The Weight of an Assassin's Mace: Vulnerabilities in the US Military's Satellite Communications and China's Information Warfare Threat

by

Benjamin M. Brooks

S.B., Aerospace Engineering (2004)
Massachusetts Institute of Technology

Submitted to the Department of Political Science in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Political Science

at the
Massachusetts Institute of Technology

September 2005

Signature of Author..
Department of Political Science
August 5, 2005

Certified by..
Taylor Fravel
Assistant Professor of Political Science
Thesis Supervisor

Accepted by..
Roger D. Peterson
Associate Professor of Political Science
Chairman, Graduate Program Committee

The Weight of an Assassin's Mace: Vulnerabilities in the US Military's Satellite Communications and China's Information Warfare Threat

by

Benjamin M. Brooks

Submitted to the Department of Political Science on August 5, 2005
in Partial Fulfillment of the Requirements for the Degree of
Master of Science in Political Science

ABSTRACT

Believing that an information Revolution of Military Affairs has occurred, the US military is currently transforming to achieve dominance over the full spectrum of deployment scenarios with a lighter, more mobile, and more capable force. Establishing a far-reaching, robust, ubiquitous ISR and telecommunications network, and a network-centered fighting doctrine are keys to this endeavor. Of the many systems needed, satellite communications are especially significant because they are the prime method of transmitting high quantities of information to remote and mobile units.

The People's Republic of China too has become aware of the information Revolution of Military Affairs, as well as the vulnerabilities associated with it. Though the People's Republic is still in the process of modernizing its society and military, the doctrines and advantages of Information Warfare have not been lost to it. It seeks to equip itself with the IT and skill sets that are becoming increasingly more available to asymmetrically affect the information usage of a technologically superior adversary.

As it stands, the military's use of satellite communications is vulnerable. Though some satellite communications have inherent protective qualities, they are still susceptible to some variants of Electronic Attack and anti-satellite attack. Military-dedicated systems do not offer enough security, and the lack of bandwidth they provide forces the military to use much less secure commercial systems.

It appears that the People's Republic presents only a moderate threat to the military's satellite communications. This will not always be the case. The rapid growth of People's Republic and its increasing informationalization, as well as the expanding US military demand for wideband systems and predictions of a continuing shortfall, all place the military's satellite communications in a precarious situation.

Thesis Advisor: Taylor Fravel
Title: Assistant Professor of Political of Science

Acknowledgements

I would like to thank all those who contributed to the completion of this project. I thank Prof. Taylor Fravel and Prof. Barry Posen for their patience, insights, critiques, and guidance, as well as Dr. Owen Cote, Jr. and Prof. Harvey Sapolsky for their helping hands. I thank my family and friends for their support, especially my mother, my father, my sister, and Stephanie. I thank MIT for giving me the opportunity to study in its hallowed halls and with its esteemed faculty and students. I also thank the Father, Son, and Holy Spirit, for they are my continual source of strength, inspiration, and hope. I am learning to trust more in the road and less in my feet.

Glossary of Acronyms

AFSATCOM - Air Force Satellite Communications

AJ – Anti-Jamming

ARM – Anti-Radiation Missile

ASAT – Anti-Satellite Attack

BER – Bit Error Rate

BLOS – Beyond-Line-of-Sight

C2W – Command and Control Warfare

C^4I^2SR – Command Control Computer Intelligence Information Sensor Reconnaissance

CBO – Congressional Budget Office

CNA – Computer Network Attack

COMERSAT – Commercial Satellite

CONUS – Continental United States

CW – Continuous Wave

dB - Decibels

DEW – Directed-Energy Weapon

DoD – Department of Defense

DSCS – Defense Satellite Communications System

EA – Electronic Attack

ECM – Electronic Countermeasures

ECCM – Electronic Counter-Countermeasures

EHF – Extremely High Frequency

EMP – Electromagnetic Pulse

EP – Electronic Protection

ES – Electronic Support

EW – Electronic Warfare

FCS – Future Combat System

FLTSATCOM - Fleet Satellite Communications

Gbps – Gigabits per Second

GBS – Global Broadcast Service

GEO – Geosynchronous Earth Orbit

GHz - Gigahertz

GPS – Global Positioning System

HEMP – High-altitude Electromagnetic Pulse

IO – Information Operations

IRBM – Intermediate Range Ballistic Missile

iRMA – Information Revolution in Military Affairs

ISR – Intelligence Sensor Reconnaissance

IT – Information Technology

ITU – International Telecommunications Union

IW – Information Warfare

J/S – Jamming to Signal Ration

JTIDS – Joint Tactical Information Distribution System

kbps – Kilobits per Second

kHz - Kilohertz

LDR – Low Data Rate

LEASAT – Leased Satellite

LEO – Low Earth Orbit

LF – Low Frequency

LOS – Line of Sight

Mbps – Megabits per Second

MEO – Medium Earth Orbit

MDR – Medium Data Rate

MHz - Megahertz

MILSATCOM – Military Satellite Communications

MILSTAR – Military Strategic and Tactical Relay

MRLS – Multiple Rocket Launchers

NCA – National Command Authority

OIF – Operation Iraqi Freedom

OPSEC – Operations Security

PLA – People's Liberation Army

PLAN – People's Liberation Army Navy

PRC – People's Republic of China

PYSOPS – Psychological Operations

RF – Radio Frequency

SATCOM – Satellite Communications

SHF – Super High Frequency

SIGINT – Signals Intelligence

SIOP – Single Integrated Operation Plan

SNR – Signal to Noise Ratio

SRBM – Short Range Ballistic Missile

SS – Spread Spectrum

TT&C – Tracking, Telemetry, and Control

UAV – Unmanned Aerial Vehicle

UFO – Ultra High Frequency Follow-On

UHF – Ultra High Frequency

USN – United States Navy

Chapter 1

Introduction

The purpose of this thesis is to evaluate the vulnerabilities that exist in the US military's satellite communications and the Information Warfare threat the People's Republic of China may pose to them. By recognizing both the vulnerabilities and accounting for the People's Republic of China's (PRC's) ability to threaten satellite communications (SATCOM) systems, this thesis finds that the PRC does pose a credible, though moderate Information Warfare threat to the US military's SATCOM in the form of noise jamming and possibly anti-satellite attack (ASAT).

The genesis of this thesis came from observations of what the US military and scholars are saying about the future and about Information Warfare (IW). The current military rhetoric of what its future warfare model will be stresses information, communication, mobility, and economy of force. Such a model requires the ability to disseminate large amounts of information to widely dispersed units. This requirement cannot be satisfied by fiber optic cable or other landlines because it would constrain how quickly the force could move. Therefore, satellite communications is considered the prevalent means through which this information will flow. This, however, is problematic for two reasons. Firstly, because, as much of what is being said about Information Warfare states, information dependent entities can be asymmetrically victimized by the disruption of information and that the means to do so are becoming increasingly accessible. Secondly, because the partially secure military-dedicated satellites that exist can only provide for a minimal amount of the enormous bandwidth demands, the military must use commercially leased satellite communications which are far less secure. Vulnerabilities in

SATCOM to IW then take on great importance, being the critical and seeming weak link in the communications chain.

Another facet of what some scholars believe to be the future is a near-term competitor in the form of the PRC. The PRC's fantastic growth over the course of the past decade, its estimated future economic and military potential, and its position near US allies and interests have all played their part in this formulation. While the PRC may be able to become a regional hegemon in the next few decades, it is currently incapable of projecting much power beyond its borders. This, however, is not stopping the PRC from working towards their goal of becoming a world power. Influenced by the US's highly successful military actions over the past decade, its information infused rhetoric, some of the asymmetric concepts of IW, and the delicate Taiwan situation, the PRC have come to believe that the US is its most obvious competitor and that IW may be a key to fighting it. The PRC may not have the same high-tech weapon systems and doctrines as the US, but it does have some technical know-how and the desire to exploit the US's information dependence. This points to China as being maybe not a near-term competitor, but a possible current IW threat.

If these hints about a potential vulnerability and Chinese IW threat proved true, it would appear that the military may not have fully realized all of the implications of IW or the true threats that are set against it. This would not bode well for a future where IW offers an advantage to lesser powers and individuals possibly too good to pass up. These conclusions are not unjustified and are worth examining.

The US military is currently in a period of Transformation. It hopes to reshape itself into this lighter, more mobile, more connected, and more capable force in order to achieve dominance in a wide range of scenarios. The great success that it achieved using precision-guided munitions, stealth technology, and an overall superior technological quality of force over the past ten years have reaffirmed the belief that technology is the key force multiplier to achieve this dominance. Increasingly, doctrines seem to be focusing more on the US's vast techno-superiority, or rather the use of that technology, as quickly as civilians have begun to integrate more technology into their lives. The single most influential technology has been Information Technology (IT).

The military has also taken note of this. It is widely believed that an information Revolution of Military Affairs (iRMA), placing information as center of gravity, has occurred.[1] The military's Joint Vision 2010 and 2020 states that *the* fundamental aspects of future warfare will be Information Dominance, knowing more than one's enemy, and Decision Dominance, using information better and faster than one's enemy. The way in which the military is trying to achieve these dominances is to have a far-reaching, robust, ubiquitous Intelligence, Sensor, Reconnaissance (ISR) and telecommunications network, as well as a network-centered fighting doctrine.[2] Millions of dollars have been and are being spent on creating the technologies, systems, and networks necessary for this endeavor.

The iRMA, however, has not only drawn the military into the Information Age with promises of an all-seeing, all-knowing, and deadly force. Because the iRMA places information as a key center from which strength can be drawn, the iRMA has also made information a critical target. From this dual nature of information, the revolution has also brought about Information Warfare, a warfare that seeks to protect and destroy information,.

This dual-edged nature of the iRMA should evoke some circumspection about the military's IT systems' vulnerabilities to Information Warfare attacks. The US military has already grasped many of the ideas behind Information Warfare as evidenced by the electronic, cyber, and physical strikes on Iraqi C^3 (command, control, communications) links in the First Gulf War. Though the US is considered the world leader in incorporating iRMA technologies and doctrines, it is questionable whether the military fully

[1] The term information Revolution in Military Affairs (iRMA) is one of the author's convenience and not official terminology.

[2] Network Centric Warfare, http://www.dod.mil/nii/NCW/.

understands the complex and costly implications of IW and net-centricity. Treatment of the telecommunications systems needed to disseminate information, or the lack thereof, is of significant concern. Of the many systems there are, SATCOM are especially significant. As the US military becomes more thoroughly transformed, soldiers and commanders will begin to depend more on highly mobile, remotely accessible, low to high data rate communications to maintain connectivity and awareness. This type of communication can only be facilitated by satellite systems. Though the military's current use of high data rate systems is not as pervasive as it will become or is as widely used as lower data rate systems, reports already exist addressing the bandwidth shortfall between the current military satellite systems' supply and the enormous demand. Some reports indicate that that military satellite communications (MILSATCOM), which are military-dedicated systems, can only provide approximately 14% of the military's bandwidth needs.[3] The difference must be made by using commercially leased satellite transponders which are not as secure. This shortfall of supply, the growing need for more, and the dependency on information has made satellite systems, especially those which are unsecure, an increasingly choice target to anyone who wishes to disrupt them.

The People's Republic of China (PRC) too has become aware of the iRMA and the vulnerabilities associated with it. The PRC has been forecast as the United States' most likely near-term competitor, but questions remain as to when and in what form it will appear as a threat. Though the PRC is rapidly growing more politically, economically, and militarily influential on a global scale, it has not yet transformed into the powerful state its neighbors and the US fear it will. Several issues impede Chinese progress and will continue to do so unless measures are taken to reform rigid sociopolitical policies and implement better education and industrial practices. In light of its shortcomings, the PRC refuses to remain toothless during its time of transition.

[3] Tim Bonds, Michael Mattock, Thomas Hamilton, et al. *Employing Commercial Satellite Communications: Wideband Investment Options for DoD* (Santa Monica, California: The RAND Corporation, 2000), pg 8.

Over the past three decades, the PRC has attempted to "catch up" to the modern world in terms of its warfighting capabilities with large steps. Through changes in its forces and command structures to changes in what it perceives as its threats as well as the strategies needed to meet them, the PRC has been almost constantly rearranging itself to take on the challenges of the modern battlefield. Through close observation of the First Gulf War, the Balkan conflicts, and US military discussions, the PRC has focused itself on preparing for the new, informationalized battlescape and fighting Information Warfare in its most recent iteration.

Belief in the iRMA and the advent of Information Warfare places the PRC in an interesting situation. The information infused military technology, equipment, and doctrines needed to take full advantage of the iRMA are currently more advanced than the PRC can produce and implement. The People's Liberation Army (PLA) is equipped with Cold War era vehicles and weapons, and its defense and private technology industries lack the organization and strength to change this quickly. However, Information Warfare presents many means of viably corrupting, disrupting, or destroying information of one's enemies. Military information technologies and doctrines can be complex and costly, but parallel civilian forms of IT can be cheap, user-friendly, and "soft" forms of IW can be easily accessible.[4] Thus, by equipping oneself with the IT and skill sets that are becoming increasingly more available, one could asymmetrically affect the information usage of an adversary without the need for developing the joint- and precision-based doctrines often associated with the iRMA. This fact has not gone unrecognized by the PLA.

Much of the work on IW discusses theory and when more practical tends to focus on Computer Network Attack (CNA). This is not wholly surprising as IW is still a relatively new concept and network/cyber war falls very stereotypically into the notion of

[4] The PRC often views IW in "soft" and "hard" terms. Soft IW focuses on attacking information and its dissemination while hard IW focuses on attacking the physical systems through which information travels.

warfare concerning information and IT. However, it is surprising that so little is being said about the vulnerabilities that may be present in SATCOM systems, especially when they are so vital to maintaining the flow of information.[5] A report of the Space Commission, which was specifically created to assess the US's space security, found that vulnerabilities in SATCOM have been overlooked and understudied. It also admonished the Intelligence Community to better evaluate the technical abilities of other states to threaten SATCOM considering the increasingly available high technology and not to disregard programs or technologies that may appear to have improbable success.[6] Being that competitors are embracing IW and understand the importance of communications, the dearth of analysis and assessment on the military's SATCOM is frightening.

China is of specific importance in this regard. The PLA has produced a number of articles and papers discussing not only the use of IW asymmetric attacks against a more technologically advanced adversary, but also naming the US as its primary opponent. China also has demonstrated some ability to engage in IW through various cyber-attacks and has recognized the importance of communications as evidenced by publications and its own focus on developing a C^3I (C^3, intelligence) network.[7] China is also growing rapidly, developing technologically, and sits across from the US in the tenuous Taiwan situation. Furthermore, scholars and analysts in the US also believe that China is the US's greatest near-term competitor. This all suggests that China should be carefully considered as a real IW threat.

[5] Bonds, Mattock, Hamilton, et al. *Employing Commercial Satellite Communications.* Like this report, many articles discuss the US military's dependency on SATCOM and SATCOM systems' vulnerability. However, they do not seem to make the logical step that a dependency on a vulnerable system is problematic, nor do they try to evaluate this problem.

[6] Commission to Assess US National Security Space Management and Organization, *Report of the Commission to Assess US National Security Space Management and Organization* (Washington, D.C.: Jan 11, 2001), pg 18.

[7] David Shambaugh, *Modernizing China's Military* (University of California Press, 2002) pg 72-73, 89. The First Gulf War revealed to the Chinese the importance of C^2, SATCOM, and communications in general to modern warfare.

To evaluate the US vulnerabilities and Chinese threats, the remainder of the thesis is segmented into three main chapters. The second chapter evaluates the vulnerabilities that exist in the military's use of SATCOM. It does so by briefly explaining aspects of satellite communications and IW that would be applicable, and then cataloguing the SATCOM systems used and their associated vulnerabilities.

The third chapter assesses the PRC's ability to threaten SATCOM by delving into what the PRC believes about IW, how developed their knowledge-base, doctrines, and industry are to prosecute IW against SATCOM. After this is done, the PRC's potential threat is scored against the aspects of IW that would be of use against SATCOM.

To make sense of two seemingly disjoint analyses, the fourth chapter offers a qualitative example of the effect of a PRC attack on the military's SATCOM by analyzing what may happen in a Taiwan crisis. Because it is impossible to know the exact outcome of such a crisis, the analysis will judge the threat level China poses in both a non-escalatory and escalatory US-PRC engagement.

Without the complete knowledge of what the PRC truly has planned and is capable of or a deep understanding of how the US military uses SATCOM, the implications and conclusions of this thesis are of a tentative nature. However, this does not imply that they are any less substantial. Having assessed and compared the US military's SATCOM vulnerabilities, and China's IW capabilities this thesis concludes that China does indeed pose a moderate IW threat to SATCOM. This finding not only expresses a need to reevaluate the use, structure, and safety of SATCOM systems for today's soldiers, but also suggests that if left unaddressed these vulnerabilities may jeopardize the very function of our future forces.

Chapter 2

Measuring Vulnerabilities

Vulnerability must first be measured before threat can be evaluated. As we continue to step further into the Information Era, the wide spectrum of Information Warfare will undoubtedly create more cause for concern for every aspect of our society. Our security forces have already begun to feel its effects and will continue to do so. As it stands, the military's use of SATCOM is vulnerable. Though SATCOM has inherent qualities protecting it against many forms of Electronic Attack, it is still susceptible to simple variants of uplink noise jamming, such as continuous wave jamming and power stealing. Military-dedicated systems offer some security, but the lack of bandwidth they provide forces the military to use much less secure commercial systems. This problem will only be exacerbated by the military's rapidly increasing bandwidth demand and its predicted inability to provide a secure supply.

