

SPACE POWER IN SMALL WARS:
THE END OF ASYMMETRIC ADVANTAGE?

BY
MAJ KELLY D BURT

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY

MAXWELL AIR FORCE BASE, ALABAMA

JUNE 2010

APPROVAL

The undersigned certify that this thesis meets masters-level standards of research, argumentation, and expression.

JOHN B. SHELDON (Date)

JAMES D. KIRAS (Date)

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University.

ABOUT THE AUTHOR

Major Kelly Burt was commissioned through the Reserve Officer Training Corps, University of Nebraska at Omaha, in 1996. Graduating from Undergraduate Space & Missile Training in 1997, he went on to serve as a Peacekeeper Missile Combat Crew Member at F.E. Warren AFB, WY. Following weapon system instructor duty at Vandenberg AFB, he completed the Space Weapons Instructor Course at USAF Weapons School in 2004. He served in a variety of duties at the Air Forces Southern Combined Air Operations Center at Davis-Monthan AFB before being selected as a Legislative Fellow in 2007. Major Burt served on the Air Staff prior to beginning SAASS in 2009. Major Burt is a master space operator. He has a bachelor's degree in Political Science from the University of Nebraska at Omaha and a master's degree in International Relations from the University of Troy. In July 2010, Major Burt was assigned as a plans officer in United States Cyber Command's Directorate of Plans and Policy.

ACKNOWLEDGMENTS

I would like to acknowledge several people without whose support I would not have made progress. I want to thank Air Force Space Command's Strategic Plans, Programs, and Lessons Learned directorate for their interest in my ideas and their willingness to sponsor my research over the past year.

I especially want to thank my thesis advisor for his insight and mentorship over the past year. Everyone should be so fortunate to have as wise and patient an advisor throughout the journey that is SAASS. I would also like to thank my thesis reader for reviewing the thesis while providing comments and food for thought throughout the duration of this project.

Most importantly, I want to express my sincere appreciation to my fiancée and to my family for their love, support, and motivation throughout the past year. Although she and the rest of the family were many miles away, it always felt as though they were right there by my side.

ABSTRACT

This study seeks to examine the relationship between space power and the conduct of irregular warfare. The author begins the examination by exploring key definitions associated with space power and irregular warfare in order to establish a vocabulary for further analysis. Next, the author evaluates satellite communications as they are exploited in irregular warfare activities. The results of this evaluation show that irregular warfare appears to increase demand for satellite communications, with some significant implications. Next, the author evaluates space-enabled surveillance and reconnaissance in irregular warfare activities. The results of this evaluation show that the US's asymmetric advantage in reconnaissance is diminishing due to a number of factors. Next, the author evaluates space-enabled positioning, navigation, and timing services in irregular warfare activities. The results of this evaluation show that PNT is becoming exceedingly difficult to exert control over without jeopardizing US interests. The final section of the study evaluates space control in irregular warfare activities, concluding that control is made all the more complex and difficult to achieve in an irregular warfare environment.

CONTENTS

Chapter	Page
DISCLAIMER	ii
ABOUT THE AUTHOR	iii
ACKNOWLEDGMENTS	iv
ABSTRACT	v
INTRODUCTION	1
1 SETTING THE STAGE FOR DISCUSSION	6
2 SATELLITE VOICE COMMUNICATIONS AND SATELLITE- ENABLED NETWORKS	30
3 SURVEILLANCE & RECONNAISSANCE	54
4 POSITIONING, NAVIGATION, & TIMING	78
5 SPACE CONTROL	98
CONCLUSION	121
BIBLIOGRAPHY	130

Introduction

One should bear in mind that there is nothing more difficult to execute, nor more dubious of success than to introduce a new system of things: for he who introduces it has all those who profit from the old system as his enemies, and he has only lukewarm allies in all those who might profit from the new system.

Niccolo Machiavelli
The Prince

Irregular warfare has experienced a revival in Western military professional and academic circles since the beginning of the 21st century. For the first time in over a generation, American military forces are beginning to think and write about insurgency and counter-insurgency.¹ As a consequence of the ongoing conflicts in both Iraq and Afghanistan, the US and its allies have dusted off some timeless thought and lessons on guerilla warfare, small wars, counter-insurgency, military operations other than war, and a number of other non-conventional warfare ideas. The contemporary emphasis on irregular warfare follows nearly three decades of doctrine based upon rapid and overwhelming conventional military capabilities in the air, on land, at sea, and now in space and cyberspace. Has irregular warfare made America's technology-driven

¹ The preface of Field Manual 3-24, Counter-insurgency (published in 2006) noted that no formal counter-insurgency doctrine had been promulgated by the US Army in the last twenty years, nor had any been promulgated by the US Marine Corps in the last twenty-five years. A generation in this case can be regarded as the traditional twenty-to thirty-year professional military career. See Field Manual 3-24/Marine Corps Warfighting Pub 3-33.5, *Counter-insurgency* (Ft Leavenworth, KS: US Army Combined Arms Center, 2006), preface.

advantage in battle irrelevant, or can conventional capabilities be applied to enhance the efforts of the US and its allies in an irregular warfare setting? What does irregular warfare portend for space power? Conversely, how does space power impact the conduct of irregular warfare? The US and its allies have taken steps to reorient the military instrument of power towards irregular warfare. Now is the time to consider what irregular warfare and space power imply for one another.

Carl von Clausewitz, one of the great military strategic intellects known to the Western world, established that all wars are fundamentally political acts.² Conventional and irregular warfare share the political nature of war as the nexus of their respective conflicts, but beyond this point, they diverge significantly in characteristics.

Conventional warfare is focused on the leadership of the opposing nation-state and its military forces. Successful conventional warfare or “victory” entails military defeat of the opposing nation-state’s military forces to deliver capitulation by the leadership of the nation-state. At the most fundamental level, irregular warfare is focused on winning the support of populations, rather than opposing nation-state military forces and their national leaders. Success in irregular warfare is entirely subjective; it may be difficult at best to define victory, let alone attain it.

Land power may be regarded as the primary means of seeking influence over a contested population, but it is not the only means of

² Carl von Clausewitz, *On War*, ed. & trans. by Michael Howard and Peter Paret, (Princeton, NJ: Princeton University Press, 1976), 87-88.

influence. Maritime power, airpower, and cyber power are also relevant to the conduct of irregular warfare because each can participate in the competition for influence over populations in its own unique way.

However, each “sub-instrument” or component of military power must be applied with an appreciation of the differences between irregular warfare and conventional warfare. Space power should be no exception.

Indisputably, space power has become an integral part of the Western way of war. Because of space power, modern military forces can operate abroad and accomplish objectives through connectivity, information superiority, and precision. Even though the means to apply force from space against insurgents and terrorists does not exist today, space power still plays a crucial role in irregular warfare through its ability to enhance the collective capabilities available to the Joint Force Commander.

Although it does not appear that even the best-resourced insurgents and terrorists operate in the domain of space on their own, space control is still of great significance in irregular warfare. The thesis of this paper is that traditional concepts of space power need to be re-examined within the context of irregular warfare so that space power is optimized for the demands of irregular warfare, as well as conventional warfare.

The US and its allies have enjoyed asymmetric advantages in space power against the opponents they have faced since the end of the Cold War, but many of those asymmetries are diminishing. Space-enabled products and services are now widely available to interested users

around the globe, and these products and services do not necessarily require investments in spacecraft or space support infrastructure. The lowered price of admission to space power for nation-states and non-state actors carries with it some significant implications. Insurgents and terrorists are able to apply space power against relevant populations in some innovative and disturbing ways. Space superiority must be redefined within the context of irregular warfare, where space power is more equitably distributed among opponents. The proliferation of space power also offers benefits in irregular warfare. Relatively low-cost means now exist for governments to build and enhance their legitimacy through space-enabled products and services. Fledgling partner-nation military forces can also improve their combat capability against insurgents and terrorists through competent advisory efforts for space-enabled products and services.

This thesis is composed of five chapters. Chapter 1 sets the stage for discussion of irregular warfare and space power by briefly examining the conventional understanding of military space operations and their function within warfare, as well as presenting an overview of irregular warfare. Irregular warfare will be defined and bounded for the purposes of this paper. Four components of irregular warfare have been chosen for study: insurgency, counter-insurgency, counter-terrorism, and building partnership capacity.

The remaining chapters examine specific elements of space-enabled warfare as well as space control and the application of those products and services within irregular warfare activities. Chapter 2 examines the use of satellite communications and networks by the US and its allies, as well as its opponents, to conduct irregular warfare. Satellite voice communications are differentiated from satellite-based data networks to provide additional clarity. Chapter 3 examines the use of space-enabled surveillance and reconnaissance for irregular warfare activities. Civil and commercial remote sensing capabilities are approaching national security levels in terms of their quality. These sensing capabilities can be used to obtain to access denied areas, and they are widely available. Chapter 4 examines the use of space-enabled positioning, navigation, and timing for irregular warfare activities and the challenges posed by the universally available Global Positioning System service. Chapter 5 explores space control for the purpose of conducting irregular warfare activities. Irregular warfare activities impose significant difficulties on attaining and maintaining freedom of action while denying the same to an opponent. The thesis closes with a discussion of the implications of irregular warfare for space power and recommendations to optimize space power for the conduct of irregular warfare.

Chapter 1

Setting the Stage for Discussion

The first, the supreme, the most far-reaching act of judgment that the statesman and commander have to make is to establish...the kind of war on which they are embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature.

Carl von Clausewitz

Agreeing on terminology is the first step towards discussing irregular warfare, space power, and strategy. A few definitions are presented to set the stage for the rest of the paper. The next step in establishing the relationship between irregular warfare and space power is to address both as they individually relate to doctrine and strategy. It is here that gaps and seams are evident between irregular warfare and space power. In an effort to begin bridging those gaps and seams, it is worthwhile to briefly examine the impact of space power on warfare in general. Finally, the impact of irregular warfare on space power will be examined as a lead-in to a series of explorations of the component parts of irregular warfare and space power.

Defining Terms

The Department of Defense has defined irregular warfare as “a violent struggle among state and non-state actors for legitimacy and

influence over the relevant populations.”¹ For the purposes of this paper, the term “irregular warfare” is used in a manner identical to Air Force doctrine. Irregular Warfare refers collectively to insurgency, counter-insurgency, counter-terrorism, and building partnership capacity. Each activity will be described in more detail below. One or more of these activities may take place simultaneously within the same context (such as NATO operations in Afghanistan) making a general description valuable for simplicity’s sake.² Irregular warfare includes other activities in addition to insurgency, counter-insurgency, counter-terrorism, and capacity building, but these four activities are where American military forces are expected to apply the bulk of their efforts.

What makes irregular warfare “irregular” is the focus of its operations: relevant populations.³ The purpose of irregular warfare is to gain and maintain some degree of control or influence over those populations primarily through informational methods, but also through economic and military methods. In contrast, the focus of conventional warfare is the leadership and the military forces of an opposing nation-state. The purpose of conventional warfare, in most cases, can be thought of as coercion of the opposing national leadership to fulfill

¹ Department of Defense Irregular Warfare Joint Operating Concept, version 1.0, 11 Sep 2007.

² Understandably, counter-insurgency operations do not occur independent of an insurgency.

³ Department of Defense Irregular Warfare Joint Operating Concept, version 1.0, 11 Sep 07.

See also James D. Kiras, “Irregular Warfare,” in *Understanding Modern Warfare*, David Jordan, et al. (Cambridge: Cambridge University Press, 2008), 229-232.

political objectives through the military defeat of their forces by one's own military forces. Irregular warfare and conventional warfare need not happen independently; an irregular warfare scenario may include episodes of conventional force-on-force combat, and conventional state-on-state wars may also include an irregular warfare subtext. The 2006 Israel-Hizbollah war has been described as a "hybrid war," with both irregular and conventional elements to the conflict.⁴ It can be difficult at best to clearly distinguish between conventional and irregular warfare. The policy maker and the strategist may have to conduct a painstaking search for adversary motivations and goals, as opposed to capabilities, in order to make the distinction.

The activities that constitute irregular warfare deserve some additional clarification before proceeding further. An insurgency is an organized movement aimed at the overthrow of a constituted government through the use of subversion and armed conflict.⁵ Conversely, counter-insurgency is an organized effort that uses military, para-military, political, economic, and informational actions to defeat an insurgency.⁶ For the purposes of this thesis, the militant group Hizbollah will be

⁴ John J. Kruzal, "Hybrid War to Pull US in Many Directions." *American Forces Press Service*, 4 May 2009, <http://www.defense.gov/news/newsarticle.aspx?id=54186>
See also Col Margaret S. Bond, "Hybrid War: A New Model for Stability Operations in Failed States," US Army War College Strategy Research Project, (Carlisle Barracks, PA: US Army War College, Mar 2007) 1-3.

⁵ Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.

⁶ Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.

treated as an insurgency vice a terrorist group, although it can be argued that the movement possesses characteristics of both, as do many other terrorist groups and insurgencies throughout the world.

Terrorism is the calculated use of unlawful violence or threat of violence to inculcate fear.⁷ The use of terrorism is intended to coerce or to intimidate governments or populations in the pursuit of goals that are generally political, religious, or ideological in motivation. Although insurgencies may employ terrorism in pursuit of their objectives, terrorist groups have traditionally stopped short of overthrow of a government as a goal. Counter-terrorism is an organized effort to prevent, preempt, or where deemed necessary, punish the actors that employ terrorism in pursuit of their political, religious, or ideological goals. Like insurgency and terrorism, counter-insurgency and counter-terrorism activities may be difficult to differentiate in practice.

Building partnership capacity activities seek to prevent the emergence of insurgencies and terrorists and to prepare the environment for future irregular and/or conventional activities by enhancing the security capabilities of partner nation-states. Perhaps the ideal time to conduct building partnership capacity activities is before insurgencies or organized terrorism emerge, but these activities may also occur in the midst of counter-insurgency and counter-terrorism activities.

⁷ Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.

The Department of Defense defines space power as “the total strength of a nation’s capabilities to conduct and influence activities to, in, and from space to achieve its objectives.”⁸ Some qualification of the DoD space power definition is necessary however, because the capability to conduct and influence activities to and from space to achieve objectives is no longer exclusive to nation-states. Both states and non-state actors can now use space power to the extent that they can conduct and influence activities from space to achieve their objectives. Space power has become more diffuse and less of an asymmetric advantage to space-faring nation-states. Space power includes national security, civil, consortia, and commercial space products and services as well as space-based and terrestrial-based infrastructure. One often overlooked element is trained personnel who enable all of the elements of space power, and who themselves constitute space power.

If policy makers and strategists have an appreciation for what space power is, then they can consider those attributes that make a nation-state or a non-state actor a space power. Michael Sheehan proposes a useful model for classifying states as space powers.⁹ Although Sheehan’s model is nation-state centric, it is adaptable to non-state actors who exploit space power. Tier One space powers consist of those actors “with dedicated space capabilities on the cutting edge of

⁸ Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.

⁹ Michael Sheehan, *The International Politics of Space* (New York: Routledge, 2007), 107.

technology.” Tier Two space powers “develop and use dual-purpose space systems for both military and civilian purposes.” Tier Three actors “lease or purchase space capabilities” from Tier One or Tier Two providers. Even a non-state actor could exhibit capabilities that would classify it as any combination of Tiers, much as Hizbollah has taken on characteristics of Tier Two space power.

Strategy is perhaps the most difficult term to define. Because the words strategy and strategic have been applied so often to so many things, they carry many different meanings to its students and practitioners. At least for the purposes of this paper, Colin Gray’s simple, yet profound definition offers a sound point of departure to discuss strategy and all things strategic: “strategy is the use that is made of force and the threat of force for the ends of policy.”¹⁰ Gray acknowledges an intellectual debt to Clausewitz’s own definition of strategy as “the use of engagements for the object of the war.”¹¹ The campaign designer and the planner require a reasonably clear concept of strategy in order to link irregular warfare activities and objectives to space power. Strategy within irregular warfare makes use of force or the threat of force to affect populations. Space power can be regarded as a means or a type of force for the ends or objectives of policy.

¹⁰ Colin S. Gray, *Modern Strategy* (Oxford: Oxford University Press, 1999), 17.

¹¹ Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 128.

Having defined a few key terms and concepts within the arenas of irregular warfare, space operations, and military strategy, it is appropriate now to turn to doctrine and strategy as they pertain to irregular warfare and space power. It is here that we can hopefully begin to see how the theoretical bases of irregular warfare and space operations begin to be translated into practice by policy makers and strategists.

Doctrine

Political scientist Barry R. Posen offers that military doctrine deals with *military* means to accomplish *military* ends (author's emphasis).¹² Doctrine for military operations other than war was understandably bland as the Vietnam conflict faded from American military institutional memory in the 1990's and the early years of the 2000's. In its place, theories of maneuver and "shock and awe" warfare emerged with an emphasis on speed, overwhelming force, and information superiority.¹³ Military doctrine has been slow to re-adapt to the challenges of irregular warfare. No doctrine for the application of space power to irregular warfare has been written, at least not formally. The landmark counter-insurgency manual for the US Army and Marine Corps was published in

¹² Barry R. Posen, *The Sources of Military Doctrine* (Ithaca, NY: Cornell University Press, 1984), 14.

¹³ Frederick W. Kagan, *Finding the Target: the Transformation of American Military Policy* (New York: Encounter Books, 2006). See also Bousquet, Antoine. *The Scientific Way of Warfare: Order and Chaos on the Fields of Modernity*. (New York: Columbia University Press, 2009).

late 2006,¹⁴ nearly five years after the US invaded Afghanistan to topple the Taliban in the opening campaign in the Global War on Terror and three years after Iraq succumbed to insurgency following the US invasion of that country.¹⁵ Although the manual is intended for those who conduct counter-insurgency activities on the ground, the document is sufficiently broad in scope to be of value to counter-insurgency forces outside of the Army or the Marine Corps. Still, the manual is likely to be insufficient to guide the efforts of sailors, airmen, space- or cyber-operators to plan and conduct counter-insurgency activities.

The Air Force published new irregular warfare doctrine in August 2007, several months after the Army/Marine Corps manual. The document captures a theory of airpower in irregular warfare, and it benefits from historical lessons from Afghanistan and Iraq as well as Corum and Wray's definitive work on airpower in "small wars."¹⁶ However, Air Force irregular warfare doctrine does not provide much in the way of detail for space power in irregular warfare. Air Force Doctrine Document (AFDD) 2-3, *Irregular Warfare*, includes parts of two pages out of its 88-page total that are devoted to the application of space power to

¹⁴ Field Manual 3-24/Marine Corps Warfighting Pub 3-33.5, *Counter-insurgency* (Ft Leavenworth, KS: US Army Combined Arms Center, 2006).

¹⁵ For additional detail on the genesis of Field Manual 3-24/Marine Corps Warfighting Publication 3-55.5, see Thomas E. Ricks, *The Gamble* (New York: Penguin Press, 2009).

¹⁶ James Corum and Wray Johnson, *Airpower in Small Wars* (Lawrence, KS: University of Kansas Press, 2003). Corum and Johnson survey a century of airpower application in insurgencies, counter-insurgencies, and stability operations, which they collectively term "small wars."

irregular warfare.¹⁷ Perhaps the closest thing to doctrine for building partnership capacity that the Air Force has is AFDD 2-3.1, *Foreign Internal Defense*. It is important to note that foreign internal defense (FID) activities focus on bilateral efforts to address threats within a nation-state's border, while building partnership capacity activities take on a more regional or multi-lateral focus against internal and external threats.¹⁸ The difference may seem minor, but policy makers and strategists should avoid losing sight of the multi-lateral imperative of building partnership capacity in pursuit of bilateral activities. To the extent that existing FID doctrine can be applied to building partnership capacity activities, AFDD 2-3.1 includes parts of two pages out of its 98-page total that are devoted to building capacity through space power.¹⁹ Both documents refer readers interested in space operations to AFDD 2-2, *Space Operations*, and AFDD 2-2.1, *Counterspace Operations*, both of which preceded Army and Air Force irregular warfare doctrine, and do not mention of irregular warfare or its associated activities.

Neither joint nor service space operations doctrine has much to offer for strategists seeking to optimize space power in an irregular warfare setting. AFDD 2-2 states: "space power should be integrated

¹⁷ Air Force Doctrine Document (AFDD) 2-2, *Irregular Warfare*, 1 Aug 2007, 17-18.

¹⁸ Air Force Doctrine Document (AFDD) 2-3.1, *Foreign Internal Defense*, 15 Sep 2007, 1-2. See also: Department of Defense Irregular Warfare Joint Operating Concept, version 1.0, dated 11 Sep 07; Air Force Doctrine Document (AFDD) 2-2, *Irregular Warfare*, 1 Aug 2007, 27

¹⁹ Air Force Doctrine Document (AFDD) 2-3.1, *Foreign Internal Defense*, dated 15 Sep 2007, 49-50.

throughout joint operations as both an enabler and a force multiplier.”²⁰ This is an important statement for military space power doctrine, but it avoids the complex nuances of irregular, conventional, and hybrid warfare. Both joint and service-level space operations doctrine have evolved over time as new command and control concepts for space force enhancement and space control have developed. Space operations doctrine appropriately emphasizes the themes found in National Space Policy: that space is vital to US interests and it is a contested environment where friendly capabilities must be defended and adversary capabilities may need to be denied.²¹ Doctrine and rhetoric must not lose sight of the fact that conflicts still occur in the terrestrial environment.

Strategy

It is important to formulate general theories of victory and to record experience as doctrine; however, writing doctrine must not be confused for developing strategy. For all of their insights, contemporary doctrine and lessons from past insurgencies and counterinsurgencies cannot account for the unique circumstances of terrain, culture, motivations, and many other contextual factors in each irregular warfare situation.²²

²⁰ Air Force Doctrine Document (AFDD) 2-2, *Space Operations*, dated 27 Nov 2006, 1.

²¹ US National Space Policy, dated August 31, 2006 <http://space.au.af.mil/histpol.htm>. The Obama administration has not yet superseded the 31 Aug 06 policy.

²² Kiras, “Irregular Warfare,” 265.

Justin Kelly and Mike Brennan offer that conventional warfare has tended towards strategies of annihilation and exhaustion (or attrition) since the Industrial Age, where nation-states attempted to out-maneuver and destroy one another, or to wear one another out in order to force the opponent's capitulation. Annihilation appears to have proven wholly unsuitable in irregular warfare settings where the support of the people is the central aim.²³ The insurgent and the terrorist have proven highly adept at blending into the population to support themselves and to defend themselves against attack. Counter-insurgent and counter-terrorist forces experience very few opportunities where the adversary can be annihilated free of collateral damage implications. Rather than continuing potentially disastrous attempts to annihilate the adversary in Iraq and Afghanistan, coalition military forces have tended towards strategies of inducement. Strategies of inducement eschew political control of the population in order to provide basic security and to win over the population "by giving them things that the enemy cannot."²⁴ If coalition forces bend too heavily towards inducement and away from annihilation, their efforts may be placed at risk by the insurgent or the terrorist able to operate with great impunity.

Kelly and Brennan suggest Admiral J.C. Wylie's theory of strategy offers a more appropriate central strategic principle than inducement in

²³ Justin Kelly and Mike Brennan, "Looking for the Hedgehog Idea," *Australian Army Journal*, Vol VII, No. 1, Autumn 2010, 41.

