12-2006

Outside the fence,' the threat to the U.S. Aviation Industry

David Thomas Ramsey
University of Tennessee - Knoxville

To the Graduate Council:

I am submitting herewith a thesis written by David Thomas Ramsey entitled "Outside the fence,' the threat to the U.S. Aviation Industry." I have examined the final electronic copy of this thesis for form and content and recommend that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Aviation Systems.

Rodney C. Allison, Major Professor

We have read this thesis and recommend its acceptance:

Frank G. Collins, Charles T. N. Paludan

Accepted for the Council:
Carolyn R. Hodges

Vice Provost and Dean of the Graduate School

(Original signatures are on file with official student records.)

To the Graduate Council:

I am submitting herewith a thesis written by David Thomas Ramsey entitled “'Outside the fence,' the threat to the U.S. Aviation Industry." I have examined the final electronic copy of this thesis for form and content and recommended that it be accepted in partial fulfillment of the requirements for the degree of Master of Science, with a major in Aviation Systems.

Rodney C. Allison, Major Professor

We have read this thesis
and recommend its acceptance:

Frank G. Collins

Charles T.N. Paludan

Acceptance for the Council:

Anne Mayhew
Vice Chancellor and Dean of
Graduate Studies

(Original signatures are on file with official student records.)

“Outside the fence,”
The threat to the U.S. Aviation Industry

A thesis
Presented for the
Master of Science
Degree
The University of Tennessee, Knoxville

David Thomas Ramsey
December 2006

Dedication

This thesis is dedicated to my wife, Kristina Ramsey, my best friend and ever present encouragement for completion of this effort. Without her support through all my Navy deployments and time away this phase of my education would have never been possible.

Acknowledgements

I wish to thank all that helped me complete my Master of Science degree in Aviation Systems. I would like to thank Mr. Allison, Dr. Paludan, Mr. Collins, Ms. Hollis and especially Mrs. Harbin from UTSI for helping me through the whole thesis process. I would like to thank CDR Bud Joyner for all the information on ShotSpotter systems, and Mr. Heidhausen for all the information on midband IR systems.

Lastly I would like to thank my father for reading through the various stages of my thesis development and providing content suggestions and guidance.

Abstract

The purpose of this thesis was to examine the threat to the Aviation Industry from within the United States. The overall investigation starts with one assumption “that there will at some time in the near future be a covert operative group that desires to attack or engage the United States in war on its home land.” The principles of war will be analyzed resulting in covert cell guidance specifically; “economy of force” will require the covert units to be as small as possible to affect as many nodes as possible. Endurance will require the covert team to restrict any tactics that would be high risk, and would prohibit the use of suicide tactics. There has also been a redefinition of warfare in the last several years. What has emerged is a form of unrestricted warfare. The covert cell may abide by the principles of war while engaging the U.S. in unrestricted warfare. These assumptions lead to a center of gravity determination and terrorism as the possible action for the desired effect. Attack and weapon selection analysis results in the selection of the 50 caliber sniper rifle with armor-piercing incendiary ammunition as the most probable attack tactic executed against urban airport environments. Possible solution analysis of acoustic, mid wave infrared and optical augmentation systems reveals the advantages of each of these approaches. The conclusion is that open system architecture should be used to tailor the sensor suite around each airport based on the vital area locations with respect to the urban layout and the best sniping positions. This will lead to a multi-layer and multi-system defensive posture around each airport significantly reducing the risk of a drawn out terror campaign which involves the airline industry.

Table of Contents

List of Tables

List of Figures

Nomenclature

mil	military reticle
gen	generation

Abbreviations

AIC	Acoustic Incident Classification
API	Armor Piercing Incendiary
AQ	Al-Qaeda
ATF	Alcohol, Tobacco, and Firearms Agency
BIAP	Baghdad International Airport
BOUNCE	Battlefield Ordnance Engagement - Network Centric Employment
BMG	Browning machine gun
BMG	Common designation of .50 caliber bullets
CAPPS	Computer Assisted Passenger Prescreen System
COG	Center Of Gravity
CT	Computerized Tomography
DC	Direct Current
DHS	Department of Homeland Security
DoD	Department of Defense
FAA	Federal Aviation Administration
FARC	Foreign Arms Regional Coalition
FBI	Federal Bureau of Investigation
FM	Field Manual
FOV	Field of View
GPS	Global Positioning Service
GWOT	Global War on Terrorism
ID	Identification
IED	Improvised explosive device
IR	Infrared
kVp	kilovolt peak
LAX	Los Angeles International Airport
MANPAD	Manned Portable Air Defense System
MOOTW	Military Operations Other Than War
NORTHCOM	Northern Command
NGO	Non Government Organization
OIF	Operation Iraqi Freedom
PI	Pulse Induction
PIBD	Point Initiating Base Detonating
RF	Radio Frequency

RPG	Rocket Propelled Grenade
RV	Recreational Vehicle
TIC	Toxic industrial chemicals
TIM	Toxic industrial materials
TSA	Transportation Security Administration
SAM	Surface-to-Air Missile
UAV	Unmanned Aerial Vehicle
USJFCOM	United States Joint Forces Command
VBIED	Vehicle borne improvised explosive device
VIPER	Vectored IR Personnel Engagement and Return fire
VPC	Violence Policy Center
911	September 11, 2001

Introduction

The airline industry of the United States is a fragile multi billion dollar enterprise that has touched almost every person in the world. The 911 attacks of 2001 displayed this and just how fragile the industry was with multiple companies requesting Chapter 11 protection within a year of the attack. The health and protection of the industry as a whole should be a concern of every household in the world, in that as the industry goes so could the free market and the health of the world economy as a whole. With limited resources for its own protection the airline industry depends on the Federal Aviation Administration (FAA) to set the standards for airport and terminal security measures. Little has been done with respect to aircraft self protection efforts. If any such efforts are to be taken it will be the FAA or highest levels of the U.S. Government that will impose the requirements for any such protecting systems to be installed. This investigation will be an evaluation of the problem of how to best protect the aviation industry and our nation with the minimal amount of resources available.

To begin any such evaluation of where to apply resources for the security of the aviation industry we must first define the threat and what we are actually trying to defend against. The typical "solution first" type of evaluation where a decision is made on whether we should invest in program A or system B is a completely flawed process, and waste of resources. If you start with the end state or solution in mind the whole decision process leading up to recommendations are themselves tainted by the requirement to end with those solutions. The best and most recent example of this process was the shoulder launched missile research that was done by multiple agencies. The solution, an aircraft carried self protection capability, was the starting point of the research. Then working off of the current state of technology and requirements for the system a decision is made whether or not to invest in the development of the solution. Once the yes or no vote on the system is made, the whole process is started over again for the next system that comes along. To end this evaluation with a meaningful solution recommendation, a more holistic approach will be taken where solutions are not the starting point.

This research assumes that there will at some time in the near future be a covert operative group that desires to attack or engage the United States in war on its home land. To truly have a holistic evaluation we will begin from this point and must then evaluate the current state of war. The *Principles of War* developed by the Army in 1949 will begin our evaluation in an effort to bound and refine the problem statement. Once the problem statement and initial assumptions are refined, we can then move toward an evaluation of the requirements for a solution to that problem. Only then can systems be evaluated against the requirements and a meaningful recommendation will be the outcome.

