. Prophet is currently deployed in support of Operation Enduring Freedom. The success and value of the system is best demonstrated by the task force commander's current request for a second system. To better support upcoming anti-terrorism/force protection operations, the Prophet Program Office is developing a quick reaction capability by expanding the current frequency coverage capability of three pre-production models.

The Army is developing a knowledge-centric warfighting concept with soldiers at the center. Commanders have always wanted to base their decisions on near-perfect knowledge, but rarely was such knowledge immediately available at the point of decision. This lack of perfect knowledge was compensated for by mass, technology, sufficient armor to survive meeting engagements, and detailed knowledge about our opponents' operational and tactical patterns. The transcendent need for speed of action, rapid deployability and full spectrum dominance mandates a transformed Army that stakes its success on the dominant understanding of the battlespace, gained through dominant knowledge. Superior intelligence, surveillance and reconnaissance, electronic warfare and cutting edge information operations are integral to achieving that dominant knowledge in the Objective Force. IEW upgrades are being applied to legacy systems in order to maintain technical

[681] Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.

relevancy, particularly in light of the current war against terrorism, but IEW modernization priorities remain focused on systems that will support the Objective Force.[682]

9.2. COMMAND, CONTROL, COMMUNICATIONS, COMPUTERS AND INTELLIGENCE (C^4I) SYSTEMS

Intelligence is actively involved in the C^4I demands of the joint warfighter and is attempting to take advantage of commercially available, high technology equipment.[683] Admiral Boarda said that "Our goal is to combine strategies and technologies to create a consistent situational awareness where information integration is seamless and warfighters are able to access information on demand. We need to make C^4I systems responsive to the warfighter, field them quickly, capitalize on advances in technology, and shape doctrine to reflect changes."[684] His goal can only be accomplished by integrating intelligence into the combat infrastructure and maintaining and enhancing our joint interoperability.

The Aerial Common Sensor (ACS) offers one representative program. The program for intelligence, electronic warfare and sensors (PEO IEW&S) oversees an array of sophisticated electronics and communications systems. An evolution from the current Airborne Reconnaissance Low (ARL) and Guardrail/common sensor (GRCS) programs, ACS will provide the Army's objective airborne intelligence, surveillance and reconnaissance (C^4ISR) system. ACS will use the operational and technical legacies of the ARL and GRCS systems, along with technological improvements, to provide a single, effective and supportable multiple intelligence (multi-INT) system for the Army. The ACS will include a full multi-INT capability, to include carrying signals intelligence (SIGINT) payloads, ELINT and infrared sensors, radar payloads and hyperspectral sensors.[685]

The ACS program is currently completing the concept exploration (CE) phase of development. The Common Ground Station (CGS) is a rapidly deployable and mobile

---

682 Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, Ibid.
683 Baus, Thomas C., "Forward...From the Sea: Intelligence Support to Naval Expeditionary Forces", U.S. Navy, April 1996, Available on site: http://www.fas.org/irp/eprint/baus.htm
684 Boorda, J.M., Adm, US Navy, "Leading the Revolution in C^4I", Joint Forces Quarterly, U.S.A., Autumn 1995, p. 15.
685 Gourley, Scott, "Command, Control, Communications, Computers and Intelligence (C4I) Systems", Army Magazine, Volume 53, Issue 10, U.S.A., October 2003, Available on site: http://www.ausa.org/www/greenbook.nsf

tactical data processing and evaluation center that integrates imagery and signals intelligence, surveillance and reconnaissance data products into a single visual presentation of the battlefield, providing commanders with near-real time situational awareness, and enhanced battle management and targeting capabilities. CGS links multiple air and ground sensors, including the joint surveillance/target attack radar system (JSTARS) aircraft, to the Army Battle Command System at various nodes, such as echelons above corps, corps, division and brigade. JSTARS is a multiservice battle management and targeting system with an airborne multimodal radar incorporating an electronically scanned antenna. The radar combines moving-target indicator (MTI) and fixed target indicator and synthetic aperture radar (SAR) functions and is carried aboard an E-8 aircraft. Radar data are broadcast to the Army through satellite communications, which can also be received from other air platforms, such as unmanned aerial vehicles (UAVs). In addition to being the Army's premier radar MTI ground station, CGS has evolved into a multisensor ground station that receives, processes and displays sensor data from the Predator UAV, tactical UAV (TUAV), airborne reconnaissance low, U-2, Guardrail/common sensor and the integrated broadcast service, while maintaining a small footprint. CGS capabilities are being channeled into a distributed common ground system-A (DCGS-A) through preplanned product improvements, which will be disseminated in a network-centric environment.

Key features include integrated communications intelligence and electronic intelligence reporting, enhanced signal classification and recognition, near-real time direction finding, precision emitter location and an advanced integrated aircraft cockpit. Preplanned product improvements include frequency extension, computer- assisted online sensor management, upgraded data links and the capability to exploit a wider range of signals. The GRCS shares technology with the ground-based common sensor, ARL and other joint systems.[686]

9.3. PROVIDING OPERATIONAL INTELLIGENCE TO THE WARFIGHTER

Data management has thus become the pivot of tactical land combat. The problem is no longer gathering sufficient intelligence, it has become screening and distributing what has

[686] Gourley, Scott, Ibid.

become an unmanageable amount of data.[687] Intelligence support to the warfighter involved in these `chaotic situations' will need to be proactive by anticipating needs (both analytical and resources) based on the commander's mission, intent and the tactical and operational situation. Mission success in the littorals will be determined by intelligence providing the right information and resources at the right time to the commander.[688] The U.S. Army has focused on these issues in a program called the Army Tactical Command and Control System (ATCCS), and in a key subprogram, the All-Source Analysis System (ASAS).[689]

ASAS systems provide operational commanders at Echelons Above Corps (EAC) down to the maneuver battalion with up-to-date and accurate pictures of enemy forces. This view is provided to ABCS and joint systems and merged into a COP that provides Warfighters with an understanding of the position of friendly and enemy forces on the battlefield. The result is a common situational awareness that facilitates a rapid decision-making process during high tempo operations. CECOM SEC IFS, as a member of Team ASAS, provides for the maintenance and near-term enhancements to these systems to meet evolving battlefield requirements. CECOM SEC IFS support includes both depot-level maintenance of system software baselines and on-site support to the soldiers operating ASAS through regional Field Software Services Support (FSSS) representatives. Through close and continuous interaction with ASAS users and their representatives CECOM SEC IFS aggressively pursues the maintenance and enhancement of ASAS to meet the needs of our Warfighters.

9.3.1. The All Source Analysis System (ASAS)

The U.S. Army operational forces are equipped and trained to respond to an ever-changing and complex array of threats to national interests. The All Source Analysis System ASAS family of systems provides soldiers with a flexible set of system tools that enable the analysis, processing, display, and dissemination of intelligence information related to these threats. Collectively, this suite of systems links intelligence functional area activities and

---

687 Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996, p. 151.

688 Baus, Thomas C., "Forward...From the Sea: Intelligence Support to Naval Expeditionary Forces", U.S. Navy, April 1996, Available on site: http://www.fas.org/irp/eprint/baus.htm

689 Friedman, George & Meredith, Ibid, p. 151.

organizations, from the national to the tactical level, in a flexible and complementary manner to provide the Warfighter with near real-time processed intelligence information.

ASAS is the central nervous system guiding field commanders to successfully execute the air/land battle... ASAS automates command and control (C^2) of IEW (intelligence and electronic warfare) operations and intelligence fusion processing. It generates a near-real time picture of the enemy situation to guide employment of maneuver forces and systems and provides coordination to systems within the ATCCS arena. Many sophisticated sensor systems provide targeting information; however, the capability to process and respond to that information is limited.[690]

The rapid advance of technology, the emphasis on joint warfighting, and the constant evolution of the threat that soldiers face are all factors that impact evolving intelligence requirements. ASAS must also evolve to provide support to the intelligence mission area. This dynamic approach to PPSS serves to provide for a family of intelligence systems that support the operational commander's requirement for battlefield situational awareness.[691]

The ASAS family of systems is composed of the ASAS-All Source (ASAS-AS), the ASAS-Single Source (ASAS-SS), the ASAS-Remote Workstation (ASAS-RWS), ASAS-Light (ASAS-L), and the ASAS-Communications Control Set (ASAS-CCS). This family of systems is employed at different echelons and designed to perform functions that collectively enable soldiers at all echelons to provide commanders with a view of the enemy threat. This information is provided to other systems within the Army Battlefield Command System (ABCS) and joint systems, such as the Global Command and Control System (GCCS), and then merged with friendly unit information to form the Common Operating Picture (COP).[692]

ASAS is intended to tie together all forms of intelligence –human, electronic, signals, imagery- and fuse them into a single information system, then distribute them to combat

[690] Friedman, George & Meredith, Ibid, p. 151.
[691] Ingrao, Joseph, "The All Source Analysis System (ASAS) Family of Systems: Providing Operational Intelligence to the Warfighter", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 2, Issue 1, U.S.A., July 2001.
[692] Ingrao, Joseph, Ibid.

commanders at all levels via the new joint Tactical Information Distribution System (JTIDS).[693]

Figure 9.1: ASAS-Remote Workstation

ASAS users are able to plot information from stored records and to develop user-definable views of the information. The operators, through the use of database queries, develop these different views. ASAS users can view selected information elements based upon parameters that they define. The result of this user-defined query could be viewed independently from other enemy information in the database and provide the commander with a clear picture of the position of enemy tank units. ASAS also provides the capability to alert the operator to the receipt of specific information via audible or visual alarm.[694]

9.3.2. ASAS-AS

The ASAS-AS provides for the collection, analysis, and dissemination of multi-intelligence products. The ASAS-AS serves as the operational link to the national Modernized Integrated Database (MIDB) and provides for the capability to fuse intelligence information across disciplines and echelons. The key enabler to this process is the All Source Correlated Database (ASCDB). The ASCDB serves as a centralized repository of information records that can be added, updated, and viewed based upon user requirements. The External Database Coordination (EDC) message is the information exchange vehicle employed by ASAS to pass ASCDB information. The ASAS-AS can tailor the information contained in the EDC messages based upon user-defined requirements and provide recurring updates to ensure that ASAS family of system

[693] Tapscott, Mark, "New Pictures Emerging in Battlefield Intelligence", Defense Electronic Magazine, U.S.A., April 1993.
[694] Ingrao, Joseph, Ibid.

databases are current and consistent. The Military Intelligence (MI) Brigade (Bde) provides ASAS-AS support to the Analysis and Control Element (ACE). Near-term PPSS efforts to enhance ASAS-AS functionality are focused toward providing soldiers with the capability to visualize the situations faced during Stability and Support Operations (SASO). The SASO environment requires the ability of the system to store, process, display, and disseminate Individual, Event, and Organization (IE&O) the information that is required for analysis of unique operational situations.[695]

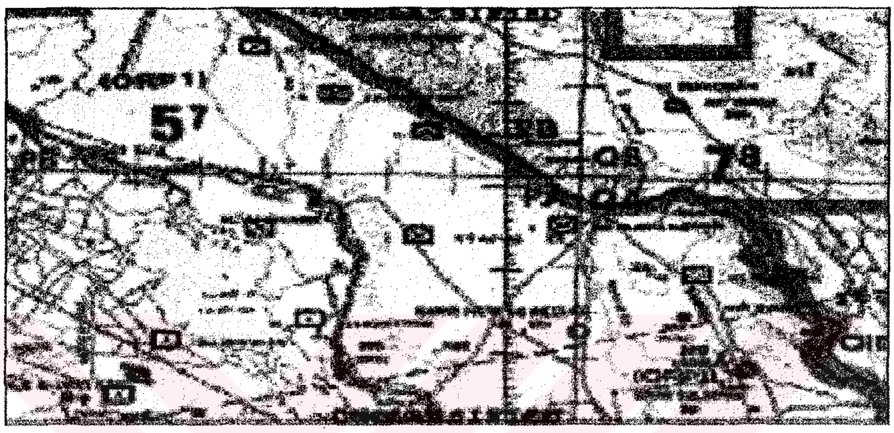


Figure 9.2: ASAS-AS Provides Multi-Intelligence Products.