²⁴ Kelly and Brennan, "Looking for the Hedgehog Idea," 49.

irregular warfare. Wylie, a veteran of surface combat in the Pacific in World War II and an observer of the Chinese revolution and the unfolding war in Vietnam, stated that the aim of warfare is “some measure of control over the enemy.”²⁵ Kelly and Brennan add that the concept of control and “the man on the scene with a gun” as the guarantor of control still apply in irregular warfare, because “only a military can establish control and until it is established, democracy, the economy, the rule of law, policing and social progress must wait. The establishment of control has two aspects: one is focused on the removal of the enemy’s ‘man with a gun’, while the other is focused on putting our soldier in that man’s place.”²⁶ Although Kelly and Brennan give short shrift to military forces as inducers, strategies of control and inducement would seem to echo the ideas of classic counter-insurgency theorist David Galula, who posited that it was necessary to control the population prior to supporting (or inducing) them.²⁷ Control and support would seem to suggest a less lethal, less damaging strategy of exhaustion (or attrition) where both the will of the adversaries and the will of the population were worn down over time to accept control.

²⁵ Wylie, J.C. *Military Strategy* (Annapolis, MD: Naval Institute Press, org. ed. 1967. rep. ed., 1989), 65-72.

²⁶ Kelly and Brennan, “Looking for the Hedgehog Idea,” 51.

²⁷ David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger, org. ed., 1964; rep. ed., 2007) 55-56.

See also: David Galula, *Pacification in Algeria: 1956-1958* (Santa Monica: Rand, org. ed. 1963, rep. ed., 2006), 246.

Space power can play a significant role in irregular warfare strategy, because the elements of space power can contribute to the general aims of control and inducement. Strategy for an irregular warfare scenario should seek to control and induce, taking advantage of all of the means available to it, including space power, in order to achieve the desired ends. Irregular warfare strategies should not neglect the value of space power to friendly and adversary forces, and to building partnership capacity.

Why Does Space Power Matter to Irregular Warfare?

There are three notable reasons why space power matters to the conduct of irregular warfare activities. First, the Western way of war depends upon spacepower, even in the conduct of irregular warfare activities. Second, insurgents and terrorists have learned to exploit space power on the opposing side of coalition irregular warfare activities. Third, space power can enhance the conduct of irregular warfare through support to the population, as well as control of the population.

Space power has become a critical enabler in the western way of war. Space power theorist Steven Lambakis notes that military forces “look to space to help accomplish routine and vital peacetime and wartime military missions...the skillful exploitation of space translates into greater efficiency in communications, navigation, and remote

sensing and it allows the armed services to reach out to any point on the globe in a reliable and timely manner.”²⁸

Space power delivers satellite communications and satellite-enabled networks to deployed forces around the world, facilitating command and control of people and drones. Space-enabled surveillance and reconnaissance can provide access to denied areas in order to support an information advantage for US forces and their allies. Space-based missile warning permits friendly forces to react rapidly to adversary ballistic missile attack with active or passive defensive measures. Space-based weather assets deliver mission-critical products to maneuver forces. Space-enabled positioning, navigation, and timing services afford friendly forces the ability to be precise with their effects against the adversary. Space control provides friendly forces with an information advantage in the domain of space by building awareness of phenomena and activities in that domain in order to support action in the terrestrial environment. Space control also holds the adversary’s own space power at risk by threatening his infrastructure on the ground and on orbit, as well as the linkages among elements of his infrastructure.

American military dependence on space power is not diminished in irregular warfare activities; rather, dependence on space power increases. Airmen deployed in support of land power irregular warfare

²⁸ Steven Lambakis, *On the Edge of the Earth: The Future of American Space Power*. (Lexington, KY: University of Kentucky Press, 2001), 32.

activities have noted: “there is a lower threshold of pain with losing space products and services in irregular warfare than there is in conventional warfare.”²⁹ Satellite communications and satellite-enabled networks often serve as the only tether between commanders and dispersed forces in an austere environment.

AFDD 2-3 mentions: “intelligence activities are often an enabler of operations in conventional warfare, but they may constitute the primary function of space capabilities in irregular warfare.”³⁰ Surveillance and reconnaissance from space cannot take the place of human intelligence activities that are conducted among the contested populations, but they can make valuable contributions to an overall understanding of the operating environment and its challenges. Surveillance from space also supports ballistic missile warning and environmental monitoring. Force tracking, or the ability to locate and identify one’s own forces in the operating environment, is becoming increasingly important as a means to avoid friendly fire incidents and to respond to threats to those forces.

The degree of precision available to friendly forces through space-enabled positioning, navigation, and timing becomes especially important in a competition for the support of the population. Weapon systems and munitions that are precise enough to be able to limit collateral damage

²⁹ Lt Col Stuart Pettis, Chief, Strategy & Doctrine, Headquarters Air Force Space Command, interview by the author, 18 Feb 10. Pettis served as an Air Liaison Officer to the 25th Infantry Division and as an Expeditionary Air Support Operations Squadron commander in Northern Iraq in 2007.

³⁰ Air Force Doctrine Document (AFDD) 2-3, *Irregular Warfare*, dated 1 Aug 07, 17.

take on a much greater significance in counter-insurgency and counter-terrorism activities conducted amongst the population.³¹ Dispersed forces under attack may enjoy no other means of support than what GPS-aided munitions can provide, making satellite-enabled positioning, navigation, and timing a matter of life and death in an engagement. Precision weapons do not eliminate risks to one's own forces or to non-combatants, but they do reduce them. Reflecting on the hazard of indirect fires in irregular warfare, one senior Air Force officer intimated that "every bomb becomes a liability...sometimes they do need to be dropped, but there is a cost attached to dropping, and it can become steep."³²

Space control takes on a greater urgency in irregular warfare. Space situational awareness and space control prevention/protection activities, linked to the commander's appreciation of the irregular warfare situation, may have life-saving implications to friendly forces in the terrestrial environment. Space control-negation may also play a significant role in irregular warfare by holding the adversary's ability to exploit space power at risk, when it is feasible to do so. The Israelis conducted space control activities in their 2006 war against Hizbollah by targeting the Al-Manar satellite television station for destruction.

³¹ Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York: Alfred Knopf, 2007). Retired British General Rupert Smith describes "war amongst the people" at length in *The Utility of Force*.

³² Director, Air Component Coordination Element (ACCE) to CJTF-82, ACCE meeting, Feb 07.

Insurgents and terrorists have learned how to exploit space power without the benefit of a robust state-based space support infrastructure. A NATO-assigned space operator fresh from service in Afghanistan remarked: “in some cases, insurgents were much more savvy in using space than the coalition forces- because they had to be.”³³ Insurgents and terrorists use satellite communications and satellite-enabled networks. They also exploit surveillance and reconnaissance from space. Insurgents and terrorists exploit space-enabled positioning, navigation, and timing. In a very limited manner, they can also conduct space control activities. In many parts of the world, satellite telephones are standard equipment for insurgents and terrorist groups.³⁴ If at first the use of a satellite phone does not appear to be an example of space power, consider that such phones are routinely used for command and control functions by dispersed forces, not unlike the manner in which dispersed friendly forces use satellite communications on the ground, at sea, or in the air. Insurgents and terrorists are also capable of exploiting surveillance and reconnaissance from space in some novel ways.

³³ Peter B. de Selding, “US Officer: Secrecy Among Coalition Forces Hinders Use of Space Assets in Afghanistan,” *Space News*, 10 May 2010, A-1.

³⁴ Two of several examples are the use of Thuraya phones by the Dec 08 Mumbai, India attackers and by Al Qaida in the Islamic Magreb throughout Mali, Chad, and Burkina-Faso.

Indrajit Basu, “Mumbai terrorists aided by technology,” *United Press International*, Dec 02, 2008.

http://www.upiasia.com/Security/2008/12/02/mumbai_terrorists_aided_by_technology/9520/

Karin Brulliard, “Moderate Mali a barrier to radical Islam,” *The Washington Post*, December 20, 2009. Reprinted in Durham Herald-Sun, Available at http://www.heraldsun.com/pages/full_story/push?article-Moderate+Mali+a+barrier+to+radical+Islam%20&id=5287506.

Insurgents have used the popular Google Earth mapping application to target friendly military facilities, which has prompted the Department of Defense and the United Kingdom's Ministry of Defence to request that images of some installations in the Google Earth database be obscured.³⁵

Insurgents and terror groups now exploit space-enabled positioning, navigation, and timing services. Terrorist groups recognize the value of positioning arms and other contraband.³⁶ Insurgents have also begun to look into GPS-aided vehicles and munitions.³⁷ It is not unreasonable to assume that operations are coordinated using GPS-derived timing, through receiver-equipped satellite phones or recreational GPS receivers. Insurgents and terrorists can conduct space control to a limited extent by preventing and protecting their limited space power. Satellite phones can be constantly switched among users to frustrate surveillance efforts. Satellite television signals can be moved. By using the same positioning, navigation, and timing service as friendly forces, insurgents and terrorist groups can frustrate efforts to deny that service. The adversary's exploitation of space power complicates matters for

³⁵ Peter Eisler, "Google Earth Helps Yet Worries Government," *USA Today*, Nov 7, 2008. Available at: http://www.usatoday.com/tech/news/surveillance/2008-11-06-googleearth_N.htm

Thomas Claburn, "U.S. Military Restricts Google Maps," March 7, 2008. Available at: <http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=206902500>.

³⁶ Karin Brulliard, "Moderate Mali a barrier to radical Islam," *The Washington Post*, December 20, 2009. Reprinted in Durham Herald-Sun, Available at http://www.heraldsun.com/pages/full_story/push?article-Moderate+Mali+a+barrier+to+radical+Islam%20&id=5287506.

³⁷ Anthony H. Cordesman, *Preliminary "Lessons" of the Israel-Hezbollah War* (Washington, DC: Center for Strategic and International Studies, April 2009) 5.

friendly forces, which must attempt to protect space power for the population while negating space power for the adversary.

Space power can enhance the conduct of irregular warfare in positive ways. The US and its coalition partners should choose to support the population by building partnership capacity. Security assistance, foreign internal defense, and even foreign military sales can enable a partner state to operate alongside the US or to defend itself partly through space power. Consistent with the constraints of amended versions of the Foreign Assistance Act of 1961 and the US Export Control Act of 1976, the US can build space power within partner nations through attaché, military group, and liaison groups.³⁸ Foreign internal defense activities or “space advisory” missions can be conducted through space power to open an added dimension of cooperation with partner nation military forces. One often-overlooked element of space power, personnel trained to exploit products and services, can make a tremendous impact in this arena. Space advisory does not necessarily require development of space support infrastructure to elevate partnering nation-states to Tier Two space powers. Partnering nation-state forces can be trained to enhance their operations through satellite communications and satellite-enabled networks, space enabled surveillance and reconnaissance, space-enabled positioning, navigation,

³⁸ Security Assistance is a collection of programs authorized by law by which the US provides equipment, training and other activities to foreign countries. See Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.

and timing, as well as limited space situational awareness and space control prevention and protection efforts. These potential efforts would require a fresh look at existing national security foreign disclosure policies, something arguably overdue in an era of alliance and coalition operations in conventional and irregular warfare. Foreign military sales consistent with existing US law offer possibilities for increased interoperability with a partner nation through its burgeoning space power. These are just a few general connections between space power and the conduct of irregular warfare; more will be explored in detail in later chapters. If it is reasonable to conclude that space power is a vital component of irregular warfare, then it is worthwhile to explore how irregular warfare can impact the application of space power in return.

Why Does Irregular Warfare Matter to Space Power?

Irregular warfare impacts space power in two principal ways: it challenges traditional concepts of space superiority, and it also creates an imperative for space power to be employed as a whole-of-government effort. Irregular warfare challenges the conventional concept of space superiority. Space superiority has been defined as “the degree of dominance in space of one force over another that permits the conduct of operations by the former and its related land, air, maritime, space and special operations forces at a given time and place without prohibitive

interference by the opposing force.”³⁹ The clause of “dominance in space” appears to give a domain-centric focus to this definition of space superiority. Irregular warfare challenges domain-centric space superiority. Friendly forces may be dominant in the domain of space, but also be unable to deny space power to insurgents and terrorists in the terrestrial environment without incurring collateral damage.

Unlike joint space doctrine, Air Force doctrine defines space superiority in a manner not unlike air superiority: “that degree of advantage of one force over another that permits the conduct of operations at a given time and place without prohibitive interference by the opposing force.”⁴⁰ This is perhaps a more inclusive concept of space superiority because it is effect-centric, as opposed to domain-centric. In either case, space operators should resist the temptation to think only of actions in space the domain of space when they consider what is necessary to attain and maintain space superiority.

Irregular warfare also demands that space power become a whole-of-government effort, rather than a military effort with civil and commercial augmentation. Without question, space power is a sub-component of both a nation’s military and economic instruments of power. Therefore, space power serves as an enabler to the nation’s diplomatic and informational instruments of power as well. Irregular

³⁹ Joint Publication (JP) 3-14, *Space Operations*, 9 Jan 2009, GL-8.

⁴⁰ Air Force Doctrine Document (AFDD) 2-2, *Space Operations*, 27 Nov 06, 7.

warfare demands a whole-of-government approach to counter-insurgency and building partnership capacity that also involves the diplomatic, informational, and economic instruments of national power. A military effort may be necessary and important to achieve control within a counter-insurgency scenario, but in order to support a population, such efforts are most effective when combined with those other instruments of national power.⁴¹ In a recent essay for *Foreign Affairs*, Secretary of Defense Robert M. Gates noted that “the US Government must get better at what is called building partner capacity: helping other countries defend themselves or, if necessary, fight alongside US forces by providing them with equipment, training, or other forms of security assistance.”⁴² Dr. Gates did not single out any one component in his exhortation to “get better,” but his point is instructive for building partnership capacity through space power. By employing space power not only to build partnership capacity through military capabilities, but also to enhance governance, national security policy makers and military strategists may further facilitate the use of diplomatic and informational instruments of power to forestall or defeat insurgencies and terrorism.

One way to build partnership capacity is through Provincial Reconstruction Teams (PRTs). PRTs offer possibilities for the application of space power to enhance government legitimacy and influence in

⁴¹ Field Manual 3-24, *Counterinsurgency*, 15 Dec 06, 2-1.

⁴² Hon. Robert M. Gates, “Helping Other Defend Themselves,” *Foreign Affairs*, May/June 2010, 1.

ungoverned spaces through interagency action. They were conceived as a means to extend the reach and enhance the legitimacy of the central government into the provinces of Afghanistan at a time when most assistance was limited to government officials, ministries, and departments in the nation's capital.⁴³ The PRT concept has been extended to Iraq, and it may survive US action in both countries to become a tool of choice in future irregular warfare scenarios. As US combat action has drawn down in Iraq, Army space forces have turned their attention towards space-enabled product support to PRTs.⁴⁴ At some point, space power could be employed in a more participatory manner if PRTs were called upon to establish turn-key space support infrastructure in remote locations to improve governance and commerce.

⁴³ Field Manual 3-24, *Counterinsurgency*, dated 15 Dec 06, 2-12.

⁴⁴ Slideshow, "34th Infantry Division Mission Rehearsal Exercise Space Ops After Action Report" dated 5 April 09, slide 6, obtained from US Army Space & Missile Defense Command/ Army Forces Strategic (USA SMDC/ARSTRAT) Future Warfare Center.

Summary

To establish a relationship between irregular warfare and space power, it is necessary to first define terms and set the stage for further exploration. This chapter framed irregular warfare, space power, strategy, and doctrine as the points of departure for a more detailed discussion of each throughout the remainder of the paper. Up to this point, this thesis has discussed space power in very general terms. In the following chapters, the relationship between irregular warfare activities and space power will be explored by examining space force enhancement in more detail, beginning with satellite communications and satellite-enabled networks.

Chapter 2

Satellite Voice Communications and Satellite-enabled Networks

The enemy is in fact more networked, more decentralized, and operates with a broader commander's intent than any twentieth century foe we've ever met.

General John Abizaid
former Commander,
US Central Command

Satellite communications have become so ubiquitous and so ingrained into modern telecommunications that it is easy to overlook them as elements of space power. For the purposes of this paper, satellite communications will be divided into satellite voice communications and satellite-enabled networks to better describe this broad category of space power. Satellite voice communications and satellite-enabled networks contribute to modern military operations in very profound ways. The impact that satellite voice communications and satellite-enabled network capabilities have on irregular warfare may be even more significant than the impact they have on conventional warfare. Satellite voice communications and satellite-enabled networks challenge hierarchical organizations to appreciate and adapt to the largely scale-free organizational behavior of insurgent and terrorist networks. The relative US advantage in technology may be diminishing as military

forces increasingly rely on the same types of services from many of the same providers as do insurgents and terror groups.

This chapter opens by exploring satellite voice communications and satellite-enabled networks in some detail before proceeding to a discussion of the significance of satellite communications in modern combat. The chapter then examines satellite voice communications and satellite-enabled networks as they affect insurgency, counter-insurgency, counter-terrorism, and building partnership capacity.

Satellite Voice Communications

Satellite voice communications permit parties to communicate with one another beyond the line-of-sight of radio signals, or where landline connectivity through a publicly operated telephone system or dedicated line is limited to non-existent. Satellite voice communications include personal communications through satellite telephony and broadcast net communications through satellite-enabled radio. Satellite communications offer a number of advantages to users over terrestrial radio and landline voice communications.¹ Users are able to communicate from fixed locations or on the move, regardless of where in the world the user is in many cases.² Satellite service does not traditionally obey district, provincial, or state boundaries. Satellite voice

¹ Bruce R. Elbert, *Introduction to Satellite Communications* (Boston: Artech House, 2nd Edition, 1999), 8-12.

² Geosynchronous or “geostationary” communications satellites are unable to repeat signals at latitudes above 60 degrees N or below 60 degrees S. Communications quality may also be impacted if the user(s) are operating well outside of the satellite’s effective “footprint.”

service, when conducted between two users, may be independent of terrestrial infrastructure or transit highly developed terrestrial infrastructure several thousands of miles away from either user. Satellite voice communications handsets continue to decrease in price, while offering a number of familiar ground-switched mobile cellular telephone features, perhaps the most significant feature being Global Positioning System (GPS) positioning and timing, which will be discussed in its own right in Chapter 4.³

Satellite-enabled radio is anticipated to possess most of the same advantages of personal satellite voice communications, without many of its limitations.⁴ Satellite-enabled radio is also intended to allow users to operate independently from terrestrial infrastructure, with the added advantages of broadcast to multiple users, and in many cases, the ability to encrypt communications. A number of states have operated military satellite radio systems for some time, and this technology is beginning to permeate the commercial telecommunications industry. At least one major commercial satellite provider offers a satellite-enabled radio or “netted communications” solution based on its existing personal communications infrastructure to interested customers.⁵

³ Elbert, *Introduction to Satellite Communications*, 8-12.

⁴ The author has coined “satellite-enabled radio” to avoid confusion with commercial satellite radio services and equipment.

⁵ Thuraya advertises a “netted comms” solution with broadcast capabilities. For more information, see: <http://www.thuraya.com/solutions/customized-solutions/nettedcomms>

The advantages inherent in satellite voice communications make a compact satellite-enabled radio a strong candidate for use in search and rescue and personnel recovery operations. DoD has already fielded a more than one generation of successful satellite-enabled survival radios across each of the services.⁶ DoD has also undertaken an ambitious effort to replace its existing air, land, and maritime tactical radios with a family of more modern satellite-enabled radios that feature data as well as voice capabilities.⁷ Other Western military forces doubtless will follow suit in the coming years with their own satellite-enabled radio systems.

Satellite-enabled Networks

Satellite-enabled networks facilitate the transmission and receipt of data, as opposed to facilitating voice communications. Data in this instance may include text, graphics, pictures, audio, or video. Data may also include commands to, and feedback from, unmanned systems. Satellite-enabled networks generally assume one of two forms: point-to-point or point-to-multipoint.⁸ Point-to-point networks include dedicated links, circuit-switched links, or packetized links. Control of an unmanned system is likely to use a dedicated link, while other data transactions, such as Internet access or private network access are likely

⁶ Boeing Network and Tactical Systems. "Combat Search and Evader Locator Overview," Available at: <http://www.boeing.com/defense-space/ic/csel/index.html>

⁷ Joint Tactical Radio System Program Executive Office, *JTRS Fact Sheet*. Available at: <http://jpeojtrs.mil/> See also: Space and Naval Warfare Systems Command, "JTRS: Why is it Important?" Available at: <http://enterprise.spawar.navy.mil/body.cfm?type=c&category=27&subcat=79>

⁸ Elbert, *Introduction to Satellite Communications*, 78-80.

to use circuit-switched or packetized links. There are two major categories of point-to-multipoint networks: broadcast networks and interactive networks. Satellite television and the DoD Global Broadcast Service and are prime examples of broadcast networks, while data-capable satellite-enabled radios are interactive networks.⁹ Very-small aperture terminal (VSAT) networks may fall into either category of point-to-multipoint network. Like satellite voice communications, satellite-enabled networks may be man-portable or vehicle-transportable, independent of local terrestrial infrastructure, and agnostic of district, provincial, or state boundaries.¹⁰ Compared to terrestrial data networks, satellite-enabled networks are relatively simple to establish, expand, and modernize for users.¹¹

The Significance of Satellite Communications in Modern Warfare

One of the earliest applications envisioned for earth-orbiting satellites, as expressed in the late 1940's RAND Corporation study *Preliminary Design of an Experimental World-Circling Spaceship* was communications.¹² A radio signal could be directed at a satellite on orbit to be repeated or "bounced" back to another point on the earth's surface. Multiple repeats between the earth's surface and the satellites would

⁹ Space and Missile Systems Center, *Global Broadcast Service Factsheet* Available at: http://www.losangeles.af.mil/library/factsheets/factsheet_print.asp?fsID=7853&page=1

¹⁰ Elbert, *Introduction to Satellite Communications*, 8-12.

¹¹ Elbert, *Introduction to Satellite Communications*, 88-90.

¹² Rick W. Sturdevant, "Giving Voice to Global Reach, Global Power: Satellite Communications in US Military Affairs 1966-2007," *Harnessing the Heavens*, ed. by Paul G. Gillespie and Grant T. Weller, (Chicago: Imprint Publications, 2008), 191.

even permit users to communicate with one another from opposite locations on the earth's surface. A single satellite could also offer an exponential increase in broadcast coverage as compared to a terrestrial radio transmitter. The coverage of a terrestrial military transmitter is on the order of some 15 millionths of a percent of the Earth's surface; however, a transmitter from a geostationary satellite can cover approximately forty-two percent—some three million times more.¹³ For military commanders concerned with managing nuclear forces deployed across the globe, satellite communications became an indispensable element to exercise command of those forces. Successive generations of satellite communications technology offered users ever-increasing amounts of bandwidth, while allowing multiple users to share resources and miniaturizing user equipment.

By the time the US and its coalition partners had ousted Saddam Hussein from Kuwait in 1991, satellite communications proved to be integral to expeditionary warfare. The United States Space Command repositioned a second-generation Defense Satellite Communications System spacecraft to supplement two other satellites already providing coverage to Southwest Asia.¹⁴ The dramatic success of the coalition in Desert Storm, supported in part by satellite communications and other elements of space power, inspired several observers to speculate that

¹³ Michael R. Frater and Michael J. Ryan, "A Taxonomy for Space Operations," *Journal of Battlefield Technology*, Vol 8, No 2, Jul 2005, 3.