In order to measure vulnerability one must have some understanding of the nature of satellite communications, how they are used, and from where vulnerabilities may arise. To aid in this understanding, this chapter contains five sections. The first briefly overviews some key ideas and concepts in satellite communications; the second highlights the current thought and use of satellite communications, as well as implications for its future; the third defines Information Warfare and vulnerabilities that satellite communications may face; the fourth details current systems, uses, and vulnerabilities; the fifth summarizes the chapter's findings.

Satellite Communications Primer

Because the topic being discussed is technical, some terms and concepts should first be defined and explained. The explanations here are not very rigorous as the intent of this section is to only give the reader a general understanding. For further depth, consult the references.

Radio Communications

Electromagnetic waves propagate throughout the universe and in different forms. Some common forms are visible light, infrared light, and microwaves, but these are just a few. Each form has a set place on the electromagnetic spectrum, consists of a specific number of electromagnetic frequencies, and contains its own spectrum. Visible light is a good example of this. Humans cannot see electromagnetic frequencies below and above the visible light spectrum, but we can identify different frequencies within the visible light spectrum. We recognize these differences as color.

Radio waves are also a type of electromagnetic propagation and, like light, exist within a specific set of frequencies and have a spectrum of its own. The radio spectrum is split into several different frequency ranges called bands. Each band contains a set number of frequencies that make up that band's bandwidth. The bandwidth of each band increases as the radio spectrum gets closer to the visible light spectrum, which is higher in frequency. Several of these radio frequency (RF) bands are used for telecommunications.

The military uses a number of RF bands, from Low Frequency (LF) to Extremely High Frequency (EHF). However, because the frequencies differ in nature, there are three reasons why they cannot all be used for the same purposes.

Table 1 – Radio Frequency Bands and Primary Propagation Types[8]

RF Band	Frequencies	Propagation Types	Uses
Very Low Frequency (VLF)	3-30 kHz	Ground Wave	Radio Navigation, Long Distance Communications
Low Frequency	30-300 kHz	Ground Wave	Radio Navigation,

[8] Adapted from National Telecommunications and Information Administration, http://www.ntia.doc.gov/osmhome/allochrt.pdf ; accessed July 11, 2005.

(LF)			Medium Distance Communications
Medium Frequency (MF)	300-3000 kHz	Ground Wave, Sky Wave	Radio Navigation, AM Broadcasting, Medium Distance Communications
High Frequency (HF)	3-30 MHz	Ground Wave, Sky Wave	Long Distance Communications, Short Wave Broadcasting
Very High Frequency (VHF)	30-300 MHz	Scatter, Line of Sight (LOS)	Long Distance Communications
Ultra High Frequency (UHF)	300-3000 MHz	Scatter, LOS	Short Distance Communications
Super High Frequency (SHF)	3-30 GHz	LOS	Short Distance Communications
Extremely High Frequency (EHF)	30-300 GHz	LOS	Short Distance Communications

Table 2 – Microwave (100 MHz – 300 GHz) Band Designations[9]

Name	**Frequency Band**
L	400 MHz – 1.5 GHz
S	1.5 – 5 GHz
C	4 – 6 GHz
X	5 – 10 GHz
K	10 – 36 GHz
Ku	15 – 17 GHz
Ka	33 – 36 GHz

Firstly, in order to efficiently receive radio signals an antenna's length should be sized in relation to the signal's wavelength. Two important characteristics of electromagnetic waves, frequency and wavelength, are inversely proportional to each

[9] Adapted from National Telecommunications and Information Administration, http://www.ntia.doc.gov/osmhome/allochrt.pdf and John Neuhaus, http://www.jneuhaus.com/fccindex/letter.html (August 27, 1999); accessed July 11, 2005.

other by the speed of light.[10] Therefore, the lower a radio frequency is, the longer its wavelength. For example, the frequency 104.1 MHz, belonging to the frequency band used for broadcast radio, has a wavelength of 2.88 meters. An antenna smaller than the wavelength of its intended signal can pick up the radio signal, but it depreciates the signal's strength. Sizing the antenna according to the harmonic modes of the signal's wavelength is one way of making smaller antennas without tremendously affecting the antenna's reception strength. Antennas which are larger than necessary are often better because they can capture more RF energy, making the signal stronger. However, large antennas can be unwieldy. Thus, the size of a frequency's wavelength, and therefore its matching antenna size, is one factor that dictates how useful it is to a user.

Secondly, the size of a frequency's wavelength affects how it propagates. The molecular qualities of the media through which radio waves travel can alter their propagation. Much like light interacting with water, ionized air molecules, the Earth, man-made structures, and other forms of matter can reflect, diffract, scatter, and absorb radio waves. This fact is observable in Table 1. Notice how the propagation type changes with the band. For example, some bands, such as HF and VHF, can be carried or reflected by ionized portions of the atmosphere allowing transmissions to travel long distances. Others, such as SHF and EHF, can penetrate those same portions of the atmosphere and so cannot take advantage of those effects. Therefore, wavelength can then determine what frequency band is used in a given situation.

Thirdly, the amount of information that can be transmitted by a radio signal is directly related to the frequency it is carried on, be it voice, images, data, etc. Digital information is transmitted in binary elements called bits that electronic devices can manipulate. Each bit represents an on or an off state, much like how Morse Code has dashes and dots. Because frequency is measured in cycles per second or Hertz (Hz), 1 Hz can maximally transfer 2 bits per second, e.g. a light switch going from off to on to off.

[10] $f = c/w$ Where f is frequency, c is the speed of light, and w is wavelength.

Bandwidth is often also used to describe the size of information throughput because the bit transfer rate over radio waves is proportional to the number of frequencies used.

Radio communication is conceptually very simply, but can be complex in its implementation. All the equipment that is necessary to communicate over radio waves is a transmitter, a receiver, and two antennas. In fact, the transmitters and receivers are quite similar with the only difference being that one has electronic components to create radio waves while the other uses similar components to interpret them. The creation a radio wave can be quite simple. Because of the nature of electricity and magnetism, changes in an electrical field will induce the creation of a magnetic field, which will induce another electric field and so on. This is how electromagnetic waves propagate. Therefore, anytime an electric field is created or oscillated, e.g. turning on an appliance or dimming a light, radio waves can be produced. What determines if the electromagnetic waves that are created are radio waves is the length of conductive material that is being electrically charged. If radio waves are created then that length of material, which can be an ordinary wire, is known as an antenna.

The antennas used in radio communication can be, but do not have to be, identical in shape and size. However, they do have to be placed within each other's eradiation patterns in order to transmit and receive signals. Because the power of a transmission decreases with distance, a radio's eradiation pattern, created by the direction and strength of a radio's transmissions, has limit in a practical sense.[11] The design and shape of an antenna influences the pattern. Most antennas one sees are omni-directional antennas, meaning their radiation is emitted in all directions. Directional antennas focus their radiation into a beam with some azimuth, much like a spot light. Omni-directional antennas are very functional because a receiver can be placed in almost any position around the transmitter and receive a signal and visa-versa. Though directional antennas

[11] While radiation may go on forever, the signal will eventually be engulfed by noise.

must be pointed at each other in order to communicate, they are more efficient than omni-directional antennas and can communicate at longer distances.

While radio waves can be produced by turning on a light, the amount of information that can be transmitted by doing so is very limited. To make better use of the medium, transmitters are constructed from electronic components that allow more control of the radio wave pattern, which is the way in which information is carried. An example of this is FM radio. The music or voice that is carried over FM waves is produced by modulating, or changing, the frequency of the wave, much like using dashes and dots in Morse Code. This and other forms of modulation can be accomplished by engineering circuit boards made from rudimentary electronic components.

Transmitting information over radio waves is affected by many properties such as distance between the transmitter and receiver, power of the transmission, how well the antennas used propagate the signal properties, internal and external electrical and conditions, thermal conditions, the presence of other radio waves, signal coverage, etc. Because of these factors determine how well radio communication works may be difficult. However, perhaps one of the most valuable metrics for evaluating radio communication is the signal-to-noise ratio (SNR) which takes into account many, if not all, of the important variables. The SNR measures the effective signal strength to the surrounding noise strength and is measured in decibels (dB), making a more positive value favor the legitimate signal. [12]

The SNR is very important because it affects the amount of information that can be communicated. For instance, in digital communication, a SNR of 0dB can generate a bit error rate (BER) high enough to preclude the reception of intelligible information. [13]

[12] Richard Poisel, *Introduction to Communication Electronic Warfare Systems* (Boston, MA : Artech House, 2002), pg 55-60. While signal strength is determined by antenna efficiencies, transmission power, distances, and so on, noise can be produced from a number of naturally occurring sources including thermal conditions, external and internal electrical conditions, and interference from other legitimate signals and reflections of the same signal.

[13] Ibid., pg 506. BER is the rate at which bits are corrupted and can be influenced by natural phenomena.

Another example is that 6dB is often viewed as the threshold SNR for differentiating between the desired signals and other spurious signals.[14]

In truth, while radio communication can be as simple as described, it can also be quite complex depending on the information being sent, the location sending to and from, the frequency band used, and a host of other factors.

Satellite Communications

There are two major advantages that satellite communications have over terrestrial wireless communications. First, for terrestrial wireless networks to be useful over large distances, transmission repeaters must be constructed to boost radio signals because radio transmissions lose power in relation to the distance over which they travel. This can be problematic for expeditionary forces who might be deployed far from friendly terrestrial repeaters, for places with rough terrain, and terrain where repeaters can be impractical e.g. oceans. Placing repeaters atop towers and mountains can extend the coverage area, but it is not a perfect solution. Because a satellite is a repeater in orbit hundreds of thousands of feet above the Earth's surface, it can cover wide expanses, some roughly a third of the Earth's surface. A satellite network, consisting of several satellites and ground stations, which can complete any gaps in the satellites' coverage by repeating message to other satellites, can be accessible to forces on a global scale, making sure they are always within communications contact.

Second, line of sight is best for making radio connections. However, this is usually not obtainable because of man-made and natural obstacles, as well as the curvature of the Earth. May forms of RF communication do not require line of sight (LOS) for maintaining links because they can take advantage of other effects, such as scatter, or can permeate some obstructions. Unfortunately, the higher data rate information flow which is becoming more important for military communications cannot be carried over these

[14] Ibid., 55-60.

bands, but must use microwave bands. Unlike lower frequency bands, microwave bands require LOS connections because obstruction affects them much more and they cannot take advantage of the same propagation effects lower bands can. Placing repeaters as high as possible is also the usual remedy for obtaining LOS communications, but this too is not perfect. Again, because satellites are in orbit far above the Earth's surface, they can offer reliable LOS communication to anyone who can "see" them.

Satellite communications have been used by the military for several decades. The majority of communications satellites orbit the Earth geosynchronously, meaning that their orbital period is or about 24 hours, though some are in low (LEO) and medium (MEO) Earth orbits.[15] In order to orbit geosynchronously, the satellites have to maintain an altitude of about 22,000 km above the equator. At this altitude, equatorial satellites can see roughly one third of the Earth's surface, save the Polar Regions. The directional antennas that satellites use focus the radio waves that eradiate into a beam, much like a spot light. This beam is called the main lobe, because other beams extending out of the sides of the main lobe can also be produced naturally. These are called side lobes and are not usually considered beneficial as they can increase the vulnerability of the satellite. This will be discussed further below. Communications satellites can focus their coverage into narrow spot beams, wider area beams, and finally Earth beams capable of servicing one-third of the Earth. Thus, only three satellites and either three ground relays or cross-links between each other, are needed to enable users to "hop" transmissions over expanses that ground relays could not, such as oceans, to almost any point in the world..

Maintaining a position in geosynchronous Earth orbit (GEO) gives satellites a stationary location relative to the surface over which they orbit. Because LEO and MEO satellites must sustain a higher velocity to counterbalance the Earth's gravity, their orbits are much faster than a GEO satellite. This means that contact with a GEO satellite can be

[15] Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 14.

maintained without having to track it as much as with lower orbiting satellites, and ground repeaters.[16]

In these ways, satellites act as repeater platforms extending users transmissions beyond the line of sight and around the world. Their wide coverage and ability to utilize higher bandwidth microwaves can create a global network well suited for mobile, remote, and information hungry users.

The military needs to be able to communicate to a variety of forces, in a number of location types, and with differing amounts of information. To optimize information flow, the military changes the way in which it communicates across the spectrum of its needs. The VHF and UHF bands are used as the main means of wireless telecommunications for the military because the equipment necessary is relatively mobile, cheap, and often used in an omni-directional fashion.[17] However, VHF/UHF communications cannot transfer the increasingly large amounts of information, or offer the great deal of security that the military needs.

While the VHF and UHF bands can theoretically transfer 540 megabits per sec (Mbps) and 5.4 gigabits per second (Gbps) respectively, there are two reasons why more bandwidth is needed. RF bands are channelized, meaning that they are split up into smaller sub-bands, so that multiple users can take advantage of each RF band. If two users were trying to send signals using the same frequency, the signals would interfere, possibly

[16] Lower Earth orbit satellites can utilize omni-directional antennas better than GEO satellites because of the distance and so tracking the satellite to maintain connection is not always necessary. Some lower earth orbit satellites circle in high elliptical orbits. This also does not require the ground receivers to track them because they orbit in such a way that they cover one portion of the Earth longer than the rest, and as one satellite falls out of view another comes into view. Therefore the connection is maintained. This method, however, does not allow very good global coverage.

[17] Omni-directional systems, which eradiate and absorb RF energy from all directions, are useful for transmitting and receiving signals from various positions without having to steer the antennas. This also makes it easier for jammers to attack such systems because they are not restricted by positioning. Omni-directional systems also tend to have lower signal strengths because the signals are not focused. This too facilitates jammers as it does not require them to emit at very high powers.

causing the signals to nullify each other. The second reason is that, even in a channelized environment, radio signals can interact with other frequencies and the media they travel in such a way that error-correction information must be sent along with an RF signal to ensure that it is accurately received. In military radio communications, still more error-correction is added to defend against enemy efforts to receive and/or disrupt communications. This will be discussed in more length in the third section. After channelization, error-correction, and anti-jamming techniques are accounted for, typical information bandwidth for UHF channel is below 64 kbps.

Information transferred lower than 64 kbps is considered narrowband communication, while information transferred at a rate above 64 kbps is considered wideband communication. Voice, teletype, and simple forms of digital data are narrow enough not to require wideband links and make up the bulk of satellite communications. However, more sophisticated information used for collaborative planning, video teleconferencing, video telemedicine, imagery distribution, video tele-training, as well as remote maintenance/ technical assistance and distribution of situational awareness cannot be passed across narrowband links.[18] Neither VHF nor UHF offers the bandwidth necessary for these wideband communications. Higher bandwidth can be obtained by using the higher, SHF and EHF, frequency bands. As much as 1.544 Mbps can be transferred over some secure EHF links. Unlike VHF and UHF, SHF and EHF bands require the transmitting and receiving antenna to be within LOS. Ground relays do exist, but because of the advantages explained above, satellites are the main relays for these bands.

SHF and EHF also require much smaller antennas because of their wavelength. For example, the wavelength of 30 GHz is only 1cm. Because of this, SHF and EHF

[18] Department of the Navy, *NTP2 Section 1 (D) Naval Telecommunications Procedures. Navy Super High Frequency Satellite Communications* (Dahlgren, VA: Naval Space Command, 1997), pg 9. Found at Federation of America Scientists, http://www.fas.org/spp/military/docops/navy/ntp2/front.htm accessed August 2, 2005.

transmissions can be made highly directional with much smaller antennas, allowing such transmissions to have Low Probability of Interception (LPI) and Low Probability of Detection (LPD). In other words, it makes it harder for adversaries to listen in on transmissions or discover where they are being sent to and from. Microwave transmissions are not without drawbacks, however. Bandwidth can also be affected by the power of the transmission and the receive/transmit antennas used just as any other RF transmission.[19] Microwave frequencies can also be attenuated by foliage and precipitation and reflected by man-made structures more easily than lower frequency bands.

Digital Need

Military satellite communications (MILSATCOM) has been in use since the 1960'.[20] MILSATCOM was mainly used for narrowband, voice or teletype communications. These systems included the Navy's Fleet Satellite Communications (FLTSATCOM) system, the Air Force's Air Force Satellite Communications (AFSATCOM) system, the Department of Defense's Defense Satellite Communications System (DSCS), and the Military Strategic and Tactical Relay (MILSTAR) system. However, the use of SATCOM has increased considerably since the iRMA began in the early 1990's. The iRMA had two impacts on the military's use of SATCOM systems. First, the iRMA's focus on information and technology allowed for doctrines and practices that required larger amounts of information. This increased information demand stressed the MILSATCOM systems by requiring them to support types or amounts of information for which they were not designed. Second, the iRMA's mirroring of the information boom in the civilian world led the military to believe that it had the information capacity civilians enjoyed.[21] However, the systems and requirements the military had for telecommunications did not support this belief. By

[19] Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications,* pg 14

[20] The difference between what the military uses for SATCOM and MILSATCOM is that MILSATCOM does not account for the commercially leased satellite transponders the military uses.

[21] The CBO, *The Army's Bandwidth Bottleneck* (August 2003), pg ix.

simply not being able to maintain the new communications links, commercial satellites, first augmenting the MILSATCOM systems in the early 1990's, began to take on a larger role as the military's SATCOM provider.[22]

Over the past decade SATCOM needs rose roughly an order of magnitude from hundreds of Mbps to single Gbps and it is projected to increase by another order of magnitude in ten years.[23] The bandwidth supply of MILSATCOM has not been able to keep up with this trend nor is it believed that it will be able to. Since the early 1990's, commercial satellites (COMERSAT) has been providing an increasing percentage of the military's SATCOM supply. In the First Gulf War some 100 Mbps were supplied through COMERSAT while in Operation Iraqi Freedom 2.4 Gbps were from COMERSAT, accounting for 84% of satellite communications.[24] The future looks no brighter for MILSATCOM as it is predicted it will only be able to supply some 4 Gbps while the need could skyrocket to more than 14 Gbps in the next decade.[25]

Each service has been affected differently by this shortfall as they each use SATCOM in different ways and to different measures. In the past SATCOM was used for narrowband, long-haul communications from units in the field to command units across distances where lines could not be established including communication to commands in the continental US (CONUS). It was and is also used as a global platform to disseminate Emergency Action Messages to strategic forces. Because of the iRMA, however,

[22] Patrick Chisholm, "Buying Time: Disconnects in Satcom Procurement," (Military Information Technology, Nov. 29, 2003) http://www.military-information-technology.com/article.cfm?DocID=285. Commercial satellites were first used to supplement MILSATCOM by taking on the maintenance of non-weapons critical links.