9.3.3. ASAS-SS

The ASAS-SS system is designed to provide the commander with processed Signals Intelligence (SIGINT). SIGINT consists of correlated Electronic Intelligence (ELINT) and Communications Intelligence (COMINT) information. SIGINT information provides commanders with an electronic enemy picture of the battlefield that is provided to the ASAS-AS, which incorporates the information into the ASCDB to display the overall situation. The MI Bde provides the ASAS-SS enclave to designated Army operational units. Near-term PPSS enhancements to the ASAS-SS are focused toward the enhancement of the map application and addition of the distributive collaborative planning product InfoWorkSpace (IWS). The addition of the IWS client to the ASAS-SS software baseline will provide users with a distributed collaborative planning capability via Joint Intelligence Virtual Architecture (JIVA) servers that have been established on the Joint Worldwide Intelligence Communication System (JWICS) network. A communication enhancement to

[695] Ingrao, Joseph, Ibid.

the ASAS-SS is being prototyped to interface with the Integrated Broadcast Services (IBS) via the Joint Tactical Terminal (JTT).[696]

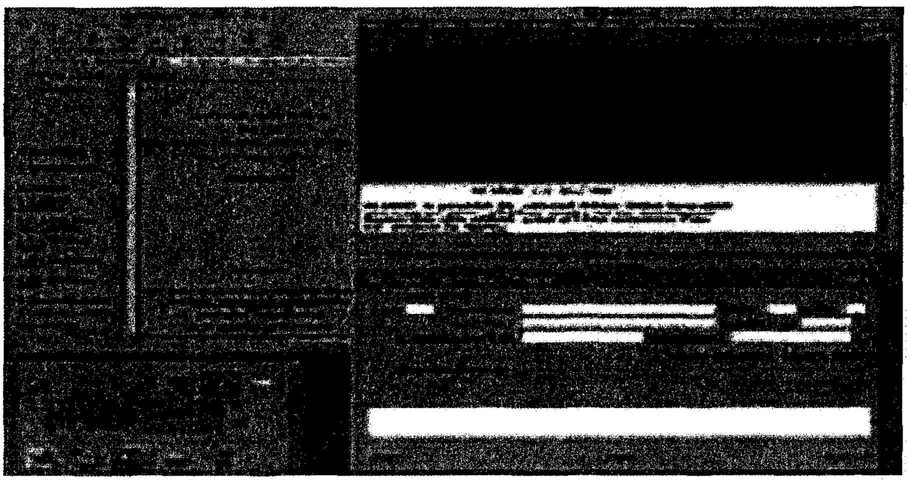


Figure 9.3: ASCDB Display the Overall Situation.

9.3.4. ASAS-CCS

The ASAS-CCS serves as the primary message processing system for the ASAS family of systems. The ASAS-CCS is specifically designed to enable information exchanges between ACE systems operating at the TS/SCI level and the majority of ABCS consumers that operate at the SECRET Collateral security level. The ASAS-CCS is composed of a Tactical Communications Support Processor (TCSP) and a Secure Messaging and Routing Terminal (SMART). The TSCP is both a store and a forward, formatted message switch that allows ACE ASAS systems to send and receive formatted messages via either the TS/SCI Defense Special Security Communications System (DSSCS) or SECRET Collateral (Automated Digital Network (AUTODIN) networks. The SMART enables SECRET Collateral level Local Area Network (LAN) connectivity between the ACE and the Collateral ASAS-RWS by serving as a security firewall. The SMART provides connectivity to Secure Internet Protocol Router Network (SIPRNET) and Mobile Subscriber Equipment (MSE) Tactical Packet Network (TPN) communication paths. The ASAS-CCS can be found at MI Bde units supporting ACEs (at the division level or above) in either shelterized or transit case configurations. Although the TCSP supports the accredited processing and exchange of formatted messages between the ASAS-AS and

[696] Ingrao, Joseph, Ibid.

Collateral ABCS systems, currently there is no methodology for supporting LAN connectivity between the TS/SCI ACE and collateral ABCS. A PM Intel Fusion initiative that will enable multi-level connectivity is the Trusted Workstation (TWS). The TWS, when fielded, will support the exchange of LAN (e-mail) traffic between Networks operating at dissimilar security classification levels.[697]

9.3.5. ASAS-RWS and ASAS-L

The ASAS-RWS is the information fusion system component of ABCS. The ASAS-RWS provides the staff intelligence officer at echelons Bde and above with analytical tools that support the operational commander's Intelligence Preparation of the Battlefield (IPB) and Situational Awareness requirements. The ASAS-RWS is typically connected to the Tactical Operations Center (TOC) LAN, and system functionality is focused toward providing operationally relevant, processed intelligence to the Warfighters. IPB tools support production of the Modified Combined Obstacle Overlay (MCOO) and assist staff officers in the analysis of potential enemy courses of action. The ASASRWS receives the EDC message from the ASAS-AS and uses this information, along with locally gathered intelligence, to maintain the most recent enemy picture for the local commander. CECOM SEC IFS supports both Block I and Block II variants of the ASAS-RWS. Both of these ASASRWS systems possess similar functionality but the Block II system was designed in a modular fashion to conform to the Defense Information Infrastructure Common Operating Environment (DII COE).

DII COE compliance facilitates the use of common software modules, such as the Joint Mapping Tool Kit (JMTK). The ASAS-L is hosted on a ruggedized laptop and effectively extends selected ASAS-RWS functionality down to the battalion level. The ASAS-L receives the EDC message from the ASAS-RWS at Bde and provides for extension of a CIP to the battalion level. Near-term enhancements to the ASAS-RWS include enhanced IE&O processing and implementation of distributed collaborative planning client software. CECOM SEC IFS recently began the transition efforts that will lead to CECOM SEC IFS assuming PPSS responsibilities for the ASAS-L.

---

697 Ingrao, Joseph, Ibid.

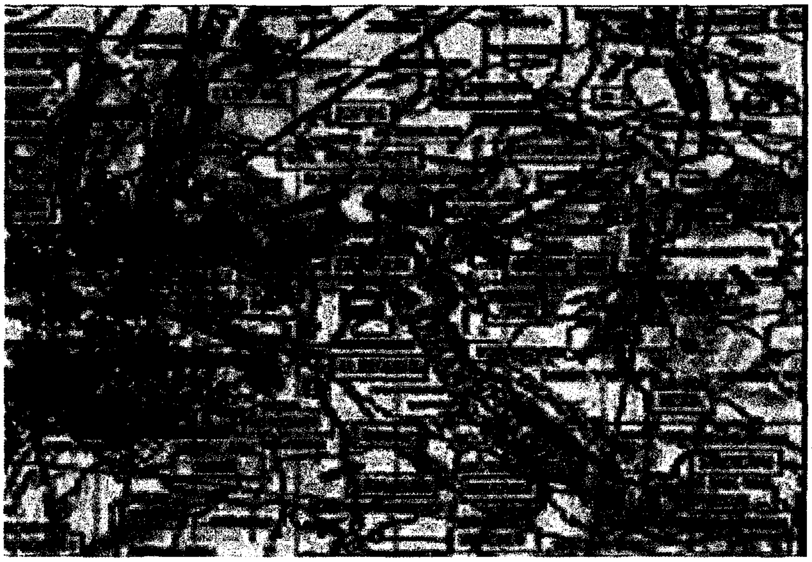


Figure 9.4: ASAS-RWS Support the Operational Commander's Intelligence

9.4. ENHANCED COMBAT POWER: GENESIS II AND DIGITAL BRIDGE

The U.S. Army will provide technological solutions to help combat commanders collect intelligence and interrupt enemy communications and intelligence systems with GENESIS II. The system will provide mission support services at Intelligence and Security Command sites and other national intelligence agency sites, and for other army tactical units worldwide. The system has a quick-reaction capability to meet intelligence requirements, including engineering and building portable electronic intelligence (ELINT) systems for ground and airborne use. CACI will also provide mission-support equipment such as power-generation systems, platforms and physical security systems.[698]

The Army's other technological solutions to help combat commanders collect intelligence and fighting units are building a "Digital Bridge" to make sure they can stay in contact with headquarters in any situation. From their earliest ideas about the new units, Army planners have made clear that the Interim Brigade Combat Teams/Stryker Brigade Combat Teams would be "full spectrum capable" forces. Many of the new units' projected capabilities are based on having new levels of situational awareness. This situational awareness, which will provide the unit with greatly enhanced combat power, will be obtained through new organizational elements like the Reconnaissance Surveillance and

[698] French, Matthew, "Army to get CACI systems", 16 September 2003, Available on site: http://www.fcw.com/fcw/articles/2003/0915/web-army-09-16-03.asp

Target Acquisition Squadron and other intelligence assets.[699] The digital bridge allows commander to see a real-time picture of the battlefield. The system is made up of several central nodes that transmit information into the main hub. The hub, in turn, transmits information digitally to the commanders on the battlefield and the tactical operation center.[700]

All of these assets and information sources will be linked through the broad implementation of multiple battlefield digitization systems contained within the Army Battle Command System. However, planners soon realized that much of this vital information could be lost when the digitized Stryker brigades were employed under non-digitized Army force or joint task force headquarters elements.[701]

The bridge gives planners a few advantages, including showing the movement of friendly and enemy soldiers and allowing information to be transmitted between the commands very quickly.[702] Digital Bridge provides the connectivity to that higher headquarters. It can also be used to provide that connectivity to an adjacent headquarters, such as another nation's defense force.

9.5. SOLDIER AS A SYSTEM: LAND WARRIOR SYSTEM

The Army has taken the next step along its critical transformation pathway with a contract award to enhance the current version of the Land Warrior system. The Land Warrior system, including key soldier elements, consists of personal electronics, communications, global navigation and other integrated equipment. It also enhances interoperability with the battlefield command and communications systems found on Stryker Brigade Combat Team vehicles, as well as on the platform components of the Army's Future Combat Systems (FCS).[703] One intelligence goal should be to provide timely and accurate sensor-to-shooter information direct to the warfighter. Another is to provide the decision maker with an estimate of threat capabilities and limitations and environmental data, specifically an

[699] Gourley, Scott R., "Building a Digital Bridge", Military Information Technology Online Edition, Volume 7, Issue 3, U.S.A., 30 March 2003, Available on site: http://www.mit-kmi.com/archive_article
[700] Jimenez, Alfredo, "Digital Bridge Brings Technology to Stryker Brigade at NTC", US Army Public Affairs, 2003, Available on site: http://w4.pica.army.mil/voice2003/030411/digitalbridge.htm
[701] Gourley, Scott R., Ibid.
[702] Jimenez, Alfredo, Ibid.
[703] Gourley, Scott R., Ibid.

assessment of physical, cultural, economic, and political characteristics and vulnerabilities. Bold, predictive analysis will be required of the intelligence analyst and expected by the commander.[704]

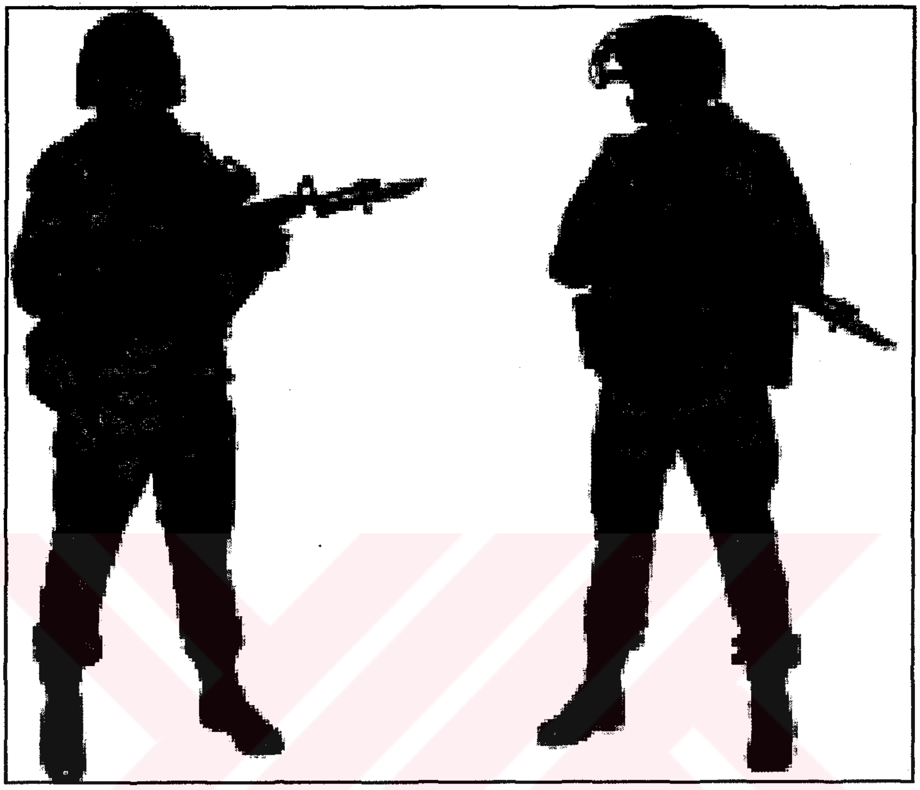


Figure 9.5: Land Warrior Program "Soldier as System"

The Land Warrior program represents the application of a "soldier as system" philosophy to the individual military combatant. The initial Land Warrior program will provide "selected premier light infantry elements" with an integrated series of components designed to enhance their situational awareness and fighting capabilities.

Soldiers in the Army's Objective Force will have a sophisticated level of functionality that not only protects them better, but also enables total integration into the advanced electronics that define the digital battlefield. Land Warrior subsystems include a weapon system, an integrated helmet assembly and protective clothing. Through a helmet-mounted display, a soldier will be able to view computer-generated graphical data, digital maps,

[704] Baus, Thomas C., "Forward...From the Sea: Intelligence Support to Naval Expeditionary Forces", U.S. Navy, April 1996, Available on site: http://www.fas.org/irp/eprint/baus.htm

intelligence information, troop locations and imagery from a weapon-mounted thermal sight and video camera.