¹⁴ Sturdevant, "Giving Voice to Global Reach," 197.

fundamental changes had taken place in the character of warfare. A new doctrine of warfare emerged that treated military forces as a network of sensors and precision attack platforms promised to lift the fog of war and rapidly deliver victory to US forces. Historian Rick Sturdevant notes: “while crises or conflicts during the latter decades of the twentieth century caused surges in demand for commercial satellite communications, military planners realized that earnest application of a network-centric warfare doctrine at the beginning of the twenty-first century meant demand for satellite communications, even in peacetime, would consistently exceed the capacity of dedicated military satellite communications systems.”¹⁵

Perhaps one of the most important applications of satellite-enabled networks in modern warfare is the ability to control remote sensors and disseminate the data that they collect. Lt Gen William Shelton, former commander of Fourteenth Air Force, commented in a 2008 interview: “satellite communications are an essential part of how we employ unmanned aerial vehicles (UAVs). They allow UAVs to operate well beyond line-of-sight. In fact, we are flying UAVs from stateside locations. This greatly reduces the footprint in theater, not just for the crews, but also for the support those crews require. Satellite communications also enable real-time dissemination of the data collected by UAVs, allowing a

¹⁵ Sturdevant, “Giving Voice to Global Reach,” 204.

wide range of users access to the critical data in real-time.”¹⁶ In addition to collecting data, UAVs, or Remotely Piloted Vehicles as they are now called, also conduct attacks against ground targets.¹⁷ These “hunter-killer” platforms rely upon the same satellite-enabled network architectures that their unarmed counterparts do in order to fly and employ munitions against targets on the ground.

US military dependence on commercial satellite communications continues apace. According to the US Army Space and Missile Defense Command, over 70 percent of military communications were provided by commercial satellites during the invasion phase of Operation Iraqi Freedom.¹⁸ At present, satellite communications industry experts estimate that 80 percent of all satellite bandwidth that the Department of Defense uses is purchased by the Defense Information Systems Agency from companies such as Inmarsat, Intelsat, and Iridium.¹⁹ Sturdevant adds: “as military demand for bandwidth grew from the early 1990’s to the early 2000’s, military satellite communications capabilities increased but failed to keep pace with demand. That situation compelled the Department of Defense to rely more than ever on commercial satellite

¹⁶ Louis M. Arana-Barradas, “The Space Link: Airmen Provide Out-Of-This-World Capabilities” *Airman* July/August 2008.

¹⁷ US Air Force, *Air Force Fact Sheet: MQ-9 Reaper*, dated November 2009. Available at: <http://www.af.mil/information/factsheets/factsheet.asp?id=6405>

¹⁸ Ann Roosevelt, “Space Control Vital for Future Operations, General Says.” *Defense Daily*, November 3, 2003, 11-12.

¹⁹ Rosenberg, Barry. “DOD’s reliance on commercial satellites hits new zenith.” *Defense Systems*, Feb 25, 2010. Available at: <http://defensesystems.com/Articles/2010/03/11/Cover-story-The-Satcom-Challenge.aspx?Page=1&p=1>

communications.”²⁰ The percentage of DoD satellite communications needs that are fulfilled by commercial vendors is expected to climb above 90 percent in the near future as unmanned aerial vehicles and other intelligence, surveillance, and reconnaissance systems begin transmitting in high definition video, which will require even more bandwidth.²¹

Satellite Voice Communications in Insurgency

Satellite voice communications have been observed as a favored means of communication among insurgencies throughout the world. The appeal of satellite voice communications is not difficult to see: they do not rely on local infrastructure; they are able to operate on the move; they do not obey political boundaries; and their equipment is often small and easy to conceal. While terrestrial cellular phone calls can be made on-the-move (where coverage exists), they can also be monitored since such calls pass through base stations within a country. Satellite phone services do not interconnect with local operators, often making it difficult for interested parties to trace the origins and termination points of satellite phone calls.²² Satellite phones in large numbers were reportedly

²⁰ Sturdevant, “Giving Voice to Global Reach,” 204.

²¹ Barry Rosenberg, “DOD's reliance on commercial satellites hits new zenith.” *Defense Systems*, Feb 25, 2010.
<http://defensesystems.com/Articles/2010/03/11/Cover-story-The-Satcom-Challenge.aspx?Page=1&p=1>

²² Indrajit Basu, “Mumbai Terrorists Aided by Technology,” United Press International, published: December 02, 2008.
http://www.upiasia.com/Security/2008/12/02/mumbai_terrorists_aided_by_technology/9520/

in use by the Taliban as early as 2003. That same year, the Taliban began using satellite phones imported from the Arabian Gulf, which were serviced by Thuraya, a regional satellite communications provider based in the United Arab Emirates. At the time, a number of Taliban leaders operated under the assumption that the Central Intelligence Agency had bugged Thuraya phones for sale within Pakistan.²³

There is a widely held assumption about insurgencies and terrorist groups that suggests that contemporary groups typically organize and behave as networks, as opposed to hierarchies.²⁴ Modern communications technology, a number of network theorists suggest, is what permits these networked organizations to behave as decentralized nodes.²⁵ Physicist Albert-Laszlo Barabasi offers that many types of networks- even organizational ones- can sometimes exhibit what is termed scale-free behavior, where there is no limit to the number of connections among nodes that they represent in total.²⁶ An insurgent group may exhibit scale-free behavior where a cadre of insurgents is able to form connections with one another and with recruits. Because of the number of connections that can be established, scale-free networks are

²³ Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age*. (Westport, CT: Praeger, 2009), 170.

See also: Ahmed Rashid, *Descent into Chaos* (New York: Penguin, 2008), 250.

²⁴ John Arquilla and David Ronfeldt, eds., *Networks and Netwars: the Future of Terror, Crime, and Militancy* (Santa Monica, CA: Rand, 2001).

²⁵ Arquilla and Ronfeldt, *Networks and Netwars*, 2001.

²⁶ Albert-Laszlo Barabasi, *Linked* (New York: Plume, 2003), 207-208, 219-224.

highly resistant to random failures.²⁷ The death or arrest of one insurgent or even an entire insurgent group does not cause the movement to collapse, because in a scale-free insurgent network, the other cells duplicate or triplicate the connections of the lost operators. It is important to note that not all insurgent or terrorist networks organize in the same manner: each network manifests its own unique strengths and weaknesses. An organization's networked behavior may be observable through the ways in which the network communicates.

Satellite Voice Communications in Counter-insurgency

Satellite voice communications are an important element of counter-insurgency. Counter-insurgency forces operate in austere environments almost as a rule. Regardless of how they organize, these forces must import communications capabilities in order to function. For units that disperse among the population in order to conduct counter-insurgency, satellite communications may be the only reliable means of communication with the chain of command and with fellow units due to the line-of-sight limitations of terrestrial radio communications. As one combat-seasoned airman has noted, "Some of the FOBs (Forward Operating Bases) are like Fort Apache- they depend on SATCOM almost exclusively to communicate."²⁸

²⁷ John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (Hoboken NJ: Wiley & Sons, 2007) 101.

²⁸ Lt Col Stuart Pettis, Chief, Strategy & Doctrine, Headquarters Air Force Space Command, interview by the author, 18 Feb 10.

One US Special Forces officer has advocated what could be considered a scale-free network approach to organizing US forces in counter-insurgency operations.²⁹ Major Jim Gant's Tribal Engagement Strategy involves decentralizing Tribal Engagement Teams to conduct classic "clear, hold and build" counter-insurgency activities across Afghanistan. Gant insists that command and control must be simplified significantly to give the Tribal Engagement Team leader a significant degree of autonomy in the field.³⁰ Gant's Tribal Engagement Strategy simply would not be practical in rural Afghanistan without satellite voice communications, a constraint that he acknowledges through the inclusion of satellite phones and UHF satellite tactical radios in his preferred kit for Tribal Engagement Teams.³¹

Satellite Voice Communications in Counter-terrorism

Although they are often able to leverage local infrastructure to support their operations, terrorists have also made use of satellite voice communications. In November 2008, a small terrorist cell successfully infiltrated Mumbai, India to carry out attacks against a number of civilian targets. Well-armed youths attacked two luxury hotels, a restaurant, a railway station, and at least one hospital.³² The operatives that carried out the attacks in Mumbai were revealed to have satellite

²⁹ Jim Gant, *One Tribe at a Time*, (Los Angeles: Nine Sisters, 2009).

³⁰ Gant, *One Tribe at a Time*, 6.

³¹ Gant, *One Tribe at a Time*, 40.

³² The Economist, "India Under Attack" *The Economist* print edition, 27 November 2008. http://www.economist.com/world/asia/displaystory.cfm?story_id=E1_TNSDRTJQ

phones in their possession, among other items. The terrorists reportedly used Thuraya and Inmarsat satellite voice handsets to maintain contact with Lashkar-e-Taiba (LeT), a militant Pakistani group that later acknowledged having provided material support for the attacks.³³ A previously little-known group called the Deccan Mujahideen claimed responsibility for the attacks: the group seems to have evolved from a decade-long campaign by Pakistan-based militants, including many fighting an insurgency in Kashmir, to incite India's 150 million Muslims to revolt. These groups have been held primarily responsible for half a dozen major terrorist attacks in Mumbai in recent years.³⁴ Both the attackers and the LeT co-conspirators were in frequent communication with each other and exchanging information with each other as regards the developments of the operations.³⁵ Other terror groups can be expected to be much more judicious with satellite voice communications.

Counter-terrorism forces, as well as terrorists, benefit from satellite voice communications. Counter-terrorism forces may seek to operate unobserved, avoiding the use of terrestrial radio or telephony in order to preserve operational security. Lt Col Wes Whitaker, a space operations

³³ Indrajit Basu, "Mumbai Terrorists Aided by Technology," *United Press International*, published: December 02, 2008.
http://www.upiasia.com/Security/2008/12/02/mumbai_terrorists_aided_by_technology/9520/

³⁴ The Economist, "India Under Attack" *The Economist* print edition, November 27th, 2008.
http://www.economist.com/world/asia/displaystory.cfm?story_id=E1_TNSDRTJQ

³⁵ A total of 41 calls were made from Taj Mahal Hotel, 62 calls were made from Oberoi/Trident and 181 calls were made from Nariman House. Source: Final Form/Report, In the Court of Addl. Ch. M.M., 37th Court, Esplanade, Mumbai.
<http://www.hindu.com/nic/Mumbai-terror-attack-final-form.pdf>

strategist who has spent much of the past decade in the special operations community, notes: “(military) UHF SATCOM service has historically been poor in the areas we operate in. I can’t tell you if it’s geography, something to do with the constellation itself, or our priority, but we’ve had to look elsewhere for service...we end up buying our own.”³⁶ To the extent that counter-terrorist forces attempt to behave like scale-free networks, or are able to swarm in order to combat terrorist groups, satellite voice communications can serve as a means of distributing mission-type orders, basic instructions, and status among operatives in the network.

Satellite Voice Communications in Building Partnership Capacity

Satellite voice communications can be used to enhance a partner military force’s ability to command and control its subordinate organizations. As we shall see, other near-peer states have demonstrated a willingness to build capacity with prospective US partner states, which could encourage a more proactive US posture in this arena, much as the Secretary of Defense has suggested recently.³⁷ Building Partnership Capacity through satellite voice communications can entail more far-reaching efforts than equipping and training partner military forces in satellite voice user equipment. Pakistan is conducting counter-insurgency and counter-terrorism operations in its restive Federally-

³⁶ Lt Col Wes Whitaker, Chief of Specialty Teams, 623d Air & Space Operations Center, interview by the author, April 8, 2010.

³⁷ Hon. Robert M. Gates, “Helping Others Defend Themselves,” *Foreign Affairs*, May/June 2010, 4.

Administered Tribal Areas and the newly-named Khyber-Pakhtunkhwa province in a loose coalition with the US. Pakistan is also in the process of building its first indigenous communications satellite, Paksat-1R, to replace the leased Paksat-1.³⁸ Paksat-1R, along with a future remote sensing satellite, was developed with assistance from the People's Republic of China. Since the Pakistanis have no space launch capability of their own, they will depend on China to launch Paksat-1R when the spacecraft is completed.³⁹ It is worth noting that Pakistan is an ally of the US in the Global War on Terror/Long War, yet it is Beijing rather than Washington that is building partner capacity with Islamabad through space power. Perhaps more could be done in the future to build Pakistani capacity through satellite communications so that the Frontier Corps is better equipped to combat Al Qaeda and the Pakistani Taliban, among other groups, as part of a regional security cooperation strategy. Export controls on satellite technology will most likely have to be altered to permit a level of cooperation between the US and Pakistan similar to that between China and Pakistan. In addition to enhancing building partnership activities through space power, updated export controls for space technologies may also enhance the competitiveness of US

³⁸ BBC News, "Pakistan to launch indigenous communication satellite from China in 2011," *BBC South Asia bureau*, April 14, 2009. From Dawn English-language website: <http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/news/business/11-cabinet-may-approve-fbs-restructuring---il--02>

³⁹ BBC News, "Pakistan to launch indigenous communication satellite from China in 2011," *BBC South Asia bureau*, April 14, 2009.

aerospace firms abroad.⁴⁰ The Secretary of Defense has emphasized the need for export control reform a number of times, noting recently that “other countries have been more quickly funding projects, selling weapons, and building relationships.”⁴¹

Future activities could include equipping fledgling Tier Two space power partners with basic communications relay spacecraft as the first “building block” in a modest indigenous space program. Although building capacity efforts may stop short of developing space launch services with partners in order to avoid ballistic missile program implications, partners could collaborate on satellite command and control capabilities for the basic satellite voice communications spacecraft.

Satellite-enabled Networks in Insurgency

Modern insurgencies have exploited information technology with great effect. Satellite-enabled networks offer a number of benefits to insurgent groups who leverage the Internet and satellite television to communicate with populations. Satellite television may seem like an odd example of a satellite-enabled network in warfare, but insurgents have demonstrated its potential for influence in irregular warfare activities. The principal use of satellite television so far has been to disseminate insurgent messages to external audiences. What the insurgent considers

⁴⁰ Reuters, “Gates Outlines Plans to Reform Export Controls,” *Reuters*, 20 April 2010. <http://www.reuters.com/article/idUSTRE63J4PY20100420>
See also: Gates, “Helping Others Defend Themselves.”

⁴¹ Gates, “Helping Others Defend Themselves,” 4.

as public affairs, the counterinsurgent may consider as propaganda. Satellite television allows the insurgent to expand his relevant population outside of the area of operations to the rest of the region and possibly to other continents. T.E. Lawrence asserts that doctrine, “the idea to convert every subject to friendliness,” is one element of a successful insurgency strategy.⁴²

There are unconfirmed reports that Hizbollah has used the Al-Manar television station not only for external communication with the greater pan-Arab population, but also as a means to survey targets in Israel during the 2006 Israel-Hizbollah War in Lebanon. Hizbollah also reportedly issued orders to some of its units in southern Lebanon over the air on Al-Manar. The US Treasury Department labeled Al-Manar Television as a “Specially Designated Terrorist Entity” in 2006, which was the first time a media outlet had been placed on the same list as al Qaeda, Hamas, and Hizbollah.⁴³ Al-Aqsa Television, the Hamas satellite television station, joined Al-Manar as a Specially Designated Terrorist Entity in March, 2010.⁴⁴

⁴² Lieutenant-Colonel Thomas E. Lawrence, “The Evolution of a Revolt,” *Army Quarterly and Defence Journal*, October 1920. Reprinted by US Army Command and General Staff College Combined Arms Research Library at

<http://www-cgsc.army.mil/carl/resources/csi/Lawrence/Lawrence.asp>

⁴³ Mark Dubowitz and Roberta Bonazzi, “Jihad TV in Europe,” *Wall Street Journal*, 18 Feb 2009.

⁴⁴ US Treasury Department press release, “US Treasury Dept Designates Hamas’ Al Aqsa Television a Specially Designated Terrorist” 18 March 2010. www.ustreas.gov/press/releases/tg594

Satellite bandwidth piracy is a matter of growing concern for communications satellite operators. In East Asia, both APT Satellite Holdings Ltd. and AsiaSat of Hong Kong have suffered the occasional piracy of television signals by groups believed to be in support of the Falun Gong dissident group in China.⁴⁵ The Liberation Tamil Tigers of Eelam (LTTE) succeeded in pirating commercial satellite signal for several months until the Government of Sri Lanka and Intelsat, a US-based company, were able to successfully identify, characterize, and halt the source of LTTE interference.⁴⁶ Intelsat terminated the “unauthorized” use of one of its satellites, Intelsat12, by the Sri Lanka-based insurgent group, which had been using the transponder for LTTE TV and radio transmissions to Europe and Asia.⁴⁷ The LTTE has since been defeated by the Sri Lankan government, but there are likely to be future instances of satellite bandwidth piracy for commercial firms to contend with.

The Department of Defense has already confronted at least one ongoing episode of satellite piracy of military communications satellite channels originating in Brazil and Colombia. Brazilian national police launched “Operation Satellite” in March 2009 to apprehend a network of satellite bandwidth pirates who were accessing US military satellite

⁴⁵ Peter de Selding, “Libya Pinpointed as Source of Months-Long Satellite Jamming in 2006” *Space News*, 7 Jul 2005.

https://www.space.com/spacenews/businessmonday_070409.html

⁴⁶ Embassy of Sri Lanka, “LTTE’S Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT Ltd,” 24 April 2007.

⁴⁷ Embassy of Sri Lanka, “LTTE’S Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT Ltd,” 24 April 2007.

channels from a number of locations across the country.⁴⁸ The federal police seized homemade transmitter equipment that had reportedly been used to illegally capture US Navy FLEETSAT satellite communications signals.⁴⁹ Although the Brazilian pirates should not be classified as insurgents or terrorists (but rather as criminals), the ease with which they have been able to pirate even an increasingly obsolete military satellite should be cause for some concern. Brazilian authorities have noted that members of the insurgent Revolutionary Armed Forces of Colombia (FARC) have also been observed routinely using pirating equipment to illegally exploit FLEETSAT transponders.⁵⁰

Satellite-enabled Networks in Counter-insurgency

Satellite-enabled networks have become an essential component of counter-insurgency. Satellite-enabled networks facilitate command and control of dispersed counterinsurgent forces, permitting dissemination of orders and intelligence. Deployable networks, including VSATs, provide connectivity to the Global Information Grid for counter-insurgency forces. The industry experts' prediction that commercial satellite communications will carry 90 percent of US Government traffic has

⁴⁸ BBC News, "Brazilian police arrest US military satellite hackers," BBC Latin America online, 4 May 2009. Accessed through Lexis-Nexis Academic database, http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518731342&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9518731345&cisb=22_T9518731344&treeMax=true&treeWidth=0&csi=10962&docNo=1

"Satelite" is the Brazilian Portuguese spelling of the English-language "satellite."

⁴⁹ BBC News, "Brazilian police arrest US military satellite hackers," BBC Latin America online, 4 May 2009.

⁵⁰ BBC News, "Brazilian police arrest US military satellite hackers," BBC Latin America online, 4 May 2009.

already borne out in at least one Area of Responsibility: US Central Command (CENTCOM) officers have publicly stated that up to ninety-six percent of satellite communications in the CENTCOM area of responsibility come from the commercial sector, while only four percent come from military satellite communications.⁵¹

Within the last three years, the US Air Force has deployed three Wideband Global SATCOM (WGS) satellites into geostationary orbit: each WGS spacecraft offers users as much bandwidth as the entire Defense Satellite Communications System constellation, yet the demand for satellite bandwidth still has not been slaked.⁵² Operations Enduring Freedom (OEF) and Iraqi Freedom/New Dawn (OIF/OND) have been acknowledged as a combined counter-insurgency and counter-terrorism efforts by policymakers for at least the past six years. Given the coalition experience in OEF and OIF/OND, irregular warfare activities do not appear to correspond with a decrease in satellite communications needs.

As the earlier example of satellite piracy indicates, interference is already emerging as a consequence of satellite communications demand. Intentional interference will be discussed in more detail in Chapter 5, but this is an appropriate point to introduce the problem. As more channels are established over more satellite transponders, radio-frequency

⁵¹ Barry Rosenberg, "DOD's reliance on commercial satellites hits new zenith." *Defense Systems*, 25 Feb 2010.
<http://defensesystems.com/Articles/2010/03/11/Cover-story-The-Satcom-Challenge.aspx?Page=1&p=1>

⁵² Air Force Fact Sheet, "Wideband Global SATCOM Satellite," 31 Dec 2009.
<http://www.af.mil/information/factsheets/factsheet.asp?id=16067>

interference is bound to result. Interference has an impact on connectivity of counter-insurgency and counter-terrorism forces, which may have life or death implications in an engagement. Interference may also impact the performance of UAVs and other sensors that depend upon satellite communications for a command and control tether. The Army and the Air Force have taken the issue seriously enough to develop and deploy detection, characterization, and geo-location systems to Southwest Asia in order to monitor prioritized satellite communications links for interference. The Air Force has also taken steps to acquire additional monitoring capabilities.⁵³ Both the public sector and private industry have also taken significant interest in interference issues. Interference can lead to lost revenue for a private firm, which is a powerful motivator for action against the problem. A number of firms have capitalized on the interference issue, offering detection and geo-location solutions to governments and fellow satellite operators.⁵⁴

While many states and private firms have taken important steps to characterize and locate the sources of satellite communications interference, resolution may prove to be very difficult in an irregular warfare scenario. Counter-insurgency and counter-terrorism forces may have few options available to resolve the situation when the perpetrator

⁵³ 21st Space Wing Fact Sheet, "16th Space Control Squadron," undated. <http://www.peterson.af.mil/library/factsheets/factsheet.asp?id=8403>

⁵⁴ Glowlink and RT Logic are just two examples of firms that have branched to the burgeoning interference resolution sector. See: www.glowlink.com and www.rtlogic.com for more details.

is operating among the population. The solution may prove to be worse than the problem if shutting down a source of interference harms the efforts of the coalition to gain and maintain the support the population.

Satellite-enabled Networks in Counter-terrorism

Like satellite voice communications, satellite-enabled networks connect decentralized counter-terrorist forces. Satellite-enabled networks also allow UAVs to inconspicuously support counter-terrorism operations without “setting foot” on exceedingly hazardous or politically sensitive territory. Not only can UAVs survey suspected terrorists, they can conduct attacks as well. The number of UAVs operating in Iraq and Afghanistan continues to climb, and with that increase comes a greater demand for satellite bandwidth. As we have seen, much of that demand may have to be met through commercial satellite services.

An important policy question may emerge in the near future as a result of UAV attacks in support of counter-terrorism. If an attacking UAV is controlled beyond line-of-sight using a relay over a satellite-enabled network, then a commercial communications satellite may be used to facilitate control of the attack, therefore carrying out a military mission. The legal status of a commercial satellite, as well as the firm that owns and operates it and the state that licenses it, comes into question in an engagement. Could commercial satellites or the firms that operate them be considered combatants? This is not to suggest that commercial satellites should carry caveats against use in counter-

terrorism and other military operations. Rather, the role of commercial satellites in combat is a policy question that may confront policy makers as well as space- and cyber-strategists in the future.

Satellite-enabled Networks in Building Partnership Capacity

Like satellite voice communications, satellite-enabled networks can enhance a partner state's military command and control architecture. Networks can go further by permitting the dissemination of images, video, and other types of data to dispersed partner-state military forces.