Chapter 1: Principles of War

The principles discussed herein are derived from the revised list and were contained in a white paper titled "Principles of War for the 21st Century."[1] The revised list includes 14 principles yet this evaluation will only discuss the principles relevant to our starting point. Each principle will be discussed and the advantages and disadvantages for the covert operational group and Northern Command (NORTHCOM[2]) will be evaluated. NORTHCOM is the single U.S. Military point of command for the defense of the homeland. This term will be used to reference the U.S efforts against the covert group even though the defense may come from several entities not specifically under NORTHCOM, for example local and state police forces. These advantages and disadvantages will serve as the guidance to activities that a covert team may use and from which solution analysis can be made.

1.1 Defining the principles

1.1.1 End state

The purpose of war is the imposition of a Nation's will and the attainment of strategic political, economic, societal, and military aims. These strategic aims must be translated into a desired military *end state* that supports these aims. The successful achievement of the military end state is through the accomplishment of desired effects. An effect as defined by the U.S. Joint Forces Command is the physical, functional, or psychological outcome, event, or consequence that results from specific military or non-military actions.[3] Commanders need to appreciate the non-military aims and end states, and understand how the military can create effects that contribute to them.[4] The desired end state for NORTHCOM is the protection of the nation as a whole. This broad open ended end state is overwhelmingly an advantage for the covert adversary operating within the United States. NORTHCOM cannot protect all vital areas of interest and thus will have multiple vulnerabilities. An intelligent adversary understands this and may look to attack in the seams or areas that are the softest targets. NORTHCOM's seemingly impossible job is to identify those seams or soft spots and harden or eliminate them completely with very limited resources.

1.1.2 Understanding

"Know the enemy and know yourself; in a hundred battles you will never be in peril."

Sun Tzu[5]

The more we know about the adversary, and ourselves, the more precisely we can apply our capabilities to produce desired effects that achieve the military end state. Without this understanding we can never hope to defeat an adversary operating from a forward base, our back yard. How do you gain an understanding in a military context for an enemy that may be your next door neighbor? An understanding of the possible actions an enemy may take without knowing the enemy's name, affiliation, or desired end state is challenging.

While more information is generally better, we must guard against information overload, and understand the balance between seeking better, or perfect, information against the requirement to act in a timely manner. When a Commander seeks completely accurate information to act upon he in turn looses the capability to act at all, always waiting for better information. Our information overload is also greatly in favor of the covert adversary. When the enemy is hidden, any and all information could be vital. Until some concrete evidence or links of disparate information are pieced together the task of controlling against information overload is of concern.

1.1.3 Integration

War is armed fighting between groups. The effectiveness of a group is a function of the effectiveness of the individual parts modified by the way those parts are employed together. They must be complementary and supportive of each other, and must be integrated in the physical, information, and cognitive domains. The organizational schemes and integrating mechanisms employed can result in an overall effectiveness that is less than, equal to, or greater than the sum of the parts. The idea behind the principle of integration is to maximize the power and effectiveness of the forces being employed through a combination of networked means and realize a synergy from those integrated means being employed as a system.

An adversary may attack at the non-integrated seams, where communication and information transfer are the most difficult: across disparate agency organizational lines.

1.1.4 Adaptability

> *No plan survives contact with the enemy.*
> Helmut von Moltke

Today's battlespace is complex and uncertain, with an adversary who will also be adaptive. We must be able to sense, understand, decide, and act faster than the adversary.[6]

Adaptability is enhanced by speed, rapidity of action. Superior speed allows us to seize the initiative, exploit fleeting opportunities, and dictate the terms of action, forcing the enemy to react to us. Relative speed in relation to the enemy is what matters, so we should take all measures to improve our own speed while degrading our enemy's.[7] This combination of mental and physical agility with its associated speed of decision-making and mobility better enables us to create and exploit opportunities.

We cannot foresee the future, nor accurately predict enemy intentions or actions, nor centrally formulate a detailed, prescriptive plan that remains unchanged from formulation to end of execution. The situation will change and the enemy will likely adapt to our plans and actions. The enemy’s capability to adapt and blend into the general populace and ability to attack with one tactic then disappear only to reappear and attack with a totally different tactic weeks or months later is a major advantage to the covert operative cells.

1.1.5 Clarity

The ultimate intent of clarity is to facilitate execution of simple actions that will contribute to the military end state. Actions begin with the strategic aims and a vision of the desired end state, then effects required to achieve it, and finally with the integration of those actions necessary to execute commander's intent. In linking the necessary tasks, effects, and the desired end state, the principle of clarity should always be observed. The clearer the envisioned plans and relationships are, the easier it will be to implement and maintain them.

Clausewitz said, "Everything in war is simple, but the simplest thing is difficult. The difficulties accumulate and end by producing a kind of friction that is inconceivable unless one has experienced war."[8] This relative clarity of required action is especially important from the perspective of the leader tasked to execute the action. The covert cells may use simple plans and will most likely be very clear in their limited actions, whereas NORTHCOM will have difficulty contacting subordinate units, much less commanding them with clarity under crisis situations.

1.1.6 Surprise

Surprise is based on two antithetical elements, secrecy and speed. Secrecy and stealth delay detection; speed hastens contact. Either of these can leave the U.S. too little time to be prepared, thus increasing the enemy's ability to cause mental or physical dislocation.

Surprise and associated shock can shift the balance of power and thus can achieve success well out of proportion to the effort expended or to overall force ratios. Surprise delays and reduces the coherence of our reactions, overloads and confuses our command and control, and induces psychological shock and disorientation.

Commanders should seek out opportunities to do the unexpected, and especially to attack asymmetrically against an adversary's vulnerabilities in order to capitalize on where, when, and how the enemy can be surprised to give us an advantage. Similar to 911 this is what the covert cells may do to the U.S. Surprise through secrecy, shock, and speed is not only an advantage to the covert cells it may be a requirement and guiding principle to each and every action they take.

1.1.7 Economy

The principle of economy of force is much more than a tactical principle, it extends much beyond applying minimum essential combat power to secondary efforts. Economy of force applies globally. Economy of force is the measured allocation of available combat power to achieve desired effects and military end state in the most effective and efficient manner.

Economy of force insists that we orient ourselves on the objective and avoid needless expenditures that do not lead us to it.[9] Understanding helps us economize by allowing more judicious application of power, allowing us to better apply the right force at the right time and place.

1.1.8 Endurance

Endurance has both a mental and a physical aspect. The mental aspect can be expressed as the *will* to see the conflict through to a decisive, lasting conclusion. *Will* is applicable at the strategic level, where it has a heavy political and social context. The perceived legitimacy of the conflict will affect the *will* of both sides to continue the conflict. Defeating an adversary's *will* to fight, although difficult, is the surest method of ending a conflict on favorable terms. *Will* is a necessary part of endurance and applies to both sides of a conflict. The physical aspect of endurance involves having the necessary people, equipment, and other resources to sustain the forces at the intensity and duration required for victory. The force must be strong enough to endure adversary attacks and defensive actions and still achieve overmatching power that enables achievement of objectives at each point of action and throughout the global battle space for as long as it takes. It requires matching the requirements to sustain the force with the right resources. Endurance incorporates both the mental willingness and the physical ability to achieve a decisive, lasting victory in war.