Developers note that this capability will allow a soldier to see around a corner, acquire a target, and fire the weapon without risking exposure to enemy fire. Menu-driven displays are controlled by the soldier from a pointing device located on the chest strap and operated by the touch of a finger.[705]

9.6. THE WARFIGHTER INFORMATION NETWORK-TACTICAL (WIN-T)

New system (WIN-T) will enable soldiers to see first, decide first and act first. When WIN-T is fielded in 2008, Army warfighters will share an information network that provides an always-current situation awareness and common operating picture. The Warfighter Information Network-Tactical (WIN-T) will provide the single integrating communications network throughout the tactical battlespace, which is fundamental to the network-centric warfare concept.[706]

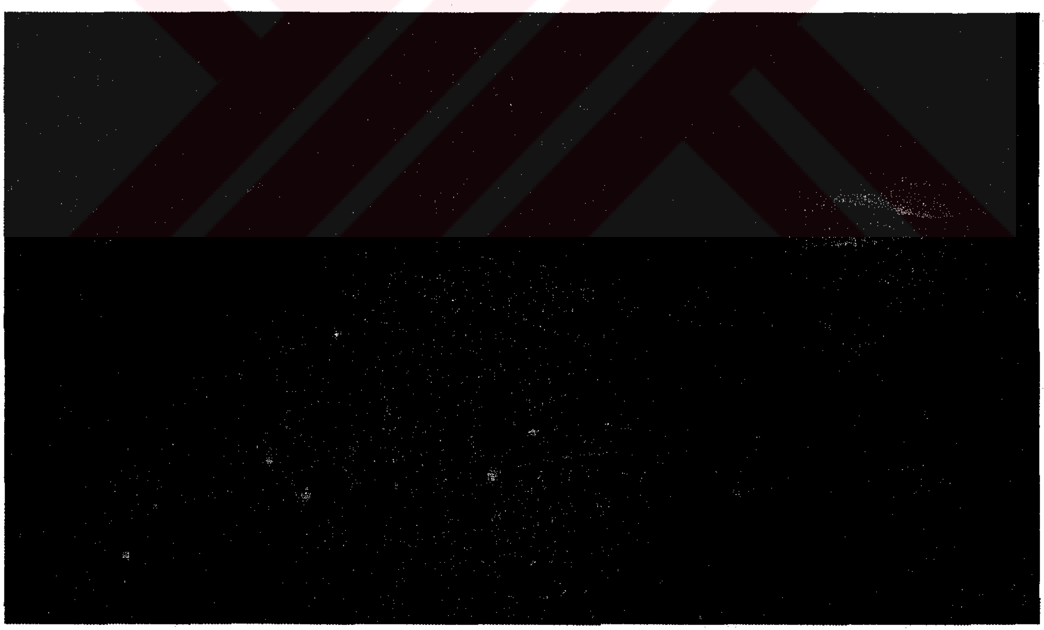


Figure 9.6: Warfighter Information Network-Tactical System (WIN-T)

[705] Gourley, Scott R., "Land Warrior Moves Forward", Military Information Technology Online Edition, Volume: 7, Issue: 3, U.S.A., 30 March 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=14.

[706] Dolan, Raymond, "WIN-T", Military Information Technology Online Edition, Volume: 7, Issue: 4, U.S.A., 19 May 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=109

WIN-T will be the high-speed, high-capacity communications network for the Objective Force, the Army's transformational vision for a fighting force that is more responsive, agile, versatile, deployable, lethal, survivable and sustainable. Using wireless systems, mobile computing, advanced networking concepts and personal communications devices, this networked communications capability will be focused on delivering a network that is also warfighter-centric.

Network-centric warfare will enable the Army and other U.S. forces to achieve an advantage through improved information sharing. The ability to develop and leverage this information advantage and use it to achieve increased combat power is a key to Joint Vision 2020. Networking the force into a single virtual infosphere provides the warfighter with a distinct information advantage.

The Objective Force will be capable of sustained operations and high operations tempo, while massing effects by networking weapons, sensors (ELINT etc.), platforms, commanders, staff, soldiers and other forces. WIN-T will provide the Objective Force with robust and continuous interconnectivity, any place, under any conditions and at anytime. It will provide the Army with the ability to see first, decide first and act first.

WIN-T will be the Army's tactical extension of the Global Information Grid. It will allow the Army to meet the battlefield C^4ISR challenges of the 21^{st} century. And it will provide the "must haves" for assured communications throughout the tactical grid. These include an overarching network operations capability for synchronized, full spectrum operations; a common set of network standards and protocols spanning all echelons; multidimensional and continuous connectivity while on the move; interoperability among existing objective, joint, allied, and coalition forces; network design and services that span all echelons seamlessly, all available to unit of employment and unit of action/battalion organizations dispersed over increased distances.[707]

Commanders will decide and provide guidance to network managers so the network will adjust automatically to satisfy warfighter information needs, no matter what the operational scenario. The Army will achieve the highest possible maneuverability through a WIN-T

[707] Dolan, Raymond, Ibid.

system that has full on-the-move capability. Smaller, low-profile radio systems and antennas will provide increased security and survivability. Precision engagement across multiple boundaries will become much simpler and virtually automatic, based on information dissemination management tools tied into multiple intelligence, surveillance and reconnaissance links with command headquarters.

WIN-T will be rapidly deployable on C-130 aircraft and able to begin operation immediately when it is offloaded. WIN-T will be soldier friendly, spectrum smart and optimized for the offense. It will require fewer resources than today's systems, leading to reduced logistics requirements. It will have an open architecture with embedded training. Currently in development, WIN-T will include components such as wireless networks, mobile computing, Joint Tactical Radio Systems (JTRS), personal communication devices, network management, information assurance and information dissemination technologies. By exploiting state-of-the-art communications, land, airborne and space-based resources, WIN-T will deliver the right information to the right person in the right place at the right time.

With the rapid pace of technology development, the WIN-T requirements to maintain high technology awareness and technology insertion capabilities offer the Army multiple opportunities for high-payoff operational improvements by leveraging and inserting WIN-T "capabilities" into existing forces. This approach will make it easier to keep the force in a high state of technology currency, while also assuring that all the pieces will fit and operate together in a single seamless tactical network.

The WIN-T program is scheduled for a first unit equipped in 2008. Critical development work is currently ongoing during the systems design development phase of the program. Army transformational programs, which are the Army in synchronizing the Future Combat System, JTRS, Land Warrior and Objective Force Warrior programs, can be sources of products to be integrated into WIN-T and existing systems.[708]

[708] Dolan, Raymond, Ibid.

9.7. WIN-T MILESTONE B (PHASE II)

In August 2003, the Warfighter Information Network-Tactical (WIN-T) program will reach its Milestone B decision, enabling both contractors to enter a 23-month system development and demonstration (SDD) phase. This will give the Army a clearer idea of the capabilities being developed for its critical battlefield communications system of the future. The next phase (Phase II) of future battlefield communications network will focus on developing system architecture, modeling and simulation and a prototype. Together with the Joint Tactical Radio System (JTRS) and Future Combat Systems (FCS), WIN-T will provide the basis of Objective Force communications from 2008, when the first unit equipped is due to be declared.

WIN-T is a transport system, not an application system; producing those applications will be someone else's job. WIN-T will enable situational awareness and command and control on the move. This is an offensive minded capability and being joint is very critical The Global Information Grid (GIG) is the context in which WIN-T and all other communications will operate. WIN-T doesn't just work with the GIG, it is a part of the GIG.[709]

Figure 9.7: WIN-T Milestone system

[709] Baddeley, Adam, "WIN-T Milestone", Military Information Technology Online Edition, Volume: 7, Issue: 6, U.S.A., 09 August 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=169

Low rate initial production for WIN-T is scheduled for 2006, and the system is slated to be ready for fielding in 2008. Full rate production for the first block is scheduled to begin in 2009. Two further WIN-T blocks are planned and scheduled to begin development in early 2006 and 2008. It is planned to have WIN-T fully fielded by about the 2016 timeframe.

WIN-T will enable capabilities in four key areas of the concept of operations: operational movement, transition, enroute and tactical engagement. Operational movement provides command and control (C2) over extended distances, virtual teaming, information dissemination management (IDM) and mobile throughput for reach and reach-back, which supports increased dispersion of units and speed of service. In the transition phase, dispersed units will seamlessly connect using very robust and flexible networks, which will provide the bridge to allow strategic and operational level C4ISR to be transported to tactical units. The third area is enroute, where WIN-T will be required to support mission planning and rehearsal in a collaborative environment, intelligence estimates and logistic applications while units are strategically deploying to the theater. Tactical engagement provides mobile throughput with increased reach over increased distances, reliability and quality of service, collaborative C2 on the move and access to joint and coalition forces. It links maneuver forces and provides the transport layer for rapid sensor-to-shooter relationships for long range networked and joint fires. Mobile throughput and reliability are probably the two key tenets of WIN-T.[710]

9.8. WIN-T ON THREE LAYERS: GROUND, SATELLITES, AND UAV

The WIN-T concept operates on three layers: ground, airborne and space. Initially the program will engage with the Wideband Gapfiller system, Advanced Extremely High Frequency (AEHF) system and Mobile User Objective System (MUOS). The highly mobile environment of WIN-T is a challenge for satcom.

One of the technology challenges is to provide an on-the-move capability using communications systems that span a wide frequency range. Second, in the broad context of ensuring this network, which has multi-directional capabilities like SATCOM, UAVs, LOS and BLOS, keeping it all connected while on the move is a challenge. Discussing how a

[710] Baddeley, Adam, Ibid.

laser-based satellite communications system linked to other satellites and aircraft and to ground networks could be integrated into the WIN-T network. That system is another piece of the GIG, extending down to the tactical level. Within the airborne layer, the systems will operate with airborne payloads carried by UAVs, such as the Global Hawk, high altitude airships, military and possibly commercial aircraft.

The goals of WIN-T are being reinforced by the experience of operations in Iraq. The one lesson that is coming to the forefront out of the recent Gulf War was the need for connectivity. The pace of movement was so fast that it stressed the current communications systems and networks that were provided, such that they initially relied on commercial connectivity because the fixed infrastructure couldn't keep pace. If you aggregate that type of operational need out of what we are seeing from the lessons learned, one of the clear challenges is to provide the warfighter with this mobile bandwidth on the move. The Army wants it to be multimedia on the move, not just voice but data and video, video imagery or video teleconferencing, and to get it to the warfighter in timely way.

The level of throughput is largely defined by the perimeters between WIN-T and the tactical Internet. The systems will support communications to and from, but not within, the unit of action (UA) info-sphere bubble. This access to WIN-T will connect UAs horizontally and vertically with higher echelons of command, providing access to command, logistics, training assets and medical support.

By 2008, there are mandates coming out related to programs that need to transition to IPv6 which has been called the 'next generation Internet', from the two-decade-old IPv4.[711]

---

[711] Baddeley, Adam, Ibid.

10. CONCLUSION

Following the appalling events in America on 11 September 2001, it was recognized that in future they may only have fleeting opportunities to strike at the enemy. As Afghanistan and Iraq have shown, it is vital to have the best available intelligence and communications to allow a rapid decision about when and where to attack. It is needed to be able to identify the enemy fast, then bring the necessary weaponry to bear in the shortest possible time. This requires extra investment in electronic intelligence (ELINT) and other sensors. It also requires extra investment in networks to pass information quickly to allow strikes by sea-launched or air-launched missiles, by artillery, or by troops on the ground.

A marked shift has been made in the balance of investment towards Information Superiority. But it is needed to do more to facilitate the necessary transition to Information Age warfare, which is central to vision for the future Armed Forces and to future ability to operate alongside Allies. *Network-Enabled-Centric Capability* is the concept of a global system of through which information can be collected, analyzed and distributed with increasing rapidity at all levels of military operations.

This is most obvious in the area of Information Technology, Electronics and Communications (ITEC), where the rate of technology advance and innovation is driven by a world economy increasingly dependent on knowledge and information. Advances in ITEC will have a major impact on future Command, Control, Communications and Intelligence (C^3I) systems, and will also be significant in such systems as new sensors and weapons. Another field of relevance to defense where there is substantial civil activity is biotechnology, where advances will have broad significance in the areas of chemical and biological defense, human performance and medical treatments. And the development of space-based electronic intelligence (ELINT) systems, originally driven by the US and others (notably Russia and China) for defense purposes, is now becoming a commercial activity, potentially bringing significant capability to a wider range of nations and organizations.

The evolution of space-based electronic intelligence (ELINT) will involve more efficient sensors and computers. The purpose of the study is to develop procedures for using satellite data to enhance conventional operations.