US Africa Command has made inroads in building partnership capacity with several African states through satellite-enabled networks. In one instance, the command equipped and trained Organization of African Union (OAU) military forces to operate and maintain a deployable VSAT network that is intended to enhance command and control of fielded OAU military forces.⁵⁵ The VSAT network has since been deployed to Mogadishu, Somalia to support the counter-insurgency efforts of the OAU Mission in Somalia.

Satellite television may also offer possibilities for building partnership capacity. Although the use of television to perform operational command and control of fielded forces would be ill advised as a project for US advisors, satellite television has demonstrated its value

⁵⁵ US Africa Command Public Affairs, "African Union Communications Capability Strengthened Through AFRICOM Training," 18 June 2008.
<http://www.africom.mil/getArticle.asp?art=1803&lang=0>

as an information operations tool and it may be helpful to a partner state in a region with a significant share of satellite television viewers.

Summary

Of all the elements of space power, the Western way of war may be most dependent upon satellite communications. The demand for bandwidth would seem to be insatiable, placing an ever-greater burden on commercial satellite communications services to complement over-subscribed US Government satellite communications. The unique demands of irregular warfare have not decreased demand in the slightest; if anything, counter-insurgency and counter-terrorism operations have increased the demand of Western military forces for satellite communications capability and capacity over the past decade. Two significant implications are emerging from these trends. Interference is becoming an issue of great importance to satellite operators. Additionally, policy has not addressed legal status for civil and commercial satellites involved in combat action.

The next chapter, entitled “Surveillance and Reconnaissance,” discusses observation from space. Surveillance and Reconnaissance services leverage the networking capabilities made possible by satellite communications in order to increase transparency among actors in irregular warfare and challenge the asymmetric advantage conferred by national overhead capabilities.

Chapter 3

Surveillance and Reconnaissance from Space

Tactical innovation is a necessary condition for all irregulars, whatever their objective. Without tactical innovation, insurrectionists are doomed to be defeated by regular armies. Mobility, harassment, and the willingness to improvise in order to achieve temporary and relative superiority are the basis of tactical innovation.

Thomas S. Rid & Mark Hecker
War 2.0

The dramatic increase in both the quality and quantity of commercial satellite imagery has begun to erode the asymmetric advantage of US military forces and their allies. Security constraints associated with US national overhead means are testing the interoperability of US forces with allies and even with agencies elsewhere in the US Government. The availability of commercial satellite imagery is also forcing the US to consider the impact of transparency on military operations.

The terms “surveillance” and “reconnaissance” are often used interchangeably, but the two concepts contain one key distinction. Surveillance is defined by the Department of Defense as “the *systematic observation* of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means

(emphasis added).”¹ Reconnaissance is defined as “*a mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area* (emphasis added).”² The key distinction between surveillance and reconnaissance, even when they are performed from space, is systematic vs. acute observation.

Intelligence is often included with surveillance and reconnaissance as a holistic enterprise; however, intelligence is not included in the space power discussion, except as an analytic function that is beneficiary of surveillance and reconnaissance from space (or any other domain). Owing to security considerations associated with national overhead systems, this chapter focuses mostly upon civil and commercial surveillance and reconnaissance capabilities.

This chapter discusses surveillance and reconnaissance as they relate to insurgency, counter-insurgency, counter-terrorism, and building partnership capacity. The chapter closes with a discussion of asymmetric advantage and the implications of surveillance and reconnaissance for that advantage. The chapter also addresses interoperability and transparency in relation to surveillance and reconnaissance within the context of irregular warfare.

¹ Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Related Terms*, 12 Apr 01, as amended thru 31 Oct 09, 528.

² Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Related Terms*, 12 Apr 01, as amended thru 31 Oct 09, 453.

Surveillance from Space

Surveillance from space permits users to exploit systematic or near-continuous observations. Observations may be collected using active or passive means. Active surveillance means emit electromagnetic energy and use returned energy to construct data on something of interest. No known active surveillance system is deployed today. At present, radar³ appears to be the leading concept for active surveillance from space. Passive surveillance means do not emit electromagnetic energy themselves, but construct data based on detected electromagnetic energy from an area of interest. Infrared sensors are the primary means of passive surveillance from space. In unique circumstances, a communications satellite with no terrestrial sensors on board can perform surveillance from space. A terrestrial beacon can purposefully transmit location data from the earth's surface to a communications satellite on a continuous or near-continuous basis, imposing a surveillance-from-space function on that communications satellite.⁴ Surveillance from space does not imply that a single satellite or capability must be continuously collecting. Satellites that are able to provide a snapshot in time can be augmented by additional capabilities

³ The acronym "radar" stands for radio detection and ranging. Radar uses reflected radiofrequency energy to determine an object's physical characteristics.

⁴ Each of the major satellite communications service providers offer a communications-based force tracking "solution" to customers. See the following sites for more details:
<http://www.iridium.com/solutions/personneltracking.aspx?applicationID=11>
<http://m-cat.acesinternational.com/m-cat/index.php>
<http://www.thuraya.com/solutions/customized-solutions/lbs>

collecting in the same or even different areas of the electromagnetic spectrum.⁵

To add a measure of precision to this discussion of surveillance, the author suggests the following categories of surveillance-from-space services: indications and warning; environmental monitoring; and force tracking. Indications and warning includes indications of activity and ballistic missile warning.⁶ Indications of activity characterize signatures or patterns in an area of interest through specified electromagnetic parameters. Ballistic missile warning specifically characterizes the signatures or patterns associated with ballistic missile launch, trajectory, and re-entry.⁷ Environmental Monitoring surveys the terrestrial domains of air, land, and sea for weather and climate data, as well as oceanographic and topographic data. Space-derived weather data, like satellite communications, has become so integral to the conduct of Western military operations that it is easy to forget that it is an active element of space power. Force tracking services monitor personnel and platforms on the earth's surface by transmitting their GPS-derived position in three dimensions through space-enabled networks to an

⁵ Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, A-1.

⁶ This categorization is inspired in part by Michael Frater and Michael Ryan's "Taxonomy of Space Operations," published in the July 2005 edition of the *Journal of Battlefield Technology*. Regrettably, Frater and Ryan compound surveillance, reconnaissance, and intelligence together as a space operation.

⁷ Traditionally, ballistic missile warning satellites have used infrared sensors to detect the plume of a ballistic missile, but newer systems, such as the Missile Defense Agency's Space Tracking and Surveillance System, also survey by sensing visible light in addition to infrared wavelengths.

interested user. Force tracking from space depends upon satellite communications and positioning, navigation, and timing for surveillance from space. For the purposes of this paper, it will be treated primarily as an element of surveillance.

Reconnaissance from Space

Reconnaissance from space permits users to capture an impression of a defined area at a defined point in time. Single low and medium Earth-orbiting systems, or architectures that provide limited numbers of low or medium orbital systems, are well suited to the reconnaissance mission. Generally, their access to specific targets is limited in time based on their orbit such that data collected will be a “snapshot” of events in the portion of the electromagnetic spectrum where they can collect.⁸ Reconnaissance from space may be cued by surveillance from space to obtain more precision in an area of interest or refinement on an object of interest. Reconnaissance includes the collection of signals intelligence, about which information is limited by security restraints. A number of states reportedly operate signals intelligence systems or are in the process of developing them; however, no civil or commercial satellite service for the collection of signals intelligence exists today, nor do any appear to be in development.

Reconnaissance from space also includes visible-light, multi-/hyper-spectral, and radar imaging. Visible light imaging may be the

⁸ Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, A-2.

most well known type of reconnaissance from space. The full extent of national capabilities is limited once again by security concerns, but it is still believed to be of greater quality than even the highest-resolution civil and commercial satellite imagery capabilities.⁹ Multi-spectral and hyper-spectral sensors combine several wavelengths of data into satellite imagery to reveal additional signatures and patterns to users. Radar imaging develops images through returned radio-frequency energy, offering users some unique and surprisingly high-resolution products. Unlike visible light imaging, radar imaging is not limited by weather or sunlight.

The Significance of Surveillance and Reconnaissance from Space

In addition to communications one of the earliest applications envisioned for earth-orbiting satellites was terrestrial surveillance and reconnaissance. Space offered an incomparable vantage point to observe events on the earth's surface, as well as features of the surface itself. The Missile Detection Alarm System, or "MIDAS," represented an early effort to detect and report the infrared plume of a ballistic missile launch using space-based sensors.¹⁰ The US Discoverer program inaugurated an era of observation from space by demonstrating the technical feasibility of photographing the earth from space, and then returning

⁹ Peter Eisler, "Google Earth Helps Yet Worries Government." *USA Today*, November 11, 2007.

http://www.usatoday.com/tech/.../2008-11-06-googleearth_N.htm

¹⁰ David N. Spires, *Beyond Horizons: a Half-Century of Air Force Space Leadership* (Maxwell AFB, AL: Air University Press, 1998), 58

images to earth.¹¹ The US also deployed its first generation of weather satellites in the early 1960's, adding significantly to weather coverage and prediction capability.¹²

The first generations of reconnaissance and surveillance systems had been designed and operated to support the major military strategic priority of the day: strategic deterrence against the Soviet Union.

Environmental monitoring is one exception to this statement, however.

The US used satellite-enabled weather forecasting to support combat operations in Vietnam, as well as operations in Grenada and Panama in the 1980's.¹³ Only after the Cold War ended did the US begin to extend national security space to more tactical requirements, and it required an event of international significance inspire many of these extensions.

Operation Desert Storm, heralded as the first “space war,” is remarkable for a number of episodes where space power was appropriated for tactical- and operational-level use as well as strategic-level use.¹⁴ In the months leading up to the August 1990 invasion of Kuwait, Iraqi forces were reportedly able to use SPOT imagery to aid planning before France embargoed SPOT sales to Iraq for the duration of the build-up of coalition forces and the conflict.¹⁵ The coalition used satellite-enabled reconnaissance for precise maps of the region, to

¹¹ Spires, *Beyond Horizons*, 58, 67, 94.

¹² Spires, *Beyond Horizons*, 146.

¹³ Michael Sheehan, *The International Politics of Space* (New York: Routledge, 2007), 98.

¹⁴ Spires, *Beyond Horizons*, 245.

¹⁵ Sheehan, *The International Politics of Space*, 98.

determine suitable areas for land, sea, and air assault, to verify targets, and to rescue downed aircrews.¹⁶ The coalition also used satellite-enabled weather services and multi-spectral imagery from the US Department of Commerce's LANDSAT system for environmental monitoring.¹⁷ The US used its Defense Support Program satellites to detect the launches of SCUD short-range ballistic missiles, initiating the use of surveillance from space to detect and report short-range missile launches along with the traditional role of long-range missile warning.¹⁸

Surveillance and reconnaissance from space have continued to improve in both quality and quantity in the nearly two decades since Operation Desert Storm. A number of commercial remote sensing systems have joined SPOT and LANDSAT, and many of these systems far exceed SPOT and LANDSAT in performance. For example, SPOT featured images with 20-meter resolution in 1990 while in 2010, the cutting-edge Geo Eye-1 spacecraft is capable of producing images of .41-meter resolution.¹⁹ Radar imagery was not available in 1990 but in 2010, Canadian and Israeli commercial vendors offer resolutions as fine as 3 meters through RADARSAT and 1 meter through TecSAR, respectively.²⁰

¹⁶ Sheehan, *The International Politics of Space*, 98-99.

¹⁷ Spires, *Beyond Horizons*, 251-254.

¹⁸ Spires, *Beyond Horizons*, 254. SPOT is "Satellite Probatoire d'Observation de la Terre," or Exploratory Satellite for Earth Observation.

¹⁹ Michael Mecham, "Remote Sensing Grows Up," *Aviation Week and Space Technology*, Vol 171, Issue 21, 7 December 2009, 70.

²⁰ MacDonald, Dettwiler, and Associates, "About RADARSAT," http://www.radarsat2.info/about/features_benefits.asp

The US has embraced the benefits of commercial remote sensing products to military operations at the strategic and operational levels of war by integrating commercial remote sensing products with national overhead products. Many commercial products are permeating the tactical level of war, as well through US Air Force and US Army initiatives.²¹ The next generation of space-based missile warning satellites will soon be deployed to replace the Defense Support Program, offering a higher level of performance against short-range ballistic missiles.²²

Over the past decade, force tracking has arguably become an indispensable service made possible by surveillance from space. In the opening phase of Operation Iraqi Freedom, more than 1,300 Blue Force Tracker units were in use among coalition forces, giving operational commanders the ability to track far-flung friendly units in an otherwise confused tactical environment.²³ Blue Force Tracker's ability to place friendly forces on a high-resolution digital map created unprecedented

See also: Defense Industry Daily, "India launches \$200M TECSAR Spy Satellite," *Defense Industry Daily*, April 20, 2009. <http://www.defenseindustrydaily.com/Logistics-amp-Support/C4ISR>

²¹ The Air Force operates a suite of commercial imagery downlink equipment through its Eagle Vision program. The Army has developed expeditionary Commercial Exploitation Teams to leverage commercial remote sensing products for forward-deployed Army units.

Headquarters Air Force, DCS for Intelligence, Surveillance, and Reconnaissance, "Eagle Vision Overview Briefing," 21 Oct 2008.

US Army Space & Missile Defense Command Future Warfare Center, "2009 CENTCOM CET Debrief," 29 July 2009.

²² US Air Force Fact Sheet, "Space-based Infrared Systems," <http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=3675>

²³ Thomas Rid and Marc Hecker, *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009) 56.

levels of situational awareness...commanders were even able to direct their forces through urbanized areas at night.²⁴ It would be difficult to contemplate combat in the future, even in an irregular warfare environment, without the benefit of force tracking.

Surveillance from Space in Insurgency

There is no evidence available at this time to suggest that contemporary insurgents have been able to exploit surveillance from space, whether it is indications and warning, environmental monitoring, or force tracking. However, state support to insurgencies and terror through surveillance from space may soon pose significant challenges to policy makers, strategists, and operatives alongside civil and commercial capabilities. The time may be fast approaching when Iran and other states that support terrorist groups and insurgents are able to lend support through space power. One of the first effects may be reconnaissance from space. It is easy to neglect the fact that Iran is pursuing a space program in addition to its ballistic missile program, but the Iranians have already successfully deployed joint venture and indigenous satellites. In 2007, Iran, China, and Thailand put a remote sensing satellite on orbit using a Chinese rocket.²⁵ An indigenously

²⁴ Rid and Hecker, *War 2.0*, 56.

²⁵ BBC News, "Iran, China, and Thailand satellite goes into orbit," *BBC Middle East*, 7 September 2008. Retrieved from Lexis-Nexis Academic database at http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518773642&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9518773652&cisb=22_T9518773651&treeMax=true&treeWidth=0&csi=10962&docNo=2

produced remote-sensing satellite is planned for launch sometime in 2010.²⁶ Iran has also progressed on a feasible space launch vehicle design, launching the Omid communications satellite in 2009 and placing a research payload into orbit in early 2010.²⁷ It is difficult to assess just what Iran's remote sensing satellite programs are capable of collecting, but the overall indigenous space program continues to make rapid technological progress. While Hizbollah and terror groups affiliated with the regime in Iran may not be able to afford the decreasing price of admission into space, they may be able to leverage space power through the regime for reconnaissance from space that civil and commercial services do not provide. As we will explore further in Chapter 5, the US may have few options available to it in order to limit or deny state support to insurgency and terrorism through space power.

Surveillance from Space in Counter-insurgency

Surveillance from space would appear to be an asymmetric advantage that Western states and their military forces maintain, for the time being, over non-state actors. The US in particular possesses significant capabilities in indications and warning, environmental monitoring, and force tracking. Insurgents who hide among the

²⁶ BBC News, "Iran to launch topography satellite in 2010," *BBC Middle East*, 24 August 2008. Retrieved from Lexis Nexis Academic database at <http://www.lexisnexis.com/us/lnacademic/search/homesubmitForm.do>

²⁷ BBC News, "Iran satellite move sparks fears," *BBC Middle East*, 3 Feb 2009. http://news.bbc.co.uk/2/hi/middle_east/7868116.stm

See also: Adam Gabbat, "Iran Space Launch Opens Cans of Worms in Space Race with West," *The Guardian UK*, 3 Feb 2010.

population and conceal their activities pose a tremendous challenge to surveillance efforts from space.

The Israeli experience against Iranian-supplied Hizbollah rockets and missiles reinforces the value of surveillance from space to counter-insurgency. In his study of the 2006 Israel-Hizbollah war, Anthony Cordesman warned that: “Iran and Syria can both supply Hizbollah with much longer-range and more precise guided missiles with larger payloads. Rockets can be equipped with crude to sophisticated chemical, radiological, and biological warheads—having a major political impact even if their military impact is limited.”²⁸ It is important to remember that irregular warfare is a contest for the relevant populations. Israel can ill-afford to fail in the defense of its own population, lest the legitimacy of the Israeli government be undermined. The Israeli government has publicly stated that Syria is supplying Hizbollah with SCUD short-range ballistic missiles, which if deployed in Southern Lebanon, would be able to strike at any point within Israel.²⁹ Although Israel appears to maintain a capable terrestrial missile warning system, the state may be compelled to add a space-based surveillance capability to supplement that system in support of active and passive missile defense against Hizbollah. Where missile warning from space was once

²⁸ Anthony H. Cordesman, *Preliminary “Lessons” of the Israeli-Hezbollah War* (Washington, DC: Center for Strategic and International Studies, April 2009) 24.

²⁹ Kim Ghalit, “US Concerned About Syrian Intentions over Hezbollah,” *BBC World Service*, 15 April 2010. http://news.bbc.co.uk/1/hi/world/middle_east/8621405.stm

the exclusive province of the US and the USSR in the Cold War, it is quickly becoming a necessity in the “small wars” of counter-insurgency.

Surveillance from Space in Counter-terrorism

Successfully identifying and tracking indications and warning of terrorist activity is perhaps the most complex challenge for terrestrial and space-based surveillance alike. Improvised explosive devices (IEDs), a favored weapon of insurgents in both Afghanistan and Iraq, further illustrate this challenge. Col David Thompson, Director of Space Forces for US Air Forces Central, offers: “space-based ISR is not particularly helpful once an IED has been emplaced: the key is to see how space can help further to the ‘left of the boom,’ in production, testing and transport phases, and in ferreting out networks.”³⁰ Regrettably, the DoD opted to cancel the Space Radar program in 2009, which had been working towards ground-mobile target indicator and broad-area surveillance capabilities from space.³¹ Gen. C. Robert Kehler, commander of Air Force Space Command, has indicated that the service may need to seek commercial contracts to fill gaps in the nation’s space-based radar capabilities. “War fighters continue to tell us that a space-based radar is a requirement for them,” said Kehler in spring of 2009 at the National Space Symposium. “The question is, ‘How do we satisfy those

³⁰ Col David Thompson, Director of Space Forces, US Air Forces Central Command, to the author, email, 23 Apr 2010.

³¹ Air Force Fact Sheet, “Space Radar,” undated.
<http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5308>

requirements?”³² Kehler surmised that the answer is a combination of government, commercial and airborne radar systems.³³ Perhaps advanced processing techniques for Canadian RADARSAT or Israeli TechSAR space-based radar reconnaissance systems will yield some of the capabilities that Space Radar promised. Foreign sources may be necessary to meet requirements, since the US aerospace industry would appear to be lagging in commercial synthetic aperture radar development as a result of long-standing legal restrictions. According to the 2003 Commercial Remote Sensing Policy, “U.S. companies are encouraged to build and operate commercial remote sensing space systems whose operational capabilities, products, and services are superior to any current or planned foreign commercial systems. However, because of the potential value of its products to an adversary, the operation of a U.S. commercial remote sensing space system requires appropriate security measures to address U.S. national security and foreign policy concerns.”³⁴ The policy is well intended as a means to preserve US advantage, but it appears to have contributed to an unfulfilled surveillance need for US forces, while being unable to restrict the growth of commercial remote sensing outside the US. On August 24, 2009 NOAA granted a license to Northrop Grumman to operate a commercial

³² Stew Magnuson, “Israel pushes new satellite as solution to US Space Radar Needs,” *National Defense*, January 2010.

³³ Magnuson, “Israel pushes new satellite”

³⁴ US Department of Commerce, Department of Commerce Fact Sheet, “US Commercial Remote Sensing Policy,” 25 April 2003.

remote sensing satellite with one-meter synthetic aperture radar (SAR) capability. It is the first U.S. license approved for a commercial radar imaging satellite at that resolution level.³⁵ This is an important first step towards making the US competitive in the SAR market, while acknowledging that the existing Commercial Remote Sensing Policy is self-defeating as a means of controlling remote sensing products.

Surveillance from Space in Building Partnership Capacity

The threat of ballistic missiles offers the US with an opportunity to build partnership capacity through space-based missile warning. It would be reasonable to assume that partnering nation-states would benefit from basic indications and warning that they were under attack. Lt Col Single, remarking on his time in Afghanistan, notes that there are difficulties with sharing space-enabled products and services with foreign militaries: “over-classification and releasability are the number one challenges: sometimes, just because a piece of information came from a space system, it was marked ‘Secret’.”³⁶ The US could expand shared early warning to partnering nation-states without disclosing details associated with sources or methods. Shared early warning would serve as an important first step towards shared defense against ballistic missile attack. As the Israeli example indicates, successful missile

³⁵ Statement by Office of Space Commercialization, US Department of Commerce, 24 Aug 2009. Retrieved at <http://www.space.commerce.gov/remotesensing/>

³⁶ Peter B. de Selding, “US Officer: Secrecy Among Coalition Forces Hinders Use of Space Assets in Afghanistan,” *Space News*, 10 May 2010, A-1.

defense- even if it is passive defense- could mean the difference between success and failure in the battle for the relevant populations.

Like satellite voice communications and satellite-enabled networks, force tracking can enhance a partnering nation-state's ability to command and control its military forces. A number of commercial satellite communications service providers offer tracking applications in addition to communications services.³⁷ A Tier Three partner could be trained to track forces through a commercial application, or a Tier Two partner could configure their communications satellites to relay beacon data to headquarters elements.

Reconnaissance from Space in Insurgency

Insurgents have taken advantage of widely available satellite imagery products to support operations against targets. Google Earth, Google Maps, and other similar imagery database services have been exploited to support insurgent and terrorist activities over the past few years. Google Earth is one example of several applications available to any Internet user to download for free, offering anyone their own geospatial database of imagery, maps, terrain, and user-developed 3-D features.³⁸ In August 2006, insurgents in Iraq circulated an

³⁷ Iridium, Inmarsat, Thuraya, and ACeS each advertise tracking solutions through their corporate websites and sales literature. For more details, see:
<http://www.iridium.com/solutions/personneltracking.aspx?applicationID=11>
<http://m-cat.acesinternational.com/m-cat/index.php>
<http://www.thuraya.com/solutions/customized-solutions/lbs>
http://www.inmarsat.com/Services/Government/Blue_force_tracking.aspx

³⁸ Google Earth description, retrieved at <http://earth.google.com/intl/en/>

instructional video on how to aim rockets at U.S. military sites using Google Earth. The video appeared to fulfill the dire predictions raised by security experts in the US and across the globe when Google began offering free Internet access to worldwide satellite imagery in 2005.³⁹ The satellite images in the Google Earth database are not updated on a regular basis, so the database would be unusable for dynamic targeting. However, some defense experts have said the easy availability of information on Google Earth can increase the risks for military organizations.⁴⁰ Officials in countries as diverse as Australia, India, Israel and the Netherlands complained publicly that Google Earth would be a boon to terrorists and hostile states, especially since the pictures often provide a site's map coordinates.⁴¹ In January 2007, British officials claimed that insurgents sympathetic to al-Qaida were using aerial photography in Google Earth to locate potential targets inside British bases around the southern Iraqi city of Basra.⁴² Palestinian militants are also reportedly using Google Earth to help plan their attacks on the Israeli military and other targets. Members of the al-Aqsa Martyrs Brigade say they use the popular Internet mapping tool to help

³⁹ Peter Eisler, "Google Earth Helps Yet Worries Government." *USA Today*, 11 November 2007. http://www.usatoday.com/tech/.../2008-11-06-googleearth_N.htm

⁴⁰ Clancy Chassay and Bobbie Johnson, "Google Earth used to target Israel," *The Guardian*, 25 October 2007. <http://www.guardian.co.uk/technology/2007/oct/25/google.israel>

⁴¹ Eisler, "Google Earth Helps Yet Worries Government."