1.1.9 Legitimacy

Long ago, Clausewitz wrote that war was not only the business of the military and the government, but of the people, as well.[10] More recently, the so-called Weinberger and Powell Doctrines urged that the U.S. military should not be employed unless they enjoyed the support of the American people. The morale of the troops is a very important factor, but the principle of legitimacy is much more encompassing than the morale of the military alone. Legitimacy encompasses the opinion and will of our nation, of the population of the nations we are engaging, and perhaps that of the entire world.

The balance between security and safety of troops and the morality and legitimacy of an action must be considered. The impact of indiscriminate use of firepower, injury to innocent civilians, and damage to property must be weighed against mission success and safety of one's unit. Balance is required.

1.1.10 Principle summary

These principles of war will be applied to the initial assumption or starting point that “there will at some time in the near future be a covert operative group that desires to attack or engage the United States in war on its home land." This will lead to several other assumptions that will guide our analysis and ultimately influence our final solution recommendation.

The principles of clarity and understanding will lead to the assumption that the attacks will be very simple with limited coordination between individual covert units other than the what, where, and when to attack? The leader or mastermind of the operations will most likely be a single person or at most a small core membership to direct operations and give commands. The simplicity this implies leads directly to the integration of the attacks. The limited guidance on how to attack each node will allow the covert units to be very adaptable giving them the flexibility to achieve the desired results without requiring them to perform specific tasks which may put them at risk. Economy of force will require the individual covert unit's size to be as small as possible to have as many teams as possible. Endurance will require the covert team, with minimal chance for re-supply or recruitment of new members once the campaign begins, to restrict any tactics that would be high risk, and would limit the use of suicide tactics unless capture were imminent.

These assumptions and the guiding principles will be applied to the analysis and effort to drive to a meaningful conclusion. Before we can continue we must define the type of warfare we are dealing with.

1.2 Unrestricted War

This section is dedicated to the redefining of warfare that has taken place. It is derived from a Chinese paper "Unrestricted Warfare" published in 1999.[11] The events of 911 caused the implications of this literature to become an immediate reality. Any solution set recommended must take into account the logical means of attack that an adversary will use. In this age of technological advances in the commercial market place severely out pacing the archaic military acquisition system, we must apply resources selectively to the capability gaps in innovative ways to maintain adaptability to the enemy's ability to learn and out think our defenses.

1.2.1 Definition

Warfare which transcends all boundaries and limits, in short: unrestricted warfare[12]

"Regardless of the form violence takes, war is war, and a change in the external appearance does not keep any war from abiding by the principles of war. If we acknowledge that the new principles of war are no longer "using armed force to compel the enemy to submit to one's will," but rather are "using all means, including armed force or non-armed force, military and non-military, and lethal and non-lethal means to compel the enemy to accept one's own interests."[13] What is compelling about this statement is that radical groups or trained covert operatives will not capitulate or submit to external interests. They will be using this Principle or form of unrestricted warfare on the U.S.

"Customizing weapons systems to tactics which are still being explored and studied is like preparing food for a great banquet without knowing who is coming, where the slightest error can lead one far astray. Viewed from the performance of the U.S. military in Somalia, where they were at a loss when they encountered Aidid's forces, the most modern military force does not have the ability to control public clamor, and cannot deal with an opponent who does things in an unconventional manner. On the battle fields of the future, the digitized forces may very possibly be like a great cook who is good at cooking lobsters sprinkled with butter, when faced with guerrillas who resolutely gnaw corncobs, they can only sigh in despair."[14] This missing the mark of where to apply the limited defensive resources that NORTHCOM has at its disposal could have enormous detrimental ramifications not only to the security of the U.S. but the stability of the world market as a whole.

"Those desires of using the magic of high technology to work some alchemy on traditional weapons so that they are completely remade have ultimately fallen into the high-tech trap involving the endless waste of limited funds in an arms race. This is the paradox that must inevitably be faced in the process of the development of traditional weapons: To ensure that the weapons are in the lead, one must continue to up the ante in development costs; the result of this continued raising of the stakes is that no one has enough money to maintain the lead. Its ultimate result is that the weapons to defend the country actually become a cause of national bankruptcy, similar to the collapse of the Soviet Union at the end of the Cold War."[15] The more likely scenario for the U.S. government would be a reduction in international affairs and commitments while attempting to deal with the war on terror at home. This reluctance to engage in new global areas or continue ongoing efforts like Operation Iraqi Freedom (OIF) might be the exact response or effect the covert operatives were looking for.

Terrorist organizations and even large Nations like China will not be able to keep up with this arms race; what will be developed are new-concept weapons. "What must be made clear is that the new-concept of weapons is not creating a new deadly device, it is taking entities that are closely linked to the lives of the common people and using them in the process of creating weapon-like effects. As we see it, a single man-made stock market crash, a single computer virus invasion, or a single rumor or scandal that results in a fluctuation in the enemy country's exchange rates or exposes the leaders of the enemy country on the Internet, can all be included in the ranks of new-concept weapons."[16] NORTHCOM is chartered to defend against an adversary's unrestricted use of all means at their disposal in an attempt to influence the U.S.

Without quoting numerous volumes of insight from these two authors, Liang and Xiangsui, let it be know that their publication references volumes of U.S. open source documents to include U.S. Joint war fighting doctrine, field manuals, war college instructional briefings, Airpower Journal, U.S. Marines magazine, Joint Force Quarterly, Army Times; the list goes on and on.

"Moreover, in terms of its operations, a traditional terror war is never bound by any of the traditional rules of the society at large. From a military standpoint, then, the traditional terror war is characterized by the use of limited resources to fight an unlimited war. This characteristic invariably puts national forces in an extremely unfavorable position even before war breaks out, since national forces must always conduct themselves according to certain rules and therefore are only able to use their comparatively unlimited resources to fight a limited war. This explains how a terrorist organization made up of a just a few inexperienced members who are still wet behind the ears can nevertheless give a mighty country like the U.S. headaches, and also why 'using a sledgehammer to kill an ant' is ineffective."[17]

1.2.2 Overall terrorist unrestricted game plan

This unrestricted view to warfare leads us to an unrestricted open analysis of what and where the terrorists may strike the U.S. on its own turf. A terrorist cell can have many reasons for attacking but in our analysis those reasons are not of consideration. The overall attack process begins by identifying those centers of gravity they wish to influence. A center of gravity is that entity, if attacked or influenced, which will cause such an impact upon the enemy that it becomes a focal point of the campaign. In a traditional sense a center of gravity would be material in nature. The oil supply attack on the Germans during WWII or the industrial blockade of the South during the Civil War would be two classic examples of attacks on a center of gravity. Once the center of gravity is chosen, the enemy must determine the effect they are looking to achieve and how to attack specific nodes to achieve those effects. This effect to nodal linkage analysis will lead NORTHCOM to what must be defended.

Once the node that may be attacked is determined specific target sets within that nodal structure can be defended. The target sets will lead to possible enemy weapon selection and specific attack profiles. Weapons selection will be a break down of capabilities, availability and training. The whole process may or may not lead to a focused answer on how we are susceptible to attack. Based on this analysis and the underlying assumptions the technology currently available will be evaluated for its use to defend against this possible attack. This will lead to recommendations on how to apply the limited resources available to acquire the solutions for an effective countermeasure to this attack.

1.3 Center of gravity determination

One of our underlying assumptions is that we do not need to determine what actual terrorist group or organization will be the most likely to attack from within the United States. The reason enemy analysis is omitted is due to the nature of the attacks. On a National scale these attacks will be minuscule, meaning they will not be attrition type attacks aimed at a material center of gravity. The attacks will most likely be unrestricted; they will not abide by any military or human rule of law or decency. These small scale attacks used in a manner to attempt to influence National level objectives will immediately reduce the center of gravity analysis to several areas that are subject to individual events.