[23] Ibid.; David Ehrhard, Major, USAF, "Standing in the Strategic Bandwidth Gap: A View of Military Communications in 2010," (Air and Space Power Chronicles, March 9, 2004) http://www.airpower.maxwell.af.mil/airchronicles/cc/ehrhard.html; Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 10.

[24] Chisholm, "Buying Time"; The CBO, *The Army's Bandwidth Bottleneck* (August 2003), pg 16. Though this number does not reveal COMERSAT usage by branch, it can be used to indicate the overall reliance on COMERSAT.

[25] Chisholm, "Buying Time"; Erhhard, "Standing in the Strategic Bandwidth Gap,"; Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 10.

communications now take on a much wider variety of forms and require wider bandwidths than they once did. Present communications can be anywhere between sharing situational awareness data between commands in mobile units to video-telemedicine between medical units and counterparts in CONUS. Stationary bases in each service have the benefit of being able to be linked with fiber optic cable or other landlines facilitating the increasingly large volumes of information to flow. Mobile commands do not share this luxury and depend on the higher data rates of SATCOM when a line connection cannot be made. This dependence is only growing as mobility, jointness, and net-centricity are new ideal qualities of the military.

The US Air Force uses SATCOM to provide C^2 communications, Emergency Action Message dissemination, force direction and reporting, communications between the Joint Chiefs of Staff and Commander in Chief, as well as some operational planning, crisis operations, exercise support, and technical training.[26] It has also identified that its SATCOM usage has become critical to its functioning and its needs are greater than its supply.[27] The Air Force uses all of the MILSATCOM systems, as well as some commercial systems.[28]

Of the services the US Navy is probably the most dependent on SATCOM because the terrain over which its fights does not permit landlines or always facilitate LOS communications. It also uses all of the MILSATCOM systems and is dependent on commercial satellites systems to fill their bandwidth gaps. The Navy uses SATCOM for everything from low data rate text and voice for tactical communications to higher data

[26] Federation of American Scientist, http://www.fas.org/spp/military/docops/army/fm24-11/Ch7.htm#ch7.

[27] Spacedaily, "Northrop Grumman Delivers 16th Joint STARS Aircraft To Air Force," (March 8, 2004) http://www.spacedaily.com/news/milspace-comms-04l.html; Lt. Dennis French Jr., "AF SATCOM: Communicators leverage future technology," http://public.afca.af.mil/Intercom/2004/APR/040402.html.

[28] Dr. James G. Roche, "Integrating Space Into Joint Warfighting: Continuing the March," (Find Articles, July 14, 2003) http://www.findarticles.com/p/articles/mi_m0PDU/is_2003_July_14/ai_109569821/pg_2.

rate logistics and operational planning, as well as video conferencing and long-haul communications to the continental US.[29]

Though the actual bandwidth needs and shortfalls in each branch may not be publicly available, a study performed by the Congressional Budget Office evaluating the US Army's bandwidth shortfall can highlight the disparity between what information throughputs the military expects and what it has available. During Operation Iraqi Freedom, units of the Army's 5th Corps, the Marine's 1st Marine Expeditionary Force, and a British armor division were equipped with components of the digital communications architecture used by the fully digitized 4th Infantry Division. This system was called Blue Force Tracker.[30] While the system was considered successful, it was often overloaded with information.

While the forces were only about 25-33% digitized, the Congressional Budget Office estimated that even fully digitized units would have an average supply bandwidth shortfall of about 82.5-86.7% of demand at peak usage considering all command levels.[31] All command levels had line-of-sight (LOS) communications systems, but only commands at the brigade level and above had access to MILSATCOM for beyond-line-of-sight (BLOS) links. This became problematic as the fast paced nature of the conflict revealed that LOS communications were not adequate to maintain communications links between certain units. To bridge the gap, units began to use available commercial satellite channels in the form of email and chat-rooms to pass information. The figures above and the action taken by the units on the ground highlight two major issues. The first is that the current LOS communications offered by ground relay is not sufficient for fast-paced combat, or situations where land-based LOS communications break down. The second is that the

[29] Globalsecurity, "Executive Summary of Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html.
[30] The CBO, *The Army's Bandwidth Bottleneck*, pg 15.
[31] Ibid., pg 16.

Army could not offer MILSATCOM to its forces because it did not anticipate its bandwidth needs.

As informationalization under Transformation continues, the need for greater amounts of bandwidth will become increasingly unmanageable, especially as wideband communications which depends on the high bandwidth, becomes more predominant. The more mobile, survivable, and lethal Objective Force is slated to enter service in 2008 with the Future Combat System.[32] The Future Combat System (FCS) is labeled as a "system of systems" working together to increase the effectiveness of the soldier. Soldiers will be able to receive video confirmation of local enemies through links to squad-commanded unmanned aerial vehicles (UAVs). Commanders will be able to use a better economy of force by having a well-developed "picture" of where his/her and enemy units are. Autonomous networked artillery and multiple rocket launchers (MRLS) systems will be able to accurately bring firepower to bear beyond the line of sight. Though this is only a partial listing of what the FCS will offer, it is obvious that the crux of the FCS is information technology, and information itself, the heart of the military's new way of war.

The bandwidth needs of an FCS equipped unit will be enormous. Given the example of OIF, and that the Objective Force is attempting to create smaller, more mobile, and more informed units, it is hard to believe that SATCOM will not be the means of choice to sustain communications links. MILSATCOM, however, is not predicted to have the bandwidth capacity necessary, even with the new systems being launched.[33] The CBO also predicts there will not be a large surplus of bandwidth in any of the communications systems when digitization will be better integrated in 2010.[34] This suggests that

[32] The Objective Force is the form into which the military hopes to transform. It stresses mobility, rapid deployment, and lethality, to name a few qualities. The Stryker Brigade Combat Teams, a stepping stone to the Objective Force, are an example of this evolution as they trade heavily armored divisions for lighter yet more mobile brigades.

[33] Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 10.

[34] The CBO, *The Army's Bandwidth Bottleneck*, pg 23.

commercial satellites will continue to play a large, if not increasing, role in enabling our forces to stay connected.

Information Warfare

Information Operations (IO) can best be described as offensive or defensive action taken to control information. Information Warfare (IW) is best described as IO conducted during times of crisis or military conflict.[35] IW is a warfare fought on the battlefields, on the seas, in the air, in outer-space and cyberspace, in the media and in the mind. Information Warfare can be as simple as hiding a piece of artillery with camouflage and as complicated as creating a national intelligence network capable of surviving attacks on independent nodes. IO campaigns can also take place before, during, or independently of military conflict. For these reason, IO and IW cover a wide spectrum of attacks and defenses that can affect every aspect of a nation using and/or depending on information.

IW theory currently defines six aspects of Information Warfare often called the "Six Pillars of IW".[36] The six include: Computer Network Attack (CNA), Electronic Warfare (EW), Psychological Operations (PSYOPS), Deception, Physical Destruction, and Operations Security (OPSEC). Command and Control Warfare (C2W) is a subset of IW that includes all the Pillars save CNA.[37] C2W is directly related to military action aimed at decapitating an adversary's military. Because of this C2W is often the focus of IW with relation to military action. There are two forms of decapitation attacks both of which are designed to sever the decision-making components of a force from its decision-enacting

[35] D. Curtis Schleher, *Electronic Warfare in the Information Age* (Norwood, MA: ARTECH HOUSE, INC., 1999), pg 3-5; Leigh Armistead ed., *Information Operations: Warfare and the Hard Reality of Soft Power* (Washington, D.C.: Brassey's, c2004), pg 212. The discussion of IO in this book is quite theoretic and states that IO's main focus is "perception management"; DoD Dictionary of Military Terms. http://www.dtic.mil/doctrine/jel/doddict/data/i/. Of the many authors that discuss IW, most use the terminology sanctioned by the military.

[36] Toshi Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* (SSI, Nov. 2001) pg 4.

[37] C2W does use CNA though it is often thought of as enabling other aspects of C2W and has no value onto itself.

components: anti-head and anti-neck. Anti-head attacks are directed at striking commanders and leaders themselves, while anti-neck attacks are directed at severing the channels through which decisions flow from commands.[38] Anti-neck attacks are the most prevalent form of C2W simply because technology allows commands to remain far away from the frontlines.[39]

Each form of C2W affects the information infrastructure of a military in different, but synergistic ways.[40] OPSEC is the enactment of procedures and guidelines that control the spread of vital information in order to maintain a superiority of knowledge. EW is military action taken to control the electromagnetic spectrum. PSYOPS are actions that are focused on depleting an enemy's morale and causing confusion. Deception is deliberately giving or allowing the enemy to have false information which will allow advantages to accrue to the deceiver. Physical Destruction is attacks on the information infrastructure itself. OPSEC, PSYOPS, and Deception are all aimed at controlling information itself, while EW and Physical Destruction are aimed at affecting the medium and technology through which information travels.

SATCOM is made of three segments, attacking any of which using IW could affect its use: the ground segment, the satellite segment, and radio transmission segment. The ground segment is composed of track, telemetry, and control (TT&C) stations, which maintain the satellites' orbits, teleports, which receive satellite signals and relay them using land lines and visa versa, hopping stations, which retransmit messages from one satellite to another, and the user-end terminals. The satellite segment is the satellite, and the radio transmission segment is the message.

This thesis focuses on the EW aspect of C2W for five reasons. Firstly, EW, Physical Destruction, and possibly CNA seem the most threatening of the Six Pillars to the ground

[38] Martin C. Libicki, *What is Information Warfare?* (Washington, DC : Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, 1995), pg 10-13.
[39] Ibid. Operations in OIF are a good example of both forms of decapitation strikes.
[40] D. Curtis Schleher, *Electronic Warfare in the Information Age*, pg 5.

segments.[41] In order to physically destroy components of the ground segment, control stations, teleports, user-end terminals, etc. would have to be attacked. This could prove difficult as many components are either within US territories, CONUS, allied nations, and carried with armed forces. This may require the use of Special Forces, long range missiles, and a willingness to attack international states that are not directly involved with the conflict as well as facilities from which the attacker may benefit. Physical Destruction of ground segments may also not prove to have more than temporary effect. Tracking, Telemetry, and Control (TT&C) links to satellites can be reestablished at other facilities, the use of hopping stations may be reshuffled, and the user-end terminals can be replaced.

While it is theoretically possible to use PSYOPS, Deception, and undermine OPSEC using CNA at ground segments, military encryption is very sophisticated and it is unlikely that it would be broken other than by an enemy of equal technological capabilities which are few.[42] CNA could be used to infect terminals with viruses, mine satellite telemetry information, overload systems, and hypothetically, corrupt control information so as to degrade satellite performance. However, CNA users would have to penetrate network security, be knowledgeable of how such systems worked, and rely on their victims to implement little to no active defense measures. This would be unlikely.

Electronic Warfare covers a wide variety of attacks including the use of directed-energy weapons (DEW) and jamming. The technological requirements for EW are as various as its forms. Some like DEW or microwave bombs necessitate high technologies that are not yet fully developed, while others like jamming need only simple, purchasable electronic components and knowledge of telecommunications because jamming is

[41] CNA is considered here because it could affect some of the ground segment elements of SATCOM even though it seems to take on a C2W support role in the literature.

[42] Libicki, *What is Information Warfare?*, pg 30-31. Digital signal encryption is very difficult be brake. Even with state of the art computers it may take impractical computation times to crack; Globalsecurity, "Executive Summary of Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html. Spread Spectrum techniques such as Frequency Hopping can also be considered a method of encryption in that the only device which can "read" a frequency hopped message is one that already knows the pseudorandom scheme. Frequency hopped message too can be deciphered, but it requires a very sophisticated device to do so.

fundamentally the same as transmitting legitimate signals.[43] Though Signals Intelligence (SIGINT) may be necessary for jamming damage assessment, the technology needed to do so is more likely to be fielded than the nuclear weapons needed for high altitude electromagnetic pulse (HEMP) attacks or DEW with enough power and mobility to threaten a large range of the SATCOM ground segment. Because jamming technologies are more easily acquired they appear to be the most threatening form of EW. Jamming too has its drawbacks in that the only way to jam a directional SATCOM ground segment, which most of SATCOM is, is through using conspicuous means of downlink jamming. This is described in more detail in a later section.

Second, the satellite segment is most vulnerable to Physical Destruction and EW. Implementing physically destructive anti-satellite (ASAT) attacks against a satellite requires satellite tracking and missile launch capabilities.[44] There are many methods of employing ASAT, some as conceptually simple as intercepting a satellite with a ground launched missile to the more complex method of attaching parasitic micro-satellites to a target to destroy the satellite at a later time.[45] In either case, while it is possible to track a satellite rather easily using telescopes and laser range finding, launching a missile against a satellite would be difficult to any but the few nations that have launch capabilities.[46]

Electronic Warfare against satellites is similar to that of EW against the ground segment of SATCOM. The main differences are that uplink jamming, jamming the satellite, must be used because downlink jamming, jamming a ground segment, does not work against satellites and that satellite tracking technologies are also needed to properly target satellites. Uplink jamming can be employed in a much more covert manner than downlink jamming because a downlink jammer must be positioned in such a way to

[43] Thomas Wilson, "Threats to the United States Space Capabilities, " Found at Federation of America Scientists, http://www.fas.org/spp/eprint/article05.html.

[44] Wilson, "Threats".

[45] Ibid.

[46] Wilson suggests that non-state actors and states without launch capabilities could buy their way onto the vehicle of a launch-capable state. This author agrees that such a possibility does exist.

mimic a satellite's directional transmission, though it too can be discovered through the SIGINT campaigns of an adversary. Although, some SATCOM systems which use Earth coverage beams, less directional beams, and neglect their side lobes may be threatened by jammers far enough away from a conflict that it may be impractical or dangerous to seek and destroy them.

Third, the radio transmission segment is an electromagnetic wave so only EW would have a direct effect. OPSEC, PYSOPS, and Deception could theoretically take advantage of the transmission, however, as mentioned before military encryption is very difficult to break and because the LPI/LPD characteristics of directional transmission make them hard to intercept. Nuclear weapons and microwave bombs could be used to electronically disrupt a local area's atmosphere enough to degrade or corrupt transmission, but these methods call for the use of weapons that are highly destructive and therefore carry the weight of international retribution or highly sophisticated technology making either of unlikely use.

Fourth, communications links are becoming the weak link in Intelligence, Sensor, and Reconnaissance (ISR) networks because of the distances between the globally and extra-globally dispersed sensors from processing centers which tend to be in CONUS.[47] Lastly, while of the Six Pillars of IW, Physical Destruction, CNA, and simple forms of EW appear to be the most threatening to SATCOM, the requirements needed for Physical Destruction and CNA to affect any aspect of SATCOM are greater than those of the equipment and competency for simple EW, which are becoming cheaper and more widespread. This suggests that an EW threat is the most likely.

Electronic Warfare

Electronic Warfare is made of three components: Electronic Attack (EA); Electronic Protection (EP); and Electronic Support (ES). Older roles such as electronic

[47] Libicki, *What is Information Warfare?*, pg 30-31.

countermeasures (ECM) and electronic counter-countermeasures (ECCM) have been recast with wider definitions giving way to more general terminology.

EA is not only concerned with jamming, but also concerns directed-energy weapons (DEW), anti-radiation missiles (ARM), electromagnetic pulse (EMP) weapons, and other attacks directed at destroying the electronics technology necessary for warfare.[48] EP includes protecting electronic equipment as well as the management of the electromagnetic spectrum. ES is the electronic supporting action, e.g. target identification, target acquisition, recognition of threats, which enable friendly forces to act and respond correctly.[49]

Of the forms of EA, jamming is probably the most likely form an opposing force would implement against SATCOM. Of the two jamming methods, noise and deception, noise jamming is the easiest and of the two strategies, uplink and downlink jamming, uplink is the least conspicuous. Therefore, uplink noise jamming will be the study of this section because it would pose the most likely threat. Of the several jamming and anti-jamming schemes that will be discussed, power stealing appears to be the most threatening jamming scheme because it is simple and effective.

Directed-energy weapons and anti-radiation missiles are generally seen as weapons for destroying physical elements such as cruise missiles and radar sites. While it is theoretically possible to construct a directed-energy weapon that could knock out a satellite, the power necessary to do so would make such an attempt highly prohibitive.[50] The use of EMP weapons such as a nuclear detonation at high altitude or a microwave pulse weapons are not unrealistic but could only be accomplished at severe international risk or by a highly technological entity. Jamming is the simplest and to some extent safest form of EA making it very appealing.

[48] EA is linked to Physical Destruction because all of five subsets of C2W interact. Categorizations in C2W are only for a simpler understanding of each synergistic element.

[49] Schleher, *Electronic Warfare in the Information Age.*

[50] Because of the distance between the Earth and a satellite in GEO a DEW would need power on the order of megawatts to gigawatts, millions to billions of Watts, in order to be successful.

To jam a transmission one only needs an antenna, a transmitter, a power source, and a target. In its essence, a jammer is exactly the same as a transmitter and so the equipment is also essentially the same. In fact, one could use legitimate signals to jam.[51] The complexity of a jammer is dependent on the jamming scheme and the target's EP. For example, to affect the usage of a certain frequency, a jammer would only need to be tuned to that frequency and transmit at a power enough to compete with any legitimate signals. Doing so increases the jamming-to-signal ratio (J/S) which is measured in decibels and is essentially a receiver's SNR inverted.