⁴² Lester Haines, "Google Erases British Bases in Iraq," *The Register UK Edition*, 1 January 2007. http://www.theregister.co.uk/2007/01/17/google_erases_brit_bases/page2.html

determine their targets for rocket strikes. Al-Aqsa is one of several militant groups firing rockets, known as Qassams, from Gaza into Israel.⁴³ While Google Earth most likely does not provide a sufficient level of precision for Western forces to use it for targeting, its precision may be “good enough” for the purposes sought by insurgents.

Google Earth and similar services carry two primary implications for insurgency, as well as counter-insurgency and counter-terrorism. Access to imagery of a quality that would likely have earned it a security classification only a few years ago has now been democratized. Because anyone can access images of any spot on the globe using Google Earth or privately-obtained imagery, Western forces must now operate more transparently than ever before. To a degree, the availability of quality geospatial information services to anyone with an Internet connection has diminished the asymmetric advantage of the US in reconnaissance from space. Presumably, US national security collection, processing, exploitation, and dissemination capabilities are still significantly better than those offered by a universally available database, but the adversary may not need exquisite capabilities to affect their targets.

Because Google Earth and the like are available to anyone, the US must become accustomed to operating under conditions closer to information parity with insurgents than information superiority over them, at least where geospatial intelligence is concerned. There may be

⁴³ Chassay and Johnson, “Google Earth used to target Israel.”

little that the US can do to rectify this situation. Although sensitive locations can be obscured, such measures may only serve to highlight that there is something worth hiding. US forces may need to acquaint themselves with advanced camouflage, concealment, and deception measures or accept a presumption of transparency to their operations.

Reconnaissance from Space in Counter-insurgency

Just as DoD has had to rely upon commercial satellite communications to an increasing degree, so it has come to rely increasingly upon commercial satellite reconnaissance, as well. Because national overhead capabilities are so heavily taxed, counter-insurgency forces have increased their dependence on commercial and civil reconnaissance from space to fulfill intelligence requirements.⁴⁴

Commercial imagery relieves some of the burden on the US Government's classified satellite network, said a spokesman at the National Reconnaissance Office (NRO), which runs the system. "We're oversubscribed," the spokesman stated, noting that intelligence and security missions get priority and often need the higher resolution and quicker returns offered by the government's own satellites. "Anytime the broader area stuff can be taken commercially, so much the better."⁴⁵

Reflecting on his experiences so far in Southwest Asia, Colonel Thompson argues that in irregular warfare, prioritization (of collection

⁴⁴ Eisler, "Google Earth Helps Yet Worries Government."

⁴⁵ Eisler, "Google Earth Helps Yet Worries Government."

requirements) demands a more nuanced approach where reconnaissance is concerned. He elaborates: "...assuming you have full access to the battlespace, you likely have an abundance of airborne ISR that is focused on the same problem sets. The key becomes, and in my opinion we do this poorly, in identifying those areas where space-based ISR is most helpful and tasking it to do those things, regardless of priority. Instead, we assign our highest priority collection requirements to the assets we own full-time (airborne assets), because we own and control them. This inefficient assignment approach leaves lesser requirements unfilled, when they might have been filled by airborne assets if we gave some of the higher priorities to space-based ISR."⁴⁶ The US and its coalition partners may not always enjoy this degree of flexibility with reconnaissance assets. Thus far, the US and its coalition partners have been able to operate unhindered in the skies above both Afghanistan and Iraq; however, if coalition air superiority was challenged for any reason, the demand on satellite reconnaissance could be expected to increase further. Since there is a finite amount of resources (and an apparently infinite amount of collection requirements), difficult choices would have to be made in a challenged environment.

Security limitations also affect how products from national assets may be used. In order to protect sources and methods, products are often limited to use by US forces with few exceptions. Lt Col Single adds

⁴⁶ Thompson, email.

that at ISAF, “due to classification levels, we (the US) can’t share with 44 nations, so we often worked issues behind closed doors.”⁴⁷ Civil and commercial products offer a greater degree of flexibility in use. Not only can they be obtained by anyone, they can be shared with anyone. Lt Col Pettis recalls: “I used commercial imagery to support drought relief planning- enemy propaganda suggested that the Kurds had purposely dammed the rivers to limit the water supply. Analysis proved that that just wasn’t true.”⁴⁸ Civil and commercial remote sensing satellites may also offer multi- and hyper-spectral imaging features that are better suited to counter-insurgency operations that seek to support the population than are close-hold national security capabilities. Lt Col Pettis recalls an occasion in Iraq where coalition members needed soil data from a contested area to support a reconstruction project. Commercial imagery offered an alternative to sending soldiers and airmen into harm’s way to obtain the data. “Commercial imagery provides access to denied areas that alternatives just do not or cannot.”⁴⁹

Reconnaissance from Space in Counter-terrorism

In 2002, two remote sensing experts argued that “the value of an overhead view of a planned target is likely to be marginal at best; most terrorist targets appear to be relatively vulnerable to attack and approachable for gathering pre-attack intelligence using traditional

⁴⁷ de Selding, “US Officer: Secrecy Hinders Use of Space Assets,” A-1.

⁴⁸ Lt Col Stuart Pettis, Chief, Strategy and Doctrine, Headquarters Air Force Space Command, interview by the author, 18 Feb 2010.

⁴⁹ Pettis, interview.

means, including inside sources.”⁵⁰ However, terror groups, like insurgents, have demonstrated a willingness to exploit reconnaissance from space in order to support their activities. Some terrorist attacks appear to have been planned with the help of Google Earth, including an event in 2006 in which terrorists used car bombs in an unsuccessful effort to destroy oil facilities in Yemen.⁵¹ Images from Google Earth and other commercial sources have been found in safe houses used by al-Qaeda and other terror groups.⁵² It may also be that in the era of the Global War on Terror/Long War, there are fewer targets that are approachable prior to attack. Steven Lambakis remarked in 2001: “within three hours of the first release of spy-quality imagery data from Space Imaging’s IKONOS satellite (inserted into orbit in September 1999), more than 386,000 people tried to download a high-resolution photo of Washington, DC.”⁵³ This is not to say that all of those who attempted to download the imagery had malicious intentions; rather, high-resolution imagery is now widely available and it will be difficult to control access to it under the best circumstances.

⁵⁰ John C. Baker and Dana J. Johnson, “Security Implications of Commercial Satellite Imagery,” *Commercial Observation Satellites: At the Leading Edge of Global Transparency*, Ed. by John C. Baker, Kevin M. O’Connell, and Ray A. Williamson. (Santa Monica: Rand, 2002), 118.

⁵¹ Eisler, “Google Earth Helps Yet Worries Government.”

⁵² Eisler, “Google Earth Helps Yet Worries Government.”

⁵³ Steven Lambakis, *On the Edge of the Earth* (Lexington, KY: University of Kentucky Press, 2001), 165.

Reconnaissance from Space in Building Partnership Capacity

Reconnaissance from space can enhance partner military force operations at the strategic, operational, and tactical levels of war. Google Earth and its geospatial database competitors offer an entry-level imagery library that Tier Three space power partner states can customize according to their needs. Images on Google Earth may serve only as a starting point for imagery users. Space Imaging, Inc., a US-based commercial satellite observation firm, offers the following on their corporate website: “Google Earth is a great addition to the growing set of software solutions devoted to viewing satellite image data from around the world. While Google Earth satellite imagery doesn’t match the quality of traditional high-resolution satellite images, it is an excellent way to determine the coordinates of a location you’d like to study further.”⁵⁴ Partnering nation-state forces should be educated in tasking, processing, exploitation, and dissemination processes so that they can make effective use of a Google Earth imagery database and efficient use of more targeted collection efforts through commercial observation services.

Using reconnaissance from space to build partnership capacity may entail a more comprehensive effort than merely providing the partner state with a database of commercial or civil imagery. Tier Two space power partner states could be advised on how to more effectively

⁵⁴ Space Imaging, Inc., “Using Google Earth to Plan High-Resolution Satellite Image Data,” http://www.satimagingcorp.com/google_earth.html

and efficiently use dual-use remote sensing systems for their security needs.

Summary

Surveillance and reconnaissance from space are rapidly transitioning from instruments of Cold War confrontation to critical enablers on the battlefield. Products of remarkable quality are now available to any interested party, creating opportunities and risks for US forces. The US can now supplement national overhead collection with excellent commercial capabilities, but policy makers must strike the appropriate balance among multiple sensors and products. Insurgents and terror groups can also leverage commercial capabilities for their own purposes. These capabilities, and their availability to almost anyone, challenge the US's information advantages from space.

The next chapter discusses satellite-enabled positioning, navigation, and timing (PNT). Surveillance and reconnaissance from space and PNT services can deliver synergistic effects in warfare: the insurgent and the counter-insurgent alike who can exploit both elements of space power can diminish the asymmetric advantage of their opponents, if not seize advantages of their own.

Chapter 4

Positioning, Navigation, & Timing

Our most vexing future adversary may be one who can use technology to make rapid improvements in its military capabilities that provide asymmetrical counters to US military strengths, including information technologies.

Joint Vision 2010
The Joint Staff, 1996

Precision is critical in a contest for relevant populations. The US Global Positioning System and Russian GLONASS civil signals are universally available to any user who can obtain proper receiver equipment. Contemporary receivers offer users a considerable level of performance that was once reserved for users of military receivers. This same universal availability offers an asset to the US as well as a liability: as the purveyor of the leading satellite PNT service of the world, the US can influence user equipment and applications. This chapter discusses satellite-enabled positioning, navigation, and timing and how these services and irregular warfare activities relate to one another.

This chapter begins with an examination of positioning, navigation, and timing in conventional warfare. The chapter then studies positioning, navigation, and timing individually as they relate to elements of irregular warfare: insurgency, counter-insurgency, counter-terrorism, and building partnership capacity. The chapter then ponders three

major implications for PNT that irregular warfare highlights: precision, universality, and friendly conquest.

Satellite-Enabled Positioning

Positioning is defined as “the ability to accurately and precisely determine one’s location two-dimensionally or three-dimensionally with reference to a standard geodetic system.”¹ Positioning provides an accurate three-dimensional position and a velocity to the receiver. GPS provides two levels of service to users: standard and precise. The standard positioning service (SPS) is available to any user with a receiver, while the precise positioning service (PPS) is available to approved government users with special receiver equipment. The difference in precision between standard and precise service was significant early in the life of the GPS program; however, the advent of GPS augmentation services and the termination of selective availability for standard service receivers have made both services comparable in accuracy.

Satellite-Enabled Navigation

Navigation is defined as “the ability to accurately and precisely determine current and intended position (either relative or absolute) and apply corrections to course, orientation, and speed in order to attain an intended position anywhere on or above the earth’s surface.”² Navigation is accomplished by the receiver, which measures actual position and

¹ Space-based Positioning, Navigation, and Timing National Executive Committee, “What is PNT?” Retrieved at <http://gps.gov/101/>

² Space-based Positioning, Navigation, and Timing National Executive Committee, “What is PNT?” <http://gps.gov/101/>

velocity against a user-referenced position in order to generate navigation information.³

Satellite-Enabled Timing

Timing is defined as “the ability to acquire and maintain accurate and precise time from a standard such as universal coordinated time anywhere in the world and within user-defined timeliness parameters.”⁴ GPS can transfer Universal Coordinated Time to users for a whole host of synchronization applications. Perhaps Lt Gen William Shelton, former commander of Fourteenth Air Force and United States Strategic Command’s Joint Functional Component Command for Space, best explains the importance of satellite-enabled timing when he stated in a 2008 interview, “most people are very familiar with GPS, and the navigation capability it provides. But few understand the crucial role of the GPS precision timing signal in both military and commercial applications. Extremely accurate timing allows for a higher data rate over communications channels. In today's information age this is critical to pushing as much data as possible through our available communications bandwidth.”⁵ Shelton goes on to say, “GPS timing allows secure encryption of communications by providing a common timing reference. Commercial users of GPS use the timing signal for applications such as

³ ARINC Research Co., *GPS NAVSTAR User’s Overview*, March 1991, 8.

⁴ Space-based Positioning, Navigation, and Timing National Executive Committee, “What is PNT?” <http://gps.gov/101/>

⁵ Louis M. Arana-Barradas, “The Space Link: Airmen Provide Out-Of-This-World Capabilities” *Airman*, July/August 2008, 12-13.

time-stamping banking transactions and Internet timing, making GPS vital to our international business and networking.”⁶

The Significance of PNT to Modern Warfare

Satellite-enabled PNT may be one of the least anticipated, yet most profound benefits of space power to military and civilian users. The US Navy initiated the TRANSIT program in the early 1960’s to aid navigation for ships at sea. TRANSIT was primitive by modern PNT standards, determining position in two dimensions (latitude and longitude), but it was accurate to 600 feet, a respectable level of precision for its time and purpose.⁷ Perhaps the most important accomplishment of TRANSIT was to prove that satellite navigation was indeed feasible.

The initial concept for the Global Positioning System (GPS) followed TRANSIT in the 1970’s, offering “the capability of supplying accurate, all-weather position data to an unlimited number of users anywhere on or near the surface of the earth.”⁸ Like almost all other national security space programs, GPS was developed according to a Cold War requirement: mobile intercontinental ballistic missiles would be accurately and precisely positioned for launch using satellite navigation.

Policy makers in the Soviet Union also realized the advantages offered by a space-based radio-navigation system for positioning their

⁶ Louis M. Arana-Barradas, “The Space Link: Airmen Provide Out-Of-This-World Capabilities” *Airman*, July/August 2008, 12-13.

⁷ David N. Spires, *Beyond Horizons: A Half-Century of Air Force Space Leadership*. (Maxwell AFB, AL: Air University Press, 2007) 150.

⁸ Spires, *Beyond Horizons*, 150.

own road and rail-mobile strategic nuclear forces. GLONASS (Global Navigation Satellite System) development proceeded GPS by only a few years. The objective system contains 20 satellites in three orbital planes, with three on-orbit spares. GLONASS provides 100 meters accuracy with its Coarse Acquisition (deliberately degraded) signals and 10-20 meter accuracy with its Precise (military) signals.⁹ Although a full constellation was achieved in 1995, the economic collapse that followed the fall of the Soviet Union led to its underfunding and eventual decline to only seven operational satellites by 2001. That year, President Vladimir Putin initiated a program to revive and modernize GLONASS.¹⁰ Russia has since moved to make GLONASS interoperable with GPS, rather than attempting to compete with the American PNT service by changing its signal scheme to mirror the one used by GPS.¹¹

As the Cold War drew to a close at the beginning of the 1990's, PNT demonstrated its dramatic potential in conventional warfare throughout the following decade. Operation Desert Storm witnessed soldiers successfully navigating the featureless deserts of Saudi Arabia, Kuwait, and Iraq using GPS.¹² Although GPS-aided munitions were not yet part of the US inventory, the Air Force was also able to exploit GPS

⁹ Jet Propulsion Laboratory, "GLONASS" *JPL Mission and Spacecraft Library*. Available at: <http://msl.jpl.nasa.gov/QuickLooks/lonassQL.html>

¹⁰ "About GLONASS" *GNSS Insider online edition*, <http://www.insidegnss.com/aboutglonass>

¹¹ Katia Moskvitch, "GLONASS: Has Russia's Sat-Nav System Come of Age?" *BBC News- Russian Edition*, 1 April 2010. <http://news.bbc.co.uk/2/hi/science/nature/8595704.stm>

¹² Spires, *Beyond Horizons*, 257.

navigation in a number of its strike aircraft to improve all-weather capability and support to ground forces.¹³ At that time, the objective constellation of twenty-four satellites had not yet been completed, resulting in two-dimensional coverage twenty-four hours a day and three-dimensional coverage nineteen hours a day.¹⁴

GPS contributed significantly to combat action in Desert Storm and its impact in subsequent operations increased. In Operation Desert Storm, ninety percent of munitions used were unguided. Of the ten percent that were guided, none were GPS-capable.¹⁵ The Air Force completed the objective GPS constellation by the late 1990's, adding increasing levels of precision and accuracy that would permit a host of new combat applications, including GPS-aided munitions. In 1999, GPS-guided weapons inaugurated all-weather precision strike capabilities during Operation Allied Force in Serbia and Kosovo. When US forces initiated their support to the Northern Alliance in Afghanistan, precision munitions comprised two thirds of all the bombs dropped during the first two months of US participation in combat. Of those precision munitions, sixty-four percent were GPS-aided.¹⁶ In a 2002 essay, then-Secretary of Defense Donald H. Rumsfeld marveled at the use of precision-guided

¹³ Spires, *Beyond Horizons*, 257.

¹⁴ Spires, *Beyond Horizons*, 257.

¹⁵ Everett C. Dolman, "Astropolitics and Astropolitik," *Harnessing the Heavens*, ed. by Paul G. Gillespie and Grant T. Weller, (Chicago: Imprint, 2008), 113.

¹⁶ Bob Preston and John C. Baker, "Space Challenges," *Strategic Appraisal: US Air & Space Power in the 21st Century*, ed. by Zalmay Khalilzad and Jeremy Shapiro, (Santa Monica: Rand, 2002), 155.

munitions called in by Special Forces troops in support of the Northern Alliance insurgency against the Taliban in Afghanistan the previous year.¹⁷ Rumsfeld heralded precision-guided munitions as one component of an ambitious program of military transformation, foreshadowing the use of these munitions the following year in the opening stages of Operation Iraqi Freedom.

By the time the US and coalition troops invaded Iraq once more in the spring of 2003, seventy percent of munitions were precision guided, more than half of those being GPS-aided.¹⁸ By the early part of the 2000's, PNT services had been "normalized" across the Department of Defense. Although Congress mandated through public law that all new or modified aircraft, ships, armored vehicles, or indirect fire weapon systems be equipped with a Global Positioning System receiver after the end of September, 2005, each of the four military services appeared to be already well on their way towards equipping all combat troops and platforms with GPS.¹⁹

The appearance of GPS jammers on the battlefield in Operation Iraqi Freedom was as noteworthy as the large-scale employment of GPS-aided munitions. The GPS signals, like any other radiofrequency signal, are subject to interference or jamming. The potential vulnerability of

¹⁷ Hon. Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs*, May/June 2002. <http://www.foreignaffairs.com/articles/58020/donald-h-rumsfeld/transforming-the-military>

¹⁸ Dolman, "Astropolitics and Astropolitik," 113.

¹⁹ Office of the Chairman of the Joint Chiefs of Staff, CJCSI 6130.01C, *2003 CJCS Master PNT Plan*, 31 Mar 03, A-2.

GPS to jamming seems to have prompted Iraq to purchase a number of GPS jammers from Aviaconversiya Ltd., a Russian company that had been selling GPS jammers at military hardware shows since 1999. The high-priced and high-powered GPS jammers offered by Aviaconversiya were said to be able to jam GPS signals for a radius of several miles. The Iraqi military used at least six of these high-powered GPS jammers, which cost \$40,000 or more apiece, during the conventional phase of the war.²⁰ The jammers had little direct impact on coalition operations. US forces quickly eliminated all six jammers over the course of two nights. “In fact, we destroyed a GPS jammer with a GPS weapon,” then-Major General Gene Renuart told reporters at a briefing following the strikes.²¹ These jammers awakened space operators, strategists, and policy makers to a willingness on the part of some adversaries to attack Western asymmetric military advantages obtained through space power. Air Force Chief of Staff General John P. Jumper wrote in 2004: “as demonstrated by the deployment of Iraqi jammers during OIF, adversaries will target space capabilities in an attempt to deny US combat advantage.”²² Something may have been overlooked in the aftermath of the opening phases of OEF and OIF: adversaries were also willing to leverage Western space power for their own advantage, rather

²⁰ Frank Vizard, “Safeguarding GPS,” *Scientific American*, April 2003.
<http://www.scientificamerican.com/article.cfm?id>

²¹ Vizard, “Safeguarding GPS.”

²² General John P. Jumper, Foreword to Air Force Doctrine Document (AFDD) 2-2.1, *Counterspace Operations*, 2 August 2004.

than targeting those capabilities. The rhetoric of the time acknowledged the possibility that PNT and other space power applications could be co-opted, but there appeared to be little exploration of implications for Western military forces.²³

As dependent as modern warfare has become on PNT services, modern civilian life may be growing even more dependent. Worldwide, the ratio of civilian to military users stands at least 100 to one, and by some estimates, commercial revenues from satellite navigation exceeded \$12 billion in 2002, growing at more than 20 percent annually.²⁴ By the end of 2008, GPS receivers had been embedded in several hundred million devices worldwide. Qualcomm alone has already sold 300 million GPS-enabled cell phone chipsets. GARMIN International has delivered 48 million portable navigation devices to date, including some 16.9 million units during 2008.²⁵ GPS could be used to provide positioning and navigation information to recreational boaters and hikers, drivers of GPS-equipped cars, surveyors, and crews of commercial vessels, among others. In addition, cellular telephones, the Internet, digital cryptography, and international financial transactions all depend on GPS-based timing information.²⁶

²³ Vizard, "Safeguarding GPS."

²⁴ David L. Braunsvig, Richard L. Garwin, and Jeremy C. Marwell, "Space Diplomacy" *Foreign Affairs*, July/August 2003, <http://www.foreignaffairs.com/articles/59009/>

²⁵ Jay Gullish and David Vaccaro, "Top Ten in PNT," *Inside GNSS* online edition, November/December 2009, <http://www.insidegnss.com/>

²⁶ Braunsvig, Garwin, and Marwell, "Space Diplomacy."

Cellular telephones present an interesting dilemma for PNT services in warfare. As service charges and handset prices have plunged and coverage areas have expanded, cellular telephone subscriptions in the developing world have surged since 2000, from just over 700 million to over 4 billion subscribers at the end of 2008, according to the U.N. International Telecommunications Union.²⁷ Of course, a vast majority of irregular warfare activity takes place in the developing world: insurgencies are active in Latin America, Africa, and Asia. Afghanistan, for example, now has upwards of two million cell phone subscribers and only 20,000 fixed-line phones. By comparison, there are an estimated 800 million subscriptions in advanced economies.²⁸ To the extent that most cellular telephone systems rely on GPS to synchronize network timing, there are potentially four-plus billion (indirect) PNT users in the developing world. An adversary that seeks to deny the use of GPS to US forces must consider the impact that denial will have on the population that they depend on for support. US forces must also consider the implications of denying PNT to adversaries that operate among the population, no matter how localized they believe that denial effect to be.