1.3.1 U.S. national will and resolve

"Public opinion is everything. With it, nothing can fail. Without it, nothing can succeed." *President Abraham Lincoln*

The Principles of legitimacy and endurance combined form a possible "center of gravity" (COG) in that the general U.S. public cannot stomach a war that has a potential to be lost in the end. The Vietnam War and Somalia campaign are two prime examples of the public outcry and outrage over poor government involvement in international affairs. It is of no surprise that the United States has a distain for drawn out wars and soldiers deaths. This distain in of itself is a statement about the U.S.'s endurance capability. If public opinion or support for a war does not exist then no matter how just the cause, that war is still not legitimate. The United States constitution is based on a military that is ultimately controlled by elected officials who are placed or removed from power by the civilian population. If an adversary can control the civilian population, over time they will be able to control the legitimacy of the campaign.

1.3.2 Economic

The U.S. military has begun a transformation led by the Secretary of Defense Donald Rumsfeld. Secretary Rumsfeld believes in a small agile force that can quickly overcome an adversary with its technological advantage. A major problem with the Secretary's transformational idea is that if you become overcommitted, both militarily and economically, you will not be able to sustain the force structure. In stability operations, like Iraq and Afghanistan, an enormous amount of funding and troop commitment must be provided to bring about a lasting peace. Trying to transform your force and maintain the technological advantage at the same time as executing stability operations is difficult. Additionally, maintaining an advantage with respect to homeland security is even tougher requiring more fiscal support. It is evident that the Secretary's transformation plan has not adequately addressed the homeland security issues. A Strategic Studies Institute report states, "the Department of Defense (DOD) budget is unlikely to be adequate to meet both the needs of continuing operations and transformation during the coming years. In light of the likely budget constraints, it is vital that the DOD undertake a fundamental reassessment of the alignment of the force structure to anticipate threats. The DOD has a vital role to play in homeland security but the department is not engaged in the interagency process and is not adequately planning for needed homeland security capabilities."[18] This deficiency in capabilities will lead to vulnerabilities in the U.S. homeland security posture, allowing an unrestricted adversary to bring a prolonged war to our door step with limited resources. Osama Bin Laden stated in his January 2006 media release, "We were patient in fighting the Soviet Union and we bled their economy and now they are nothing. In that there is a lesson for you."[19] This is a direct attempt to apply the principles of economy of force and endurance into his posturing and in turn hopefully inject that sentiment into the anti-war factions within the political structure of our country.

With respect to the economy as a COG let us not forget the principle of end state. End state will play against the U.S. for eternity in that even if there is no unrestricted threat poised to strike from within our borders, we must always be prepared against such an attack. The end state of a secure nation is one that will exist and be a requirement for the military and the DHS until the last day of this country's existence. We will never be able to ignore the threat of economic attack from any number of adversaries.

1.3.3 Military commitments

If a small covert adversary attacks the U.S. they are not taking on the military head to head in attrition warfare in an attempt to win the war. A RAND study reports, "the 1968 Tet offensive in Vietnam, the bombing of the Marine Barracks in Beirut, and "Bloody Sunday" in Mogadishu were all strategic events; yet none of them could be described as a major military defeat. The initially successful Tet offensive resulted in the annihilation of the Viet Cong as a militarily significant force;

the loss of Marines in Beirut was a command failure and a profound human tragedy, but it did not materially affect U.S. military capabilities in Lebanon; and the Rangers in Somalia suffered relatively light casualties compared with those they inflicted on their adversaries. Nevertheless, each of these events was a watershed in U.S. involvement and led to dramatic reverses in U.S. policy."[20] The covert cell's desired effect would be to cause enough public fear that the military would be needed to defend against the unrestricted threat at home. This would stretch the already over-committed military resources trying to defend against the possibility of attacks at any location at any time.

U.S. military commitments and international involvement may be the center of gravity but most likely any contact with the military would be strictly out of the question for an adversary abiding by the Principles of economy and endurance**.**

1.3.4 Propaganda

Propaganda itself can be a COG in that a small radical group needs the media to distribute its message to a much greater audience than they could reach through direct contact. These small radical groups need the propaganda for proclamations of strength, spreading their message to the world, and general showing of power.

Larger groups like Osama Bin Laden's Al Qaeda (AQ) network may actually use the media to send messages to remote sleeper cells that cannot risk direct communications. Large networks will also use propaganda to spin events in their favor for recruitment of new personnel and to sway public opinion. This extensive use of the media is evidenced by Osama Bin Laden's 20 January 2006 pre-recorded message release. The release came only days after the most debilitating precision strike to AQ since the fall of the Taliban regime. This precisely timed media release may have been used to quell the fear of the AQ network over the Damadola attack. On January 13, 2006 U.S. aircraft fired missiles into the Pakistani village of Damadola in the Bajaur tribal area, about 7 km (4.5 miles) from the Afghan border, killing at least 18 people: the Bajaur tribal area government confirmed that at least four foreign members of AQ were among the dead. The attack targeted Ayman al-Zawahiri, purportedly second-in-command of AQ after Osama bin Laden. The damage done to AQ at Damadola could be enormous.[21] Bin Laden said that even if the U.S. does prevail in the war, "the nights and days will not pass without us taking vengeance like on Sept. 11, God permitting. The operations are under preparation and you will see them in your homes the minute they are through, with God's permission."[22] Bin Laden will obviously be counting on large media coverage should an attack take place and will most likely have a pre-recorded message ready for dissemination to Al-Jazerra and continued propaganda.

1.3.5 Center of gravity summary

The four COGs presented are so closely related that you cannot singularly affect one without affecting the others. A more plausible scenario is that all of these COGs will be targeted together where there is a much greater synergistic effect from your singular attacks. What is clear from the COG determination is that the media, as a form of communication and information distribution, will be used extensively. A 1995 RAND study on attacks against air facilities states, “beyond the immediate military effect of a successful air facility attack, the broader impact on the attitudes of leaders in the allied coalition, on legislators and other political elites in the United States, and on public opinion must be considered. News reporters and critics are likely to seize on a successful air facility attack as evidence of the ferocity and skill of the opponent, of U.S. ineptitude and the vulnerability, and of the likely high cost of the campaign."[23]

Once the center of gravity determination of influencing a nation's resolve, health of its economy and its military commitment through the use of the media is complete; a selection of what tactic to use must be made. The most commonly used method of achieving this goal by radical groups, if diplomatic and political efforts are not an option for them, is through the use of terrorism.

1.4 Terror

1.4.1 Terrorism as an effect

Terrorism is the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.[24] An effect as defined by the U.S. Joint Forces Command is the physical, functional, or psychological outcome, event, or consequence that results from specific military or non-military actions.[25] Indirect effects are those which are created through an intermediate effect or mechanism, producing another outcome or result, commonly referred to as 2nd and 3rd order effects. A cascading effect is an indirect effect that ripples through a system, often affecting other systems.[26] Based on the previous definitions, is the effect a terrorist organization looking for terror or fear to influence the center of gravity of the United States and its population? The direct effect is attacks to spur the media response; which in turn will cascade into fear and a change of the population's habits and confidence in its own country. As previously discussed a population response requesting better security at home will ultimately result in a reduction in U.S. influence abroad due to the withdrawal of resources both economic and militarily to fight the war being waged locally.