Other sensor platforms will continue to be used. Even so subsonic manned air craft, such as JSTARS, become increasingly vulnerable to smart antiaircraft weaponry, an entire generation of unmanned aerial vehicles (UAVs), sometimes little more than radio-controlled model airplanes, sometimes as sophisticated as flying platforms, stand ready to assume the tactical electronic intelligence (ELINT) role. Powered by the sun, lithium batteries, or microwave radiation beamed from the ground, the vehicles will be able to hover thousands of feet above the battlefield, while using the same sort of ELINT sensors used by satellites.

Unmanned Aerial Vehicles can never replace satellites because of strict limits on their field of vision. Even from high altitudes, they can observe no more than a radius of a couple of hundred miles. Where the battleground is clearly defined this systems are useful. When targets are at intercontinental distances and commanders need to track enemies with centimeter precision, they will be insufficient. So, one can expect UAVs to serve as tactical and operational electronic intelligence (ELINT) platforms for ground forces already committed to combat in a specific theater.

For the general deployment of global firepower, space-based electronic intelligence (ELINT) is perfect, and the flow of data is integrated with weapons systems able to strike at targets on land and sea, command of space will come to mean command of the earth. Any nation wishing to defend itself against a powerful military opponent will have to try to deny the enemy the use of space, it will have to destroy or paralyze the enemy's satellites and, with them, the ability to see globally and to use intercontinental weapons.

It follows from this that as anti-satellite weapons are developed, anti-satellite weapons will also be developed. As was the case with aircraft, satellites will have to become increasingly agile to evade threats, while other types of spacecraft, space fighters will also evolve to protect electronic intelligence (ELINT) craft from predators. As the long data link between earth-based weapons and space-based surveillance becomes more and more vulnerable, and as the experience of combat in space increases, explosive missiles will move from earth into space.

New technology will offer the potential to achieve military objectives in different ways and indeed provide means to do completely new things. Consequently new technology will, in some cases, require the development of new doctrine and concepts of operation. Military advantage will rest with those who most effectively identify and exploit technology. This will place a premium on the ability to generate and identify opportunities, adapt them for military use and integrate them rapidly into equipment platforms, weapons systems and force structures.

In absolute terms, the US spends approximately seventy times as much as the Turkey does on defense research, while Europe as a whole spends approximately twenty times as much as Turkey. Maintaining close collaboration with these partners, and with the civil sector, will be vital in order to maximize the benefits of research investment and maintain a technological lead over potential adversaries while minimizing costs. We will need to recognize that we cannot do everything ourselves, and that we must be selective in how, when and where we invest defense research funds and how we make use of civil derived technology.

On the other hand, the most important issue is, the electronic intelligence (ELINT) must national origin concepts for a state. In this regard, since the Cold War interests radically have been changed, Turkey under the big pressure to create a new electronic intelligence strategy which final threat structure order this development plans. In order to enhanced the national security and defense capabilities, electronic intelligence requires creative, innovative and flexible plans and programs parallel to the rapidly changing information technologies. In order to minimize the loss of the equipment and personnel in future conflicts, it is needed to increase the national electronic intelligence capabilities.

The mismatch in research expenditure between the US and Europe may lead to a widening technological and capability gap. This could have implications for the ability of NATO to conduct effective multinational operations. The most potent threats to allied forces across this period are likely to come from attack helicopters, long-range indirect fire, mine and torpedo warfare and ground-based air Defenses. Advanced explosives may also be an increasing threat. The future battlespace will be inherently joint and multi-dimensional, encompassing space, cyberspace and the electro-magnetic spectrum, as well as air, maritime and ground elements. The use of directed energy weapons in the battlespace seems likely to increase.

Because of the widening technological and capability gap between advanced technology states and undeveloped countries, it is possible that undeveloped countries are inclined to have *Mass-Destructive-Weapon* and *Terror*.

In future conflicts we will wish to fight from a distance for as long as possible, in order to preserve the force. Capabilities which enable us to prepare and deploy force rapidly in order to create an early effect will be important. Although the build-up to crisis and the need for coalition forming theoretically allows considerable time for force preparation, the precise role and composition of an intervening force will not be known until the last minute. Even with total combat superiority, inadequate deployment and support capabilities may threaten the achievement of operational goals.

I hope in this research, most important lesson for Turkey; immediately develop new electronic intelligence policies in mid and long term perspectives. For accomplish this projection, the R&D laboratories, specialized electronic intelligence man power, financial support and effective tactical systems must develop in future's battlespace picture.

The all four elements of the armed forces (land, naval, air force, gendarme) have cooperate their electronic intelligence capabilities especially with changing nature of the enemy structures and threat capabilities. All these info its tactics must applied in operative and tactical multidimensional military exercise and evaluate the resolutions in order to learn and detect requirements.

REFERENCES

Aaart, Dick van der, "Aerial Espionage: Secret Intelligence Flights by East and West", Arco/Prentice Hall, New York, U.S.A. 1985.

Ackerman, Robert K., "Tactical Goals Encompass Sensors, Autonomous Arts", Signal Magazine, U.S.A., December 1995.

Air University, "Key Air Force Programs: Space", Air Force University, Maxwell, Alabama, U.S.A., 2003, Available on site: http://space.au.af.mil/space.pdf

Albert, D., J. Gartska, and F. Stein, "Network Centric Warfare", CCRP Publication Series, DoD, Washington D.C., U.S.A., 1999.

Alfonso, Lazaro, "SEC and LRC Resolve Intercept Management Subsystem (IMS) Audio Issues", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 1, Issue 4, U.S.A., January 2001.

Allan, C.T., "Electronic Warfare: Foundation of Information Operations", U.S.A., Nov. 1999, Available on site: http://www.infowar.com/MIL_C4I/99/mil_c4i_031199a_j.shtml

Allard, C., "Command, Control, and the Common Defense", Yale University Press, New Haven, U.S.A., 1990.

Anderson, Jack, "There's Nothing New About Military Satellites in Space", Long Island Newsday, U.S.A., 11 February 1985.

Andrew, C., and O. Gordievsky, "KGB, The Inside Story", Harper Collins Publisher, New York, NY, U.S.A., 1990.

Angelfire Web Page, "Singapore Looking for a SIGINT Aircraft", Gulfstream News, Available on site: http://www.angelfire.com/biz6/gulfstream/gulfnews.html

Anthony, R., "Space Today Online-The Satellite Wars- Afghanistan and Yugoslavia", U.S.A., 2001, Available on site: http://www.spacetoday.org/Satellites/YugoWarSats.html

Arkin, William, and Robert Windrem, "The U.S.-China Information War: Machine-to-Machine, Battles a Backdrop to EP-3 Incident", MSNBC Web Page, U.S.A., 19 August 2001, Available on site: http://www.msnbc.com/news/607031.asp?cp1=1.

Army Science Board, "Final Report - Priotirizing Army Space Needs", Department of the Army, Washigton, D.C., July 1999.

Arquilla, J., and D. Ronvelt, "Cyberwar Is Coming!", Rand, Santa Monica, California, U.S.A., 1992.

Asker, James R., "Washington", Aviation Week & Space Technology Magazine, Vol. 158, Issue 1, U.S.A., 6 January 2003, p.19.

Atkins, Robert L., Duane A. Lamb, Marlene L. Barger, Larry N. Adair, and Michael J. Tiernan, "2025 In-Time Information Integration System (I3S)", U.S. Air Force, April 1996, Available on site: http://www.au.af.mil/au/2025/volume1/chap03/v1c3-1.htm

Australian Department of Defense, "Notice of Intention for the Relocation and Modernization of the Naval Communications Station Canberra", Canberra, Australia, October 1990.

Aviation Week Editor, "Invasion Tip", Aviation Week & Space Technology, 6 August 1990, p. 15.

Baddeley, Adam, "WIN-T Milestone", Military Information Technology Online Edition, Volume: 7, Issue: 6, U.S.A., 09 August 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=169

Bahçebaşı, A, "Uydu Sistemlerinin Askeri Maksatlı Kullanımı", MEBS Okulu ve Eğt. K.lığı, MEBS İletişim Dergisi, Yıl 3 Sayı 8, Ankara, 1999.

Ball, Desmond, "Desperately Seeking bin Laden: The Intelligence Dimension of the War against Terrorism", Ed. Ken Booth and Tim Dunne, Palgrave/St Martins, London and New York, 2002.

Ball, Desmond, “Developments in Signals Intelligence and Electronic Warfare in Southeast Asia”, Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, December 1995.

Ball, Desmond, “Over and Out: Signals Intelligence (SIGINT) in Hong Kong”, Intelligence and National Security, Vol. 11, No. 3, Australia, July 1996.

Ball, Desmond, “Signals Intelligence (SIGINT) in South Asia: India, Pakistan and Sri Lanka (Ceylon)”, Canberra Papers on Strategy and Defense No. 117, Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, 1996.

Ball, Desmond, “Signals Intelligence in China”, Jane's Intelligence Review, Vol.7, No.8, Australia, August 1995.

Ball, Desmond, “Signals Intelligence in Taiwan”, Jane's Intelligence Review, Australia, November 1995.

Ball, Desmond, “Silent Witness: Australian Intelligence and East Timor”, The Pacific Review, Vol.14, No.1, Australia, 2001.

Ball, Desmond, “The US-Australian Alliance: The Strategic Essence”, Australian Journal of International Affairs, Vol. 55, No. 2, Australia, July 2001, p.239-240.

Ball, Desmond, and Euan Graham, “Japanese Airborne SIGINT Capabilities”, Strategic and Defense Studies Centre, Australian National University, Canberra, Australia, December 2000.

Ball, Desmond, “Soviet Signals Intelligence (SIGINT)”, Canberra Papers on Strategy and Defence No. 47, Strategic and Defence Studies Centre, The Australian National University, Canberra, Australia, 1989.

Bamford, James, “Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World”, Century, London, U.K., 2001.

Barker, Geoffrey, “RAAF Spy Planes Secretly Watch Indonesia”, Australian Financial Review, Australia, 11 May 2000.

Barlow, John Perry, "Why Spy?", Forbes Magazine, Vol.170, Issue 7, U.S.A., 7 October 2002, pp.42.

Barnett, Jeffery R., "Future War - An Assessment of Aerospace Campaigns in 2010", Air University Press, Maxwell Air Force Base, Alabama, U.S.A., January 1996.

Barr, Larine, "Dull, Dirty and Dangerous", Military Aerospace Technology Online Edition, Volume 2, Issue 3, U.S.A., 10 July 2003. Available on site: http://www.mat-kmi.com/archive_article.cfm?DocID=152

Baus, Thomas C., "Forward...From the Sea: Intelligence Support to Naval Expeditionary Forces", U.S. Navy, April 1996, Available on site: http://www.fas.org/irp/eprint/baus.htm

Bilgin, H., "Siber Terörizme Karşı Gelişmiş Ülkelerin Aldıkları Tedbirler Işığında İnternet Sisteminin Siber Terörizmden Etkilenmemesi İçin Alınması Gereken Tedbirlerin Askeri Yönden de İncelenerek Belirlenmesi", Unpublished Thesis, Harp Akademileri, İstanbul, 2001.

Blackwell, J., "Battlefield of Future: Overview: Information Warfare Issues", Air Force University Press, Maxwell, Alabama, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles/battle/ov-6.html

Blackwell, J., "Battlefield of the Future: Chapter 1, Overview: New Era Warfare? A Revolution in Military Affairs?", Air Force University Press, Maxwell, Alabama, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles/battle/ov-2.html

Boorda, J.M., Adm, US Navy, "Leading the Revolution in C4I", Joint Forces Quarterly, U.S.A., Autumn 1995.

Bourne, Jim, "New Spy Satellite Arrives in Orbit Riding Atlas", Space.com Web Page, 11 September 2001, Available on site: http://www.space.com/missionlaunches/atlas launch 010908.html.

British Ministry of Defense, "Operations in Iraq: First Reflections", Ministry of Defense, London, U.K., July 2003, Available on site: http://www.mod.uk/

Britt, Robert Roy, “Satellites Play Crucial Roles in Air and Ground Battles”, Space News, U.S.A., 09 October 2001, Available on site: http://www.space.com/news/

Britt, Robert Roy, “War on Terrorism Could Clog Military's Space Airwaves”, U.S.A., 08 October 2001, Available on site: http://www.space.com/news/

Broder, Jonathon, “The Threat Over the Horizon”, MSNBC Web Page, U.S.A., 27 April 2001, Available on site: http://www.msnbc.com/news/561893.asp

Brower, J. Michael, “Netting the Force”, Military Information Technology Online Edition, Vol.7, Iss.1, 17 Jan 2003, Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=39

Brunson, Curtis, “Interview: L-3 Communication Systems-West”, Volume: 6, Issue: 9, U.S.A., 15 Nov 2002, Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=56

Buchan, Glenn C., “Strategic Appraisal: The Changing Role of Information in Warfare - Implications of Information Vulnerabilities for Military Operations”, Chapter 10, RAND Publications, MR1016, Santa Monica, California, U.S.A., 1998.

Busey, Adm James B., "MILSTAR Offers Tactical Information Dominance," Signal Magazine, U.S.A., July 1994.