²⁷ International Telecommunications Union press release: "Worldwide cellular telephone subscribers to reach 4 billion mark by end of 2008," posted September 25,th 2008. Retrieved at: http://www.itu.int/newsroom/press_releases/2008/29.html

²⁸ Malcolm Foster, "Cellular Phones Vital in the Developing World," *The Washington Post*, 27 January 2007, <http://www.washingtonpost.com/wp-dyn/content/article/2007/01/27/AR2007012700662.html>

PNT in Insurgency

Insurgencies have been able to use PNT services in some novel and unexpected ways. Insurgents have demonstrated an understanding of the advantages of satellite-enabled PNT over other positioning and navigation means, and they have put these capabilities to use. The Groupe Salafist pour la Prédication et le Combat (GSPC), recently rechristened Al-Qaida in the Islamic Maghreb (AQIM), splintered from the insurgent Islamic Army Group (GIA) in 1998, after the latter proved incapable of challenging the Algerian government.²⁹ AQIM has operated in the Saharan desert since its inception, extending its reach beyond Algeria. AQIM has been observed marking and navigating to its weapons and fuel caches in the Saharan desert using GPS positioning. The group has targeted tourists traveling in the remote deserts of southern Algeria, Mali, and Mauritania in order to obtain satellite phones, GPS and other navigation devices, and four-wheel drive vehicles.³⁰ North Africa security expert Geoff Porter notes that the introduction of handheld GPS devices to the region has made it easier for people to navigate the Sahara

²⁹ Leanne Kennedy Boudali, *The GPSC: Newest Franchise in Al-Qa'ida's Global Jihad* (West Point, NY: Combating Terrorism Center, US Military Academy, April 2007)

³⁰ Karin Bruilliard, "Moderate Mali a Barrier to Radical Islam," *Washington Post*, December 2009. Reprinted in Durham Herald-Sun, Available at http://www.heraldsun.com/pages/full_story/push?article-Moderate+Mali+a+barrier+to+radical+Islam%20&id=5287506.

and Sahel without relying on the few paved roads and established tracks even when they have limited familiarity with the terrain.³¹

In October 2008, Algeria Telecom launched GPS augmentation service for much of southern Algeria for personal GPS devices and GPS-compatible cell phones.³² Further enhancement of GPS capabilities in the Sahara and Sahel are likely in order to support energy development. Since there does not appear to be any way for Algeria Telecom to selectively deny exploitation of its GPS augmentation service, AQIM will likely use these improvements to facilitate movement around the desert and improve its ability to plan and carry out attacks.³³

Some insurgents are taking advantage of PNT-enabled weapons platforms. The Israeli Defense Force observed Hizbollah using Iranian-supplied unmanned “Ababil” aerial vehicles (UAVs) during the 2006 Israel-Hizbollah war. The Ababil is assessed by Israeli experts to be capable of carrying 40-50 kilograms of explosives, with a 450-kilometer range, and is equipped with GPS guidance.³⁴ Israeli defense experts estimated that 24-30 Ababils remain in Hezbollah hands.³⁵ Dakota Wood, a defense analyst for the Center for Strategic and Budgetary Assessments, predicts that GPS-aided munitions and other precision

³¹ Geoff D. Porter, “AQIM and the Growth of International Investment in North Africa,” *Sentinel: a Publication of the Combating Terrorism Center*. Nov 2009, Vol 2, Issue 11, 11.

³² Porter, “AQIM and the Growth of International Investment in North Africa,” 11.

³³ Porter, “AQIM and the Growth of International Investment in North Africa,” 11.

³⁴ Anthony H. Cordesman, *Preliminary “Lessons” of the Israeli-Hezbollah War* (Washington, DC: Center for Strategic and International Studies, April 2009), 5.

³⁵ Cordesman, 5.

weapons will find their way into the arsenals of Hizbollah and other insurgent groups in the near future.³⁶ Wood stated that “proliferation of precision” will greatly accelerate in coming years as munitions become more precise, with increased range, easier to use and more widely available to “irregular warriors.”³⁷

PNT in Counter-insurgency

Attempting to combat insurgent exploitation of PNT is a complex endeavor. Although it is technologically possible for space operators to use a system feature called selective availability to degrade the accuracy of the civil GPS signal, there are national-level policy implications to doing so since selective availability will impact all civil users. Realizing the economic and diplomatic potential of GPS as the worldwide PNT standard, no less a figure than the President of the United States decided to end the use of selective availability in 2000.³⁸ It seems unlikely that selective availability would be reinstated, except under the most severe national crisis. Policy makers have gone so far as to eliminate the selective availability feature from GPS III, the next generation PNT space system currently under design, which according to the White House, “reflects the United States’ strong commitment to users of GPS that this free global utility can be counted on to support peaceful civil activities

³⁶ Greg Grant, “Hizbollah on Steroids” *DoD Buzz*, 1 July 2009. Available at: <http://www.dodbuzz.com/2009/07/01/hezbollah-on-steroids/#axzz0jrHPGi31>

³⁷ Grant, “Hizbollah on Steroids.”

³⁸ Office of the President of the United States, *Statement by the President Regarding the United States’ Decision to Stop Degrading Global Positioning System Accuracy*, 1 May 2000.

around the world.”³⁹ As mentioned earlier, attempts to deny PNT services to users through indiscriminate electronic attack are fraught with risk. Unless US counter-insurgency forces can identify and selectively deny individual PNT receivers, they may be forced to accommodate adversaries who, if properly resourced, can be nearly as accurate and precise in combat as Western forces are.

As important as PNT services are for the conduct of modern conventional warfare, they are arguably even more important for the conduct of counter-insurgency. It is imperative for counter-insurgency forces to be precise in targeting insurgents. To gain and maintain the support of the majority of the population, counter-insurgency forces must minimize casualties and collateral damage among that population. Lt Col Stuart Pettis, reflecting on his air-ground coordination experiences in Iraq, noted that “in an irregular warfare fight, I’ve got to have the level of precision a JDAM offers, both to address dispersed targets and to minimize collateral damage or else I have to rely on laser-guided bombs.”⁴⁰ The US Army has also incorporated GPS-aided munitions into its field artillery (or indirect fires) systems to deliver precise effect against

³⁹ Office of the President of the United States, *Statement by the Press Secretary on the President’s Decision to End Procurement of GPS Satellites that have the Capability to Intentionally Degrade the Accuracy of Civil Signals*, dated September 18, 2007.

⁴⁰ Lt Col Stuart Pettis, Chief, Strategy and Doctrine, Headquarters Air Force Space Command, interview by the author, 18 Feb 2010.

insurgents, mindful of the consequences of collateral damage in a counter-insurgency campaign.⁴¹

The Israeli Defense Force received considerable condemnation from world observers for its targeting methodology against Hizbollah in Lebanon,⁴² but air and ground forces did emphasize precision in every bomb dropped. One month into the conflict, the IAF had flown some 8,000 fighter sorties and 1,600 attack helicopter sorties with no losses to combat, and with considerable effectiveness – at least in missions supporting Israel’s land operations. IDF army officers at the front noted that most such sorties were flown with delivery accuracies approaching 10 meters and close air support was extremely responsive.⁴³ PNT services are only one element of precision- target location and weapons function also matter. However, to the extent that space operators can assure the best possible performance of PNT services, successful counter-insurgency demands that they do just that.

PNT in Counter-terrorism

Terrorists have used personal GPS devices in the past to support their operations. The Deccan Mujahideen, the group that carried out the 2008 attacks in Mumbai discussed earlier in Chapter 2, carried GPS

⁴¹ SGT Henry Selzer, “Excalibur Round Debuts in Afghanistan,” *Army.Mil News*, 10 May 2008.

<http://www.army.mil/-news/2008/03/10/7842-excalibur-round-debuts-in-afghanistan/index.html>

⁴² William Arkin encapsulates international criticism of the Israeli bombing campaign in his study of the 2006 war. See William M. Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War* (Maxwell AFB: Air University Press, 2009).

⁴³ Cordesman, *Preliminary “Lessons” of the Israeli-Hezbollah War*, 22.

receivers as well as satellite phones. The terrorists, who are alleged to have come from Karachi, Pakistan, hijacked a fishing trawler off Porbandar port in the Indian state of Gujarat, killed the four-member crew, and navigated their way to their entry point in Mumbai using GPS equipment and a satellite phone.⁴⁴ Authorities who recovered the equipment found the route from Karachi to Mumbai programmed into one of the units, along with a number of targets programmed as waypoints.⁴⁵

Countering terrorist use of PNT requires an added level of precision beyond what may be necessary even to counter insurgent use of PNT. Although terrorists may operate in built-up or urbanized areas that subject PNT services to masking effects, terrorists can often leverage urban augmentation services to supplement PNT. That terrorists use GPS is another indication of just how pervasive PNT services (namely GPS) have become in the past two decades. GPS would appear to be moving towards what RAND analyst Martin Libicki refers to as “friendly conquest.”⁴⁶ Friendly conquest builds initially on voluntary transactions, in this case purchasing GPS-equipped devices and using

⁴⁴ Indrajit Basu, “Mumbai Terrorists Aided by Technology,” *United Press International*, 2 December 2008.
http://www.upiasia.com/Security/2008/12/02/mumbai_terrorists_aided_by_technology/9520/

⁴⁵ Court of Addl. Ch. M.M., Final Form/Report, “Terrorist Attacks on Mumbai,” (37th Court, Esplanade, Mumbai), 2009), 37-38, <http://www.hindu.com/nic/Mumbai-terror-attack-final-form.pdf>

⁴⁶ Martin C. Libicki, *Friendly Conquest in Cyberspace* (Cambridge: Cambridge University Press, 2007), 126.

the service, as the Deccan Mujahideen did in Mumbai. Friendly conquest is said to have taken place if “subsequent interactions and dependencies enable the conqueror to make reliable and effective use of the assets of the conquered.”⁴⁷ The key to conquest will be making reliable and effective use of the adversary’s GPS device to assist counter-terrorism and counter-insurgency operations. Friendly conquest through GPS may someday open the door for cyber power to be used in conjunction with space power to attack an adversary through his own receiver. Until that is possible, the US may be forced to tolerate adversary exploitation.

PNT in Building Partnership Capacity

As free and universally available services, satellite-enabled positioning, navigation, and timing offer tremendous potential for building partnership capacity efforts. In one example of building partnership capacity using PNT, the Combined Air Power Transition Force in Afghanistan is training Afghan National Security Forces aviation units to navigate aircraft using commercial GPS receivers.⁴⁸ Although Afghan pilots are learning to navigate using GPS at a lower level of sophistication than the US and many of its coalition partners, this is an important step towards interoperability.

⁴⁷ Libicki, *Friendly Conquest in Cyberspace*, 126.

⁴⁸ Brig Gen Michael Boera, Commanding General, CAPTF and Commander, 438th Air Expeditionary Wing, in discussion with the author, 13 May 2010.

In another example Naval Special Warfare Unit 10, a Navy force provider to US Africa Command's Special Operations Command-Africa, is working with select partner nations to increase their capacity to secure their coastlines by training and advising maritime counter terrorism units. Cameroon elite Battalion d'Intervention Rapide forces have trained with SEAL and Special Warfare Combatant Craft operators on basic boat handling skills, waterborne patrols, GPS navigation and vessel interdiction.⁴⁹ This is only one minor example of many potential examples of building partnership capacity through PNT capabilities.

Building capacity through PNT can involve a comprehensive effort beyond training partner state counter-insurgency forces how to navigate using personal devices. Space operations trainers and advisors can instruct partner state space operations candidates on a host of PNT-related applications. The Director of Space Forces at Twelfth Air Force/Air Forces Southern, working with strategists at US Southern Command, has initiated a pilot program to train a number of Latin American representatives on GPS Operations Center applications.⁵⁰ In the future, the US might leverage private industry to equip partner state forces with augmentation systems, especially in parts of the partner state where topography limits GPS signal reception.

⁴⁹ MCC S. Travoli, "Unit 10: a Force Multiplier," *Ethos: Naval Special Warfare*, Issue 8, undated, www.navsoc.navy.mil/pdf/Ethos/ETHOS_ISSUE_8.pdf

⁵⁰ Lt Col Dan Jones, Director of Space Forces, 612th Air & Space Operations Center, to the author, email, 9 March 2010.

The US Government must determine on a case-by-case basis those partner states that it is willing to share the PPS service with. In those instances where PPS is not deemed appropriate for the partner state, SPS service, especially when it is coupled with augmentation services, can provide a significant degree of precision to partner states.

The example of how AQIM has been able to exploit GPS and the Algerie Telecom GPS augmentation service is not only instructive of one way in which insurgencies can leverage PNT services, but also of how a potential capacity-building effort could be turned against the partner state. This is not to say that building partnership capacity should not be accomplished through GPS or GPS augmentation, but rather that there is an inherent risk that universal services like GPS can be exploited by friend and foe alike.

Summary

Satellite-enabled positioning, navigation, and timing have become the standards for maneuvering and synchronizing in modern warfare. The impact of these services is in no way diminished by the conduct of irregular warfare; in fact, their impact is probably even greater. Precision in irregular warfare has become an imperative. The universality of PNT services carries both challenges and opportunities. US preeminence in satellite-enabled PNT may be the greatest future guarantor of space superiority, at least as it relates to positioning and timing.

This chapter, along with the first three chapters, has alluded to the premise of space superiority: assuring one's freedom of action to use space power while being prepared to deny the same freedom to the adversary. The next chapter, entitled "Space Control," draws threads together from the preceding chapters in a more detailed discussion of space superiority and space control.

Chapter 5

Space Control

The mission of space control has not yet been at the forefront of military thinking because our people haven't yet been put at risk by an adversary using space capabilities. That will change.

Hon. Peter B. Teets
Undersecretary of the Air Force
2002

This chapter discusses space control and its relationship with irregular warfare. Each of the mission areas within space control has an impact on irregular warfare activities, while each mission area is impacted by irregular warfare in return. The objectives of space control and space superiority are also affected by the conduct of irregular warfare activities by multiple actors in the confrontation. Because other actors may exploit the same services that friendly forces do, traditional concepts of space control must be altered and the notion of space superiority must address a greater level of complexity.

This chapter opens by describing the space control mission and each of its sub-missions or elements. Each element of the space control mission is then related to individual irregular warfare activities: insurgency, counter-insurgency, counter-terrorism, and building partnership capacity.

The *mission* of space control attains and maintains a desired degree of space superiority by allowing friendly forces to exploit space capabilities while denying an adversary's ability to do the same.¹ Steven Lambakis offers that the *condition* of space control is "the ability to prevail over the enemy's hostile use of spacecraft when and where it matters, and to be able to use space at will for such purposes as the establishment of command, control, communications, and information networks."²

Space operations doctrine divides the mission of space control into the sub-missions of offensive and defensive space control. Space control is also divided among four mission sub-sets: space situational awareness, prevention, protection, and negation. For the sake of precision, these four sub-sets will be used for discussion in this chapter in lieu of offensive and defensive space control.

Space Situational Awareness

Space situational awareness (SSA) is defined as "the requisite current and predictive knowledge of the space environment and the operational environment upon which space operations depend – including physical, virtual, and human domains – as well as all factors, activities, and events of friendly and adversary space forces across the

¹ Air Force Doctrine Document (AFDD) 2-2, *Space Operations*, 27 Nov 06, 5.

² Steven Lambakis, *On the Edge of the Earth* (Lexington, KY: University of Kentucky Press, 2001), 141.

spectrum of conflict.”³ As it is defined, space situational awareness occupies a continuum of knowledge, where requisite knowledge is relative to the operator and his/her location in the system. SSA is not a mission that is performed, per se, but rather the product of awareness-building activities that in turn enables space operations.⁴ SSA-building activities include surveillance, and reconnaissance, and the analysis that turns their data into intelligence. Environmental monitoring and monitoring one’s own space system status also contribute to building and maintaining SSA.

Although the national security space enterprise has pursued some level of situational awareness from the earliest days of the American Space Age, SSA as a doctrinal concept is relatively new, taking the place of space surveillance as an element of space control.⁵ However, it is important to note that SSA and space surveillance are not one and the same. Space surveillance activities inform space situational awareness, but they do not substitute for the knowledge condition of awareness.

SSA has traditionally been regarded as a global (or multi-theater) mission, performed by the combatant command with functional responsibility for space operations. Since 2002, United States Strategic Command has conducted the SSA “mission,” delegating responsibility to

³ Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, GL-10.

⁴ Maj Tyler Evans, “Space Coordinating Authority,” *Space Power Integration: Perspectives from Space Weapons Officers* Ed. by Lt Col Kendall H. Brown. (Maxwell AFB: Air University Press, 2006), 20.

⁵ David N. Spires, *Beyond Horizons: a Half-Century of Air Force Space Leadership* (Maxwell AFB, AL: Air University Press, 1998), 72.

its Joint Functional Component Command for Space.⁶ The global SSA mission has taken on a renewed level of urgency in recent years, owing to two major events. In 2007, the People's Republic of China tested a ground-launched Anti-Satellite (ASAT) weapon against an obsolete weather satellite, destroying the satellite and littering the spacecraft's low-earth orbital plane with debris.⁷ In 2009, an Iridium satellite collided with a Russian Cosmos spacecraft, destroying both and creating additional debris in low-earth orbit.⁸ Both events have highlighted the need for better intelligence and better sensors to support more comprehensive situational awareness at a global level. US-conducted space debris tracking and orbital collision avoidance functions have become imperatives for safe and effective space operations. These functions not only support national security space operations, but also civil and commercial space operations. Foreign space operations have also begun to depend upon the JFCC-Space SSA mission for debris and collision avoidance.

Space Control-Prevention

Space Control-Prevention is defined as “measures to preclude an adversary's hostile use of US or third party space systems and services.”⁹

⁶ USSTRATCOM Fact Sheet, “JFCC-Space” Jan 2008, <http://www.stratcom.mil/factsheets/space/>

⁷ Jim Wolf, “US details China satellite debris” *Reuters online edition*, 10 April 2007. <http://www.reuters.com/article/idUSN1044576620070411>

⁸ Jim Wolf, “US, Russian satellites collide in space” *Reuters online edition*, 11 Feb 2009. Retrieved at <http://www.reuters.com/article/idUSTRE51A8IA20090211>

⁹ Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, II-5.

Prevention is proactive versus reactive, setting the conditions before conflicts erupt and space capabilities are usurped by an adversary. Space operations doctrine offers that prevention “can include diplomatic, economic, and informational measures as appropriate.”¹⁰ Citing the French agreement not to sell SPOT imagery to Iraq during Operation Desert Shield, Michael Sheehan offers that the US could conduct “diplomatic space control” by encouraging states not to provide adversaries with support during conflicts.¹¹ The US may have limited options for conducting prevention actions. Prevention is likely to demand a whole-of-government approach in collaboration with the Departments of State and Commerce, as well as private industry to produce meaningful results.

Prevention efforts must begin well in advance of a conflict and continue throughout a conflict in order to be effective. Policy makers and strategists must commit to a long-term and adaptive prevention effort that leverages multiple elements of national power. It is important to note, however, that prevention will be difficult to achieve through space powers with which the US has no diplomatic or economic ties.

Space Control-Protection

Space Control-Protection is defined as “active and passive defensive measures ensure that US and friendly space systems perform

¹⁰ Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, II-5.

¹¹ Michael Sheehan, *The International Politics of Space* (New York: Routledge, 2007) 107.

as designed by overcoming an adversary's attempts to negate friendly exploitation of space, or minimize adverse effects if negation is attempted.”¹² Active defensive measures could include such measures as: maneuver of spacecraft on orbit out of harm's way; boosting power to electromagnetic links between the spacecraft and the ground and/or the user segment; or in the future, deploying decoy or bodyguard spacecraft to divert attack, to name only a few examples.¹³ Passive defense measures could include such measures as: shielding and camouflaging; performing changes to negated electromagnetic link waveforms; distributing a mission among several spacecraft on orbit, or enhancing the physical- and cyber-security of the ground segment.¹⁴

Space Control-Negation

Space Control-Negation is the set of active and offensive measures that are intended to interfere with another actor's ability to exploit space power. Space operations doctrine describes negation activities in terms of the effects that the activities produce: deceive, disrupt, deny, degrade, or destroy.¹⁵ Privately-run space systems, especially satellite communications and satellite-enabled networks, pose two fundamental problems for negation efforts: hostile party users must be identified out of all service users and targeting US-owned or consortia satellites carries

¹² Joint Publication (JP) 3-14, *Space Operations*, 6 January 2009, II-5.

¹³ Air Force Doctrine Document (AFDD) 2-2.1, *Counterspace Operations*, 2 Aug 2004, 26-27.

¹⁴ Air Force Doctrine Document (AFDD) 2-2.1, *Counterspace Operations*, 2 Aug 2004, 27.

¹⁵ Joint Publication 3-14, *Space Operations*, 6 January 2009, II-5.

significant legal issues.¹⁶ For regimes that attempt to abide by internationally-accepted norms of behavior, collateral damage to other satellite users could be a significant issue, as would be targeting satellites registered by friendly and neutral states. Steven Lambakis states: “the denial and negation of third-party satellites used for hostile purposes becomes a severe military and diplomatic challenge if the enemy can skillfully use international, commercial, globalized, networked space systems, thereby retrieving militarily useful products from different places, some through third parties and others under assumed names.”¹⁷

Negation efforts may pursue effects through destructive and non-destructive means. Destructive (or kinetic) negation could use terrestrial-based anti-satellite weapons, such as the ground-based direct-ascent weapon that China tested in 2007¹⁸ or the F-15 delivered air-to-space missile tested in the mid-1980’s.¹⁹ Co-orbital weapons could also be used to maneuver and destroy targeted satellites in orbit. Destructive means may also use directed energy from one of the terrestrial domains or on orbit. Non-destructive means could use electromagnetic energy to jam or blind a targeted satellite. Unlike destructive means, their effects could be both temporary and reversible.

¹⁶ Steven Lambakis, *On the Edge of the Earth*. Lexington, KY: University of Kentucky Press, 2001, 87.

¹⁷ Lambakis, *On the Edge of the Earth*, 184.

¹⁸ Sheehan, *The International Politics of Space*, 167.

¹⁹ The anti-satellite weapon was officially named the “Miniature Homing Device.” See Spires, *Beyond Horizons*, 188.

Negation need not target the satellite to affect a space system: the ground segment, the radio-frequency links, and the user segment can each be held at risk, as well. As we will see later in the chapter, jamming either the uplink or downlink radio-frequency links of a space system has become a favored negation tactic.

Space Control in Insurgency

Space Situational Awareness would seem to be an odd concern for insurgents. Insurgents may have little use for a comprehensive space picture, but to the extent that they leverage space capabilities, SSA is a factor nonetheless. Some degree of SSA is necessary for the insurgent to exploit space power, while preventing interference, protecting their continuous exploitation, and even negating the capabilities of their adversaries.

Recall the satellite communications piracy episodes in Brazil and Sri Lanka that were described in Chapter 2: both the Brazilian satellite bandwidth pirates and the LTTE required some level of understanding (albeit primitive) of the systems they were pirating in order to effectively exploit the signals they used. A Brazilian amateur radio operator who had studied the Satelite Bolinha (little ball satellite) campaign over several years was able to document how simple it was for pirates to obtain widely available specifications and frequency information over the

Internet, some of which was open-source DoD tactics, techniques, and procedures for UHF satellite communications access.²⁰

Satellite over-flight data could be of great value to insurgents for camouflage, concealment, and deception purposes. Satellite tracking data is widely available to interested users over the Internet, and the track data on a number of sites is of notable quality.²¹ Although no evidence exists to suggest that insurgents or terrorist groups are exploiting open source satellite-tracking data, policy makers and strategists must realize that space operations, like terrestrial military operations, are more transparent to interested parties than ever before.