1.4.2 How to cause terror

The fanatical use of terror techniques has been in existence for hundreds, even thousands of years. To find the single most effective terrorist attack, look no farther than September 11, 2001. In terms of terrorism, what made this attack successful? To answer this you must first answer how does one cause terror in common people. What action must you take to get the effect, terror, you are looking for? In today's media rich environment large scale media coverage is a must. A news clip on the local economy page is not what the modern terrorist is looking for. The front page of every paper and interruption of every news and TV show in the world would be considered a success. The 911 attacks no doubt had the shocking effect of a large one-time event that was covered world wide for many weeks and months. But a single event similar in scale to 911 will not satisfy the desired effect of the terrorist group to influence the center of gravity of the United States. Five years after the attack much has changed in the United States economy but it is fair to say that the memory of the 911 attacks has faded far from memory and is not driving the general population to demand more homeland defense spending. What key elements did the 911 attacks lack to cause a longer lasting effect?

1.4.3 Elements of terror

It is easy to understand that a large shock effect is a key element to a successful terrorist attack. One look at Figure 1 brings back all sorts of memories and even a direct reflection of where you were when you first saw this image. The elements of this attack were the large shocking effect, with its associated large scale media coverage. There was the helplessness factor with the image of hundreds of people locked in an aircraft with no chance for escape. The final factor which may be the largest of all was that the terrorist took a completely new method in turning the aircraft themselves into a weapon and unleashed it on the general public, at work, at their desks; "unrestricted warfare."

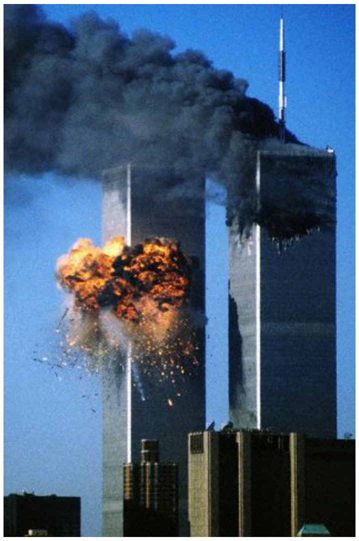


Figure 1: Twin Towers on September 11, 2001[27]

Again, what did this attack lack to cause a more lasting large scale effect on public behavior, economic health, and military commitments? To answer this we will analyze another recent media event, the DC Sniper case.

The DC Sniper case was where two men, Figure 2, with a single weapon went on a shooting spree that locked the nation's capitol in fear for 23 days. There are murders and killings everyday in America. What were the elements about the DC Sniper case that made it so terrifying? If we look back at the relevant portions of the definition of terror "the unlawful use of violence against persons to intimidate the civilian population in furtherance of social objectives." What was the objective, fear itself? If you are not sure if it was terror an example, the reaction to the violence against the civilian population in the DC area due to the attacks, will be convincing. The following list of county and district school events is a direct result of the sniper targeting a young boy leaving school to get into his parent's car. This is the public list of actual closures; there is no documentation of the change in public behavior that took place during this 23 day terror spree.

Figure 2: DC Snipers[28]

Maryland:
Anne Arundel County Schools: All schools locked, After-school activities canceled, No evening high school classes, Indoor recess and activities

Baltimore City Schools: No afternoon pre-kindergarten, No outdoor events

Calvert, Frederick and Charles County Schools: Students being kept inside schools, No after-school activities

Howard County Schools: Modified lockdown status, No afternoon kindergarten or special education, No outdoor recess or activities

Montgomery and Prince George's County Schools: Code Blue status, No afternoon pre-k or kindergarten, Extra security in schools, All field trips canceled, Indoor recess and lunch All after-school activities canceled, All school doors monitored by security

Queen Anne's County Schools: No after-school activities

District:
D.C. and Archdiocese of Washington Schools: No outdoor lunch or recess, No outdoor after-school activities, All field trips canceled

Virginia:
Alexandria City and Arlington County Schools: No outdoor recess or physical education classes, After-school activities canceled[29]

These murders were a sniping spree that lasted 23 days killing 10 people and injuring 3 more.[30] Even when it was apparent that there was one single shooting team, millions of people were forced to change their lives. It was the common everyday aspect of the killings that added to the fear. Similar to the 911 attacks with people at work in an office building being targeted, the snipers targeted people shopping, buying gas, and even a child walking from school to his parent’s car. The killings also had no common thread, all ages, races, and genders were targets. The indiscriminant aspect of the murders made it impossible for people to ignore the fear that they could be the target. There is a morbid sense of security due to being excluded from the targeted group.

The final key aspect to the DC snipers killings was the fact that there were no clues to catch the perpetrators, thus they could strike again. If the snipers had not left clues themselves it is quite possible that they would still be committing murders. Authorities received more than 60,000 tips during the sniper investigation.[31] The Montgomery County police hot line had so many reports or calls to the sniper hot line that it completely overwhelmed the investigative force. The massive influx of leads from the general populace during a 911 or DC Sniper type scenario is a known outcome that a terrorist could use to delay investigative efforts. This unknown aspect of the killings adds to the fear that it will happen again and no one is safe. The "every person I see could be a terrorist" feeling is very real and discomforting, causing people to report things that have no relevance to the case. When suicide bomber type terrorism takes place some sense of finality exists in that the perpetrator is also dead and will not strike again. So the unknown or lack of a conclusion is a key contributor to the fear.

These two recent terrorist events reveal the key tenants to causing fear or terror in the hearts of mankind. First you must touch a large audience which is through the media. Second there must be no excluded groups or locations where one can be allowed to feel safe. And lastly there has to be as many unknowns to the attacks as possible with no foreseeable end to the terror.

1.5 Airline Industry

The Violence Policy Center states, "the first terrorist mid-air bombing of an airliner took place in 1949. But terrorists did not begin to target civil aviation intensively until the mid 60s. The first armed assault of an airliner took place in June 1968, and the first terrorist hijacking for political extortion in July 1968. Although the number of airliner attacks peaked in the 1980s and has declined since then, the number of casualties has steadily increased, even excepting the catastrophic consequences of September 11, 2001. In other words, terrorist attacks on civil aviation have become more and more deadly over the past decade."[32] The airline industry could be attacked with multiple techniques at many critical nodes. The most obvious attack technique would be a terrorist from within the aircraft, 911 being the perfect example, bringing the aircraft down. The bulk of the defense and security measures to prevent attacks have been in the screening of personnel and baggage. Secondary to the internal attacks is the external attack from weapons or vehicle-borne improvised explosive devices (VBIED). Increased security patrols and added perimeter/fence defenses have been the only increase in security in this area.[33] The training required to attack the airline industry is as varied as the attack methods. Our goal would be to maximize the difficulty in adversary training and planning, thus the maximizing the manning and monetary resources needed to attack. The reaction or fear the attack could generate is perhaps the most extraordinary. The fascination with flight and the reflection on the 911 success would provide any future attack on the aviation industry with cascading effects like no other attack. A recent Rand study estimated the combined consumer and producer loss of a one week airline shutdown in the area of 3.4 billion dollars with cascading effects and losses in the 15 billion dollar range for a single aircraft being shot down.[34]

The number one requirement for the beginning of a terror campaign is a large amount of media coverage and the associated shock factor. The large amount of media coverage that would be generated by an airline industry event will result in future attacks of this critical node.