Jammers can also be designed to meet various deployment needs. Some jammers may require a considerable amount of power and so must be positioned near a sufficient power sources or carry one if the jammer is to be mobile. Jammers can be as large and as complex to necessitate its own facilities, or as small and as simple to require a backpack and some batteries. The jammers needed for attack SATCOM could be fit to a ship, an aircraft, or even a truck. Stationary jammers would also not require large facilities and could be hidden in a civilian population.

Two general forms of jamming exist: noise jamming and deception jamming. In the context of communications, noise jamming is the use of radio wave energy to disrupt or distort the opposing force's ability to transfer useful information via radio wave by making it difficult to "hear" useful signals. Deception jamming is the intentional use of radio wave energy to deceive the opposing force's radio devices with false information. Each requires the correct deployment strategy to be successful against opposition EP and visa-versa.

Deception jamming can be categorized into three schemes: Manipulation, Simulation, and Imitation. Each scheme either can jam a communication system with methods as complex as masquerading false signals as true signals or as simple as repeating an opponent's old messages causing confusion. In any case, deception jamming can be

[51] If you've ever tried to listen to a radio station, but couldn't hear it well because another station's transmission was interfering, you've experienced RF jamming.

quite difficult as it can require a deep understanding of an opponent's communication structure, highly advanced encryption breaking devices, and even the use of an opponent's equipment.[52] For these reasons, this thesis will focus on the SATCOM vulnerabilities to EA in the form of noise jamming which can be undertaken more easily because it only seeks to disrupting messages. Thus, a vulnerability to noise jamming would indicate a more likely threat to the communications network.[53]

With digital signals, jamming can be effective against both the frequency and the synchronization of transmissions. Jamming affecting the frequency of a transmission seeks to block out sections or the whole of a transmission's bandwidth with enough power that messages become useless. In other words, it seeks to decrease the SNR of the target below the threshold of intelligible communication. Jamming affecting synchronization seeks to demodulate signals in such a way that they cannot be processed correctly.

SATCOM can be attacked at the satellite through uplink jams or at the user-end terminal with downlink jams. Because of the nature of SATCOM, uplink jamming is simpler and more effective than downlink jamming. Uplink jamming against a GEO satellite targets a stationary platform, and if successful can cut off all of the connections the satellite was making, thus disturbing a part if not all of the network. This, however, is contingent on being able to locate the satellite. Because satellites use directional antennas, a jammer must be positioned correctly as to interact with the main or side lobes of its target, just as any transmitter would. This is not always an easy task because directionality makes it difficult to find from where a satellite is receiving.

Downlink jamming has to be done from locations in between the satellite and the terminal because satellite transmissions tend to be directional. This would not be necessary for terminals that use omni-directional antennas. Airborne jammers would

[52] Michael R. Frater, *Electronic Warfare for the Digitized Battlefield* (Boston, MA : Artech House, 2001), pg 157-162.

[53] For the remainder of this work the word "jamming" should be understood as "noise jamming". However, deception jamming, when done correctly, can also have many of the same effects as noise jamming.

therefore be the most likely platform to downlink jam from. UAVs would be particularly useful in this endeavor as they could be used expendably, flying directly over enemy troops.[54] In essence, the jammer would effectively be acting as a satellite itself. Downlink jamming is possible and the techniques used are very similar to uplink jamming. However, downlink jamming can be more challenging and conspicuous to implement than uplink jamming, making it less effective in many cases. For these reasons, uplink noise jamming will be the focus of this discussion.

There are several general methods of noise jamming: narrowband, wideband, continuous wave (CW), and pulse jamming. These, however, are not without countermeasures and there exist anti-jamming techniques that can be practiced, thus giving way to the back-and-forth nature of EW. Anti-jamming (AJ) Electronic Protection methods also come in various forms. EP measures can be taken with the antenna, the transmitted message, and the frequencies it travels over. The military employs all three to varying degrees of success.

Narrowband Jamming

Narrowband jamming focuses on a single frequency, called spot jamming, or small number of frequencies, called combined jamming, and can be accomplished from stand-off jamming, which is jamming at a distance from the target.[55] Narrowband jamming is also probably one of the easiest jamming schemes to implement. Focusing on a small number of frequencies allows for more powerful jamming, but is not very effective at disrupting high bandwidth transmissions. One set of techniques of anti-jamming technique that work well against narrowband jamming is called Spread Spectrum (SS) techniques. These techniques trade full bandwidth capacity for protection. The two most common methods are frequency hopping and direct sequencing.

[54] Poisel, *Introduction to Communication Electronic Warfare Systems,* pg 193-194.
[55] Ibid., pg 190.

Frequency Hopping is the most common Spread Spectrum technique. This technique takes a small number of frequencies that transmit information and "hops" them within a larger bandwidth. Hopping is usually done hundreds of times a second and follows a pseudorandom order that both the transmitter and receiver know. Many of the jamming methods described above don't fare well against a frequency hopped transmission because they would only affect parts of the bandwidth.[56]

Direct Sequencing is much like encryption for the frequency itself. The true information is merged with a higher bit rate signal that carries no information. The merged signal is then transmitted and demodulated by the receiver which knows the waveform of the "encryption" signal. By merging the true signal with a higher bit rate signal, this technique adds bandwidth to the transmission so that jammers have a more difficult time jamming the proper signal. Essentially, Direct Sequencing hides the true signal in noise.

By employing either of these techniques, a narrowband jammer would find it difficult, if not impossible, to focus on a small number of frequencies and remain effective. However, how well a SS technique works is inherently tied to the amount of information that needs to be passed and the amount of bandwidth it has available around which it can spread its message. Thus, if not given enough bandwidth, SS technique can fail against narrowband jamming.

Wideband Jamming

Wideband or barrage jamming is very similar to narrowband jamming except that it attempts to blanket as much of the transmission bandwidth as possible for as long as possible and is more successful then narrowband. However, because wideband jamming affects multiple frequencies at once, it requires larger amounts of power than narrowband

[56] Poisel, *Introduction to Communication Electronic Warfare Systems,* pg 202-203. In order to block a frequency hopped transmission a follower jammer, which tracks the hops, can be employed. However, such a device can be very complex and tracking would still be difficult.

jamming which can be prohibitive because it attempts to jam more frequencies at once. It is best attempted with stand-in jamming, jamming near the target, to compensate for its power requirements.[57]

SS techniques are more susceptible to wideband jamming because wideband jamming can affect a larger portion of the frequency band, thus whether either hopped or sequenced the signal can potentially have more of its message jammed. Even so, because wideband jamming requires a good deal of power and some band such as SHF and EHF are quite wide, wideband jamming can still be effectively countered by SS techniques.

CW and Pulse Jamming

CW jamming does not focus on any one frequency but sweeps across the entire bandwidth. This method requires less power than wideband jamming, but is more effective than narrowband jamming. Pulse jamming is similar to wideband jamming but transmits in pulses instead of continuously. This is also a way of jamming many frequencies with less power requirements than wideband jamming. However, rapidly switching from one frequency to another as CW and pulse jamming can require necessitates complex equipment.

These forms of jamming can be effective against Frequency Hopping SS techniques because they can cover larger amount of the bandwidth without requiring very high amounts of power. Direct Sequencing SS can fare better against them because it spreads its message it such a way that small frequency gaps are not as deleterious. Again, SS techniques can counter these jamming methods, though only if it has the bandwidth to do

[57] Ibid. The power a jammer requires to be effective is directly related to its distance from its target, and the other transmitter/receiver in the target's communications link. The greater the jammer's power the more distance it can put between itself and its target. While there are many properties from distance between transmission, reception, and jamming sources to transmission and jamming power to antenna properties that determine a jammer's ability to be effective, perhaps one of the most valuable metrics is the J/S ratio. The J/S ratio is similar to the SNR. Both the J/S is measured in decibels, making a more positive value favor the jamming signal.

so and the jammer doesn't use overwhelming amounts of power or can tune very quickly through the band.

The message being transmitted itself can also have AJ properties. As noted previously, radio waves can interact with the different media through which it must travel in ways that can affect the message. Error-correction is used so that the correct message can be received even if parts of the message are corrupted. Error-correction is also effective against jamming. There are several forms of error-correction, the simplest being to transmit the same message multiple times. This can be an effective method against narrowband, wideband, CW, and pulse jamming because it relies on redundancy to get them message across. However, repeating a message multiple times can slow the information throughput and if the right equipment and power is used, wideband and CW jamming methods can be effective.

Other Forms of Jamming

Two other forms of jamming attack the nature of the satellite and digital SATCOM itself. One simple method known as "power stealing" attempts not to disrupt other transmissions directly, but to trick the satellite into jamming friendly transmissions. When communications satellites receive signals they attempt to weed out noise, which occurs naturally, from the signals they are trying to receive.[58] The satellite takes higher power signals, amplifies them, and retransmits them to their destination or another relay point. In this way, the noise is drowned out. Power stealing uses this process to its advantage by transmitting high power noise to the satellite, usually trying to achieve about a 6dB J/S. Unaware that the higher power signal is pernicious, the satellite amplifies the jamming signal and drowns out the friendly signal. This is also know as the "near-far" problem and most forms of anti-jamming EP are vulnerable to this as this simple method

[58] Ibid., pg 55-60. Noise can be produced from a number naturally occurring sources including thermal conditions, external and internal electrical conditions, and the interference from other legitimate signals and reflections of the same signal.

preys on the satellite itself.[59] Very simple equipment can be used for this technique as it only requires high power, on the order of kilowatts or lower, and not complex signal outputs.

The second form attempts to disable the user terminal from being able to track, or follow, a friendly satellite signal. By energizing a satellite with signals of the correct power and frequency, jammers can cause the satellite to retransmit modulated signals which confuses the ground terminal into following a jamming signal. This method of signal desynchronization takes advantage of the satellite and the harmonic nature of radio frequencies. However, this method requires knowledge of the systems it is trying to jam which may be difficult to obtain.

Power stealing and desynchronization are not easily protected against by SS techniques because they attack the satellite itself. However, by equipping a satellite with onboard processing capabilities, which many satellites do not have, it can better distinguish and attenuate unwanted signals. There are AJ methods that can counter power stealing and desynchronization. These methods take advantage of, and sometimes imitate, naturally occruing phenomena. As mentioned beforehand, directional antennas focus most of their radiated energy into a single beam, called the main lobe, which extends outwards in one direction with some azimuth. However, some of the energy is radiated in other directions called side lobes. In between the main and side lobes are "nulls", the absence of radiated energy. Because jammers need to interact with the lobes of the antenna in order to be effective some antennas use a method called null steering to protect themselves. Null steering uses the natural nulls of an antenna, or creates them with other antennas, and positions them over areas where a jammer is believed to be. This AJ

[59] Ibid., 197. Direct sequenced Spread Spectrum techniques are inherently vulnerable to this form of jamming. This is because it reduces the signal-to-noise ratio in order to hide the signal in noise, making it harder to discover. However, this consequentially increases the jamming-to-signal ratio making it easier for a jamming signal to overpower a legitimate signal.

technique is effective against all forms of jamming because it disallows the jammer from interacting with its target.

Another form of AJ, or rather jam resistance, antennas have comes from the nature of the frequencies it uses. Transmissions using the SHF and EHF bands can create very narrow main lobes. The narrower the main lobe is, the closer the jammer has to be to the receiving terminal to be effective. While this property of highly directional transmissions can combat the ease at which a jammer can affect a target, it is more a passive than an active defense. Omni-directional receivers cannot benefit from this property.

Today's Systems

Today's MILSATCOM consists of three satellite systems: Ultra High Frequency Follow-On (UFO); the Defense Satellite Communications System (DSCS); and the Military Strategic and Tactical Relay (MILSTAR). However, because commercial satellites are used by the military, COMERSAT has also been included.

As is may be understood from the descriptions of the jamming and anti-jamming techniques, very few jamming techniques are made impossible by the use of AJ. They are only made more difficult. How well one employs a jammer is also an important factor in determining the effectiveness of a jamming scheme. Therefore, it is better to measure vulnerability by comparing each system's specifications and AJ capabilities to the level of technology required to threaten the system.

UFO

The Ultra High Frequency Follow-On system, consisting of ten GEO satellites was created to carry on the mission of several other systems at the end of their lifetimes. UFO currently takes the place of the US Navy's Fleet Satellite Communications (FLTSATCOM) system, takes on some of the US Air Force's Air Force Satellite Communications (AFSATCOM) system's mission, as well as provides UHF links previously shouldered by leased satellites (LEASAT). The primary mission of UFO is to service tactical users with low to medium information.[60] It is also primarily a US Navy system.

UFO's key vulnerabilities stem from the fact that many of its links do not employ AJ techniques. All of the UFO satellites have the capacity for UHF links, which are inherently more vulnerable because the UHF band is not large and so doesn't allow for much Spread Spectrum AJ or error-correction. The UHF links also do not provide onboard processing. This allows them to be vulnerable to many forms of jamming including power stealing. The SHF links that the system provides are also at risk because they do not perform sufficient Spread Spectrum AJ or onboard processing. The EHF links are better protected with Spread Spectrum techniques and onboard processing, this includes the Global Broadcast Service (GBS) links.[61] The longitudinal location of UFO satellites can also be found in open sources. While their exact location may be unknown, GEO satellites tend to be equatorial and changing orbits can drastically reduce the lifetime of a satellite.

Each of the ten satellites has twenty-one narrowband UHF channels at 5 kbps, seventeen relay channels at 25 kbps, and one fleet broadcast channel totaling 555 kbps of UHF bandwidth. Three satellites also provide some SHF links for mobile communications. The EHF payloads on three satellites carry eleven low to medium bit rate channels, the rest carry twenty channels. Each satellite shares its EHF channels between an Earth beam and a spot beam. The GBS equipped satellites can each handle 96 Mbps with its three steerable downlink antennas, and its one steerable, one fixed uplink antennas.[62]

[60] Globalsecurity, http://www.globalsecurity.org/space/systems/ufo.htm; The Boeing Company, http://www.boeing.com/defense-space/space/bss/factsheets/601/uhf_followon/uhf_followon.html; Accessed August 2, 2005.

[61] Donald H. Martin, "A History of Military Satellite Communications Systems," (Crosslink) http://www.aero.org/publications/crosslink/winter2002/01.html.

[62] The Boeing Company, http://www.boeing.com/defense-space/space/bss/factsheets/601/uhf_followon/uhf_followon.html; Accessed August 2, 2005.

DSCS

The Defense Satellites Communications System was first put into orbit in the 1960's as the Initial Defense Satellite Communications System. Since that time the Department of Defense (DoD) has put up two more versions of the system and is currently on its third. The current system, using DSCS-III satellites, serves a host of users from the White House Communications Agency, to mobile military terminals, to the State Department and Strategic Command. The main purpose of DSCS is to provide long-haul, high data rate communications to the aforementioned users.[63]

The vulnerabilities in DSCS arise from its use of two Earth coverage receive antennas, allowing jammers to be positioned far from a conflict, and the lack of onboard processing.[64] The longitudinal locations of the satellites are also in open sources, and they cover the East and West Atlantic and Pacific as well as the Indian Ocean. However, the DSCS satellites do have some AJ capabilities. All save one of the DSCS channels use the SHF band, which is wider than the UHF band and allows for better encryption schemes. The other single channel uses both UHF and SHF for Emergency Action Message broadcast and does not present a major vulnerability unless in nuclear crises. The satellites also carry multibeam antennas that allow selective nulling, a form of null steering, and jammer location electronics.[65]

DSCS is made up of five active satellites in GEO, with four as back-ups, creating nearly complete global coverage. Each satellite can transmit across six X-band channels (from 7.25-8.4 GHz) using three receive and five transmit antennas.[66] One of the receive and two of the transmit antennas are multibeam lenses, allowing them to create sixty-one controlled beams and selective nulling. It also has four Earth coverage antennas, two receive and two transmit, as well as one mechanically gimbaled transmit antenna. The

[63] MILSATCOM Joint Program Office,http://www.losangeles.af.mil/SMC/MC/dscs.htm; Accessed August 2, 2005..

[64] GlobalSecurity, http://www.globalsecurity.org/space/systems/dscs_3.htm; Accessed August 2, 2005.

[65] Globalsecurity, http://www.globalsecurity.org/space/systems/dscs_3-substm.htm.

[66] GlobalSecurity, http://www.globalsecurity.org/space/systems/dscs_3.htm; Accessed August 2, 2005.

DSCS-III satellites can use spot, area, global coverage, and rapidly selective coverage beams. The six channels have an average bandwidth of 71.6 MHz and a total bandwidth covering 500 MHz, and up to 200 Mbps.[67] The DSCS-III satellites also carry a single channel for Emergency Action Message broadcast.

MILSTAR

MILSTAR is the DoD's most reliable SATCOM system. The Military Strategic and Tactical Relay satellite system was created to supply long-haul links of communication for the President, the DoD, and the Armed Services in jamming environments and even in nuclear war. Detonation of nuclear devices can change the atmosphere enough that radio waves, below the microwave band cannot pass through them for a period of time. Nuclear detonations could also destroy valuable ground relay stations, severing the ground hop that SATCOM often uses. For these reasons, MILSTAR was designed as an EHF band communications satellite, which are not as distrupted by atmospheric effects present after a nuclear detonation, and as a system that could transmit information directly from one satellite to another utilizing cross-links.

Vulnerability in MILSTAR would result from its use of Earth coverage beams though this is compensated for by its robust AJ capabilities. All of MILSTAR's links are in EHF band, meaning that it supplies ample room for Spread Spectrum techniques, especially because the data rates at which it performs do not take up a considerable amount of EHF's bandwidth. The higher data rate transponders also carry antennas specifically designed for null steering, and the satellites implement onboard processing.[68] Though these measures account for all of the jamming techniques described above, it would be remiss to say that MILSTAR is jam-proof.