Prevention in insurgency seeks to deter or dissuade other actors from interfering with the insurgent's ability to exploit space power. The other actors may include the government, an occupying force, or a competitor insurgency operating in the same environment. Perhaps the optimal means of prevention for the insurgent is state support through space power mentioned in Chapter 3, which may pose significant diplomatic and military challenges to the regime and its support. If Sheehan's diplomatic space control does not suffice to prevent state support to an insurgency, and negation efforts against that state pose unacceptable consequences, then the counter-insurgency forces may be

²⁰ Adinei Brochi, *Satelites Bolinha* (self-published, undated), <http://www.py2adn.com/artigos/Satelite-Bolinha>
Referenced by Marcelo Soares, "The Great Brazilian Sat-Hack Crackdown," *Wired*, 20 April 2009, <http://www.wired.com/politics/security/news/2009/04/fleetcom>

²¹ One example is www.n2yo.com, which advertises "real time satellite tracking" for a variety of military, civil and commercial spacecraft.

forced to cope with the effects provided to insurgents by state support. Should Iran opt to share data on Israel from its planned family of remote sensing satellites, or bandwidth over its communications satellites with Hizbollah, Israel and its allies may be left with few options to disrupt Hizbollah space power that do not risk a greater regional conflict with Iran.²²

Protection in insurgency seeks to defend insurgent space power against the negation efforts of another actor. Redundancy may offer insurgents the best defense against negation. Tier Three space powers may leverage the services of multiple providers to insure themselves against negation efforts. Although the US has listed Al-Manar as a terrorist organization and many European states have successfully removed its broadcasts using legal action, Hizbollah is still able to transmit Al-Manar over leased channels aboard regional carriers²³

Insurgents who are able to take on attributes of Tier Two space power enjoy greater flexibility for the protection of their space capabilities. In the opening hours of the Israeli offensive, fighter-bombers attacked and destroyed the Al-Manar building. In spite of the

²² BBC News, "Iran set to build three remote sensing satellites," *BBC Trans-Caucasus Monitoring*, 3 March 2009. Accessed at Lexis-Nexis Academic database: http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518889519&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9518889524&cisb=22_T9518889523&treeMax=true&treeWidth=0&csi=10962&docNo=1

²³ Doreen Carvajal, "France bans Al-Manar TV channel" *New York Times online edition*, 15 December 2004, http://www.nytimes.com/2004/12/15/news/15iht-t5_17.html Erik Kirschbaum, "German government blocks Al-Manar" *Variety*, 23 November 2008. <http://www.variety.com/article/VR1117996353.html?categoryid=14&cs=1>

Israeli strike, programming was back on the air no later than ten minutes after the attack.²⁴ Hizbollah had anticipated Israeli strikes against Al-Manar, and took steps well in advance to build redundancy into its satellite broadcast system.

Although the US can implement some procedural controls to limit insurgent access to US commercial imagery, these controls may be insufficient to significantly impact the insurgent. Michael Sheehan reasons that users are unlikely to wait until a confrontation begins before stockpiling imagery resources, rendering shutter control and diplomatic measures “too little, too late” in many cases.²⁵

Insurgents who use GPS for positioning, navigation, and timing services must operate under the assumption that other actors cannot selectively target users for degradation or denial. Insurgents must also operate under the assumption that any degradation or denial effort that another actor undertakes will impact civilian users, just as it would impact the insurgent. In the future, the Galileo constellation may offer insurgents an alternative to GPS should their assumptions not bear out in conflict.

Negation as it applies to insurgency seeks to diminish other actors’ abilities to utilize space power. Insurgents may even operate against some combination of the three actors. Although the perpetrators behind

²⁴ Thomas Rid and Marc Hecker. *War 2.0: Irregular Warfare in the Information Age* (Westport, CT: Praeger, 2009),155.

²⁵ Sheehan, *The International Politics of Space*, 107.

the satellite bandwidth piracy episodes recounted in Chapter 2 did not appear to seek negation of satellite voice communications or satellite-enabled networks, they achieved these effects nonetheless, if in a very limited scope. The ability to engage in satellite bandwidth piracy connotes to the ability to negate a satellite communications signal. Strategists and policy makers should be aware that negation through intentional interference represents a considerable asymmetric advantage to adversaries that requires little in the way of resources or expertise.

Negation may occur in the terrestrial domains or air, sea, or land, without affecting the space segment. Recall the Aviaconversia jammers that the Government of Iraq employed against coalition forces during the conventional phase of Operation Iraqi Freedom: in that instance, a state had attempted to degrade GPS service to affect another state's military forces.²⁶ There is widespread concern that insurgents and terrorists could attempt similar action against US forces in the future. Because the GPS signals are relatively weak and their frequencies are public knowledge, jammers are not especially difficult to devise or use. The US Department of Transportation stated as early as August 2001 that "some jamming devices/techniques are available on the Internet and proliferation will continue, because a single device that could disrupt military and civil operations worldwide would be attractive to malicious

²⁶ Frank Vizard, "Safeguarding GPS." *Scientific American*, April 2003.
<http://www.scientificamerican.com/article.cfm?id>

governments and groups."²⁷ If no insurgent groups in Iraq or Afghanistan have used GPS jammers against coalition forces in the past seven years, perhaps it is because they are also exploiting GPS and they recognize the potential to negate themselves.

Space Control in Counter-insurgency

Space Situational Awareness in counter-insurgency provides regimes and counter-insurgency forces with the requisite understanding of space as it relates to the operating environment. SSA should not only inform counterinsurgent forces of the conditions under which they will exploit space power: SSA should also build awareness of how the insurgent is attempting to exploit space power.

Prevention in counter-insurgency employs measures to prevent the insurgent from holding one's own space capabilities at risk. Again, the satellite piracy episodes from Chapter 2 are instructive: DoD appeared to detect the pirate signal over Fleetsat and geo-locate its source to Brazil with relative ease.²⁸ As stated earlier, however, military satellite communications depend on an increasing share of commercial satellite communications services. Policy makers and strategists must take into

²⁷ Bob Brewin, "Homeade GPS jammers raise concerns" *Computerworld* online edition, 17 January 2003.
http://www.computerworld.com/s/article/77702/Homemade_GPS_jammers_raise_concerns

²⁸ BBC News, "Brazilian police arrest US military satellite hackers," *BBC World Service online*, 4 May 2009. Accessed through Lexis-Nexis Academic database,
http://www.lexisnexis.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518731342&format=GNBFI&sort=RELEVANCE&startDocNo=1&resultsUrlKey=29_T9518731345&cisb=22_T9518731344&treeMax=true&treeWidth=0&csi=10962&docNo=1

account that commercial providers deliver a service agnostic of its use unless the firm detects technical problems with that service. Intelsat appeared to be unaware that anything was amiss aboard Intelsat 12 until the Government of Sri Lanka notified the firm that the LTTE had pirated a channel on the satellite over a two-year period.²⁹ Intelsat 12, formerly named “Europe Star 1,” joined the Intelsat fleet as part of the acquisition of the PanAmSat company.³⁰ This is not to suggest that Intelsat was negligent as a service provider, only that commercial service providers may lack the sophisticated detection and geo-location abilities that US military forces have demonstrated. As commercial satellite communications providers carry an increasing ratio of military communications, this is a limitation that policy makers and strategists need to take into account.

Protection in counter-insurgency assures the use of one’s own space power capabilities when insurgents can hold those capabilities at risk. A poorly resourced insurgency is unlikely to hold spacecraft at risk with anti-satellite capabilities, but they may be able to hold links and user segments at risk. Passive protection measures such as maneuver, power increases, and changes to channel assignment may not always be feasible. Maneuvers may disrupt other service customers. Spacecraft

²⁹ Embassy of Sri Lanka, “LTTE’S Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT Ltd,” 24 April 2007. www.slembassyusa.org/press_releases/spring_2007/lttes_transmissions_24apr07.html

³⁰ Embassy of Sri Lanka, “LTTE’S Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT Ltd,” 24 April 2007.

design may not permit power level changes to the signal. Channel reassignment may not be practical aboard a spacecraft at or near maximum capacity in terms of users. The head of one commercial satellite communications firm stated publicly that his company has purposely offered narrow beams for certain markets to make it more difficult to invade the signal, particularly in Asia.³¹ Several commercial satellite-fleet operators have stated they are considering the addition of nulling antennas or other onboard gear to provide at least some protection to their satellite signals. But the cost of the added hardware remains an issue.³²

Returning once more to satellite bandwidth piracy, several months of bandwidth piracy elapsed before the Government of Sri Lanka and Intelsat were able to successfully force the LTTE off of the Intelsat 12 transponder.³³ The Government of Sri Lanka, the US Department of State and the Department of Commerce, and Intelsat Ltd., collaborated over time to resolve the piracy issue. A lengthy, hard-won diplomatic/economic effort may be the last resort to regain and protect a contested resource. Sheehan's diplomatic space control might more appropriately be characterized as diplomatic-economic space control under such conditions.

³¹ Peter de Selding, "Libya Pinpointed as Source of Months-Long Satellite Jamming in 2006," *Space News*, 7 Jul 2005, https://www.space.com/spacenews/businessmonday_070409.html

³² de Selding, "Libya Pinpointed as Source."

³³ Embassy of Sri Lanka, "LTTE'S Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT Ltd" 24 April 2007.

Turning towards the protection of PNT services, the next two generations of planned GPS spacecraft will feature enhancements that increase signal power in a threatened environment, as well as both a distinct military (or “M”) code and a civil-use frequency.³⁴ Although added power and frequencies do not preclude interference, they do offer regimes with a greater degree of redundancy of PNT service.

Negation in counter-insurgency seeks to diminish the insurgent’s ability to utilize space power. Insurgents that have taken on characteristics of Tier Two space powers may offer opportunities for other actors to negate insurgent capabilities by disrupting or destroying space power infrastructure. One example is the Israeli Air Force attack against the al-Manar station.³⁵ However, most insurgent groups can be anticipated to exhibit Tier Three space power, prompting the regime to pursue diplomatic space control or temporary, reversible measures.

Almost any conceivable act of destruction entails risk for counter-insurgency forces. There is an inherent risk that destruction will cause collateral damage, as well as a risk that destruction simply will not deliver the desired outcome. Precision is a key consideration in any negation effort, whether it is destructive or non-destructive in intent. Col Thompson offers: “a higher level of target development and precision in targeting is required (in irregular warfare). Assuming again we are

³⁴ US Air Force Fact Sheet, “Global Positioning System” 22 Mar 2007, <http://www.af.mil/information/factsheets/factsheet.asp?id=119>

³⁵ William Arkin, *Divining Victory: Airpower in the 2006 Israel-Hezbollah War* (Maxwell AFB, AL: Air University Press, 2007), 112, 170, 204.

operating in battlespace conditions in which insurgents/irregulars are intermixed with friendlies or non-combatants, it is counter-productive to target and deliver effects broadly and in a manner that deprives everyone of the capabilities you wish to deny the enemy.”³⁶

Precision may not be sufficient to assure that negation will be successful, however. William Arkin remarks: “Israel found, as the United States has found ever since it mounted attacks on Iraq’s state-run media in the 1991 Gulf War and Serbian media in 1999: modern broadcasting is far too dispersed and robust to disrupt...when Israel did attack Al-Manar television in south Beirut, the signal reappeared within minutes; despite additional “nodal” targeting of transmitters and destruction of the fixed broadcasting studio in Beirut, Hizbollah was able to continue broadcasting throughout the conflict.”³⁷

Israel turned to non-kinetic negation efforts within several days of its initial strikes because it had been unsuccessful at taking Al-Manar off the air by destroying its known broadcast sites in Lebanon. Israel went one step further than interfering with the Al-Manar signals: they were allegedly able to pirate the Al-Manar television signal with a broadcast signal of their own. According to an unconfirmed report by Egypt's Middle East News Agency, Israel managed "to intercept the satellite transmissions of Hezbollah's al-Manar TV channel over three successive

³⁶ Col David Thompson, Director of Space Forces, Air Forces Central Command, to the author, email, 23 Apr 2010.

³⁷ Arkin, *Divining Victory*, 114.

days, replacing it with Israeli transmissions that reportedly showed Hezbollah command sites and rocket launching pads that Israel claimed it had raided".³⁸ In pirating a television signal aboard a non-Israeli commercial satellite, Israel has crossed into undefined diplomatic and economic territory. Although negation may have been well justified in this case (and preferable to destruction for a variety of reasons), it does carry a host of implications that policy makers and strategists must carefully consider for the future.

Space Control in Counter-terrorism

Space Situational Awareness in counter-terrorism, not unlike counter-insurgency, provides regimes and counter-terror forces with the requisite understanding of space as it relates to the operating environment. SSA should not only inform counter-terror forces of the conditions under which they will exploit space power, but SSA should also build awareness of how terrorist groups are attempting to exploit space power.

Prevention in counter-terrorism attempts to keep space power out of the hands of terror groups. While regimes and commercial firms may be able to force pirates off of satellite channels, it may be much more difficult to prevent terror groups from exploiting satellite voice communications and satellite-enabled networks. Indeed, it may be preferable not to prevent terror groups from exploiting satellite

³⁸ Peter Feuilherade, "Israel steps up "psy-ops" in Lebanon," *BBC News-Middle East*, 26 July 2006, http://news.bbc.co.uk/2/hi/middle_east/5217484.stm

communications, so that the regime can realize intelligence benefits from this exploitation.

Counter-terrorism forces may also attempt to limit access to surveillance and reconnaissance products. Steven Lambakis notes: “the ability of regional powers to view objects and activities on earth is a source of some concern – so much so that US policy makers have gone about the nearly impossible task of controlling domestic imagery distribution using “shutter control” measures and by trying to persuade our allies to do the same.”³⁹ Shutter control policy allows the US Government to halt collection of an area of concern by US commercial satellite observation providers in an emergency. While shutter control may offer a means to deny terror groups some US commercial imagery, it can do nothing to deny them imagery from foreign providers. Here, Sheehan’s diplomatic space control concept may be of some value, although shutter control and diplomatic/economic space control presuppose insight into terrorist targeting methodologies.⁴⁰

Protection in counter-terrorism seeks to defend regime space power from attack by terrorist groups. Although no example of terrorist attack against space power infrastructure has been documented as of this time, the possibility exists that terrorists could target fixed user or ground

³⁹ Lambakis, *On the Edge of the Earth*, 166.

⁴⁰ Sheehan, *The International Politics of Space*, 107.

segments. Terrorist groups could also undertake non-destructive negation efforts against regime space capabilities.

Negation in counter-terrorism seeks to deny the use of space power to terror groups. Negation to support counter-terrorism must be even more focused and precise than negation for conventional warfare or counter-insurgency, because the terrorist can blend in to the population with significant effectiveness. The potential for collateral damage, even when using non-destructive means, is even greater in counter-terrorism than it is in counter-insurgency.

In perhaps the most persistent jamming event ever recorded in the commercial satellite sector, Libyan nationals compromised the L-band communications signals from Thuraya for more than six months in 2006.⁴¹ The interference reportedly ceased only after the government of the United Arab Emirates made a diplomatic initiative to the government of Libya.⁴² A representative from the United Arab Emirates intimated: "Those doing the jamming were apparently concerned that smugglers carrying contraband items from Chad or Niger into Libya were using Thuraya satellite phones. They wanted to disrupt their operations and thought this was a way to do it. I don't know whether they even realized the effect this was having on the Thuraya signal way beyond the borders

⁴¹ de Selding, "Libya Pinpointed as Source."

⁴² de Selding, "Libya Pinpointed as Source."

of Libya."⁴³ Although it would be difficult to classify the episode as a counter-terrorist operation, Libya's ham-fisted approach to negation should serve as a warning to future negation efforts in support of counter-terrorism and counter-insurgency operations. If the smugglers were in fact using Thuraya phones in the beginning, they likely would have moved on to other means of communication well before Libya halted its jamming campaign against Thuraya.

Space Control in Building Partnership Capacity

At first, space control seems to be an unlikely candidate for building partnership capacity efforts. However, space situational awareness, prevention, and protection measures should be developed to some extent to enable the partner state military forces to utilize space capabilities as Tier Three space powers.

Building partnership capacity through space situational awareness measures should provide the partner state with a suitable level of awareness of the space environment in order to utilize space power effectively. Building capacity through SSA can also permit partner states to conduct space operations independently as Tier Two space powers, to the maximum practical extent.

A number of leaders in the US national security space enterprise have spoken publicly of the need to improve space situational awareness through additional sensor capacity. General Kevin P. Chilton noted his

⁴³ de Selding, "Libya Pinpointed as Source."

2010 United States Strategic Command posture hearings before Congress: “we must continue to work with international partners to expand the few sensors that make up our current capability.”⁴⁴ Additional sensors could contribute to the comprehensive space picture that US policy makers and strategists seek.

Prevention measures for building partnership capacity should emphasize limiting opportunities for insurgents or terrorists to exploit partner state space power. For those states that qualify as Tier Three space powers, there may be little that can be done to prevent exploitation of space services and products by insurgents and terrorists beyond Sheehan’s concept of diplomatic space control. Partner states and their military forces may be obliged to operate under conditions of space parity with their adversaries. States that seek to become Tier Two space powers must guard against the exploitation of their dual-use space systems by insurgents and terrorists.

Building partnership capacity through protection measures must focus on defending friendly users from insurgent and terrorist negation efforts. Partner state military forces that operate as Tier Three space powers should be equipped with redundant capabilities and the capacity to reconstitute space-enabled services and products after an insurgent or terrorist attack. States that possess Tier Two space power may be

⁴⁴ Gen Kevin P. Chilton, *2010 Posture Statement to US House of Representatives Armed Services Committee, Subcommittee on Strategic Forces*, 16 March 2010.

candidates for status reporting and active defensive features for their satellite designs.

Summary

Space power is no longer the exclusive purview of nation-states and so the ability to conduct space control activities is no longer limited to nation-states. Even in the context of irregular warfare, each actor attempts to build some degree of space situational awareness in order to effectively exploit space power. Each actor attempts to prevent others from exploiting his space capabilities, while protecting those capabilities from attack. Finally, each actor attempts to negate the space capabilities of others to secure advantage over the other actors. The insurgent and the terrorist will not require the same degree of awareness to operate effectively as Tier Three space powers, nor are they impacted as significantly by negation. Policy makers and strategists should consider carefully what can be controlled through space control measures and just what degree of superiority over the insurgent and the terrorist is feasible. In many, if not all cases, a whole-of-government and a combined government-private industry effort are key for successful control.

Conclusion

Insurgencies, counter-insurgencies, terrorism, and counter-terrorism change the ways in which policy makers and military strategists should think about the use of space power in conflict. Building partnership capacity in friendly nation-state military forces also demands fresh thinking on the exploitation of space power. The US and its allies have enjoyed asymmetric advantages in space power against their opponents since the end of the Cold War, but those asymmetries are diminishing, even against non-state actors with very limited space power resources. Space-enabled products and services are now widely available to interested users around the globe, and these products and services do not necessarily require investments in spacecraft or space support infrastructure.

Irregular Warfare within Space Power

Space forces must think about and conduct irregular warfare differently than they do other forms of warfare. Irregular warfare is perhaps more of a diplomatic, economic, and informational effort than it is a military effort. Space power can no longer be regarded as distinct units of national security space, civil space, and commercial space. To conduct irregular warfare activities effectively, space power must be regarded not only as a combined government and private industry enterprise, but also as a whole-of-government enterprise.

Space power thinking must become user- and link-focused, rather than spacecraft-focused. This is not to say that the space segment is irrelevant, but rather that the user is the central element of a space system in an irregular warfare setting. Irregular warfare activities put a premium on specially trained personnel who can effectively exploit space power as participants in counter-insurgency, counter-terrorism, or advisory efforts.

In the decade following the end of the Cold War, a number of analysts seemed to develop an expectation that a technology-driven Revolution in Military Affairs (RMA) would permit Western wars to be conducted relatively quickly, at a minimal cost in blood and treasure. An emerging body of network-centric doctrines of warfare promised to lift the fog of war through the control of information in the battlespace.¹ Over the past decade, strategies of annihilation have given way to strategies of inducement and attrition, neither of which are rapid, bloodless, nor inexpensive.²

Space Power within Irregular Warfare

Although no two insurgencies are the same, nor are any two terrorist groups, it is becoming increasingly difficult to find examples of irregular warfare activities where space power does not play some role.

¹ David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), 7-8; 49-93. See also: Frederick W. Kagan, *Finding the Target: The Transformation of American Military Policy*. (New York: Encounter Books, 2006)

² Justin Kelley and Mike Brennan. "Looking for the Hedgehog Idea," *Australian Army Journal*, Vol VII, No. 1, Autumn 2010, 41.

Western forces, insurgents, terrorists, and populations all use space power to some degree. This is not to say that space power can be decisive in irregular warfare, only that irregular warfare may be even more protracted, bloodier, and costlier without the benefits of space power.

The Western way of warfare depends upon space power to a remarkable degree. Antoine Bousquet notes: “no technology has been more crucial...than the artificial satellites now orbiting the earth in their thousands, our communications relays and eyes in the sky.”³ One could also add PNT satellites as our maps in the sky, as well. Information superiority, precision, and mobility have become the hallmarks of US and coalition forces in combat. Each of these attributes has been carried over to irregular warfare in some manner. The demands placed on satellite communications and surveillance and reconnaissance from space do not diminish in irregular warfare. In fact, they appear to increase. Space control is made more complex in irregular warfare, but it is no less important to success on the ground. Irregular warfare is a voracious consumer of space power, far from what the terms “small wars” or “low-intensity conflicts” might imply.

Professor James Kiras writes that the key distinction between irregular and other forms of warfare, and among different types of irregular warfare, rests on resources and the ability to translate them

³ Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 133.

into effective capabilities.⁴ Although they lack the infrastructure of the US and other Tier One space powers, insurgents and terrorists are able to behave as Tier Three and often Tier Two space powers, free of many of the constraints that Tier One status confers. Insurgents and terrorists do not have to invest in research and development in hopes of improving space power. Insurgents and terrorists do not need to maintain the launch, satellite control, or satellite tracking facilities that Tier One space powers do in order to exploit space capabilities. Insurgents and terrorists also do not have to concern themselves with collision avoidance, environmental monitoring, or other SSA-building activities. Insurgents and terrorists may also someday benefit from the support of states that wield Tier Two space power through dual-use space systems. Perhaps this is the real asymmetric advantage in irregular warfare with regard to space power: insurgents and terrorists can enjoy most of the benefits of space with few, if any of the responsibilities.

It is important to remember that influence over the relevant populations is the central consideration in irregular warfare activities. Just as modern insurgents and terrorists exploit space power along with Western military forces, so do the people for whose support irregular warfare is waged. Measures taken to control space-enabled products and services may have unfortunate collateral effects on the population at stake.

⁴ James D. Kiras, "Irregular Warfare," in *Understanding Modern Warfare*, David Jordan, et al. (Cambridge: Cambridge University Press, 2008) 231.

Finally, relatively low-cost means now exist for governments to build and enhance their legitimacy through space-enabled products and services. Fledgling partner-nation military forces can also improve their combat capability against insurgents and terrorists through competent advisory efforts for space-enabled products and services.