A successful attack on a U.S. aviation facility will most definitely have a strategic effect out of proportion to the resources expended. Immediate reflection to the 911 attacks and America's fascination with flight are both amplifying factors in the enemy's decision to target the airline industry. The economic impact of an aviation industry shut down as the Rand Study high lights would be a severe blow to the U.S. economy. Additionally, some of the other promising nodes to attack like tunnels and nuclear power plants pose too great a risk of capture or death and would violate the principles of economy and endurance. We shall apply the assumptions and principles of war to further covert cell attack planning and detailed analysis of the security measures in place at U.S. aviation facilities.

Chapter 2: Airline and Airport Defenses

The airline industry, specifically the commercial terminals, have multiple layers of security from the fence and roving patrols to strict terminal procedures to prevent hazardous materials and personnel from entering an aircraft. Another form of aircraft defense, traditionally seen on military combat aircraft, is self protection devices. The covert cells leadership may determine the method of attack to take down an aircraft loaded with passengers. The most basic of decisions is whether to attempt an internal attack through the terminal security measures or an external attack with some form of kinetic weapon and a delivery platform. We will analyze the aircraft’s susceptibility to attack from external means first, then the terminal’s security measures in order to continue solution analysis.

2.1 Airline external security

2.1.1 First line of defense

The first line of defense in airport security is the most obvious: fences, barriers and walls. Tall fences that would be difficult to climb enclose the entire airport property. Security patrols regularly scan the perimeter in case someone tries to cut through the fence, especially near sensitive areas like fuel depots. The terminals and baggage handling facilities are even more secure, with more fences and security checkpoints. All access gates are monitored by either a guard station or surveillance cameras.

Another risk is that someone could drive a truck or car containing a bomb up to the airport terminal entrance and just blow up the airport itself. Airports have taken several steps to prevent this. Large concrete barriers, designed to block vehicles up to the size of large moving trucks, can be deployed if a threat is detected. Loading zones, where people once parked their cars to get their baggage in or out of the trunk, are now kept clear of traffic. No one is allowed to park close to the terminal.

2.1.2 On deck defenses

Currently, the only on deck defenses that aircraft have are the defenses that are provided by the airport itself and the security infrastructure. Large aircraft are not agile enough to avoid a VBIED with turns, and cannot leave the paved surface while attempting some type of evasive maneuver. Any options for self protection measures to be installed on aircraft come with the safety requirements that these systems be off while on the ground. This is to prevent accidents and hazards to airport ground personnel. Any investment in expensive missile defense systems like lasers or flares would be ineffective at providing protection while on deck before takeoff and after landing.

Another threat to aircraft on deck with their limited taxi area and extremely tight parking areas in and around the terminal is from fratricidal explosions. A fratricidal explosion takes place when an explosion from one large aircraft is close enough to actually set ablaze and ignite another aircraft causing it to explode.

Figure 3, from airlines.com, depicts a situation where fratricidal explosions could quickly become out of control. If the 747 at the top left of the figure, closest to the airport perimeter, were to explode due to a terrorist attack during a crowded ramp or terminal time, then the whole row of five possible 747's may be subject to fratricidal explosions. Depending on the state of refueling and current fuel capacity of the aircraft parked at the terminal, the explosion could be large enough to spread to the aircraft and terminal at the lower portion of the figure. Several explosions of this size outside the terminal would most likely set the terminal on fire causing an enormous amount of casualties and destruction. Simultaneous refueling operations around the terminal would also be a high risk time for security personel.

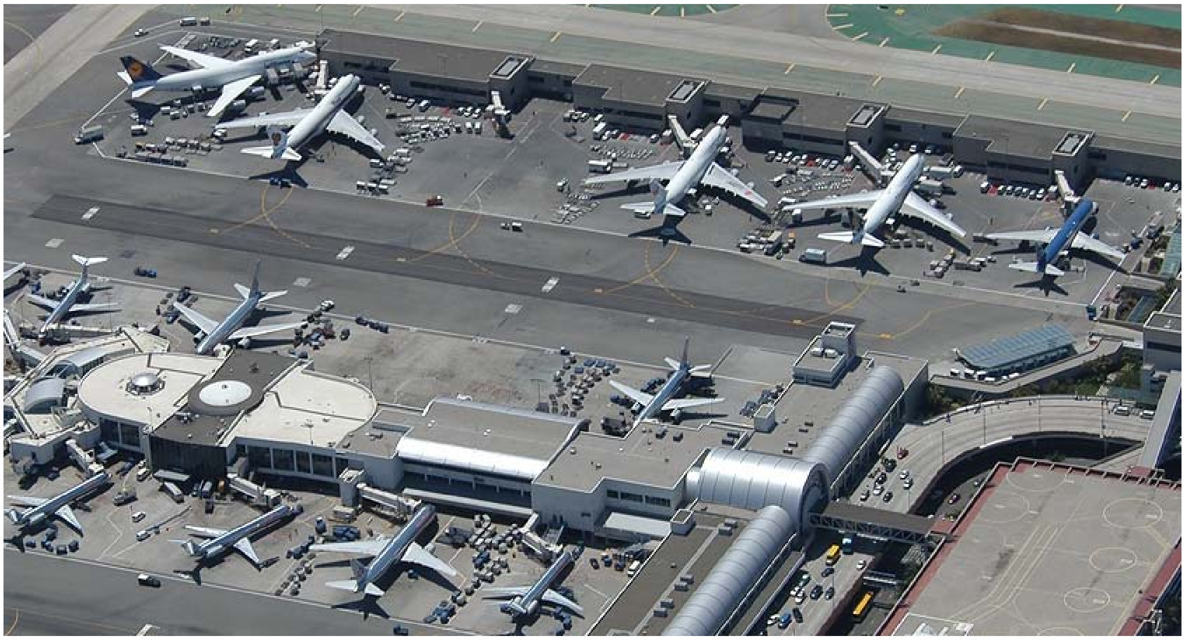


Figure 3: LAX terminal areas from Airlines.com

2.1.3 Transition defenses

One of the most vulnerable times for an aircraft would be its approach to landing, when its speed is relatively low and it is on a predictable path toward the runway. Figure 4, from Dakotakid.com, is a 747 on final approach at Los Angeles International airport. "Aircraft taking off are particularly vulnerable to missile attack; they are low and slow, heavy and have poor downward visibility as they climb out. Aircraft on approach are also low and slow but have much less flammable fuels on board and have better visibility."[35]

The covert cell may use all available information in planning its attack like the required aircraft altitudes while on an instrument approach, available from multiple agencies. These altitudes and airspeeds will tell the covert cell vital targeting information.