[67] MILSATCOM Joint Program Office, http://www.losangeles.af.mil/SMC/MC/dscs.htm; Accessed August 2, 2005.

[68] Donald H. Martin, "A History of Military Satellite Communications Systems," (Crosslink) http://www.aero.org/publications/crosslink/winter2002/01.html.

Five MILSTAR satellites orbit the Earth in GEO. Two, MILSTAR-I satellites, can only have low data rate (LDR) payloads allowing for data rates of 75 bps to 2.4 kbps in 192 channels. The other three, MILSTAR-II satellites, have both LDR and medium data rate (MDR) payloads. The MDR payloads can transmit data from 4.8 kbps to 1.544 Mbps in 32 channels.[69] The LDR payloads have antennas for Earth coverage up and downlinks, positional up and downlink beams, and 2 narrow and 1 wide spot beam. The MDR payloads offer 8 antennas, 6 for area coverage and 2 for nulling.[70]

The MILSTAR system is the most robust of the three MILSATCOM systems. The MDR payloads offer area beams and 2 antennas dedicated to nulling, making the antenna system quite robust against jamming attempts. Onboard processing and use of Spread Spectrum techniques over the EHF band protects the system from power stealing, desychronization, and most other forms of noise jamming.

COMERSAT

The systems described above only account for MILSATCOM and only make up approximately 14% bandwidth needs for peacetime activities, tactical patrols, and training.[71] The remainder of bandwidth must be obtained commercially. The design of commercial satellites is not driven by the requirements of MILSATCOM and thus COMERSAT is quite vulnerable to jamming. They are designed to transfer data over the C, Ku, and Ka bands and to offer the most users the most amount of bandwidth possible, not to offer robust, secure communications links in an EA environment. As a result, they sacrifice the protection that comes from having wide, open bandwidths for Spread Spectrum techniques and do not have onboard processing for the most part.[72] Other AJ

[69] MILSATCOM Joint Program Office, http://www.losangeles.af.mil/SMC/MC/milstar.htm; Accessed August 2, 2005.

[70] Ibid.

[71] Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 8.

[72] Globalsecurity, "Executive Summary of Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html.

systems, such as dedicated null steering antennas or AJ detection equipment, are also rare because they require space and power that could be used by revenue producing transponders. However, while the majority of systems are quite vulnerable, some systems are providing better measures of protection in order to shield their transmissions from technically capable vandals.

Commercial satellites orbit in GEO as well as Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) and carry Earth, area, and spot beams, though the spot beams are not as narrow as the military satellites can provide.[73] Their orbits are also well documented and accessible.[74] The technology and SATCOM knowledge required to jam a commercial satellite is easily accessible and becoming more so as IT usage increases around the world. One anecdote suggests that a common commercial satellite can be jammed by any TV technician with $1000 of easily acquirable electronics equipment.[75] Another COMERSAT vulnerability comes in a legal form. Being that COMERSAT is regulated by civilian entities such as the UN's International Telecommunications Union (ITU), landing-rights, or rights to transmit and broadcast over a state, are regulated by each individual state. This could mean that a state in a conflict with the US could effectively deny the use of COMERSAT within its boundaries. Such an action, however, could also affect the state's use of COMERSAT. This all does not bode well for the military's SATCOM users.

Unfortunately, MILSATCOM's future use will still have its problems. The SATCOM usage rate of growth is projected to continue to far exceed MILSATCOM's capacity for the next ten years. Even with the incorporation of the Advanced EHF, GBS, and Wideband Gapfiller satellites, MILSATCOM could fall short some 1-10 Gbps.[76] Thus,

[73] Bonds, Mattock, Hamilton, et. al., *Employing Commercial Satellite Communications*, pg 70. While satellites in LEO and MEO do not have relatively constant locations, they can be followed using satellite tracking technology, such as radar, which is an essential technology for SATCOM and does not require highly complex equipment.

[74] This is especially true for states that use COMERSAT because this information can be accessed through the satellite control corporations and international regulatory organizations such as the ITU.

[75] Ibid., pg 74.

[76] Ibid., pg 10.

MILSATCOM will have to continue to depend on less than secure links to communicate its rising amounts of information.

Summary

Table 3 below summarizes the vulnerabilities of each of the military's SATCOM systems by considering each system's vulnerabilities and the difficulty to exploit those vulnerabilities as mentioned in EW subsection. The vulnerability of UFO was given a vulnerability score of medium-high because its UHF and SHF links present a considerable vulnerability, while its EHF links do not. Though the DSCS system does not perform onboard processing, the use of the SHF band, its null sterring capabilities, and its jammer location electronics amount to a medium score of vulnerability. The MILSTAR is the least vulnerable because of its robust AJ, compensating for its use of Earth coverage beams. COMERSAT is the most vulnerable because it does not implement many of the AJ techniques used in MILSATCOM, being specifically designed to provide large amounts of bandwidth not protection. A lack of onboard processing also makes it highly vulnerable to the simple technique of power stealing.

Table 3 – SATCOM Vulnerabilities to Jamming

System	Vulnerability	Technology Required to Jam	Level of Vulnerability
UFO	UHF band, Earth Coverage Beams, Partial Onboard Processing	Low - Mid-level	Medium-High
DSCS	Lack of Onboard Processing, Earth Coverage Beams	Low - Mid-level	Medium
MILSTAR	Earth Coverage Beams	High-level	Low

Commercial	Lack of Onboard Processing, Wide Coverage Beams, Not Designed to Survive AJ Environment	Low-level	High

While the majority of the MILSATCOM systems are only medially vulnerable on average, the highly vulnerable COMERSAT supplies almost all of the military's bandwidth. This may not change as the voracious bandwidth demand brought on by the iRMA cannot be sated by MILSATCOM nor will it be able to in the near future. As Information Warfare is better understood and implemented by state and non-state actors and as the military better integrates the joint, precision and net-centric doctrines of the iRMA, these vulnerabilities will without doubt have an impact on the military's ability to carry on its many tasks.

Chapter 3

Assessing the Chinese Threat

A measurement of a system's or its implementation's vulnerability alone is insufficient to assess the level of threat an adversary can pose to it. One must also understand the adversary's abilities. As the US military has transformed and integrated the doctrines and tactics that the iRMA have allowed, so too has the PLA. Though the PRC is still many years behind the US, this has not stopped them from seeking ways to defend against, and possibly overcome, the US's superior might. The PLA understands the advantages and disadvantages of the iRMA, and after carefully noting recent US military actions, it has discovered some of the vulnerabilities associated with it, vulnerabilities which it seeks to exploit. The PRC's knowledge-base and doctrinal and tactical means of using Information Warfare are not highly advanced, but their rapid economic and technological growth over recent years has made them a credible threat.

As described in the previous chapter, jamming the most likely form of IW an adversary would carry out against the military's SATCOM and so is the focus of this chapter. Physical destruction, cited in the previous chapter as a less likely form of IW, may also be of use to the Chinese as they do have indigenous launch capabilities. Though the assessment of Chinese capabilities completed here is not definitive on whether the PLA can or will jam, or physically attack SATCOM because of the nature of the sources, PLA IW rhetoric and current technical capacity suggest it would be best to assume they can and will.

This chapter attempts to evaluate the PRC's ability to threaten the US military's SATCOM systems. The chapter is segmented into five sections. The first discusses how the PRC understands the iRMA, and what strategies it can implement accounting for it. The second section gauges the PRC's knowledge-base of the technology needed to perform successful IW against SATCOM. The third assesses the military infrastructure and force structure built around IW. The fourth brings together the previous three sections to understand the PRC ability to threaten SATCOM. The final section summarizes the chapter.

The sources used here based their research on Chinese doctrinal writings, articles in the PLA Daily, interviews with Chinese sources, historical research, and previous studies. Much of the Chinese writing pertaining to IW and their military technology capabilities is theoretic and opaque. This is either because they have very little to say or because they are performing an Information Operation. In any case, knowledge of their true capabilities can become lost in generalities and rhetoric. Because of this, scholars often overestimate or underappreciate Chinese capabilities. While this author believes that both practices can lead to dangerous misperceptions, he also believes that in a case where facts are few, one must seriously consider any that are found and with reason assess how to weigh them. The sources used here touch on both sides of the spectrum and so the findings here should be taken with a hint of caution as the author does.

Understanding the Chinese iRMA

Deciphering how another state is influenced by an event such as the iRMA can be a difficult task, but it is an important one as this can aid in the prediction of a state's actions. Recognizing and understanding the theories, assumptions, and beliefs of a state as well as its history of strategies can provide invaluable insight into why and how a state will shape itself to meet the threats it perceives. By surveying the modernization developments, how the iRMA has affected the Chinese mindset, IW rhetoric, as well as a how the Chinese use war, it appears that that the iRMA has not gone unnoticed in China's efforts to step into the modern world and that attacking communications is considered an important IW tactic.

It should be noted, however, that while intentions and abilities to commence C2W and EW are present, they are not highlighted as much as the evidence surrounding China's IW competency involves CNA and OPSEC. This alone should not suggest that the Chinese are not as involving in EW theory, but simply that evidence has little to say on the subject. This could be because the Chinese truly are not focusing on EW, they are practicing OPSEC about their capabilities and intentions, or that researchers have considered China's CNA more than other forms of IW. Though the reason is unknown, a subtle clue as to whether EW if of interest to the Chinese may be their focus on communications systems and their protection.

Prior to 1979 the PLA was structured around fighting a "people's war". "People's war" was a defensive war fought on Chinese soil that aimed to grind an adversary away through a war of attrition.[77] This was facilitated by scattering key facilities and centers throughout the country, disabling an adversary from quickly destroying China's warfighting capabilities. The PLA's large and antiquated forces were equipped for fighting such a war which relied more on numbers than firepower. This is changing.

The PLA is now trying to fit itself with modern equipment and doctrines believing it must be able to survive "local war under informationalization". This shift began following the return of Deng Xiaoping to the chief of the General Staff in the Central Military Commission, the leading body of the PLA, in 1975. At that time, the complexities of the international system have impressed upon the Chinese that the world was much smaller than they once thought. States had grown interdependent through economics, politics, and treaties. This interdependence and the ever present threat of nuclear war spawned the belief that local or limited war, war which is confined, quick, and fought to create diplomatic success, was becoming the most likely form of military conflict in the

[77] Shambaugh's *Modernizing China's Military* was used as the major source for China's modernization history.

modern world.[78] Under Deng's guidance, the PLA attempted to rapidly restructure itself to meet the future. Defense commissions, departments, organizations, and the PLA force structure were streamlined in the attempt to create a more centralized and flexible force. Though the first reconstruction ended without creating the efficiencies that the PLA hoped to gain, several more followed and continue today.

Soon after the shift to local war took hold, the ending of the Cold War drastically changed the global political landscape. The new unipolar world created a situation where the PRC could continue to flex its muscles, as it believed it could during the superpower stalemate in the mid-80's, but it now had to be wary not to offend the allies of the now unrivaled Western superpower. This new development forced the PLA leaders to realize that their actions could very well place them opposite the battleline of the most powerful nation in the world.

A few years later, the First Gulf War revealed to the PRC what it would be up against. The lightening fast war spurred on by ship-fired cruise missiles, stealth bombers, precision-guided munitions, and joint warfare astounded the PLA leadership. They found that while their unsuccessful streamlining was a step in the right direction, they were still far behind the state they began to see as their primary opponent. The advances in US military technology were so impressive that many in the PLA were convinced that a new era of warfare was upon them; one that was based on computer and information technology, mobility, and jointness. It took special note of the US's Electronic Warfare campaign, and the use of satellites and communications which it saw as critical to the Allied success.[79] This information Revolution in Military Affairs prompted further reorganization and modernization of the PLA structure.

The US-led intervention during the First Gulf War as well as the Balkan conflicts also had another effect. While direct conflict with the US was very unlikely, the PLA

[78] Mark Burles and Abram N. Shulsky, *Patterns in China's Use of Force: Evidence From doctrinal Writings*, (Santa Monica, California: The RAND Corporation, 2000), pg 29-35.
[79] Shambaugh, *Modernizing China's Military*, pg 73.

feared that a crisis could arise that would pit it against the US through one of its eastern allies. These US-led interventions, the 1996 Taiwan Strait Crisis, and the more recent actions in Afghanistan and Iraq, reaffirmed and fueled these fears and the belief that the US is securing for itself global hegemony. It is for all of these reasons that the PRC believes it must prepare for "local war under informationalization", suggesting that it believes it may have to fight a limited conflict with a technologically superior, informationalized adversary, the US.

Though the PLA lags behind the US in modernization and its implementation of the iRMA, it is not without insights. The PLA is aware that the information, and the communication on which it depends, both strengthens joint and precision warfare as well as creates a critical link in the armor that can be targeted and destroyed with considerable consequences. It also understands the unique nature of the iRMA in that the same technology which makes its enemy so formidable can also enable its own weaker forces to strike back through IW.[80] Armed with this knowledge, the PLA hopes to become not a victim of the iRMA, but a master of it.

Information Warfare, as described in the previous chapter, can affect a wide range of apparati and there is some question as to how well the Chinese understand IW, EW in particular. Much of what the PLA publishes on IW is heavily adapted, if not taken, from US sources and theoretic in nature.[81] This is not to say that they haven't any grasp of it. The PLA appreciates both its offensive and defensive nature as well as its military and civilian uses.[82] C2W, EA, and CNA are common topics in PLA publications and they have discussed implementing elements of IW from spreading computer viruses to using high-

[80] Shambaugh, *Modernizing*, pg 70-73.

[81] James C. Mulvenon, "The PLA and Information Warfare," in *The People's Liberation Army in the Information Age*, James C. Mulvenon and Richard H. Yang ed. (Santa Monica, CA: The Rand Corp., 1999), pg 177; Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, pg 23-25.

[82] Shambaugh, *Modernizing*, pg 74-81; Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, pg 28-29; Mulvenon, "The PLA and IW," pg 179; Mark A. Stokes, *China's Strategic Modernization* (SSI, Sept. 1999), pg 52.

power microwave weapons.[83] There have been several papers concerning the attack of logistics and C^2 communications, GPS, the Joint Tactical Information Distribution System (JTIDS) and SATCOM.[84] Military training programs have also been established to create "cyber soldiers" capable of hacking their way through an adversary's software defenses to mine information or infect systems with viruses. These soldiers may have already seen action in cyber battles with the Taiwanese and possibly the US.[85] The US-China Economy and Security Review Commission claims that the PLA may also have developed a laser cannon able to strike 100 plus kilometers into space with which to "blind" reconnaissance satellites.[86] Having studied the First Gulf War and the Balkan conflicts, the PLA has also learned the value of shielding electronic equipment, hardening and creating redundant communications nodes, as well as the value of hiding equipment more effectively. The PRC has been identified as one of the world's top producers of obscurants which are effective against sensor and guidance technologies.[87] It may also have initiated the interlacing of military communications with civilian systems believing that the US would seek not to destroy vital civilian links.[88] Furthermore, the Chinese believe that IW is central to fighting future war and remaining abreast with the modern world.[89]

[83] Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, pg 13; Stokes, *China's Strategic Modernization*, pg 52-53.

[84] Michael Pillsbury, "China's Military Strategy Toward the US: A View from Open Sources," (Nov. 2001) http://www.uscc.gov/researchpapers/2000_2003/pdfs/strat.pdf
,pg 11-12; Stokes, *China's Strategic Modernization*, pg 53.

[85] Damon Bristow, "China and Taiwan: information warfare," (Global-Defense) http://www.global-defence.com/2000/pages/china.html; Accessed August 2, 2005; Robert Vamosi, "Will China (cyber) attack Taiwan, US?"(CNET: May 3, 2002) http://asia.cnet.com/news/perspectives/0,39037107,39041620,00.htm; Accessed August 2, 2005; Global Information Warfare pg 218-220, 224-234. This book as collected a number of news clippings from various source citing the use of IW, CNA especially, by the PRC.

[86] US-China Economy and Security Review Commission, *2004 Report to Congress*, (Washington, D.C.: GPO, 2004), pg 202. Blinding a satellite requires much less power than shooting one down.

[87] Burles and Shulsky, *Patterns*, pg 66; Bernard D. Cole and Paul H.B. Godwin, "Advanced Military Technology and the PLA: Priorities and Capabilities for the 21st Century," in *The Chinese Armed Forces in the 21st Century*, (SSI), pg 173.

[88] Burles and Shulsky, *Patterns*, pg 66-67.

[89] Mulvenon, "The PLA and IW," pg 179; Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?*, pg 6.

It is unclear how the PLA intends to implement IW, but they do hope to do so against an adversary far superior in its iRMA ability and depth of integration.[90] A survey of papers and articles suggests that the PLA considers theories of asymmetric warfare important.[91] Asymmetric warfare implies that a weaker force will fight a stronger force through exploitation of its vulnerabilities. This is of considerable importance as it implies that the Chinese readily acknowledge the disparity between the US forces and their own. Often surrounding the discussion of IW is talk of "Inferior Defeating the Superior" strategies and of "Assassin's Maces". An Assassin's Mace can be likened to a "silver bullet" or secret weapons which, leveraged correctly, can defeat an opponent who is superior in strength. Of the many Assassin's Maces that are written about, IW is a major one. Fantastic as such a weapon may sound, the discussion of it should not be taken lightly as high ranking military officials and President Jiang Zemin himself has called for their creation. [92] Thus, considering that the PLA sees the US's dependence on information technology as a weakness, it would be prudent to believe that they do plan on attacking the vulnerabilities in our information systems.[93]

Recognizing past PLA uses of force and their theory of limited war may allow for an even better understanding of how they may implement IW. A study completed by the RAND Corp. highlighted several strategic patterns the PLA tends to use. They are Surprise, Psycho-Political Shock, Opportunistic Timing, and the Use of Crises.[94] Each of these strategies is aimed at affecting the will of the adversary more so than its ability to fight. Surprise can be understood on a tactical and strategic level. Tactically, surprise can be viewed as using deceit to create a battlefield advantage such as feigning retreats or changing the war's pace by preemptively striking. Strategic surprise could be the concealment of force strengths, doctrines, and capabilities. Psycho-Political Shock can be

[90] Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?,* pg 9.