Implications

There are a number of implications for the use of space power in irregular warfare. Space-enabled products and services will continue to present users with a host of opportunities and challenges.

The demand for commercial satellite communications continues to grow apace, even in the conduct of irregular warfare. Not only will Western forces continue to consume commercial satellite voice communications and satellite-enabled network services, but insurgents, terrorists, regimes and populations will as well. Interference is emerging as a serious challenge to satellite operators and users. In addition, legal questions remain to be addressed for commercial satellites that are used to support combat.

Commercial imagery now places a tremendous selection of high-quality products at the fingertips of any interested user. There may be very little that the US can do to forestall access to these products, and it may have to adjust to operating under a greater degree of transparency itself. The policy of the US Government is to enable US industry to compete successfully as a provider of remote sensing space capabilities

for foreign governments and foreign users, while ensuring *appropriate measures* are implemented to protect national security and foreign policy (emphasis added).⁵ Commercial remote sensing capabilities are likely to continue to improve in quality, in spite of measures that the US Government may attempt in order to control improvements in capabilities or access to product. Just as GPS has been questioned as the global satellite PNT standard owing to the perception that it can be “turned off,” the competitiveness of the US commercial remote sensing industry will be impacted by policies that permit the US Government to limit collection and/or dissemination of certain data and products.⁶ Remote sensing policies would appear to have hamstrung the competitiveness of the US aerospace industry, while doing nothing to halt advancements in foreign remote sensing technology. Ultimately, high-quality commercial imaging products may still be available to those who have the resources to pay for them, regardless of US policy.

There may be little that the US can do to control exploitation of GPS. By posturing GPS as the world standard for satellite-enabled positioning, navigation, and timing, the US has created something of a dilemma for itself. US PNT policy over the last decade has removed

⁵ US Department of Commerce. *DoC Factsheet: US Commercial Remote Sensing Policy*. 25 April 2003.

⁶ US Department of Commerce. *DoC Factsheet: US Commercial Remote Sensing Policy*. 25 April 2003.

degradation features as an option for military strategists.⁷ This may be just as well: although there may be sound operational reasons to deny or degrade GPS accuracy, doing so may inflict unacceptable levels of collateral effects on other users. US policy now seeks to provide uninterrupted PNT services in order to remain the world's preeminent PNT service.⁸ US policy also seeks to deny PNT services from GPS to adversaries without disrupting civil, commercial, or scientific PNT uses.⁹ One can see where these policy goals may conflict, just as remote sensing policy does, to an extent. By degrading or "turning off" GPS, the US would fulfill the suspicions that have inspired competing foreign PNT programs, and it would risk losing its position as the world standard to one or more of those competing PNT programs.

Space control has become a more complex endeavor for the US. Preventing exploitation of space power has become increasingly difficult as commercial space-enabled products and services improve and proliferate. Prevention will also be made difficult as more states, some of which will not be sympathetic to US strategic aims, ascend to Tier Two and then to Tier One space power status. Protection has become more

⁷ Office of the President of the United States. *Statement By The President Regarding The United States' Decision To Stop Degrading Global Positioning System Accuracy*. 1 May 2000.

See also: Office of the Press Secretary. *Statement by White House on President's Decision to Procure Future PNT Satellites Without SA Feature*. 18 September 2007.

⁸ Office of the President of the United States. *Factsheet on US Space-based Positioning, Navigation, and Timing Policy*. 15 December 2004.

⁹ Office of the President of the United States. *Factsheet on US Space-based Positioning, Navigation, and Timing Policy*. 15 December 2004.

complex, owing to dependence on commercial space systems that are not designed with self-defense features. In order to avoid collateral damage, negation must utilize very precise and measured effects to limit exploitation of space power.

These are but a few implications of irregular warfare for space power. One of the more significant implications calls into question the traditional concept of space superiority as “that degree of advantage of one force over another that permits the conduct of operations at a given time and place without prohibitive interference by the opposing force.”¹⁰

Space Superiority or Space Parity?

Because it has become so difficult to control the diffusion of space power, space superiority is rapidly becoming a very acute condition in conflict. As the preeminent Tier One space power, it is difficult to argue that the US holds advantages in space that afford the conduct of operations without interference from insurgents and terrorists. Must insurgents or terrorists negate elements of US space power in order to threaten space superiority?

¹⁰ Air Force Doctrine Document (AFDD) 2-2, *Space Operations* 27 November 2006, 7.

If insurgents and terrorists are able to exploit space-enabled services and products without prohibitive interference from the US, then do those friendly forces also enjoy a condition of space superiority? If superiority is zero-sum, then perhaps counter-insurgency and counter-terrorism forces will have to adjust to space parity, where both parties can exploit space without prohibitive interference from the opposing force.

Bibliography

Academic Papers

- Billman, Lt Col Gregory M. "The Space of Aerospace Power: How and Why," Master's Thesis, General Ridgway Center for International Security Studies, University of Pittsburgh, May 2000.
- Bond, Col Margaret S. "Hybrid War: A New Model for Stability Operations in Failed States." Research project, Army War College, 2007.

Articles

- Arana-Barradas, Louis M. "The Space Link: Airmen Provide Out of this World Capabilities," *Airman*. July/August 2008.
- Basu, Indrajit. "Mumbai Terrorists Aided by Technology," United Press International, Dec 02, 2008.
http://www.upiasia.com/Security/2008/12/02/mumbai_terrorists_aided_by_technology/9520/
- Boeing Network and Tactical Systems. *Combat Search and Evader Locator Overview*. Undated. Retrieved at:
<http://www.boeing.com/defense-space/ic/csel/factsheet>
- Braunsvig, David L., Richard L. Garwin, and Jeremy C. Marwell, "Space Diplomacy," *Foreign Affairs*, July/August 2003.
- "Brazilian Police Arrest US Military Satellite Hackers," BBC World Service, May 4, 2009. Accessed through Lexis-Nexis Academic database,
http://www.lexisnexus.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518731342&format=GNBFI&sort=R_ELEVANCE&startDocNo=1&resultsUrlKey=29_T9518731345&cisb=22_T9518731344&treeMax=true&treeWidth=0&csi=10962&docNo=1
- Brewin, Bob. "Homeade GPS Jammers Raise Concerns," *Computerworld online edition*, January 17th, 2003. Retrieved at:
http://www.computerworld.com/s/article/77702/Homeade-GPS_jammers_raise_concerns
- Brulliard, Karin. "Moderate Mali a Barrier to Radical Islam," *The Washington Post*. December 20, 2009.
- Carvajal, Doreen. "France Bans Al Manar TV Channel," New York Times online edition, December 15, 2004. Retrieved at:
http://www.nytimes.com/2004/12/15/news/15iht-t5_17.html

Chasay, Clancy and Bobbie Johnson. "Google Earth Used to Target Israel," *The Guardian UK*, October 25, 2007.

Claburn, Thomas. "U.S. Military Restricts Google Maps," *Information Week*. March 7, 2008.

de Selding, Peter. "Libya Pinpointed as Source of Months-Long Satellite Jamming in 2006," *Space News*, July 7, 2005.

de Selding, Peter. "US Officer: Secrecy Among Coalition Forces Hinders Use of Space Assets in Afghanistan," *Space News*, 10 May 2010, A-1.

Dubowitz, Mark and Roberta Bonazzi, "Jihad TV in Europe," *Wall Street Journal*. February 18, 2009.
<http://online.wsj.com/.../SB123490878778903321.html>

Eisler, Peter. "Google Earth Helps Yet Worries Government," *USA Today*, November 7, 2008.

Feuilherade, Peter. "Israel Steps Up "Psy-Ops" in Lebanon," *BBC News Service-Middle East*, July 26, 2006. Retrieved at:
http://news.bbc.co.uk/2/hi/middle_east/5217484.stm

Foster, Malcom. "Cellular Phones Vital in the Developing World," *The Washington Post*, January 27, 2007.

Frater, Michael and Michael Ryan. "Taxonomy of Space Operations," *Journal of Battlefield Technology*. July 2005.

Gabbat, Adam. "Iran Space Launch Opens Cans of Worms in Space Race with West," *The Guardian UK*, February 3, 2009.

Gates, Hon. Robert M. "Helping Others Defend Themselves," *Foreign Affairs*. May/June 2010.

"Gates Outlines Plans to Reform Export Controls," *Reuters*. April 20, 2010.

Ghalit, Kim. "US Concerned About Syrian Intentions over Hezbollah," *BBC World Service*. April 15, 2010.
http://news.bbc.co.uk/1/hi/world/middle_east/8621405.stm

GNSS Insider, "About Glonass" *Global Navigation Satellite System Insider online edition*, <http://www.insidegnss.com/aboutglonass>

Grant, Greg. "Hezbollah on Steroids," DoD Buzz, July 1, 2009.
 Retrieved at: <http://www.dodbuzz.com/2009/07/01/hezbollah-on-steroids/#axzz0jrHPG131>

Gulish, Jay and David Vaccaro. "Top Ten in PNT," *Inside Global Navigation Satellite Systems online edition*. November/December 2009.

Haines, Lester. "Google Earth Erases British Bases in Iraq," *The Register UK edition*, January 1, 2007.
http://www.theregister.co.uk/2007/01/17/google_erases_brit_bases/page2.html

International Telecommunications Union press release, "Worldwide Cellular Telephone Subscribers to Reach 4 Billion Mark by End of 2008," posted September 25, 2008.

- “Iran, China, and Thailand Satellite Goes Into Orbit,” BBC World Service, September 7, 2008. Retrieved from Lexis-Nexis Academic database at http://www.lexisnexus.com/us/lnacademic/results/docview/docview.do?docLinkInd=true&risb=21_T9518773642&format=GNBFI&sort=R ELEVANCE&startDocNo=1&resultsUrlKey=29_T9518773652&cisb=2 2_T9518773651&treeMax=true&treeWidth=0&csi=10962&docNo=2
- “Iran to Launch Topography Satellite in 2010,” BBC World Service, August 24, 2008. Retrieved from Lexis-Nexis Academic database, <http://www.lexisnexus.com/us/lnacademic/search/homesubmitForm.do>
- “Iran Satellite Move Sparks Fears,” BBC World Service, February 3, 2009. http://news.bbc.co.uk/2/hi/middle_east/7868116.stm
- Kelly, Justin and Mike Brennan. “Looking for the Hedgehog Idea,” *Australian Army Journal*. Vol VII, No. 1, Autumn 2010.
- Kirschbaum, Erik. “German Government Blocks Al Manar,” *Variety*, November 23, 2008. Retrieved at: <http://www.variety.com/article/VR1117996353.html?categoryid=14&cs=1>
- Kruzel, John J., “Hybrid War to pull US in many directions.” American Forces Press Service, 4 May 2009. Retrieved at: <http://www.defense.gov/news/newsarticle.aspx?id=54186>
- Lawrence, Lieutenant-Colonel T.E. “The Evolution of a Revolt,” *Army Quarterly and Defence Journal*, October 1920.
- Magnuson, Stew. “Israel Pushes New Satellite as Solution to US Space Radar Needs,” *National Defense*, January 2010.
- Mecham, Michael. “Remote Sensing Grows Up,” *Aviation Week and Space Technology*. Vol 171, Issue 21. December 7, 2009. 70.
- Moskovitch, Katia. “GLONASS: Has Russia’s Sat-Nav System Come of Age?” *BBC News-Russian Edition*, April 1, 2010. <http://news.bbc.co.uk/2/hi/science/nature/8595704.stm>
- “Pakistan to Launch Indigenous Communication Satellite from China in 2011.” *BBC World Service*. 14 April 14, 2009. From Dawn English-language website: <http://www.dawn.com/wps/wcm/connect/dawn-content-library/dawn/news/business/11-cabinet-may-approve-fbs-restructuring---il--02>
- Porter, Geoff. “AQIM and the Growth of International Investment in North Africa,” *Sentinel: A Publication of the Combating Terrorism Center*. November 2009, Vol 2, Issue 11.
- Roosevelt, Ann. “Space Control Vital for Future Operations, General Says,” *Defense Daily*. November 3, 2003.
- Rosenberg, Barry. “DoD’s Reliance on Commercial Satellites Hits New Zenith,” *Defense Systems*. February 25, 2010. <http://defensesystems.com/Articles/2010/03/11/Cover-story-The-Satcom-Challenge.aspx?Page=1&p=1>

Rumsfeld, Hon. Donald H. "Transforming the Military," *Foreign Affairs*. May/June 2002.
<http://www.foreignaffairs.com/articles/58020/donald-h-rumsfeld/transforming-the-military>

Selzer, SGT Henry. "Excalibur Round Debuts in Afghanistan," *Army.mil News*, May 10, 2008.

Soares, Marcelo. "The Great Brazilian Sat-Hack Crackdown," *Wired*, April 20, 2009.
<http://www.wired.com/politics/security/news/2009/04/fleetcom>

Tavoli, MCC Stan. "Unit 10: A Force Multiplier," *Ethos: Naval Special Warfare*, Issue 8, undated. Retrieved at:
http://www.navsoc.navy.mil/pdf/ethos/ETHOS_ISSUE_8.pdf

US Africa Command Public Affairs, "African Union Communications Capability Strengthened Through AFRICOM Training," June 18, 2008. <http://www.africom.mil/getArticle.asp?art=1803&lang=0>

Wolf, Jim. "US Details China Satellite Debris," *Reuters*, April 10, 2007.
<http://www.reuters.com/article/idUSN1044576620070411>

Wolf, Jim. "US, Russian Satellites Collide in Space," *Reuters*, February 11, 2009.
<http://www.reuters.com/article/idUSTRE51A8IA20090211>

Vizard, Frank. "Safeguarding GPS," *Scientific American*. April 2003.
 Retrieved at: <http://www.scientificamerican.com/article.cfm?id>

Books

Arkin, William N. *Divining Victory: Airpower in the 2006 Israel-Hezbollah War*. Maxwell AFB, AL: Air University Press, 2007.

Arquilla, John and David Ronfeldt, eds., *Networks and Netwars: the Future of Terror, Crime, and Militancy*. Santa Monica: Rand, 2001.

Baker, John C., Kevin M. O'Connell, and Ray A. Williamson, eds. *Commercial Observation Satellites: at the Leading Edge of Global Transparency*. Santa Monica: Rand, 2002.

Barabasi, Albert-Laszlo. *Linked*. New York: Plume, 2003.

Bousquet, Antoine. *The Scientific Way of War: Order and Chaos on the Fields of Modernity*. New York: Columbia Press, 2009.

Brown, Lt Col Kendall K., ed. *Space Power Integration: Perspectives from Space Weapons Officers*. Maxwell AFB: Air University Press, 2006.

Clausewitz, Carl Von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton, NJ.: Princeton University Press, 1976.

Corum, James and Wray Johnson. *Airpower in Small Wars*. Lawrence, KS: University of Kansas Press, 2003.

Elbert, Bruce R. *Introduction to Satellite Communications*. Boston: Artech House, 1999.

- Galula, David. *Counterinsurgency Warfare: Theory and Practice*. Westport, CT: Praeger Security International, org. ed., 1964. Rep. ed., 2007.
- Galula, David. *Pacification in Algeria: 1956-1958*. Santa Monica: Rand, org ed., 1963. Rep. ed., 2006.
- Gant, Maj Jim. *One Tribe at a Time*. Los Angeles: Nine Sisters, 2209.
- Gillespie, Paul G. and Grant T. Weller, eds. *Harnessing the Heavens*. Chicago: Imprint Publications, 2008.
- Gray, Colin S. *Modern Strategy*. Oxford: Oxford University Press, 1999.
- Jordan, David, James D. Kiras, David J. Lonsdale, Ian Speller, Christopher Tuck, and C. Dale Walton. *Understanding Modern Warfare*. Cambridge: Cambridge University Press, 2008.
- Kagan, Frederick W. *Finding the Target: The Transformation of American Military Policy*. New York: Encounter Books, 2008.
- Khalilzad, Zalmay and Jeremy Shapiro. *Strategic Appraisal: US Air & Space Power in the 21st Century*. Santa Monica, CA: Rand, 2002.
- Kiras, James D. *Understanding Modern Warfare*. Cambridge: Cambridge University Press, 2008.
- Lambakis, Steven. *On the Edge of the Earth: The Future of American Space Power*. Lexington, KY: University of Kentucky Press, 2001.
- Libicki, Martin C. *Friendly Conquest in Cyberspace*. Cambridge: Cambridge University Press, 2007.
- Lonsdale, David J., *The Nature of Warfare in the Information Age: Clausewitzian Future*. London: Frank Cass, 2004.
- Posen, Barry R., *The Sources of Military Doctrine*. Ithaca, NY: Cornell University Press, 1984.
- Rashid, Ahmed. *Descent into Chaos: The US and the Disaster in Pakistan, Afghanistan, and Central Asia*. New York: Penguin Press, 2008.
- Ricks, Thomas E. *The Gamble: General David Petraeus and the American Military Adventure in Iraq, 2006-2008*. New York: Penguin Press, 2009.
- Rid, Thomas S. and Marc Hecker. *War 2.0: Irregular Warfare in the Information Age*. Westport, CT: Praeger Security International, 2009.
- Robb, John. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. Hoboken, NJ: John Wiley & Sons, 2007.
- Sheehan, Michael. *The International Politics of Space*. New York: Routledge, 2007.
- Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York: Alfred Knopf, 2007.
- Spires, David N. *Beyond Horizons: A Half-Century of Air Force Space Leadership*. Maxwell AFB, AL: Air University Press, 1998.
- Uncredited, *GPS NAVSTAR User's Overview*. ARINC Research Co., 1991.
- Wylie, J.C. *Military Strategy*. Annapolis, MD: Naval Institute Press, org ed. 1967. Rep. ed. 1989.

Government Documents

- 21st Space Wing Factsheet: 16th Space Control Squadron. Undated.
- 34th Infantry Division Space Support Element. 34th Infantry Division Mission Rehearsal Exercise Space Operations After Action Report, dated 5 April 2009.
- Air Force Doctrine Document 2-2, *Space Operations*, 27 Nov 2006.
- Air Force Doctrine Document 2-2.1, *Counterspace*, 2 Aug 2004.
- Air Force Doctrine Document 2-3, *Irregular Warfare*, 1 Aug 2007.
- Air Force Doctrine Document 2-3.1, *Foreign Internal Defense*, 15 Sep 2007.
- Army Field Manual (FM) 3-24/Marine Corps Warfighting Publication 3-33.5, *Counterinsurgency*, 15 Dec 06.
- Department of Defense Irregular Warfare Joint Operating Concept, version 1.0, 11 Sep 07.
- Jet Propulsion Library "GLONASS" JPL Mission and Spacecraft Library. Retrieved at: <http://msl.jpl.nasa.gov/Quicklooks/glonassQL.html>
- Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms*, April 2001, as amended 31 Oct 2009.
- Joint Publication 3-14, *Space Operations*, 9 Jan 2009.
- Joint Tactical Radio System Program Executive Office. JTRS Fact Sheet. Retrieved at: <http://www.jtrspeo.mil>
- Chairman of the Joint Chiefs of Staff Instruction 6130.01C, "2003 CJCS Master PNT Plan," 31 Mar 03.
- Office of the President of the United States. Statement by the President Regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy, 1 May 2000.
- Office of the President of the United States. Statement by the Press Secretary on the President's Decision to End Procurement of GPS Satellites that have the Capability to Intentionally Degrade the Accuracy of Civil Signals, dated September 18, 2007.
- Office of the President of the United States. *US National Space Policy*. August 31, 2006.
- Retrieved at: <http://www.space.au.af.mil/histpol.htm>.
- Space and Missile Systems Center. Global Broadcast Service Fact Sheet. Retrieved at: http://www.losangeles.af.mil/library/factsheets/factsheet_print.asp?fsID=7853&page=1
- Space and Naval Warfare Systems Command. *JTRS: Why is it Important?* Retrieved at: <http://enterprise.spawar.navy.mil/body.cfm?type=c&category=27&subcat=79>

US Air Force. Air Force Fact Sheet: Global Positioning System. March 22, 2007. Retrieved at:
<http://www.af.mil/information/factsheets/factsheet.asp?id=119>

US Air Force. Air Force Fact Sheet: MQ-9 Reaper. November 2009. Retrieved at:
<http://www.af.mil/information/factsheets/factsheet.asp?id=6405>

US Air Force. Air Force Fact Sheet: Space-based Infrared Systems. Undated.
<http://www.afspc.af.mil/library/factsheets/factsheet.asp?id=3675>

US Air Force. Air Force Fact Sheet: Space Radar. Undated.

US Air Force. Air Force Factsheet: Worldwide Global SATCOM satellite. Dec 2009.

US Department of Commerce. DoC Fact Sheet: US Commercial Remote Sensing Policy. April 25, 2003.

US Department of Commerce. Statement by US DoC Office of Space Commercialization on SAR License to Northrup Grumman. August 24, 2009.

US Treasury Department. Statement by US Treasury Dept on Designation Hamas' Al-Aqsa Television a Specially-Designated Terrorist. March 18, 2010.
 Retrieved at: <http://www.ustreas.gov/press/releases/tg594>

Embassy of Sri Lanka. "LTTE's Transmissions of TV and Radio Programs to Europe and Asia Terminated by INTELSAT, Ltd." 24 April 2007.

Personal Communications - Interviews/E-Mails

Boera, Brig Gen Michael, Commanding General, Coalition Air Power Transition Force and Commander, 438th Air Expeditionary Wing, Southwest Asia. In discussion with the author, 14 May 2010.

Thompson, Col David, Director of Space Forces, Air Forces Central Command, Southwest Asia. To the author. E-mail, 23 April 2010.

Jones, Lt Col Dan, Director of Space Forces, 612th Air & Space Operations Center, Davis-Monthan AFB, AZ. To the author. E-mail, 9 March 2010.

Pettis, Lt Col Stuart, Chief, Strategy & Doctrine, Air Force Space Command, Peterson AFB, CO. Interview by the author, 18 February 2010.

Whitaker, Lt Col Wes, Chief, Specialty Teams, 623d Air & Space Operations Center, Hurlburt Field, FL. Interview by the author, 8 April 2010.

Coffey, Mr. William, contractor. Future Warfare Center, US Army Space & Missile Defense Center, Peterson AFB, CO. In discussion with the author, 15 Feb 2010.

Reports

- Brochi, Adinei. *Satelites Bolinha*. self-published, undated. Retrieved at: www.py2adn.com/artigos/Satelite-Bolinha.pdf
- Chilton, Kevin P. *2010 Posture Statement to US House of Representatives Armed Services Committee, Subcommittee on Strategic Forces*, 16 March 2010.
- Cordesman, Anthony H. *Preliminary "Lessons" of the Israeli-Hezbollah War*. Washington: Center for Strategic and International Studies, April 2009.
- Kennedy Boudali, Leanne. *The GPSC: Newest Franchise in Al Qaeda's Global Jihad*. West Point, NY: Combating Terrorism Center, US Military Academy, April 2007.
- Final Form/Report, "Terrorist Attack on Mumbai," In the Court of Addl. Ch. M.M., (37th Court, Esplanade, Mumbai, 2009), 37-38.
<http://www.hindu.com/nic/Mumbai-terror-attack-final-form.pdf>

Speeches

- Kehler, Gen C. Robert. Commander, Air Force Space Command.
Address. National Security Space Symposium, Colorado Springs, CO, 31 Mar, 2009.