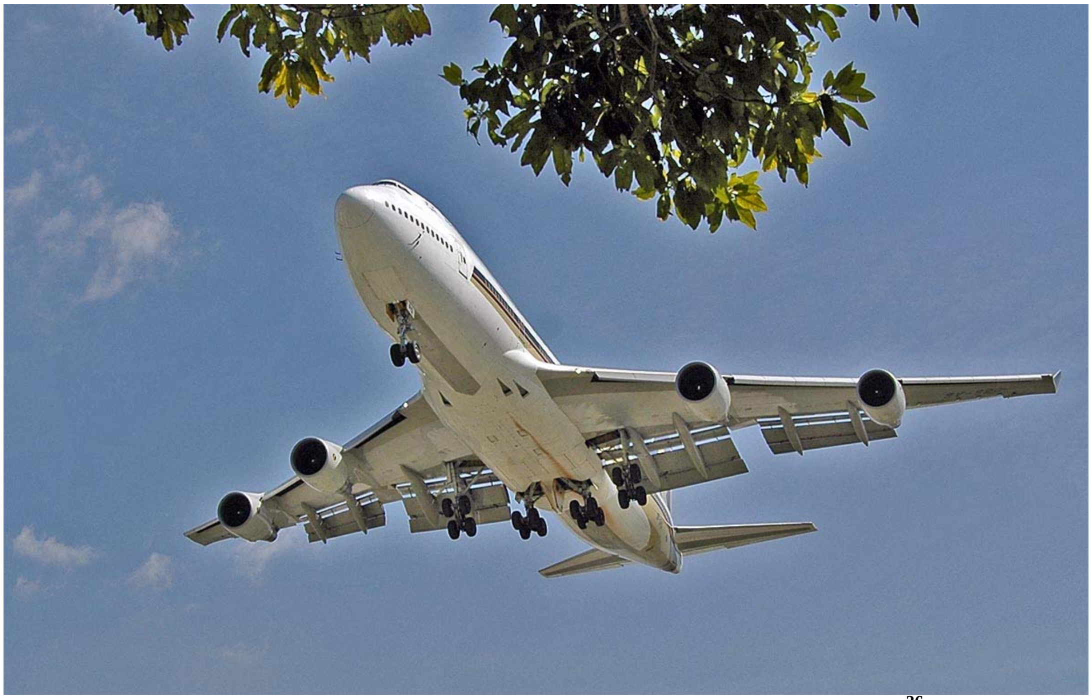


Figure 4: 747 Final approach to LAX from outside the fence line.[36]

The intriguing point of targeting an aircraft when it is low, yet attacking while positioned outside the confines of the outer airport defense, is the lack of a coherent security force that is focused on this type of threat. Capitalizing on the Principles of unity of effort and integration, or the lack there of, a covert cell may be able to execute an attack and leave the operating area before there is even a realization that the attack came from outside the airport's defenses.

2.1.4 Cruise defenses

While an aircraft is in transit and above 18,000 feet there is very minimal chance that it would be taken down by an external threat. Only the very latest model shoulder fired weapons have the capability to hit high altitude aircraft. The probability of a hit at the extreme edges of the operating envelope goes down significantly. A covert cell that went through the planning to acquire such a weapon would most likely increase its chances for success by attacking the aircraft while in transition, yet as far away from security forces as possible.

2.2 Internal airport security

2.2.1 Terminal passenger check-in

One of the most important security measures at an airport is confirming the identity of travelers. This is done by checking a photo ID, such as a driver's license. If you are traveling internationally, you need to present your passport. Simply taking a look at a photo ID isn't enough, however. The latest high-tech systems in airport security screening today use biometrics. Biometrics essentially means checking fingerprints, retinal scans and facial patterns using complex computer systems to determine if someone is who they say they are, or if they match a list of people the government has determined might be potential terrorists.

A new system called CAPPS II could help accomplish some of this. Short for Computer Assisted Passenger Prescreening System, CAPPS II will require more personal information from travelers when they book their flights. This will lead to a risk assessment of no risk, unknown risk, elevated risk, or high risk. Passengers considered risky will be further screened. Although the system has been delayed and isn't in place yet, the Department of Homeland Security (DHS) predicts that CAPPS II, or some form of the same technology under a different name, will make check-in faster for the average traveler.

Many new basic security measures have been put in place post 911: the public address system at an airport replaying an automated message telling you not to leave your bags unattended is an example.

Just a month after the 911 attacks, the President signed a new law that restructured and refocused the airport security efforts of the U.S. Aviation and Transportation Security Act establishing a new agency, the Transportation Security Administration (TSA). The TSA is part of the Department of Homeland Security. The TSA's mission is to; prevent attacks on airports or aircraft, prevent accidents and fatalities due to transport of hazardous materials, and ensure safety and security of passengers.

While the TSA deals with all forms of transportation, the Federal Aviation Administration (FAA) is devoted entirely to the operation of the U.S.'s civil aviation. FAA agents are located at every major airport for immediate response to possible threats. Most major airports also have an entire police force, just like a small town, monitoring all facets of the facility. Background checks are required on all airport personnel, from baggage handlers to security-team members, before they can be employed. All airport personnel have photo-ID cards with their name, position and access privileges clearly labeled.

After the identity check process only traveling personnel are allowed into the terminal area. At this point every traveler is channeled through control points, where every person must walk through a metal detector and all items must go through an X-ray machine. Almost all airport metal detectors are based on pulse induction (PI). Typical PI systems use a coil of wire on one side of the arch as the transmitter and receiver. This technology sends powerful, short bursts (pulses) of current through the coil of wire. Each pulse generates a brief magnetic field. When the pulse ends, the magnetic field reverses polarity and collapses very suddenly, resulting in a sharp electrical spike. This spike lasts a few microseconds and causes another current to run through the coil. This subsequent current is called the reflected pulse and lasts only about 30 microseconds. Another pulse is then sent and the process repeats.

A typical PI-based metal detector sends about 100 pulses per second, but the number can vary greatly based on the manufacturer and model, ranging from about 25 pulses per second to over 1,000. If a metal object passes through the metal detector, the pulse creates an opposite magnetic field in the object. When the pulse's magnetic field collapses, causing the reflected pulse, the magnetic field of the object makes it take longer for the reflected pulse to completely disappear. This process works something like echoes: If you yell in a room with only a few hard surfaces, you probably hear only a very brief echo, or you may not hear one at all. But if you yell into a room with a lot of hard surfaces, the echo lasts longer. In a PI metal detector, the magnetic fields from target objects add their "echo" to the reflected pulse, making it last a fraction longer than it would without them.

A sampling circuit in the metal detector is set to monitor the length of the reflected pulse. By comparing it to the expected length, the circuit can determine if another magnetic field has caused the reflected pulse to take longer to decay. If the decay of the reflected pulse takes more than a few microseconds longer than normal, there is probably a metal object interfering with it.

The sampling circuit sends the tiny, weak signals that it monitors to a device call an integrator. The integrator reads the signals from the sampling circuit, amplifying and converting them to direct current (DC). The DC voltage is connected to an audio circuit, where it is changed into a tone that the metal detector uses to indicate that a target object has been found. If an item is found, you are asked to remove any metal objects from your person and step through again. If the metal detector continues to indicate the presence of metal, the attendant uses a handheld detector, based on the same PI technology, to isolate the cause.

2.2.2 Carry-on baggage

The next section is what happens to carry-on items while going through the metal detector. A conveyor belt carries each item past an X-ray machine. X-rays are like light in that they are electromagnetic waves, but they are more energetic, so they can penetrate many materials.

The most common machine used in airports is based on a dual-energy X-ray system. This system has a single X-ray source sending out X-rays, typically in the range of 140 to 160 kilovolt peak (kVp). KVp refers to the amount of penetration an X-ray makes. The higher the kVp, the further the X-ray penetrates. After the X-rays pass through the item, they are picked up by a detector. This detector then passes the X-rays on to a filter, which blocks out the lower-energy X-rays. The remaining high-energy X-rays hit a second detector. A computer circuit compares the pick-ups of the two detectors to better represent low-energy objects, such as most organic materials.