[91] Shambaugh, *Modernization,* pg 74-81; Toshiro pg 6-7; Michael Pillsbury, "China's Military Strategy".

[92] Pillsbury, "China's Military Strategy," pg 13-15.

[93] Shambaugh, *Modernization,* pg 61-71, 89.

[94] Burles and Shulsky, *Patterns,* pg 5-20.

exampled by implementing tactics that produce high causalities to both sides in order to declare willingness to fight and to force their adversary to realize that costs will be high. This strategy would work best against casualty-adverse states, which the PLA believes the US to be.[95] Opportunistic Timing is a strategy which waits to create large, favorable force imbalances before attacking. This imbalance can also be created by coaxing an enemy into a position which overstretches his logistic lines or distance from friendly bases. The Use of Crises is more benign. While also aimed at defeating an adversary, crises may be incited or exploited to create a political situation or statement to cause an adversary to rethink his diplomatic and even military strategies.

The PLA's objective of fighting limited war complements the fact that the US forces are superior well. If the objective is to weaken the US's political and military resolve, the PLA forces need not rank with the US's. It only need to produce effects that would give the US pause. The strategies listed above may be able to do just that by working asymmetrically against a particular US weakness, be it casualty aversion or the PRC's distance from the US. While the exact strategy that would be used is unknown, nor is it clear that the PLA would target SATCOM, the PLA's insights into the iRMA, and the US's strengths and weaknesses as well as its own, suggest that IW, especially against communication systems, will be a key factor to any implementation.

Gauging the Chinese Knowledge-Base

Comprehending the PLA's intent to use IW and the strategies it would implement against the US is important. However, partaking in IW requires technical knowledge. SATCOM, while conceptually simple, can be quite complex in its undertaking. The electronics used to develop and operate a satellite constellation, its ground relay network, and the user-end terminals are not crude devices and require proficiencies in a number of technical areas. Without familiarity and a grounded knowledge of the intricacies of

[95] Ibid., pg 61-71.

satellite technology, constructing an effective countermeasure to SATCOM would be very difficult. Though the Chinese are not as technologically developed as the US, it does appear that they grasp many of the concepts and can produce much of the equipment necessary for executing EW against SATCOM.

China's first experimental communications satellite was launched into GEO in 1984. Since that time China has launched a number of communications satellites by itself and through joint ventures with other nations. Though SATCOM is now vital for television broadcasts and telecommunications throughout most of China, only a small portion of it is provided by indigenously built Chinese satellites. The majority of throughput comes from foreign satellites either through leased transponders or foreign procurement.[96] The PLA's use of SATCOM has also been reliant on foreign satellites. Several failures with its DFH-3 series satellites, a joint project with the Daimler-Benz company in Germany, pushed the PLA to leasing transponders from commercial providers.[97] New satellites such as the Chinese built DFH-IV and the military-dedicated FH-I series satellites may enable the PLA to meet their telecoms needs once these satellites are launched and integrated into their appropriate C^4 I^2SR (command, control, communications, computer, intelligence, information, sensor, reconnaissance) networks.[98] While not directly related to SATCOM, China also possesses a number of ISR satellites and is working on microsatellites.[99] Some of these satellites do require telecommunications to transfer data and perform maintenance. This all suggests that the Chinese are adept in SATCOM.

[96] Roger Cliff, *The Military Potential of China's Commercial Technology* (Santa Monica California: The RAND Corporation, 2001), pg 19.

[97] Cole and Godwin, pg 180-181; Chinese Defence Today, (December 8, 2002) http://www.sinodefence.com/space/spacecraft/dfh3.asp; Accessed August 2, 2005.

[98] Chinese Defence Today, http://www.sinodefence.com/space/spacecraft/fh.asp; Accessed August 2, 2005.; Chinese Defence Today, (December 8, 2002) http://www.sinodefence.com/space/spacecraft/dfh4.asp; Accessed August 2, 2005.

[99] DoD, *Report to Congress,* pg 35-36.

While the PRC has demonstrated its ability to use SATCOM, many of the technologies and components that are used are of foreign origin or constructed through joint ventures with foreign companies. In order for this to change, the PRC must educate more engineers and better foster industrial innovations. China does possess a cadre of scientists, engineers, and technicians but organizational factors can often be attributed to their slow progress.[100] It also only graduates a small percentage of its population with advanced science and engineering degrees. Estimates state China graduated some 1-2 million students per year from institutions of higher learning in recent years. Of these, only about 7% of those educated are engineers, and the percentage of graduates with advanced degrees in computer science and mathematics is lower.[101] In comparison, the US graduates roughly the same number of students from post-secondary schools of which 5% were in engineering in the year 2002.[102] Though the numbers are similar, the US graduates 4 times as many students by percentage of population. Some Chinese students do technical studies in Western countries, but few of them return to add to the domestic technical knowledge-base.[103]

The technology industry also suffers from a lack of strength. Telecommunications technologies, as stated above, are heavily dependent on foreign companies. While China does produce a number of technological goods, such as computers, fiber optic cable, and communications switching systems, it is not able to produce some of their vital components.[104] Nonetheless, China is not without some strength. Foreign IT developments and telecommunications modernization are growing rapidly and do benefit the state as

[100] Modernizing China's Military pg 190.

[101] Shambaugh, *Modernization*, pg 249-250; Chinese Education and Research Network, (January, 19, 2005) http://www.edu.cn/20050119/3127194.shtml; Accessed July 27, 2005.

[102] *Digest of Education Statistics, 2003*, (National Center for Education Statistics) http://nces.ed.gov/programs/digest/d03/tables/dt255.asp; Accessed July 27, 2005.

[103] Shambaugh, *Modernization*, pg 250.

[104] Cliff, *TMPCCT*, pg 11-21.

foreign companies are pressed into sharing their technology.[105] The PLA will also benefit from the highly innovative public IT sector China is developing as well as from its own close ties to the state's telecommunications services.[106] Both its indigenous microwave transmission technology and software production capabilities are approaching, if not meeting international standards and are important for IW.[107]

In summary, the PRC's knowledge of SATCOM and some associated technologies is present. The presence and use of SATCOM knowledge indicates that the fundamental concepts of jamming SATCOM are available to the PRC. Its competency in constructing technical goods and in its own microwave technology suggests that the technical knowledge needed to construct jammers that can affect SATCOM is also available. Though the PRC's dependence on foreign electronic components and technologies and its small percentage of technical training may suggest that the PRC's knowledge-base is still not yet mature, this does not represent an inability to prosecute jamming, especially in the form of power stealing which does not require very high technologies or technical knowledge. Coupled with this fact is that the high influx of foreign technologies and the innovations that the public IT sector are seeing, will, if not already, have transferred over to some military capability.

Assessing Means

In order to have a decisive effect on the US military's use of SATCOM, the PRC would need to have more than just the intent and knowledge-base to do so; it must also have the means. As the US's SATCOM networks become better integrated and robust, so too must the PRC's ability to exploit its vulnerabilities. Against a well connected force,

[105] Keith Crane, Roger Cliff, Evan S. Medeiros, et al., *Modernizing China's Military: Opportunities and Constraints* (Santa Monica, CA: The Rand Corp., 2005), pg 188.

[106] Ibid.; James Mulvenon and Thomas J. Bickford, "The PLA and the Telecommunications Industry in China," in *The People's Liberation Army in the Information Age,* James C. Mulvenon and Richard H. Yang ed. (Santa Monica, CA: The Rand Corp., 1999).

[107]Cliff, *TMPCCT,* pg 15-18.

momentary disruptions in a small number of systems would only have minimal effects. For IW, and specifically attacks against SATCOM, to have a chance of deterring or defeating the US by providing an asymmetric advantage or an Assassin's Mace, it must be undertaken methodically with the proper doctrine and in a centralized manner with the proper equipment.

It appears that China has neither the doctrines nor the equipment is known to be in place to implement EW. However, the opacity of doctrinal writings and desire to keep capabilities secret imply that a dearth of evidence does not indicate a lack of means. Several components necessary for jamming SATCOM, such as microwave technology and satellite tracking, are provided for by the PRC. Coupling this fact with their desire to utilize the advantages of IW, it would remiss to believe the PRC does not have the means to attack SATCOM.

Any detailed IW doctrine or order of battle that the PLA may have has not yet been discovered. Some sources indicate that it does not have an independent IW strategy, but four facts must be recognized.[108] First, as aforementioned, the PLA does recognize the potential of IW against a technologically dependent adversary. Efforts have been made to harden communications nodes, upgrade electronics equipment with better shielding, interlace military communications links with civilian links, create better concealment methods, etc. Schools and centers of excellence of IW have been established, units are being educated in ways of cyber-warfare, and IW has been practiced in war games.[109] Second, as mentioned before, the Chinese do find that communications links are critical to the success of modern militaries and their disruption could be decisive. Third, the "24-Character" strategy and "peaceful rise" rhetoric highlights the PRC's drive to develop into an international power without frightening its neighbors and other world powers. While

[108] Mulvenon, "The PLA and IW," pg 185; Yoshihara, *Chinese Information Warfare: A Phantom Menace or Emerging Threat?,* pg 9, 15;

[109] Shambaugh, *Modernization,* pg 76-81; Department of Defense. Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2005* (Washington, D.C: 2005), pg 36; Mulvenon, "The PLA and IW," pg 179.

the PRC focuses greatly on building up its economic strength, it also believes that building the military will play a key role in its ascension. To modernize without creating fear or impedance, the 24-Character strategy suggests concealing capability. Fourth, the PRC has successfully employed the art of deception in both tactical and strategic terms in the past, and continues to teach its practice.[110] Though these facts do not dictate that an IW doctrine, or one specifically focusing on jamming, does exist, they do point to its likelihood.

How well organized an infrastructure and training program such a doctrine may have is another question that must be asked. The State Council's *China's National Defense in 2004* implies the PLA intent on creating such an infrastructure stating:

> The PLA takes as its objective to win local wars under the conditions of informationalization and gives priority to developing weaponry and equipment, to building joint operational capabilities, and to making full preparations in the battlefields.[111]

Unfortunately, how developed the force and infrastructure are is also difficult to discern from open sources. Reports have been made about a number of well-organized, deliberate cyber-attacks allegedly Chinese in origin. The Korean Information Security Agency stated that 10,628 cases of hacking had been logged in the first half of 2004 alone. In an attack in 2005, hackers were able to mine sensitive information from South Korean government computers. Officials stated that one of the attackers was identified as a student in a PLA-run school.[112] The nature of these attacks intimates that the PLA does have units training in IW and may even have some that are operational. Though this does

[110] DoD, *Annual Report,* pg 11, 16; Pillsbury, "China's Military Strategy," pg 10. In fact, Pillsbury writes that the information that can be found in the open sources about China's IW capabilities only scratches the surface of what they are truly capable of and conceiving.

[111] People's Daily Online, http://english.people.com.cn/whitepaper/defense2004/defense2004(2).html; Accessed July 31, 2005.

[112] The American Thinker, "The Approaching Chinese Cyber Storm" (July 21, 2005) http://www.americanthinker.com/articles.php?article_id=4665; Accessed on July 31, 2005.

not directly imply that units and equipment exists to prosecute EW against SATCOM, it does reveal that the Chinese are making strides in making their military IW ready.

As mentioned in the previous chapter SIGINT can be important to EW campaigns. China does posses significant ground, sea, and air-based SIGINT capabilities and has had previous success with space-based SIGINT.[113] In peacetime, these capabilities could enable the Chinese to better catalogue and identify civilian COMERSAT transmissions which could allow them to more easily identify military communications, and therefore which commercial satellites an adversary was using. Such a catalogue would be useful when developing a jamming strategy and target lists. In war, their SIGINT capabilities could enable them to better track satellite usage as for target identification and to assess whether their jamming efforts were being effective. While SIGINT is not necessary for jamming a satellite, without being able to discern what or who to jam, an EW campaign could easily lose its tactical and strategic usefulness.

It would not be difficult to believe that the Chinese do have some means to prosecute EW against SATCOM. The equipment necessary for "soft" IW, which attempts to disrupt or destroy information throughput, e.g. jamming and computer viruses, requires technologies in which the PRC are at least somewhat proficient and which are easier to conceal. This is not to say that the PLA's IW capabilities are completely developed. "Hard" IW, which attempts to destroy physical information infrastructure, on the other hand, often requires technologies in which the PRC has trouble demonstrating competency, and which foreign companies and nations may be unwilling to open up to the PRC.[114]

[113] Stokes, *China's Strategic Modernization*, pg 32-35. Globalsecurity, http://www.globalsecurity.org/space/world/china/geo-sigint.htm; Chinese Defense Today, http://www.sinodefence.com/c4i/command/default.asp.

[114] Two major legal issues have created roadblocks in the path of technological development for the PRC. The first is the arms embargo which was set in place by the G7 nations as a punitive measure for the Tiananmen Square Incident in 1989. The second is the lack of Chinese Intellectual Property Laws. Piracy and reverse engineering are widespread in China making many companies fear sharing technology that may be stolen without being able to take legal action.

The Potential Threat

By understanding the Chinese view of the iRMA, taking stock of their knowledge-base and means, it appears that the Chinese do have the will, skills, and equipment to implement IW against SATCOM in the form of jamming and possibly physically destructive ASAT. Though China appears to grasp all of the aspects of the Six Pillars, only Electronic Warfare and Physical Destruction are directly applicable to affecting SATCOM. Operations Security is more concerned with keeping information from the enemy, not disrupting the enemy's information. Psychological Operations and Deception can be manifest in the form of deception jamming, however, message and signal encryption combat this well.

In a practical sense, softer forms of C2W such as EW seem the most likely manner through which China may seek to exploit vulnerabilities in SATCOM. CNA could be effective but because they affect only a few aspects of SATCOM, e.g. the maintenance stations and teleports information gathering such as mining databases on exact locations of satellites may be its most valuable contribution. In order to successfully jam SATCOM China would need at a bare minimum satellite tracking and microwave transmission technologies as well as platforms from which to perform uplink or downlink jamming. As stated before, many of the MILSATCOM and commercial systems are locatable through open sources, some low-tech methods, and satellite tracking facilities which China does possess.[115] Microwave technology is also one of the few technologies that China has been able to develop indigenously and a skill in SATCOM has been demonstrated, both of which are critical to jam SATCOM. China has a capable SIGINT infrastructure with land, sea, and air-based sensors as well, making it easier to find the SATCOM targets and assess damage. Furthermore, it is unlikely that the large foreign investments into China's telecommunications infrastructure have not provided for a better understanding of modern communications systems.

[115] Chinese Defence Today, http://www.sinodefence.com/space/facility/default.asp.

While China is still unable to produce many high-end electronics itself, the components necessary for jamming systems can be purchased from the foreign companies present in China and are often benign enough to be purchased internationally. It also must be noted that though the PRC may have difficulty producing components, it does have the knowledge and capability to assemble devices such as computers and communications switches. This all suggests that the Chinese possess both the technology and know-how for jamming SATCOM.

The manner in which the Chinese may choose to deploy a jamming asset is speculative. The exact depth of knowledge and technology the Chinese have pertaining to SATCOM is unknown, but from the above assessments it may be possible to theorize what strategies and forms jamming would take on.

Of the two jamming strategies, uplink and downlink jamming, uplink jamming seems the easiest and more advantageous of the two. Downlink jamming requires a jammer to be positioned in between the satellite and the ground segment to which it is communicating. Aerial vehicles would fit well in this strategy. The Chinese are investing in UAVs which can be converted into very capable downlink jamming platforms.[116] However, with the widespread modernization the PLA is undergoing, the expendable nature of a UAV jammer may make their use too expensive. Other aircraft could be used for downlink jams, but doing so place the aircraft at unacceptable risk because of its nearness to the ground segment which may be a military unit.

Uplink jamming can be executed from a number of platforms, from manpacks to ground vehicles to ships and can provide mobility and covertness. Though attacking a satellite through narrow spot beams, or even area beams, may force the jammer to be deployed near enemy forces, the distances are not as close as those required by downlink jamming. Uplink jammers could also take advantage of Earth coverage beams from distance within the Chinese mainland.

[116] Chinese Defence Today, http://www.sinodefence.com/airforce/uav/default.asp.

Because the US military's SATCOM systems employ different AJ techniques, there is no one jamming method that would work for all of them. Of the MILSATCOM systems, power stealing appears to be the best method because few of UFO's and none of DSCS's transponders use onboard processing. As mentioned before, power stealing is a simple method and only requires a power source on the order of kilowatts. The current state of the Chinese SATCOM capabilities suggests that this method is well within their ability to implement. MILSATCOM's more robust EHF transponders on MILSTAR and UFO would be more difficult to disrupt and possibly too difficult for the Chinese. A jamming scheme such as barrage jamming or continuous wave jamming may be able to affect the EHF links, however a great deal of power would be required for barrage jamming to be effective and Spread Spectrum Frequency Hopping in the wide EHF band can probably handle CW. To reduce the power requirements for barrage jamming, the PRC could deploy closer to ground segments, but this again would be more dangerous and may provoke an aggressive US response. Narrowband jamming would probably have little effect to a frequency hopped EHF transmission as it would only cover a small portion of the wide bandwidth EHF can offer. China could deploy the use of a follower jammer, a device that scans the radio waves for a frequency that is being used and then jams it. This type of device, however, would require a considerable amount of complexity and power in order to scan for jam a message that is being hopped around hundreds of times a second.