Cabasso, Jacqueline, “Joint Warfighting Science and Technology Plan: Combat Identification-Chapter IV”, Western States Legal Foundation, Oakland, California, 2003, Available on site: www.wslfweb.org/docs/dstp2000/jwstppdf/08-CID

Callaghan, Dennis, “e.Intelligence BI software predicts future”, eWeek Magazine, Vol. 19, Issue 4, U.S.A., 28 January 2002.

Cameron, K., “Unmanned Aerial Vehicle Technology”, Defense Science and Technology Organization, Melbourne, Australia, February 1995.

Can, S., “Uzayda Trafik Yoğun”, Ulusal Strateji Dergisi, Yıl 3, Sayı 17, CNR, İstanbul, 2001.

Carlson, Margeret, "Someone to Watch over Me", Time Magazine, Vol. 158, Issue 2, U.S.A., 16 July 2001, p. 80.

Carmichael, Bruce W., Troy E. DeVine, Robert J. Kaufman, Patrick E. Pence, and Richard S. Wilcox, "Strikestar 2025", U.S. Air Force 2025, 1996, Avaliable on site: http://www.au.af.mil/au/2025/volume3/chap13/v3c13-9.htm#v3c13-9

Caşın, M. Hakkı, "Digital Revolution for the Military: The Effects of the Electronics Revolution in the 21st Century on the International Security Strategy", Armed Forces Communications and Electronics Association, AFCEA, Ankara, September 1995.

Caterinicchia, Dan, "DoD Advancing High-Tech Projects", 6 March 2002, Available on site: http://www.fcw.com/fcw/articles/2002/0304/web-actd-03-06-02.asp

Cebrowski, A., and J. Garstka, "Network-Centric Warfare", CCRP Publication Series, DoD, Washington D.C., U.S.A., 1997.

Cebrowski, Arthur K., and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," U.S. Naval Institute Proceedings, U.S.A., January 1998, Available on site: http://www.usni.org/Proceedings/Articles98/PROcebrowski.htm

Cereijo, Dr. Manuel, "Cuba and Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. The Bejucal Base", Available on site: http://www.futurodecuba.org/INFOWAR_202.htm

Cereijo, Manuel, "Information Warfare (IW): Signals Intelligence (SIGINT), Electronic Warfare (EW) and Cyber-Warfare. Asia and Cuba", Cuba Information Links Web Page, Cuba, February 2003, Available on site: http://www.cubainfolinks.net/Articles/bejucal.htm

Cfar.umd.edu Web Page, "Automatic Target Recognition", 1996, Available on site: http://www.cfar.umd.edu/cvl/projects/automatic_target_recognition.html

Chaisson, Kernan, "New Radar for Raptor's New Mission", Journal of Electronic Defense, U.S.A., November 2002. Available on site: http://www.jedonline.com

Chaisson, Kernan, and Brendan P. Rivers, with Patrick Brunet, "Lead Story: US-Led War on Terror Staged Over Afghanistan", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

Ciufo, Chris A., "UAVs: New Tools for the Military Toolbox", COTS Journal, U.S.A., June 2003.

Clark, Phillip, "The Decline of Russia's ELINT Satellite Programmes", Jane's Intelligence Review, U.S.A., November 2000.

Clarke, Patrick E., "'Reachback' for the Warfighter", Military Information Technology Online Edition, Volume: 7, Issue: 4, U.S.A., 19 May 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=113

Clarke, Patrick E., "Nerve Centers for Air Warfare", Military Information Technology Online Edition, Volume: 7, Issue: 7, U.S.A., 01 September 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=183

Clarke, Patrick E., "Sun Never Sets on NETCOM Operations", Military Information Technology Online Edition, Volume: 7, Issue: 8, U.S.A., 13 October 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=231

Cohen, William S., "Annual Report to the President and the Congress – Information Superiority and Space", Secretary of Defense, DoD, U.S.A., 1999. Available on site: http://www.defenselink.mil/execsec/adr99.htm

Cooper, Jeff, "Toward a Theory of Coherent Operations," SRS Technologies Magazine, U.S.A., 30 June 1994.

Cooper, Jeffrey, "Another View of Information Warfare: Conflict in the Information Age", SAIC, Publication Draft for 2025 Study Group, U.S.A., 1996.

Cordesman, Anthony H., "Struggle for Air Supremacy", Center for Strategic and International Studies CSIS, Washington, D.C., U.S.A., 15 October 1994, Available on site: http://www.csis.org_burke_reports_941015lessonsgulfIV-chap06

Cordesman, Anthony H., "The Lessons of the Iraq War: Executive Summary", Center for Strategic and International Studies, Washington, DC, U.S.A., 21 July 2003, Available on site: http://www.csis.org/features/iraq_instantlessons_exec.pdf

Cordesman, Anthony H., and Abraham R. Wagner, "The Lessons of Modern War-Volume 1: The Arab-Israeli Conflicts 1973-1989", Westview Press, Boulder, CO, U.S.A., 1990.

Cossa, Ralph A., "U.S.-China Relations: The Crew's Home; Now What?", PacNet 15A, CSIS, U.S.A., 16 April 2000, Available on site: http://www.csis.org/pacfor/pac0115A.htm

Covault, Craig, "Eavesdropping Satellite Parked Over Crisis Zone", Aviation Week & Space Technology Magazine, U.S.A., 18 May 1998, p.30.

Covault, Craig, "Recon Satellites Lead Allied Intelligence Effort", Aviation Week and Space Technology Magazine, U.S.A., 4 February 1991.

Covault, Craig, and Joseph C. Anselmo, "Titan Explosion Destroys Secret 'Mercury' SIGINT [Satellite]", Aviation Week & Space Technology Magazine, U.S.A., 17 August 1998, p.29.

Crapanzano, Michael, "Palladium Modem in Approval Stage to Become Catalyst for Improved - ARAT SIPRNET Dial-Up Connectivity", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 2, Issue 1, U.S.A., July 2001.

Creveld, Prof. Martin Van, "Command in War", Harvard University Press, Cambridge, MA, U.S.A., 1987.

Crickmore, Paul F., "Lockheed SR-71 - The Secret Missions Exposed", Osprey Aerospace, London, UK, 1993.

Danskine, William B., "The Time-Critical Targeting Model", Air University, Maxwell Air Force Base, Alabama, U.S.A., April 2000.

David, Leonard, "Space Junk and ISS: A Threatening Problem", Space.com Web Page, U.S.A., 7 Jan 2002, Available on site: http://space.com/missionlaunches/junk_iss_020107.html

Defense Science Board, "Report of the Defense Science Board Task Force on Information Warfare-Defense (IW-D)", Defense Science Board, Washington, D.C., U.S.A., 1996. Available on site: http://www.au.af.mil/au/awc/awcgate/infowar/iwd/iwd-a.htm

Demarest, Marc C., "New Technologies on the Horizon for Access to ARAT", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 2, Issue 1, July 2001.

Department of Defense, "Space Technology Guide-FY 2000-01", U.S. Secretary of Defense, Washington, U.S.A., 2002, Available on site: http://www.defenselink.mil/myer.pdf

Department of Defense, "Conduct of the Persian Gulf War: Final Report", Secretary of Defense, Washington, U.S.A., 1992, Available on site: http://www.defenselink.mil/ezecsec/

Dishman, Chris, "Looking to Future, CIA Should Focus on Human Intelligence", The Christian Science Monitor – Opinion & Essays, U.S.A., 6 August 1997.

Dolan, Raymond, "WIN-T", Military Information Technology Online Edition, Volume: 7, Issue: 4, U.S.A., 19 May 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=109

Douglas, Barrie, "Strategic Investment", Aviation & Space Technology, Vol.158, Issue 20, London, Great Britain, 19 May 2003.

Dranidis, Dimitris V., "Backboards of the Fleet: Shipboard Phased-Array Radars", Journal of Electronic Defense, U.S.A., May 2003. Available on site: http://www.jedonline.com

Electronic Defense Magazine, Washington, U.S.A., May, 1991.

Eliot A. Cohen, "Gulf War Air Power Survey", Volume IV, Part I, Department of the Air Force, Washington, D.C., U.S.A., 1993.

Evers, Stacey, "ARPA Pursues Pocket-Sized Pilotless Vehicles", Jane's Defence Weekly Magazine, Vol.26, No.12, UK, 20 March 1996.

Evers, Stacey, "US Research on Micro Air Vehicles Design Takes off", Jane's Defence Weekly Magazine, Vol.27, No.23, UK, 11 June 1997.

Far Eastern Economic Review, "Indonesia Seeks Israeli Defense Help", Far Eastern Economic Review, U.S.A., 5 October 2000, p.10.

Federation of American Scientists Web Page, "Advanced Radar Systems", U.S.A., Available on site: http://www.fas.org/man/dod-101/navy/docs/es310/syllabus.htm

Federation of American Scientists Web Page, "DQ-1", FAS Space Policy Project, 30 June 1998, Available on site: http://www.fas.org/spp/guide/china/military/sigint/dq-1.htm

Federation of American Scientists Web Page, "SJ-2", FAS Space Policy Project, 1998, Available on site: http://www.fas.org/spp/guide/china/military/sigint/sj-2.htm

Federation of American Scientists Web Page, "SIGINT Programs and Activities–Russia", 1997, Available on site: http://www.fas.org/irp/world/russia/program/sigint.htm

Federation of American Scientists Web Page, Space Policy Project, "Tselina 2", U.S.A., 2002, Available on site: http://222.fas.org/spp/guide/russia/military/sigint/tselina2.htm.

Federation of American Scientist Web Page, "Joint Warfighter DTOs Combat Identification", 1997, Available on site: http://www.fas.org/spp/military/docops/defense/97_dtos/jw_dtos/jw_dto_c.htm

Federici, Gary, "From the Sea to the Stars: A History of U.S. Navy Space and Space-Related Activities", Department of the Navy-Naval Historical Center, Washington, D.C., U.S.A., June 1997.

Feeney, Christopher, "A Star Wars Non-Fictional Technical Commentary", University of Southern California, U.S.A., Available on site: http://www-scf.usc.edu/-recker/swreal.htm

Fisher, Richard D., "Heritage Report on China's 1998 Zhuhai Air Show", The Heritage Foundation, 1998, Available on site: http://www.heritage.org/exclusive/zhuhai/part1.html

Fisher, Richard D., Jr., "PLAAF Equipment Trends", National Defense University Conference on PLA and Chinese Society in Transition, U.S.A., 30 October 2001, Available on site: http://www.ndu.edu/inss/China_Center/RFischer.htm.

Fisher, Richard D., Jr., "Questions About the Air Battle Dimension of the PLA's Developing Information-Strike Combine", National Defense University Center for the Study of Chinese Military Affairs, U.S.A., 27 October 2000, Available on site: http://www.ndu.edu/inss/China_Centre/paper8.htm.

FitzGerald, M.C., "Russian Views on IW, EW, and Command and Control: Implications for the 21st Century", CCRP, Department of Defence, Washington, D.C., 1996, Available on site: http://www.dodccrp.org/1999CCRTS/pdf_files/track_5/089fitzg.pdf

Fowler, Will, "Battlefield communications", Available on site http://www.combat-online.com/radio.htm

Frater, Michael R., and Michael Ryan, "Electronic Warfare for the Digitized Battlefield", Artech House, Boston, U.S.A., 2001.

Freeman, Tony, "What is imaging Radar", Jet Propulsion Laboratory, Pasadena, CA, 1996, Available on site: http://www.spaceimaging.com/products/radarsat/whatisradar.htm

French, Matthew, "Army to get CACI systems", 16 September 2003, Available on site: http://www.fcw.com/fcw/articles/2003/0915/web-army-09-16-03.asp

Friedman, George & Meredith, "The Future of War", Crown Publishers Inc., New York, U.S.A., 1996.

Friedman, Norman, "Seapower and Space: From the Dawn of the Missile Age to Net-Centric Warfare", Naval Institute Press, Annapolis, MD, U.S.A., 2000.

Fulghum, David A., "DarkStar First Flight Possible in March," Aviation Week and Space Technology Magazine, U.S.A., 19 February 1996.

Fulghum, David A., "International Market Eyes Endurance UAVs," Aviation Week and Space Technology, U.S.A., 10 July 1995, p. 40-43.

Fulghum, David A., "China May Sell EP-3 Secrets", Aviation Week & Space Technology Magazine, U.S.A., 16 April 2001.

Fulghum, David A., "Fast Forward," Aviation Week Magazine, U.S.A., 28 April 2003.

Fulghum, David A., "Flexibility, Endurance Are Valued EP-3 Assets", Aviation Week & Space Technology Magazine, U.S.A., April 2001.

Fulghum, David A., "Gulfstream Plans UAV", Aviation Week & Space Technology, Vol. 159, Issue 2, Washington, D.C., U.S.A., July 2003.

Fulghum, David A., "International Market Eyes Endurance UAVs", Aviation Week and Space Technology, U.S.A., 10 July 1995.

Fulghum, David A., "Key Decisions Remain For New Intel Aircraft", Aviation Week & Space Technology, Vol.157, Issue 4, Washington, U.S.A., 22 July 2002.