COMERSAT is much more vulnerable to many forms of jamming. The lack of onboard processing, lack of AJ capabilities, and ease of tracking suggest that methods such as power stealing and CW could be successfully deployed. The wider beams that are used also could allow China to position jammers on the mainland. However, because COMERSAT is a civilian endeavor, jamming COMERSAT would disrupt more than just an adversary's military communications. Because COMERSAT leases usage to many users jamming it could bring about pressure from other nations and its own civilian sector, not to mention the PLA SATCOM that utilizes COMERSAT.

It should also be remembered that because jammers send out a signal, either to a satellite or a ground segment, they can also be found using SIGINT. Aerial downlink jammers, already vulnerable because of their proximity to adversarial forces, can be further threatened because of this. Uplink jammers deployed on the mainland have an advantage in that they can be concealed if pursued, can be mobile enough to evade some attacks, and can be defended by anti-air or other military forces. Ship-borne jammers, however, cannot hide so easily, but may be able to put up a fight if attacked.

To physically destroy elements of SATCOM, the Chinese would have to either strike the ground stations maintaining the satellites, the ground relaying transmissions stations, teleports, the user-end terminals, or the satellites themselves. Destroying the maintenance stations, ground relays, or teleports may prove very difficult and very risky because these elements are often outside the theater of conflict, in other nations, and, in the case of TT&C stations, can be located on US soil. While user-end terminals can be within striking range and within internationally or Chinese controlled locations, they are carried by military units as the name implies. Thus, China would be attacking military units directly.

Physically destroying a communications satellite is another option. While not the focus of this study, China does appear to have some of the technologies capable of performing simple forms of ASAT. For this reason it is given some breadth. However, because its capabilities in this regard are speculative, it is best to view this option with some reservation.

ASAT technology has caught the interest of the Chinese though their currently ability to hit a satellite is questionable.[117] Using directed-energy weapons (DEW) for ASAT strikes would require a considerable amount of power even for attacking satellites in LEO. Kinetic missile ASAT is also daunting as homing in and destroying a target that is moving several thousand kilometers per hour at distances equal to half the circumference

[117] DoD, *Annual Report*, pg 36; Globalsecurity, http://www.globalsecurity.org/space/world/china/asat.htm.

of the Earth can be an insurmountable task without a great deal of technology. However, China has demonstrated the ability to launch satellites, as well as humans, into space. Some methods of ASAT are as simple as launching a rocket into an intercept course with a satellite. Given China's ability to track satellites, which is often done by amateur civilians, and the public knowledge of orbital characteristics of many satellites, this should not be overlooked. A space-detonation nuclear weapon is also a valid option, though it is doubtful whether China believes affecting SATCOM warrants the use of such a weapon considering the international backlash it would receive.

These options however do not account for less straightforward ASAT methods.[118] Microsatellites could be deployed to parasitically attach themselves to target satellites, waiting for a time to detonate. Because microsatellites, weighing only a tenth of a regular satellite, and are so small, they could potentially be carried by larger satellites and deployed covertly before a conflict arose. Various other methods using space mines and other sleeper type weapons could be implemented as covertly with devastating effects. Some of these methods, however, require orbital control technology that may be beyond the Chinese abilities.

Another, much simpler method, would be to not require such much control. Instead of targeting a specific satellite, it would be theoretically possible to force a satellite to pass through a shrapnel field by launching hard particles, such as sand or metal fragments, into a satellite's orbit. The particles themselves would not necessary need to be moving very quickly because the satellite is. A collision between the particles and the fast moving satellite would essentially have the effect of sending the particles into the satellite at thousands of kilometers per hour. This could easily disable if not destroy a satellite. While such an attack method is speculative, China's competency in space launch and its desire to find Assassin's Maces suggest that this may not be a wholly unrealistic threat.

[118] Wilson, "Threats". Wilson has a thorough discussion describing various ASAT techniques.

ASAT also has interesting defensive properties. Depending on the ASAT method, it may also be possible for the Chinese to launch an attack from as deep in the mainland as they desire. This could significant reduce the ability of the US or another adversary from executing successful interdiction operations because of the anti-air defense that could be put in place. Also, once launched ASAT weapons become very hard to destroy and if deployed before a conflict, as with sleeper type weapons, it may be impossible to know if one was launched. If implemented correctly, ASAT attacks cannot be easily linked to a deliberate IW offensive because the harsh environment of space could also be blamed for satellite failures. This suggests that if China truly does have an ASAT capability, it would be hard to defend against.

Summary

Table 4 below summarizes the threat the China poses to the military's use of SATCOM. Threat here indicates an ability to take advantage of vulnerabilities that may exist. Because of the level of secrecy and opacity of the Chinese publications, the ratings in Table 4 should be thought of as conservative at best. Without a full understanding of how China intends on implementing EW and Physical Destruction, its true knowledge of SATCOM and ASAT, or its means to affect SATCOM, it is best to approximate China's capabilities.

Table 4 – Chinese Threat to SATCOM

SATCOM Systems	EW Threat	ASAT Threat
UFO	Medium - High	Medium
DSCS	Medium	Medium
MILSTAR	Low	Medium
COMERSAT	High	Medium

The EW threat China could pose to the UFO system are given a score of medium to high because China does possess the technology to implement power stealing and other forms of jamming which could exploit the lack of onboard processing and UHF links. However, the UFO system does use EHF links which would be difficult to jam. The DSCS system is scored as medium because power stealing and other forms of jamming such as CW could be implemented, but the system does have some AJ capabilities. The EHF transponders and onboard processing of the MILSTAR system would probably be difficult for the Chinese to affect with their current technological level, so the threat to MILSTAR is considered low. The Chinese do seem to have the necessary technologies to widely affect COMERSAT through EW, though it is questionable whether they would attack satellites that it and non-adversarial actors may be using. Because it is very likely that they could successfully attack COMERSAT, COMERSAT is scored as high.

The Physical Destruction threat China poses to the military's SATCOM is scored as medium. It is possible that China possess a developed ASAT that it does not publicize, but some of technologies needed to implement some of the forms described seem to be beyond China's reach. For this reason, Physical Destruction is scored as a medium. All the systems are scored as medium is because the methods to directly attack any satellite in orbit used are very similar. Armoring satellites is not a common practice and so all are assumed to be equally vulnerable. The only difference would be between GEO and lower orbiting satellites, because GEO satellites are much further away, but China has the launch capability to reach GEO.[119]

As shown, the Chinese pose a threat in the areas of Physical Destruction and EW. The PLA is wrestling with the concepts of IW, as theoretic as they may be, and developing insights that should not be overlooked. The PRC's technical ability is not yet on par with that of the US and cannot be relied upon to produce some of the high technology required for IW. However, as foreign investment continues to pour into China and knowledge trickles from the private sectors into the military, this will change. Many of the doctrines associated with the iRMA such as joint and precision warfare are

[119] Chinese Defence Toady, http://www.sinodefence.com/space/satellite/default.asp.

currently beyond the ability of the Chinese to implement, though it does appear to have some capacity for IW and C2W.

Of the Six Pillars, EW and Physical Destruction are the most influential in affecting SATCOM. The IW forte of the Chinese seems to be CNA, at least from open sources, but China's present status suggests that it could undertake an EW, and possibly an ASAT campaign against SATCOM.

While this finding is approximate at best, perhaps the two most important aspects of China's ability to partake in IW are its secrecy and its desire to develop asymmetric weapons with which to defeat a technologically superior adversary. If Assassin's Mace rhetoric and the evidence of some IW capability only hint at China's true ability as some authors believe, then it would be best to assume that China does indeed pose a threat to SATCOM.

Chapter 4

IW and the Taiwan Scenario

After considering the PRC's views of the iRMA, its growing knowledge-base, and probable means to successfully attack SATCOM, it appears that the PLA could possibly exploit vulnerabilities in the military's use of SATCOM. Knowing that vulnerabilities do exist and that the PLA could take advantage of them does not, however, indicate the level of threat this poses. Real life situations can include factors that may inhibit or enhance the potential threat of an adversary. In order to better demonstrate the level of this threat, a scenario in which the US responds to a PLA blockade of Taiwan was developed to provide a simple qualitative measurement. After assessing both an escalatory and non-escalatory IW campaign, this analysis finds that the PRC does pose an IW threat, though not as great as their capabilities alone may suggest.

This chapter is broken into four sections: the first describes the scenario being used, the second outlines the SATCOM systems that would be used by the US forces, the third describes China's IW options, and the final section details the results.

Scenario Background

If there is to be any US conflict with the PRC in the near-term, it would most likely concern Taiwan. The fragile US-PRC-Taiwan relationship is a complex one allowing for no easy solutions. Each country is tied together through ideology, economics, or treaties, yet the recently increased friction between the independence movements in Taiwan and "one China" rhetoric of the PRC are making a confrontation ever more likely. Though the US has not promised to aid the Taiwanese if it declares independence, it is hard to believe that it would not become involved regardless of who shoots first given its interests to protect its Taiwanese trade partner, maintain stability in the Far East, and resist China's territorial expansion.

The Department of Defense's (DoD) *The Military Power of the People's Republic of China 2005* describes several options the PLA may implement to reclaim Taiwan. Of the four force options which would draw in the US, this author believes blockading Taiwanese trade routes would be the most likely choice for several reasons. Firstly, the other options, Limited Force, Air and Missile Campaign, and Amphibious Invasion all create scenarios in which the US, not to mention other nations, could enter on the side of Taiwan. Secondly, violent actions could easily foment Taiwanese nationalistic resolve, making a successful campaign against Taiwan long, difficult, costly, and allowing more time for outside intervention. Thirdly, victory would not be a given. The Taiwanese are not without defense and cross-strait balance is not yet fully in favor of the PLA. Lastly, blockading seems offensive enough to put a strain on Taiwan, yet benign enough to make it difficult for the US to legitimate a use of force.

The DoD document describes the various forms of blockades the PRC might implement, from laying mines near ports to forcing ships to be inspected on the Chinese mainland before going to Taiwan to performing military exercises in the Taiwanese shipping lanes. However, because the PLA Navy (PLAN) has limited blue-water capabilities, it would only be able to implement some forms of blockade. Implementations that require the PLAN to remain closer to Taiwan may prove too challenging for the PLAN, while interdicting merchant vessels in the South and East China Seas would be the least strenuous for the PLAN.[120] In any scenario, the US's first military response would most likely be the deployment of one or two carrier groups.[121] The US may seek to

[120] DoD, *Annual Report*, pg 41.

[121] Though it is also likely that US Air Force elements would partake in the counter-blockade, naval forces would present the most visible statement to the Chinese and the world. Naval forces are also physically able to shield merchant vessels without firing weapons. An attack on the US Navy would then be of more importance as it would have a larger effect.

counter-blockade the PLAN or create a protected lane through which merchant vessels may travel.

The Navy's Use of SATCOM

How then does attacking SATCOM affect this situation? The US Navy (USN) uses SATCOM for a variety of forms of communications because the terrain over which it fights does not permit the use of landlines or LOS communications very often. SATCOM is used for communications between ships, submarines, land bases, and aircraft.[122] Because describing the SATCOM links between individual ships, submarines, and so on can become very lengthy, it may be easier to understand SATCOM as it is used tactically, operationally, and strategically.

On a tactical level, SATCOM is used for coordination using data, voice, and fax. It is also used for establishing and maintaining situation awareness. Because of the low bandwidth requirements to transmit these types of information, low data rate or narrowband systems, such as MILSTAR's LDR or UFO's UHF transponders, are often used.

Operationally, SATCOM is used to connect higher bandwidth, long-haul information, data, intelligence, voice, logistics planning, air tasking orders, video conferencing, battle damage assessment, operations planning, and C^2 information. These types of communication require higher bandwidths than SATCOM's tactical links so medium data rate systems, transmitting between 64 kbps and 1.544 Mbps, such as DSCS are used.

In a strategic sense, SATCOM is used to link data, intelligence from national and strategic sources, voice, CONUS logistic support, video conferencing, and Single Integrated Operational Plans (SIOPs). For bandwidth and secure reasons, strategic

[122] Globalsecurity, "Executive Summary of Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html.

information is transmitted over SHF, EHF, and COMERSAT links.[123] Other types of information that SATCOM carries which don't fall easily into any one category are video telemedicine, imagery distribution, video tele-training, as well as remote maintenance/ technical assistance.

Of the MILSATCOM systems, UFO would probably be used the most since it was created to replace the Navy's FLTSATCOM and has both UHF and EHF capabilities. However, for wider bandwidth operational and strategic information, DSCS would be the primary SATCOM provider. MILSTAR could be used for both LDR and MDR transmissions and would undoubtedly supplement the other systems.

However, there are two reasons why MILSATCOM could not provide all of the Navy's SATCOM needs. First, SATCOM is used very heavily by the military throughout the world; therefore the Naval forces in this conflict could not use all of MILSATCOM's available bandwidth. Second, the MILSATCOM systems are distributed around the world in order to achieve as much global coverage as possible, meaning within each system the satellites do not cover the same areas. Because of this, the Naval forces here simply would not have access to the aggregate bandwidth capacity of MILSATCOM.

Though it is uncertain exactly how much bandwidth beyond MILSATCOM the Navy would need, the facts that COMERSAT is widely used to make up bandwidth shortfalls, that the SATCOM usage of engaged units increases greatly over peacetime usage, and that leasing COMERSAT appears to be a regular occurrence in the Navy suggest that COMERSAT will also most likely be used.[124] Some of the COMERSAT systems that would likely be utilized are the Telstar, Inmarsat, Intelsat, and Iridium systems.[125] Telstar, Inmarsat, and Intelsat all provide GEO, narrow and wideband coverage

[123] Ibid.

[124] Chisholm, "Buying Time".

[125] Hunter C. Keeter, "Despite Delay, Navy Is Committed To Satellite Communication Program,"(Sea Power, March 2004). Found at Find Articles, http://www.findarticles.com/p/articles/mi_qa3738/is_200403/ai_n9371219#continue; Globalsecurity, http://www.globalsecurity.org/space/systems/inmarsat.htm; Globalsecurity, "Executive Summary of

to the South-East area of China, each with a few satellites.[126] These could be used for operational to strategic SATCOM. The Iridium system provides wide area, narrowband coverage over the area from many LEO satellites.[127] Because the Iridium only provides narrowband SATCOM, about 2.4 kbps, it could only be used for low data rate communications such as voice, fax, and teletype. The vulnerability of SATCOM in this scenario therefore covers the entire spectrum from the highly secure EHF links from UFO and possible MILSTAR, to the vulnerable UHF and COMERSAT links.

Alternatively, if the IW threat to SATCOM is deemed too high, the USN forces could fall back on other, non-SATCOM forms of telecommunication. However, to deploy forces BLOS, this would require the use of frequency bands, such as UHF, VHF, and HF, which do not have the bandwidth to transmit the wider band information that is becoming critical. USN forces could deploy in such as way as to maintain LOS to attempt microwave communication, though this may not be reliable on rolling seas nor does it allow information to be dispersed quickly. Having to remain in LOS could also severely impinge on its ability to effectively operate.

China's IW Options

As described in the previous chapter, China could best threaten SATCOM using EW and, for completeness sake, physically destructive methods. An EW campaign against SATCOM could call for the deployment of land-based, ship-based, and aerial jammers for uplink and downlink jamming, depending on the deployment strategy of the USN because distance from the jamming target can determine effectiveness. Such a campaign would also require the launching of a Signals Intelligence (SIGINT) and CNA campaign to

Commercial Satellite Communications (SATCOM) Report," http://www.fas.org/spp/military/docops/navy/commrept/index.html.

[126] Intelsat, http://www.intelsat.com; Inmarsat, http://www.inmarsat.com; Loral Skynet, http://www.loralskynet.com.

[127] Iridium Satellite, http://www.iridium.com.

properly map the SATCOM coverage areas for successful EW deployment and damage assessment.

If the PRC does blockade Taiwan by redirecting merchant vessel to the mainland first, the PRC could take advantage of the fact that US ships would have to be deployed near China's coast by using uplink jammers positioned within protected and concealed locations on the mainland. Doing so would allow them to inflict damage on the USN's SATCOM while remaining relatively safe. If designed correctly, uplink jammers may also be able to be deployed in fishing vessels, which may be able to approach the US ships with less suspicion. If the USN does use COMERSAT systems such as Iridium, downlink jamming may also be possible through the use of ground-based and ship-based platforms because their user-end devices tend to be omni-directional.

Physical Destruction in this scenario could be accomplished by destroying the ships, submarines, and aircraft in the area with SRBMs, IRBMs, anti-ship missiles, and a host of other means depending on the deployment strategy the US Navy uses. Ground bases in Taiwan and Japan, as well as the Pacific US territories and CONUS could also be fair game. Furthermore, China could launch an ASAT assault against the military and possibly even the commercial satellites orbiting over that sector of the world using primitive methods such as the ones mentioned in the previous chapter.

Striking preemptively before the Navy can enter into the conflict would also make it difficult for the US to come to the aid the Taiwanese. However, because the SATCOM spot beams can be narrow and a jammer must be within the main or side lobes of a satellite's antenna to harm it, EW would not be as effective as in this case. This would not be the case with ASAT against MILSATCOM. If used early enough, ASAT could slow the US entrance into the conflict by forcing them to cope with their communications problems. This may give the Chinese the advantage they need in forcing the Taiwanese to capitulate. Attacking MILSATCOM in this way could look very suspicious and escalate the blockade crisis into an open conflict. Thus, IW against SATCOM would be best used in-theater, near the Chinese mainland.