Fulghum, David A., "Long-Range UAV Exports Face Arms Control Hurdles", Aviation Week & Space Technology Magazine, U.S.A., 11 June 2001.

Fulghum, David A., "Micro and Nano Sats.", Aviation Week & Space Technlogy Magazine, Volume 158, Issue 24, Tel Aviv, Israel, 16 June 2003.

Fulghum, David A., "Predator to Make Debut Over War - Torn Bosnia", Aviation Week and Space Technology, 10 July 1995.

Futrell, Robert F., "The USAF in Korea 1950-1953", Office of USAF History, Washington, D.C., 1983.

Gallimore, Jack M., "Jack's Journal", Clemmons NC, U.S.A., 18 November 2001, Available on site: http://www.aipress.com/jackmem_06.BOZTEPE.pdf

Gallimore, Jennie J., "Uninhabited Combat Aerial Vehicles in the Military SEAD Mission", Wright State University, Dayton, OH, U.S.A., 14 March 2000.

Garamone, Jim, "From the U.S. Civil War To Afghanistan: A Short History of UAVs", American Forces Press Service, Washington, U.S.A., April 2002, Available on site: http://www.defendamerica.mil/articles/apr2002/a041702a.html

Gegax, T.Trent, "Wired for Battle", Newsweek Magazine, Vol.141, Is.9, 3 March 2003.

Gertz, Bill, "US Breathes Easier as it Spots Iraq's Jamming Gear", The Washington Times, Washington, D.C., U.S.A., 9 October 1990.

Gertz, Bill, and Rowan Scarborough, "Inside the Ring: China Eavesdropping", The Washington Times, Washington, U.S,A., 5 May 2000.

Gilleo, Ken, "The Real Warbots", Reed Electronic Group, U.S.A., 2002, Available on site: http://www.reed-electronics.com/semiconductor/index.asp

Gilley, Bruce, "Pacific Outpost: China's Satellite Station in Kiribati has Military Purposes", Far Eastern Economic Review, Australia, 30 April 1998, p.26-27

Gorn, Dr Michael H., "Prophecy Fulfilled: Toward New Horizons and Its Legacy", Air Force History and Museums Publications, U.S.A., 1994.

Goure, Daniel, and Christopher M. Szara, "Air and Space Power in the New Millennium", Center for Strategic and International Studies, Washington, U.S.A., 1997.

Gourley, Scott R., "Building a Digital Bridge", Military Information Technology Online Edition, Volume 7, Issue 3, U.S.A., 30 March 2003, Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=16

Gourley, Scott R., "Land Warrior Moves Forward", Military Information Technology Online Edition, Volume: 7, Issue: 3, U.S.A., 30 March 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=14

Gourley, Scott, "Command, Control, Communications, Computers and Intelligence (C4I) Systems", Army Magazine, Volume 53, Issue 10, U.S.A., October 2003, Available on site: http://www.ausa.org/www/greenbook.nsf

Grahm, Bradley, and Vernon Loeb, "An Air War of Might, Coordination, and Risks", Washington Post, Washington, D.C., U.S.A., 27 April 2003.

Grahn, Sven, "An Analysis of the Design of GRAB, the First ELINT Satellite", Available on site: http://www.svengrahn.pp.se/radioind/GRABELINT/GRABELINT.html

Grier, Peter, "Joint STARS Does Its Stuff", Air Force Magazine, U.S.A., June 1991.

Guillemette, Roger, "Trio of NRO Spy Satellites to be Launched During Next Two Months", Space.com Web Page, U.S.A., 6 September 2001, Available on site: http://www.space.com/missionlaunches/nro preview 01906.html

Hacket, James T., "Tracking Targets from Space," Washington Times, 8 July 2003.

Hager, Nicky, "Secret Power: New Zealand's Role in the International Spy Network", Craig Potton, Nelson, New Zealand, 1996.

Hall, Keith, "Prepared Remarks at the Naval Research Laboratory 75th Anniversary Event", National Reconnaissance Office, U.S.A., June 1998. Available on site: http://www.globalsecurity.org/space/library/news/1998/grab-698.html

Hallion, Richard P., "Storm over Iraq Air Power and the Gulf War", Smithsonian Institution Press, Washington. D.C., U.S.A., 1992.

Harrill, Rob, "World's Smallest Self-Propelled Satellite Nearly Ready for Air Force, NASA", Space Daily Newsletter Online Edition, Seattle, U.S.A., 2 November 2001, Available on site: http://www.spacedaily.com/nanosats.html

Harshberger, Edward and Ochmanek, David, "Information and Warfare: New Opportunities For U.S. Military Forces", Ed: Zalmay M. Halizad, John P. White, The Changing Role of Information in Warfare", RAND, California U.S.A., 1999.

Hewish, Mark, and Joris J. Lok, "Naval Surveillance Fixes Gaze on a New Breed of Radar", Jane's International Defense Review, Vol.31, Essex, UK, October 1998.

Hewish, Mark, and Joris J. Lok, "The Intelligent War", Jane's International Defense Review, Vol.30, Essex, UK, December 1997.

Howard, Stephen P., "Special Operations Forces and Unmanned Aerial Vehicles: Sooner or Later", Air University, Maxwell AFB, Alabama, U.S.A., June 1995.

Hutcherson, Norman B., "Command & Control Warfare", Air University Press, Maxwell, Alabama, U.S.A., September 1994.

Ingrao, Joseph, "The All Source Analysis System (ASAS) Family of Systems: Providing Operational Intelligence to the Warfighter", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 2, Issue 1, U.S.A., July 2001.

Inggs, M.R., and Lord, R.T., "Applications of Satellite Imaging Radar", University of Cape Town, South Africa, 2002, Available on site: http://rrsg.ee.uct.ac.za/applications/applications.html

Ives, John W., "Army Vision 2010: Integrating Measurement and Signature Intelligence", U.S. Army War College, Pennsylvania, U.S.A., April 2002.

Jane's Defense Weekly, "Ministry Will Test Eagle Scout Drone", Jane's Defense Weekly Magazine, Vol.32, No.18, UK, 24 April 2002.

Jimenez, Alfredo, "Digital Bridge Brings Technology to Stryker Brigade at NTC", US Army Public Affairs, 2003, Available on site: http://w4.pica.army.mil/voice2003/030411/digitalbridge.htm

Johnson, Milton H., "The Impact of Doctrine on Air Force Roles and Missions", Air University, Maxwell Air Force Base, Alabama, U.S.A., April 1997.

Johnson, Nicholas, and David Rodvold, "Europe and Asia in Space 1993-1994", Kaman Sciences, A.F. Phillips Laboratory, U.S.A., 1996, Available on site: http://www.plk.af.mil/

Joint Publication 3-51, "Joint Doctrine for Electronic Warfare", U.S. Marine, Washington, D.C., U.S.A., April 2000.

Jones, Christopher A., Maj., "Unmanned Aerial Vehicles (UAVS) An Assessment of Historical Operations and Future Possibilities", US Air Command and Staff College, U.S.A., March 2003, Available on site: www.fas.org/irp/program/collect/docs/97-0230D

Journal of Electronic Defense, "US Navy Looks to Protect Smaller Vessels", November 2001. Available on site: http://www.jedonline.com

Keaney, Thomas A. and Eliot A. Cohen, "Gulf War Air Power Survey: Summary Report", Department of the Air Force, Washington, D.C., U.S.A., 1993.

Kenyon, R., "Air/Space Based Platforms", U.S.A., 2000, Available on site: http://www.highfrontier.org/hf_spacebased.html

Keys, Ronald E., "Airspace Control in the Combat Zone", Air Force Doctrine Document 2-1.7, Air Force Doctrine Center, U.S.A., 4 June 1998.

Kılıçaraslan, M.A., "Bilgi Harbi Nedir? TSK'nın Mevcut Yapısını da dikkate alarak Bilgi Harbini Etkin Bir Şekilde Uygulayan Gelişmiş Orduların Uygulamalarına Karşı Alınacak Tedbirleri Araştırınız", Unpublished Thesis, Harp Akademileri, Ist., 2000.

Kitfield, James, "The Permanent Frontier", The National Journal, U.S.A., 17 March 2001, Available on site: http://www.globalsecurity.org/org/news/2001/010317-nj.htm.

Kosan, Keith J., "United States Air Force Precision Engagement Against Mobile Targets: Is Man in or out?", Air University, Maxwell, Alabama, U.S.A., June 2000.

Krane, J., "Sign on San Diego Military-In Terror War, High-Tech Military Tools could be Used to Hunt Low-Tech Foes", San Diego, U.S.A., 2001, Available on site: http://www.uniontrib.com/news/military/20010923-1313-attacks-high.html

Krause, Merrick E., "Decision Dominance: Exploiting Transformational Asymmetries," Defense Horizons Magazine, No. 23, Center for Technology and National Security Policy, National Defense University, Washington, D.C., U.S.A., February 2003.

Krepinevich, Andrew F., Jr., "The Military Technical Revolution: A Preliminary Assessment," Air Command and Staff College, War Theory Course Book, Volume 3, Maxwell AFB, Alabama, U.S.A., September 1995.

Krepinevich, Andrew, "Air Force of 2016", CSBA Publications, October 1996, Available on site: http:www.csbaonline.org/4Publications/Archive/Air_Force_of_2016.htm

Kugler, Richard L. and Hans Binnendijk, "Transforming America's Military - Choosing A Strategy", Ed. Hans Binnendijk, National Defense University, U.S.A., June 2002.

Lapointe, Mike, "Future Spaced Based Radar", NSSA, U.S.A., July 1999, Available on site: http://www.fas.org/spp/military/program/nssrm/initiatives/sbr_dod.htm

Lashmar, Paul, "Spyflights of the Cold War", Sutton Publishing Ltd., Gloucestershire, U.S.A., 1996.

Lewis, Mike, "The Future of EW Threat Databases - Project K2000", Avionics/ Intelligence and Electronic Warfare Bulletin, Volume 2, Issue 1, U.S.A., July 2001.

Libicki, Martin C., "Information Dominance", National Defense University, U.S.A., November 1997, Available on site: http://www.ndu.edu/inss/strforum/SF132/forum132.html

Libicki, Martin, "What is Information Warfare", National Defense University, U.S.A., 1995, Available on site: http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003ch04.html

Lin, H.S., "Realizing the Potential of C4I", National Academy Pres, Washington, D.C., U.S.A., 1999.

Loeb, Vernon, "Commander Defends Iraq War Comments," Washington Post, U.S.A., 8 May 2003.

Loeb, Vernon, "Intense, Coordinated Air War Backs Baghdad Campaign", Washington Post, U.S.A., 6 April 2003.

Logsdon, John, "Just Say Wait to Space Power," Science and Technology Magazine, U.S.A., Spring 2001, Available on site: www.nap.edu/issues/17.3/p_logsdon.htm.

Longino, Dana A., Lt Col, "Role of Unmanned Aerial Vehicles in Future Armed Conflict Scenarios", Air University Press, Maxwell AFB, Alabama, U.S.A., 1994.

Mann, Edward, "Desert Storm: The First Information War?", Aerospace Power Journal, Winter 1994, Available on site: http://www.iwar.org.uk/iwar/resources/airchronicles/man1.htm

Marietta, Martin, "SB-WASS - Consolidated Program", US Air Force Laboratory, Washington, D.C., U.S.A., 1995, Available on site: http://www.afbmd.laafb.af.mil/XRT/xrte/recon/index.html

Marks, James A., Brigadier General, "Interview: Intelligence Warrior", Military Information Technology Online Edition, Volume: 6, Issue: 8, 10 October 2002. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=?

Martel, William, ed., "The Technological Arsenal: Emerging Defense Capabilities", Smithsonian Institution, Washington, DC, U.S.A., 2001.

Mason, Tony, "The Role of European Ground and Air Forces After the Cold War: Roles, Missions and Means for the Specific Use of Aerial Forces", Ed. Gert de Nooy, Netherlands Institute of International Relations 'Clingendael', Netherlands, 1997.

Mathews, Tom, "The Secret History of the War", Newsweek Magazine, New York, NY, U.S.A., 18 March 1991.

McCarter, Mickey, "IA: The Challenge of Enforcement", Military Information Technology Online Edition, Volume: 7, Issue: 7, U.S.A., 01 September 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=?

McCleskey, Edward R., "Urban Warfare at the Operational Level: Identifying Centers of Gravity and Key Nodes", Air University, Maxwell AFB, Alabama, U.S.A., 1999.

McConnell, K., M. Meermans, "Nowhere to hide: A Prescription For Attacking Fleeting, Mobile Battlefield Targets", Armed Forces Journal, U.S.A, July 2001.

McKaughan, Jeffrey D., "Eyes in the Sky", Military Aerospace Technology Magazine, Volume: 2, Issue: 1, U.S.A., 02 February 2003. Available on site: http://www.mat-kmi.com/archive_article.cfm?DocID=90

McLendon, J.W., "Battlefield of Future: Chapter 7, Information Warfare Impacts and Concerns", Air Force University Press, Maxwell, Alabama, U.S.A., 1998, Available on site: http://www.airpower.af.mil/airchronicles/battle/chp7.html

McPeak, Gen Merrill A., “Selected Works 1990-1994”, Air University Press, Maxwell AFB, Alabama, U.S.A., August 1995.

Meilinger, Col Phillip S., “10 Propositions Regarding Air Power”, Air Force History and Museums Program, Maxwell AFB, Alabama, U.S.A., 1995.

Mermet, François, “The Role of European Ground and Air Forces After the Cold War: European Political-Military Analysis and Decision-Making”, Ed. Gert de Nooy, Netherlands Institute of International Relations ‘Clingendael’, Netherlands, 1997.

Meyerriecks, Dawn, “Net-Centric Enterprise Services”, Military Information Technology Online Edition, Volume: 7, Issue: 3, U.S.A., 30 March 2003. Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=23

Miller, Jay, “Lockheed's Skunk Works: The First Fifty Years”, Aerofax, Inc., Arlington, Texas, U.S.A., 1993, p.134-135; Rich, Ben R., “Skunk Works”, Little, Brown and Co., New York U.S.A., 1994.

Miller, Gregory J., Kurt C. Fecht, Barbara Jefts, Laura J. Sampsel, and Patrick J. Smith, “Virtual Integrated Planning And Execution Resource System (VIPERS): The High Ground Of 2025”, A Research Paper Presented to A.F., Washington, U.S.A., 1996

Ministry of Defence “The Future Strategic Context for Defence - The Technological Dimension”, Secretary of State for Defence, London, U.K., November 2001, Available on site: http://www.mod.uk/issues/strategic_context/physical.htm

Ministry of Defence, “The New Chapter To The Strategic Defence Review: A Progress Report”, Speeches & Statements, Secretary of State for Defence, London, U.K., 23 May 2002, Available on site: http://news.mod.uk/news_press_notice.asp?newsItem_id=1727

Minnick, Wendell, “Taiwan-USA Link Up on SIGINT”, Jane's Defense Weekly, Vol.31, No.4, UK, 24 January 2001.

Molander, Roger C., Andrew S. Riddile, and Peter A. Wilson, “Strategic Information Warfare: A New Face of War”, Santa Monica, RAND, California U.S.A., 1996.

Monthly Economic News on Israel, "Elisra Offers Low-Cost Intelligence-Gathering by UAV in Asia", Embassy of Israel, Singapore, Singapore, 10 March 2002, Available on site: http://www.israelbiz.org.sg.

Morris, William R., "The Role of China's Space Program in Its National Development Strategy", Maxwell Paper No. 24, Air War College, Maxwell AFB, Alabama, 2001.

Morse, Stan, ed., "Gulf Air War Debrief", Aerospace Magazine, London, U.K., 1991.

Möller, Ralf, "Wings", Artificial Intelligence Lab, University of Zurich, Available on site: http://www.cis.plym.ac.uk/cis/InsectRobotics/Wings.htm

Munro, Neil, "The Quick and the Dead", St. Martin's Press, New York, U.S.A., 1991.

Munson, Kenneth, "Jane's Unmanned Aerial Vehicles and Targets", Jane's Information Group Limited, Surrey, UK, 1996.

Myer, Charles R., "Viet Cong SIGINT and U.S. Army COMSEC in Vietnam", Cryptologia, Vol.13, No.2, U.S.A., April 1989

Nardulli, Bruce R. and Thomas L. McNaugher, "Transforming America's Military - The Army: Toward the Objective Force", Ed. Hans Binnendijk, NDU, U.S.A., 2002.

Naval Research Laboratory, "G R A B, Galactic Radiation and Background, World's First Reconnaissance Satellites", Naval Research Laboratory, Washington, D.C., U.S.A., 2002, Available on site: http://www.nrl.navy.mil/

Naval Studies Board, "Technology for the United States Navy and Marine Corps, 2000-2035 Becoming a 21st Century Force, Volume 3: Information in Warfare", National Academy of Science, Washington, U.S.A., 1997, Available on site: http://www.nap.edu/html/tech_21st/iwindex.htm

National Academy of the Science Web Page, "4: Sensors", NAP, U.S.A. Available on site: http:www.nap.edu/html/tech_21st/t4.htm

Nederveen, Gilles Van, "Sparks Over Vietnam - The EB-66 and the Early Struggle of Tactical Electronic Warfare", Airpower Research Institute, ARI Paper 2000-03, U.S.A., 2000, Available on site: http://www.airpower.maxwell.af.mil/airchronicles/ct/research/sparks

Nemzetvédelmi, Zrínyi Miklós, "Advanced Military Technology Related Research Work at Electronic Warfare", National Defense University, U.S.A., 2002, Available on site: http://www.zmka.hu/tanszekek/ehc/konferencia/may/makkay.htm

Neri, Flippo, "Introduction to Electronic Defense Systems", Artech House, Boston, 1991.

Nitschke, Stefan, "The Role of Electronic Warfare in Naval Warfare", Naval Forces Magazine, No.IV/2002, Vol.XXIII, Bonn, Germany, 2002.

Ortiz, David, "A New Role for Today's UAVs", Aerospace Power Journal, Oklahoma, U.S.A., Fall 2000.

Owens, Adm William A., "The Emerging System of Systems," Proceedings Magazine, U.S.A., May 1995.

Özdemir, Eşref, "Bilgi Savaşları", IQ Kültür Sanat Yayıncılık, İstanbul, 2003.

Pan, Philip P., "Banned Falun Gong Movement Jammed Chinese Satellite Signal", Washington Post Web Page, U.S.A., 9 July 2002, Available on site: http://www.washingtonpost/com/wp-dyn/articles/A41297-2002Jul$.html

Parker, S., H. Neimeier, "C4ISR Analytic Performance Evaluation Models", MIT Publication, USA, 1998, Available on site:http://www.mitre.org/pubs/edge/august_98/cape.html

Peebles, Curtis, "High Frontier: The U.S. Air Force and the Military Space Program", Government Printing Office (DoD), Washington, DC, U.S.A., 1997.

Petersen, John L., "The Road to 2015, Profiles of the Future", Waite Group Press, Corte Madera, California, U.S.A., 1994, p. 284-285.

Pietrucha, Maj Michael, "Needles in the Haystack: Hunting Mobile Electronic Targets", Air & Space Power Journal Magazine, U.S.A., Spring 2003.

Pike, John, "Integrated Overhead SIGINT Architecture", Global Security Web Page, Washington, D.C., U.S.A., November 2002, Available on site: http://www.globalsecurity.org/Space/Integrated.htm

Pike, John, "Intruder", Global Security Web Page, Washington, D.C., U.S.A., October 2002, available on site: http://www.globalsecurity.org /Space/INTRUDER.htm

Pike, John, "Military Communications", Global Security Web Page, Washington, D.C., October 2002, Available on site: http://www.globalsecurity.org/Space/Military.htm

Pike, John, "Project Tattletale: Galactic Radiation Background Experiment (GRAB)", Washington, USA, 2002, Available on site: http://www.globalsecurity.org/Space/GRAB.htm

Pike, John, "SIGINT Overview", Global Security Web Page, Washington, U.S.A., 8 October 2002, Available on site: http://www.globalsecurity.org/space/systems/SIGINT

Pike, John, "Signal Intelligence", Global Security Web Page, Washington, D.C., October 2002, Available on site: http://www.globalsecurity.org/space/systems/SIGINT

Pitts, Joseph R., "What is Electronic Warfare?", A Speech to the Lexington Institute, Washington, D.C., U.S.A., 22 October 2003, Available on site: http://www.house.gov/pitts/Commentary from.htm

Polanco, Benjamin, "PM/ACS and SEC Provide an Innovative Training Solution for Guardrail Common Sensor Systems", Avionics/Intelligence and Electronic Warfare Bulletin, Volume 1, Issue 4, U.S.A., January 2001.

Preston, Bob, "Space Weapons Earth Wars" RAND Publications, Santa Monica, CA, U.S.A, 2001.

Price, Alfred, "EW additions for the RAF", Military Technology Magazine, U.S.A., December 1991.

Pronobis, Mark, "Battlespace Awareness through Information Fusion", Ref: IF-00-17, Air Force Research Laboratory, 2002, Available on site: http://www.afrl.af.mil/techconn/index.htm

Public Affairs Office, "Naval Special Warfare and Special Operations", United States Naval Academy, U.S.A., 2003, Available on site: http://www.usna.edu/Training_probook/spring03/proman

Puttre, Michael, "Middle East Report – Israeli SIGINT Aircraft Finalized", Journal of Electronic Defense, U.S.A., May 2002. Available on site: http://www.jedonline.com

Raj, Manoj, "Airborne Electronic Countermeasures", Air Combat Information Group, U.S.A., January 2003, Available on site: http://www.acig.org/artman/publish/article_56.shtml

Randolph, Stephen P., "Transforming America's Military - Controlling Space", Ed. Hans Binnedijk, , National Defense University Press, U.S.A., June 2002.

Redman, Lt. Col. Douglas, and Lt. Col. Jack Taylor, "Intelligence and Electronic Warfare System Modernization", Army Magazine, U.S.A., April 2002.

Reimer, D. "Foreword - War in the Information Age: New Challenges for U.S. Security Policy", Ed.R.Pfaltzgraff and R.Shultz, Brassey's, Washington D.C., U.S.A., 1997.

Reports, "Military Communication", U.S.A., Available on site: http://www.defensedaily.com/reports/probudiansky.htm

Rich, Ben R., "Skunk Works", Little, Brown and Company, New York, U.S.A., 1994.

Richelson, J., "The U.S. Intelligence Community", Ballinger, Cambridge, MA, U.S.A., 1985.

Richelson, Jeffrey T., "Foreign Intelligence Organizations", Ballinger, Cambridge, Massachusetts, U.S.A., 1988.

Richelson, Jeffrey T., "Foreign Intelligence Organizations", Ballinger, Cambridge, Massachusetts, U.S.A., 1988.

Richelson, Jeffrey T., "The U.S Intelligence Community", 4th Edition, Westview Press, Boulder, Colorado, U.S.A., 1999.

Richelson, Jeffrey, "Despite Management/Budget Woes, NRO Launches Continue", Defense Week Magazine, U.S.A., 12 August 1996, p.16.

Richelson, Jeffrey, T., "America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite Program", Harper & Row Publications, New York, N.Y., U.S.A., 1990.

Ricketts, Peter, "Special Mission Aircraft: Same Result, Lower Cost", Asia-Pacific Defense Reporter, Australia, March/April 2002.

Rivers, Brendan P., "Global Hawk Preps for German - European Report", Journal of Electronic Defense, U.S.A., January 2003. Available on site: http://www.jedonline.com

Rivers, Brendan P., with Michael Puttré, "Predator Unleashes Hellfire", Journal of Electronic Defense, U.S.A., November 2001, Available on site: http://www.jedonline.com

Rivers, Brendan. P., "CEC Passes OPEVAL", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

Rivers, Brendan. P., "New RWRs on the Way for US Carriers", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

Rivers, Brendan. P., "Russia Closing ELINT Base in Cuba", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

Rivers, Brendan. P., "TADIRCM Testing Continues at China Lake", Journal of Electronic Defense, U.S.A., November 2001, Available on site: http://www.jedonline.com

Rivers, Brendan. P., "US Navy Looks to Protect Smaller Vessels", Journal of Electronic Defense, U.S.A., November 2001. Available on site: http://www.jedonline.com

Robert K. Ackerman, "Tactical Goals Encompass Sensors, Autonomous Arts", Signal Magazine, December 1995.

Robinson, Clarence A., "The Electronic Battlefield", Faircount.com Web Page, Available on site: http://www.faircount.com/web04/yid/articles/electron.html

Royal New Zealand Navy Web Page, "Defence Technology Agency Earns International Awards", New Zealand, 2003, Available on site: http://www.navy.mil.nz/rnzn/article.cfm

Sample, Doug, "Pentagon Plans Heavy Investment in UAV Development", American Forces Information Service, News Articles, Washington, USA, 18 March 2003. Available on site: http://www.dod.mil/news/Mar2003/n03182003_200303186.html

Scarborough, Rowan, "Myers Says: Annihilation of Iraqi Army wasn't Goal", Washington Times, U.S.A., 30 June 2003.

Schiesel, Seth, "On the Ground in Iraq: The Best Compass Is in the Sky", New York Times, U.S.A., 17 April 2003.

Schmidt, Eric, "In the Skies Over Iraq, Silent Observers Become Futuristic Weapons", New York Times, U.S.A., 18 April 2003.

Schneider, B.R., "Battlefield of Future: Principles of War for the Battlefield of Future", Air Force Press, Maxwell, U.S.A., 1998, Available on site: http://www.airpower.maxwell.af.mil/airchronicles/battle/chp1.html

Schwarzkopf, H. Norman with Peter Petre, "General H. Norman Schwarzkopf, the Autobiography: It Doesn't Take a Hero", Bantam Books, New York, U.S.A., 1992.