Selectively choosing to attack narrow or wideband SATCOM can be accomplished by using different jamming schemes or attacking certain satellite constellations. However, because wideband RF bands can be used for narrowband communications, e.g. MILSTAR's LDR EHF links, specifically attacking narrowband or wideband SATCOM could necessitate attacking both narrow and wideband satellites. Attacking the SATCOM of a specific vessel or unit can also be challenging as it would require the use of downlink jamming or direct physical attack. It may be easier therefore to attack specific SATCOM systems.

Each element of MILSATCOM is used for different yet important purposes. Which systems the Chinese attack will depend on how they wish to affect the USN's efforts. If UFO is attacked, tactical communication will be disrupted making it difficult for the USN to perform operations. If DSCS is attack, collaborative planning between carrier groups, CONUS based commands, and National Command Authorities (NCAs), logistics information, and some operating communication could be affected. Disconnecting the USN forces from the US in such a way may create a latency or confusion in deciding how the USN forces should operate, which could politically jeopardize the US's efforts in deterring China's blockade and may unnecessarily escalate the crisis. Attacking MILSTAR or COMERSAT will also produce problems comparable to that of a dysfunctional UFO or DSCS because they are used for similar types of communication.

Evaluating the Campaign

It cannot be known if the Chinese would try to maintain the blockade without escalating the crisis into a shooting war with the US, or whether they may act on the belief that its IW campaign would give them the chance to attack and defeat the USN forces. However, this author believes that, while an IW campaign may make operations and diplomacy more difficult, it would be highly unlikely that a campaign alone would enable the PRC to defeat the USN, and that PLA officials would probably agree. An evaluation of a non-escalatory and an escalatory IW campaign proved useful in understanding what level of threat the Chinese could pose. From this evaluation is appears that a non-escalatory implementation would allow the Chinese the most success because the US response in an open conflict may be prove insurmountable. However, even the success gained during a stand-off may not be decisive enough to halt the USN's efforts.

Non-Escalatory IW Campaign

As found in the previous chapter, China poses the greatest IW threat to SATCOM in the forms of EW jamming and possibly ASAT. However, some of the actions included in implementing these forms of IW may incite an unwanted escalation of the crisis. Using aerial downlink jammers, or ship-borne jammers may place PLA forces into a proximity to the USN forces that may provoke retaliation or produce a tenser diplomatic situation. Land-based jammers could be employed less provocatively, and because they could be possibly concealed or mobile, there would be less hard evidence of intentional jamming. Using land-based jammers would also allow the Chinese to defend their jamming positions, possibly deploy their jammers deeper into the mainland, and even within civilian populations. This would have the added advantage of deterring US interdiction strikes that may have negative diplomatic consequences.

Even so, the US would not be without its own defenses. Given the wide usage of SATCOM and its overall superiority, it is hard to believe that US would not perform Electronic Protection operations to counter such attacks with some success, such as performing SIGINT operations of own to avoid jammers or trying to position the satellite coverage beams so that it would be difficult for China's jammers to effect SATCOM. The presence of US forces could also make Chinese SIGINT operations difficult. The US forces could also deliberately disrupt them, or flood the skies with misleading "military transmissions", and thus prohibiting the Chinese from tracking SATCOM traffic well and taking full advantage of their jamming capabilities.

Physically attacking the ground segment of USN forces would be out of the question, as they could be directly linked to the Chinese and would be considered an act of war. Commencing ASAT operations, however, could be executed more covertly. While missile launches could be detected by US surveillance systems, it would be difficult to link the destruction or disruption of a SATCOM element to it. Furthermore, deploying sleeper type ASAT weapons prior to the blockade could allow the Chinese to destroy satellites with near impunity. [128] However, these systems require higher technologies than launching debris and may be outside of China's capacities.

COMERSAT, however, may be better protected from either EW or Physical Destruction attack than MILSATCOM because the satellites the USN forces are using could also be used by other states' as well as the PRC's own civilians and military forces. Attacking the control stations, teleports, and hopping stations for COMERSAT would also be seen as escalatory, and may even incite international retaliation. Downlink jamming, however, may still prove useful.

In all, it appears possible for the Chinese to widely affect almost every MILSATCOM system without instigating a shoot war. The USN forces could attempt to purchase more COMERSAT space, but they may find themselves competing with a commercial market that may not be very sympathetic to their needs, depending on COMERSAT providers that may not be able to quickly meet their needs, and having to reequip in order to use some COMERSAT systems. Thus, a non-escalatory IW campaign could prove very useful in maintaining a Taiwanese blockade and sowing doubt of the US's ability to protect Taiwan in the minds of US and Taiwanese officials alike. Such doubt, combined with economic strain could force the Taiwanese into capitulating.

[128] This is of course contingent on the Chinese not destroying the satellites in a manner that would suggest deliberate attack.

Escalatory IW Campaign

If the Chinese do not wish to maintain a peaceful blockade of Taiwan, their IW campaign can be wider in scale. The EW campaign would probably look quite similar to that of a non-escalatory campaign with the exception of using aerial and ship-borne jammers. However, the land-based jammers would need to be better defended, concealed, or mobile. The difference would come because of the US response. If a shooting war broke out, the USN would probably exercise much less restraint and aggressively go after jammers. This could include air interdiction and cruise missile strikes, as well as anti-ship and anti-air actions. Depending on the level of pressure the USN forces are able to leverage, the Chinese may find it difficult to jam USN forces as persistently as in a non-escalatory campaign, creating less than a total disruption of SATCOM and more of a nuisance.

Attacking SATCOM ground segments physically becomes a more applicable option in an escalatory campaign. However, for the Chinese to affect the ground segments, it must be able to attack ships, as well as bases on US territories and in CONUS effectively. The Chinese do possess a vast number of ballistic missiles, but they are not believed to be accurate enough to efficiently attack ships or conventionally strike bases in the US or its territories.[129] An air campaign against the USN forces could only be successful if the Chinese were willing to take many losses. In all likelihood, a ground segment strike may not prove any more useful to the Chinese given their outdated equipment, and the USN's superiority of force. It should also be noted that implementing this form of IW does not allow the Chinese to take advantage of the asymmetric nature of IW, but rather forces them to fight against US strengths.

ASAT attacks, however, would be more effective than in a non-escalatory campaign. No longer fearing the implications of a direct attack, the Chinese could launch

[129] Michael O'Hanlon, "Why China Cannot Conquer Taiwan," *International Security,* vol. 25, no. 2 (2000).

attacks against every MILSATCOM satellite orbiting over the area. Because they could do so from almost anywhere in China, launch facilities could be protected by the long stretch of enemy airspace USN air strikes would have to fly through to interdict them. Sleeper ASAT weapons deployed prior to the conflict would also prove far more effective, because their placement would have been unknown.

COMERSAT, again, may be better protected from either EW or Physical Destruction attack than MILSATCOM in this case. An aggressive USN campaign may make even downlink jamming problematic. Attacking the control stations, teleports, and hopping stations for COMERSAT may be beyond Chinese capabilities, and could easily incite international retaliation.

In summary, an escalatory IW campaign may not provide the Chinese with many more advantages of disabling SATCOM then a non-escalatory campaign. The major difference comes from the increased implementation of ASAT. Again, it is doubtful that the Chinese would attack COMERSAT in such a way because the satellites the USN uses may also be providing SATCOM for other states' as well as its own citizens and military forces. The strategies for jamming SATCOM would not be very different, though the US response would be, thus making an effective campaign more difficult. Physically destroying ground segments of SATCOM also appears to be too difficult for the Chinese, or not to their advantage.

Results

In either case, EW and Physical Destruction could produce a real impact on the US efforts. The US Navy's dependence on SATCOM for basic forms of communication could allow a successful SATCOM attack to hamper, though probably not stop, it from defending Taiwan. Without a connection back to commands in the US, the carrier groups would probably find it difficult to negotiate the conflict as its logistics and coordination efforts would be disrupted. However, the EP campaigns the US forces may be able to commence would probably make such disruptions only momentary.

A non-escalatory campaign seems to be more advantageous to the PLA than one which leads to open conflict for two reasons. First, a standoff between PLA and USN forces may make it diplomatically difficult for the US to aggressively enter Chinese airspace to interdict land-based jammers without facing irreparable consequences, and so would give a freer hand to the Chinese to disrupt the USN forces. Second, creating an open conflict with the US would force the Chinese to fight a war which they are not ready for, and would not allow IW to be the asymmetric edge it is believed to be. An IW campaign in other scenarios, such as the ones described by the DoD Report, may also prove less effective than the non-escalatory blockade because of these same reasons.

In conclusion, there are a number of vulnerabilities in the US's use of SATCOM stemming from its dependence on SATCOM and inherent system weaknesses of which the Chinese can take advantage. This qualitative analysis of a blockade scenario, which this author believes is the most likely near-term situation which would place the PRC across from the US, shows that China's IW capabilities may in fact be most threatening in a peaceful blockade because international politics would allow them to be used more asymmetrically than in an open conflict. Given the Chinese IW capabilities, it appears that the UFO's UHF and DSCS's SHF transponders present the greatest vulnerability in this scenario. Both of these are vulnerable to power stealing, and while DSCS does have some AJ capabilities, even temporary collapses in the operational communication, which would be of importance in a Taiwan crisis, could have large effects. However, a successful IW campaign would prompt a quick US EP response, suggesting that China's effectiveness would then be a function of how well it could thwart the US's countermeasures, which is questionable. Though COMERSAT is a choice target, the Chinese may inadvertently be harming their own efforts by attacking and so may choose not to attack it. ASAT appears to be of great concern because it can greatly affect the US efforts before and during any counter-blockade actions and because it may be difficult to deter. However, as noted in the previous chapter, the China's true ASAT capabilities are speculative, perhaps more so than its EW capabilities, and so the findings of its threat here should be viewed as cautionary and not descriptive.

Chapter 5

Conclusion

The purpose of this thesis was to evaluate the vulnerabilities that exist in the US military's satellite communications and the Information Warfare threat the People's Republic of China may pose to them. In order to do so, this thesis evaluated the vulnerabilities that exist in the military's use of SATCOM, assessed the PRC's ability to threaten SATCOM, and then made a qualitative analysis of the effect of a PRC attack on the military's SATCOM during a blockade of Taiwan. As a result, this thesis posits that the PRC can present a real threat to the military's use of SATCOM.

Though the level of this threat must be conservatively judged as moderate because of the speculative nature of some of China's capabilities, it must be recognized that this threat will grow with time. With every foreign military system and the rights to build them, with every foreign joint commercial venture, and with every foreign technology factory the PRC acquires, the more able it is to create its own high-tech systems.[130] The establishment of a national C^3I network, its high rate of ISR satellite launches, and its development of a new MILSATCOM series suggests that the PRC is becoming increasingly familiar with the technologies necessary to implement a wide spectrum of Information Warfare tactics.[131]

[130] Sumner Lemon, "Report: Lenovo-IBM Deal to Face Review" (PC World; January 28, 2005) Accessed from http://www.pcworld.com/news/article/0,aid,119488,pg,1,RSS,RSS,00.asp. The Lenovo Group, China's largest PC-maker and of whom the Chinese government owns the largest stock share, recently acquired IBM's PC division which some believe will be a boost the modernization of the PRC and PLA; Accessed August 2, 2005; DoD, *Annual Report*, pg 23-25. Russia continues to be the PRC's largest supplier of foreign arms which have included the advanced Su-30MK2 fighter, Sovremennyy-class destroyer, and Kilo-class submarine though Britain and Israel have also sold technology. These past and continuing acquisitions have consternated those who fear a cross-Strait balance that favors the PLA.

[131] Chinese Defence Today, (February 6, 2005) http://www.sinodefence.com/c4i/command/military_communications.asp; Accessed August 2, 2005; DoD,

Implications for US SATCOM

The US military's satellite communications remain in a precarious situation. Its dedicated systems, UFO, DSCS, and MILSTAR are only able to provide minimal, semi-secure links, and the commercial systems that are used to fill the bandwidth shortfall are vulnerable to most forms of noise jamming. The systems being launched in the near future will have little impact in stemming this problem, further pushing the military to depend on unreliable commercial sources. Even this source may not be a solution as the much lower cost of sending information through fiber optic cable could stagnate the growth of the COMERSAT market.[132] There are only two solutions to this problem: build and launch secure satellites that will better fill the gap, or reorient our forces to depend less on satellite communications. These solutions, however, are not without their own drawbacks.

In order for new satellites to satisfy the needs of the military, the satellite constellation would have to be enormous. Using MILSTAR-II satellites as a model, the system would need approximately 48 satellites and would cost $38.7 billion dollars.[133] Even if the satellite system wouldn't be operational until 2015, it would cost $3.87 billion annually, equating to 5% of the FY06 Defense appropriations budget.[134] If split up among the services, it would cut 14 %, 5.6 %, and 5.1 % out of the Army, Navy, and Air Force appropriations budgets respectively. Initial procurement cost, however, would not be the

Annual Report, pg 35-36.From 2004-2006 the PRC intends to launch 10 satellites a year and reach an orbital total of over 100 satellites by 2010. It also hopes to launch 100 more satellites by 2020.

[132] Erhhard, "Standing in the Strategic Bandwidth Gap,".

[133] MILSATCOM Joint Program Office, http://www.losangeles.af.mil/SMC/MC/MILSTAR.htm; Accessed July 10, 2005. Though MILSTAR is the most costly of the systems, it was chosen here because it is also the most robust.

[134] Department of Defense. Office of the Secretary of Defense (Comptroller), "Procurement Programs (P-1)" *Department of Defense Budget Fiscal Year 2006*, http://www.dod.mil/comptroller/defbudget/fy2006/fy2006_p1.pdf; Accessed July 10, 2005.

total cost of the new system as with every passing year satellites in orbit get closer to needing replacement. This is a costly solution.

Other alternatives may be more viable. If the military could utilize an air breathing system costs could be cut dramatically. A network of high altitude aircraft, fitted with the requisite equipment could service large areas by way of wide beams. The beams could be narrow enough that jammers would need to be near the receiving antenna to uplink jam, assuming active nulling is performed. The communications payloads could also be upgraded and, if need be, repaired much easier than on a satellite.

One drawback to this alternative is that the aircrafts cannot provide a stationary platform, requiring users to constantly adjust their antennas to stay connected. While this is not entirely problematic, mobile tactical users may find that having to continually seek a "satellite" creates unacceptable gaps in their information throughput. Specific flight patterns could mitigate this drawback, but it can heighten another. Aircraft can be found and shot down much easier than satellites allowing the Physical Destruction aspect of EA to take on a larger role. Specific flight patterns would only make it easier to take advantage of the aircrafts' nearness to Earth.

Much of today's bandwidth demand use comes from streaming video data. Video conferencing can be a helpful tool in decision-making but it is not a critical one. Voice conferencing supplemented with a non-streaming picture capability for sharing plans pictorially could greatly reduce the burden on MILSATCOM. However, the many UAV's of the FCS are also planned to provide streaming video to their users creating the necessity for large amounts of bandwidth.

A quickly updatable digital representation of the combat situation is also growing as a battlefield necessity, and is all but written into doctrine with the plans for FCS and the Joint Visions. Obtaining Situational Awareness was one of the purposes of digitalization and is fundamental to gaining Decision Dominance. It is unlikely that the use of streaming video or the need for quickly updating Situation Awareness will change for the better, especially as more forces are equipped to handle such information. Creating better data compression methods and efficient usage of bandwidth may be the only ways to cope with the information throughput needs.

Looking Towards the Future

In conclusion, the use and control of information is becoming a fundamental aspect of the way the military fights. Therefore, the communications links over which the information flows must be secure, reliable, robust, and ubiquitous. Satellite communications do offer some advantages in bringing this capability to the military's forces, but the current systems which are used are lacking and will most likely continue to lack in security.

The only options the military has then are to create the bandwidth necessary for its communications or reduce its use of them. The monetary and political issues that would surround the quick construction of a dedicated military satellite system to fill the need, and the drawbacks of using alternative sources of bandwidth suggest that the architecture of MILSATCOM should be given serious thought. Realistic measurements of bandwidth need and supply must be performed before the military can structure its forces around such systems.

Drawing back from such a heavy use of information would be almost, if not completely impossible. Information is so central to the military's current and future doctrines that a major shift in the way defense decision-makers think about warfare would have to occur. In fact, after all the rhetoric permeating the defense world about information, stepping away from the ubiquitous use of information would be the equivalent of saying that the information RMA is really not a revolution after all. This is unlikely to happen.

The way the military uses satellite information is vulnerable to Electronic Attack in the form of noise jamming, as well as anti-satellite attack. This vulnerability has both a technological aspect and a political one. Technologically, the military's use of SATCOM is vulnerable because some of the MILSATCOM systems are less than secure, and because the commercial systems that are used were not designed to survive in an environment of deliberate EA. Politically, SATCOM is vulnerable because of the dependence of inadequately protected commercial and military systems which stems from a disconnect between the military's bandwidth needs and its ability to supply it, as well as a misperception of the threats the iRMA can produce. Until considerable thought, trade-analysis, and architecture redesign are completed, the military's use of satellite communications will continue to be a critically weak link of the transforming forces.

This thesis has shown that the PRC poses a moderate threat to the use of SATCOM. This suggests that technologically similar states, more modern states, and proficient non-state actors can pose a threat as well. The distinction between state, military, and individual is an important one in the discussion of IW because of the power leveling nature of IT.[135] A vulnerability may not only be threatened by another nation's military, but it can still be exploited by smaller groups or individuals. As the world becomes smaller through globalization and informationalization, the number and potency of threats becomes greater. If the vulnerabilities that SATCOM and other national IT systems have are not addressed thoroughly and quickly[136], both our security forces and our society may find themselves prey to entities such as the People's Republic of China, and even individuals, who identify the US as an enemy and have the desire to enjoy the asymmetric advantages Information Warfare offers them.

[135] Armistead, *Information Operations*, pg 32.

[136] Armistead, *Information Operations*. This source assesses the vulnerabilities in a number of governmental department and agencies and finds that better EP measure need to be taken.