Scott, William B., "Kinetic-Kill Boost Phase Intercept Regains Favor", Aviation Week and Space Technology Magazine, U.S.A., 4 March 1996, p. 23.

Secretary of State for Defence, "Kosovo: Lessons From The Crisis", Ministry of Defence, London, 2002, Available on site: http://www.mod.uk/publications/kosovo_lessons/chapter7.htm

Secretary of State for Defence, "Ministry of Defence Investment Strategy 2002", Ministry of Defence, London, 2002, Available on site: http://www.mod.uk/issues/investment_strategy/02/investment.htm

Shenxia, Z., Z. Changzai, "Chinese Views of Future Warfare, Part Four, The Revolution in Military Affairs: The Military Revolution in Air Power", Ed.: M. Pillsbury, National Defense University Press, U.S.A., 1996.

Sherman, Kenneth B., "Asia-Pacific Report", Journal of Electronic Defense, U.S.A., March 2003, Available on site: http://www.jedonline.com

Sherman, Madeline W., (ed.), "TRW Space Log, 1957-1982", Electronics and Defense Sector, TRW, Redondo Beach, California, U.S.A., 1983.

Signal, "Optical Space Communications Cross Links Connect Satellites", Signal Magazine, U.S.A., April 1994.

Sinodefense Web Page, "Chinese Defense Today: Tu-154 Jet Transport", Available on site: http://www.sinodefense.com/airforce/aircraft/transport/tu154.asp.

Sinodefense Web Page, "WZ-5 Unmanned Reconnaissance Aerial Vehicle", Chinese Defense Today, Available on site: http://www.sinodefense.com/airforce/aircraft/uav/wz5.asp.

Sirak, Michael, and Andrew Koch, "USAF, USN Consider New Missions for Global Hawk", Jane's Defense Weekly, Vol.31, No.33, UK, 15 August 2001.

Slade, Stuart L. "Littoral Warfare: Ships & Systems from the Sea to the Land", Forecast International/DMS, Available on site: http://www.defensedaily.com/reports/shipsys.htm

Slipchenko, Vladimir I., "A Russian Analysis of Warfare Leading to the Sixth Generation", Field Artillery, October 1993.

Smith, Charles R., "Chinese Airlines Serve PLA Military", Newsmax Web Page, 16 Apr 2002, Available on site: http://www.newsmax.com/archives/articles/2002/4/15/172400.shtml

Souder, Jeffrey K., "Computer-Network Defense - The relationships of space, time, and force in cyberspace", Journal of Electronic Defense, U.S.A., October 2001. Available on site: http://www.jedonline.com

Space Daily Web Page, "Both Civil and Military Needs Driving European UAV Market", San Jose, 07 January 2004, Available on site: http://www.spacedaily.com/news/uav-04a.html

Special Operations Web Page, "EC-130E Airborne Battlefield Command and Control Center", 2002, Available on site: http://www.specialoperations.com/Aviation/EC_130.htm

Spires, David, "Beyond Horizons: A Half Century of Air Force Space Leadership", Government Printing Office (DoD), Washington, DC, U.S.A., 1998.

Steele, Dennis, "The Hooah Guide to Army Digitization", Army Magazine, U.S.A., September 2001.

Steele, Robert D., "A New Approach to Collection, Sharing and Analysis", OSSA: Open Source Solutions Academy, Fairfax, VA, U.S.A., 2000

Steele, Robert D., "Presidential Leadership & National Security Policymaking", Open Source Solutions Academy, Fairfax, VA, U.S.A., 1999, Available on site: http://www.defensedaily.com/reports/securpolicy1099.htm

Steele, Robert David, "The Asymmetric Threat to the Nation", Open Source Solutions Academy, Fairfax, VA, U.S.A., June 1998, Available on site: http://www.defensedaily.com/reports/takedown.htm

Streetly, Martin, "Airborne Electronic Warfare, History, Techniques and Tactics", Jane Publishing Group, New York, NY, U.S.A., 1988.

Streetly, Martin, "Asia Pacific Boosts Airborne Surveillance", Jane's Defense Weekly, Vol.32, No.7, UK, 13 February 2002.

Streetly, Martin, "Asia Pacific Boosts Airborne Surveillance", Jane's Defense Weekly, Vol.32, No.7, UK, 13 February 2002.

Streetly, Martin, "Iraq - The Airborne Electronic Warfare Perspective", Jane's Defence Weekly, London, Vol.33, No.12, U.K., 21 March 2003.

Sullivan, Gordon R. and James M. Dubik, "War in the Information Age," Military Review, U.S.A., April 1994.

Sweeney, Dan, "Information Warfare", America's Network Magazine, Vol. 105, Issue 18, U.S.A., 1 December 2001.

Sweeney, John, “NATO bombed Chinese deliberately”, The Observer, London, U.K., 16 October 1999.

Sweetman, Bill, “HALE Storms to New Heights”, Jane’s International Defense Review, Vol.34, Essex, UK, March 2001.

Tadiran Electronic “Electronic Warfare Integrated System (EWIS)”, Tadiran Electronic System Ltd., Holon, Israel, 2003. Available on site: http://www.tadsys.com/EWIS.pdf

Tapscott, Mark, “New Pictures Emerging in Battlefield Intelligence”, Defense Electronic Magazine, U.S.A., April 1993.

Teke, Murat, “Priorities for the Possible Impact of the Information Warfare on the Future Battlefield”, Unpublished Master Thesis, Yeditepe University Graduate Institute of Social Sciences, Istanbul, 2002.

Terry, I., “Networked Specific Emitter Identification in Fleet Battle Experiment Juliet”, U.S. Navy Tactical Electronic Warfare Division, San Diego, California, U.S.A., 2003, Available on site: http://www.nrl.navy.mil/content.php?P=03REVIEW207

The U.S. Army Web Page, “Reconnaissance, Surveillance and Target Acquisition”, Fort Monroc, Virginia, U.S.A., 2002, Available on site: http://www-tradoc.army.mil/dcscd/spaceweb/chap07d.htm

Thomson, Allen, “The U.S. Navy's ‘White Cloud’ Spaceborne ELINT System”, (By:Maj.A.Andronov), Foreign Military Review, No.7, U.S.A., 1993.

Thornborough, Anthony M., “Sky Spies: Three Decades of Airborne Reconnaissance”, Arms and Armor Press, London, England, 1993.

Timperlake, Edward, and William C. Triplett, “Red Dragon Rising: Communist China's Military Threat to America”, Regnery, Washington, D.C., U.S.A., 1999.

Toffler Alvin, “Powershift: Knowledge, Wealth, and Violence at the Edge of the 21st Century”, Bantam Books, New York, U.S.A., 1990.

Toffler, A., and H. Toffler, "War and Anti-War: Survival at the Dawn of the 21st Century", Little Brown, Boston, MA, U.S.A., 1993.

Trimble, Stephen, "GPS is Surviving Jamming Threat, Pentagon Says," Aerospace Daily, U.S.A., 22 April 2003.

U.S. Army field Manual FM 100-6, "Information Operations", August 1996.

Ünal A. N., "Elektronik Saldırı", Ulusal Strateji Dergisi, Yıl: 3, Sayı: 17 CNR, Istanbul, 2001.

Urban, Vladimir, "But Globus Keeps on Spinning", Current Digest of the Post Soviet Press, Vol.53, Issue 43, Cuba, 21 November 2001.

U.S. Air Force 2025 Concept, "Surveillance and Reconnaissance, Real-Time Integration", 2025 concept briefing, Maxwell AFB, Alabama, U.S.A., 19 January 1996, Available on site: http://www.au.af.mil/au/2025/2025_concept

U.S. Air Force, "Air Force Doctrine Document 2-1.1: Counterair Operations", Secretary of the AF, USA, 1998, Available on site: www.fas.org/man/dod-101/usaf/docs/afdd/afdd2-1-1

US Department of Defense, "Annual Report on the Military Power of the People's Republic of China: Report to Congress Pursuant to the FY2000 National Defense Authorization Act", U.S.A., 12 July 2002, Available on site: http://www.defenselink.mil/news/Jul2002/d20020712china.pdf.

US Department of Defense, "Science and Technology-Chapter 17", U.S.A., 1996, Available on site: http:// www.defenselink.mil/execsec/adr96/chapt_17.html

USAF Scientific Advisory Board, "New World Vistas: Air and Space Power for the 21st Century", Summary Volume, USAF Scientific Advisory Board, Washington, 15 Dec 1995.

Vakin, S.A., et. al., "Fundamentals of Electronic Warfare", Artech House, London, U.K., 2001.

Vane, Michael A., and Joseph M. Ozoroski, “Transforming the Doctrinal Development Process”, Army Magazine, U.S.A., June 2003.

Vectorsite.net Web Page, “The Lightning Bug Reconnaissance Drones”, 1 February 2002, Available on site: http://www.vectorsite.net/avuav3.html.

Vectorsite.net Web Page, “US Endurance UAVs”, 1 February 2002, Available on site: http://www.vectorsite.net/avuava.html

Velocci, Anthony L., “Consolidation Juggernaut Yet to Run Its Course,” Aviation Week and Space Technology Magazine, U.S.A., December 3, 2001.

Verton, Dan, “Study Finds Intelligence Software Lacking”, Computerworld Magazine, Vol. 34, Issue 48, U.S.A., 27 November 2001.

Wagner, William, “Lightning Bugs and Other Reconnaissance Drones”, Aero Publishers, Inc., Fallbrook, California, U.S.A., 1982.

Wall, Robert, “Costs Spur Drive to Tweak Global Hawk”, Aviation Week & Space Technology Magazine, U.S.A., 17 June 2002.

Wall, Robert, “Global Hawk in Australia Auditions for New Role”, Aviation Week & Space Technology Magazine, U.S.A., 30 April 2001.

Wall, Robet, “Intelligence Lacking on Satellite Threats”, Aviation Week & Space Technology Magazine, U.S.A., 1 March 1999.

Wallace, Michael A., "HF Radio in Southwest Asia," IEEE Communications Magazine, U.S.A., January 1992.

Waltz, E., “Information Warfare: Principles and Operations”, Artech House Inc. London, U.K., 1998, p. 17.

Warfighting Center, "Warfighting Vision: 2010 A Framework for Change," Joint War fighting Center, Ft Monroe Va., U.S.A., August 1995, p.10.

Watson, Bruce W., eds., “Military Lessons of the Gulf War”, Greenhill Books, London, U.K., 1991.

Watts, Barry, “The Military Use of Space: A Diagnostic Assessment”, Center for Strategic and Budgetary Analysis, Washington, DC, U.S.A., February 2001.

Weatherington, Dyke, “Unmanned Aerial Vehicle Roadmap Report”, Technology and Logistics Magazine, U.S.A., 18 March 2003.

Weaver, Samuel, and Kelvin Wagner, “Real-time Optical SAR Image Generation, Speckle Reduction and Target Recognition”, U.S.A., Available on site: http://drip.colorado.edu/~samw/research/SAR-summary/SAR.project.summary2.htmlver.html

Weiss, Peter, “These New Gadgets Have Minds of Their Own”, Consumers’ Research Magazine, Vol.86, Issue 6, Ontorio, Canada, June 2003.

Wentz, Larry K., “Bosnia: Intelligence Operations”, DDOCCRP Web Page, Chapter IV, U.S.A., Available on site: http://www.ddoccrp.org/bosend.htm

West, Togo D., “Army Science and Technology Plan: Close Combat Light”, Secretary of the US Army, 1998, Available on site: http://www.fas.org/man/dod-101army/docs/astmp98/sec3h.htm

White, Captain Todd G., “Giving Warfighters the JTRS”, Vol. 2, Issue: 4, U.S.A., 15 September 2003, Available on site: http://www.mat-kmi.com/archive_article.cfm?DocID=?

Wiley, Richard G., “Electronic Intelligence: The Interception of Radar Signals”, Artech House, Dedham, MA, U.S.A., 1985.

Yuhas, John S., “Enabling a Transformation in Joint Operations”, Military Information Technology Online Edition, Volume: 7, Issue: 1, U.S.A., 17 January 2003, Available on site: http://www.mit-kmi.com/archive_article.cfm?DocID=35

Zaloga, Steven J., "Unmanned Aerial Vehicles," Aviation Week and Space Technology, U.S.A., 8 January 1996.

CIRRICULUM VITAE

of

Mustafa KAYAR

Kişisel Bilgiler :

Doğum Tarihi	: 06.04.1977
Doğum Yeri	: İzmir
Medeni Durumu	: Bekar

Eğitim :

Lise (1991-95)	: Maltepe Askeri Lisesi
Lisans (1995-99)	: Kara Harp Okulu Sistem Müh.
Y.Lisans (2002-04)	: Yeditepe Üniversitesi Sosyal Bilimler Enstitüsü

Çalıştığı Birlikler :

1999 -2000	Piyade Sınıf Okulu Tuzla-İstanbul
2000 - ……	Piyade Okulu Öğrenci Alayı Tuzla-İstanbul