Since different materials absorb X-rays at different levels, the image on the monitor lets the machine operator see distinct items inside your bag. Items are typically colored on the display monitor, based on the range of energy that passes through the object, to represent one of three main categories; organic, inorganic, and metal.

While the colors used to signify "inorganic" and "metal" may vary between manufacturers, all X-ray systems use shades of orange to represent "organic," Figure 5. This is because most explosives are organic. Machine operators are trained to

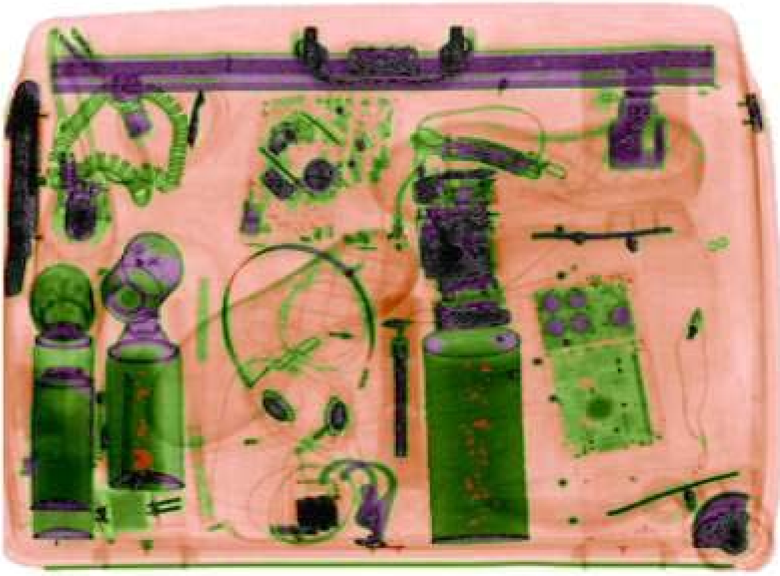


Figure 5: An X-ray of a bag.
Notice that all organic items are a shade of orange[37]

look for suspicious items, and not just obviously suspicious items like guns or knives, but also anything that could be a component of an improvised explosive device (IED). Since there is no such thing as a commercially available bomb, IEDs are the way most terrorists and hijackers gain control. An IED can be made in an astounding variety of ways, from basic pipe bombs to sophisticated, electronically-controlled component bombs. Electronic items, such as laptop computers, have so many different items packed into a relatively small area that it can be difficult to determine if a bomb is hidden within the device. That's why travelers may be asked to turn their laptop or PDA on. But even this is not sufficient evidence since a skilled criminal could hide a bomb within a working electronic device. For that reason, many airports also have chemical sniffers. This is essentially an automated chemistry lab in a box. At random intervals, or if there is reason to suspect the electronic device that someone is carrying, the security attendant quickly swipes a cloth over the device and places the cloth on the sniffer. The sniffer analyzes the cloth for any trace residue of the types of chemicals used to make bombs. If there is any residue, the sniffer warns the security attendant of a potential bomb. In addition to desktop sniffers like this, there are handheld versions that can be used to "sniff" lockers and other enclosed spaces and unattended luggage. Walk-through models are also available. These sniffers can be used to detect explosives and narcotics.

2.2.3 Checked baggage

In addition to passenger baggage, most planes carry enormous amounts of cargo. All of this cargo has to be checked before it is loaded. Most airports use one of three systems to do this; Medium X-ray systems, Figure 6, which are fixed systems, can scan an entire pallet of cargo for suspicious items. Mobile X-ray components in a large truck can comprise a complete X-ray scanning system. The truck drives very slowly beside another stopped truck to scan the entire contents of that truck for suspicious items. Fixed-site systems can be entire buildings that are one huge X-ray scanner. A tractor-trailer is pulled into the building and the entire truck is scanned at one time.

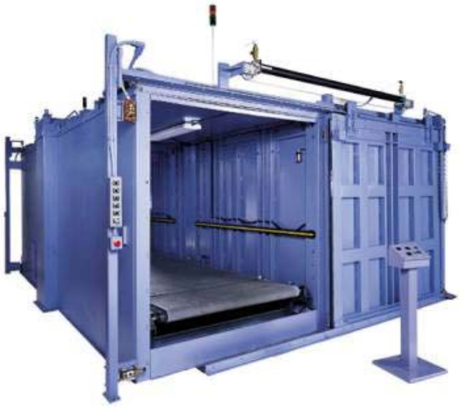


Figure 6: Checked luggage goes through some type of X-ray machine[38]

One old-fashioned method of bomb detection still works as well or better than most hi-tech systems, the use of trained dogs. These special dogs, called K-9 units, have been trained to sniff out the specific odors emitted by chemicals that are used to make bombs. Incredibly fast and accurate, a K-9 barks at a suspicious bag or package, alerting the human companion that this item needs to be investigated.

In addition to an X-ray system, many airports also use larger scanners, called CT Scanners, Figure 7. The first security check that your checked bags go through depends on the airport. In the United States, most major airports have a computerized tomography (CT) scanner. A CT scanner is a hollow tube that surrounds your bag. The X-ray mechanism revolves slowly around it, bombarding it with X-rays and recording the resulting data. The CT scanner uses all of this data to create a very detailed tomogram (slice) of the bag. The scanner is able to calculate the mass and density of individual objects in your bag based on this tomogram.

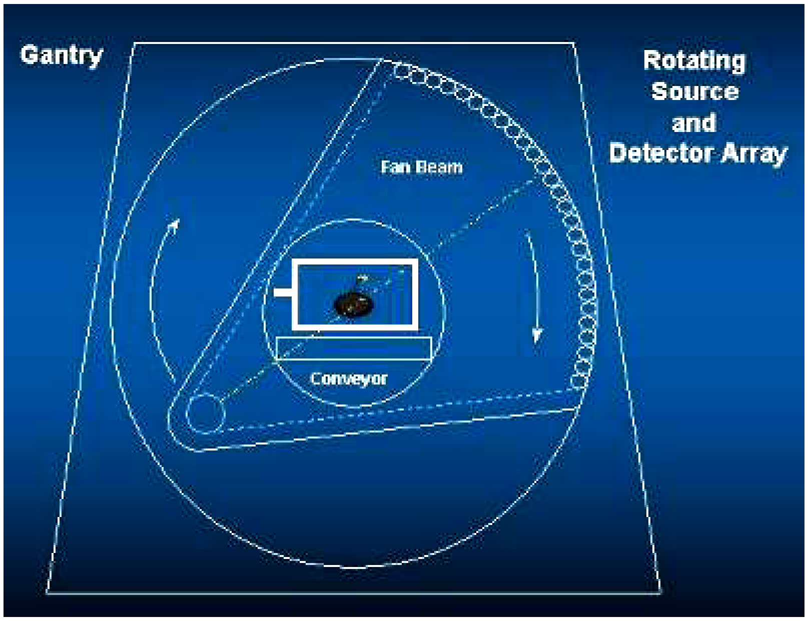


Figure 7: The X-ray system in a CT scanner rotates around a bag[39]

If an object's mass/density falls within the range of a dangerous material, the CT scanner warns the operator of a potential hazardous object. CT scanners are slow compared to other types of baggage-scanning systems. Because of this, they are not used to check every bag. Instead, only bags that the computer flags as "suspicious" are checked. These flags are triggered by any anomaly that shows up in the reservation or check-in process. For example, if a person buys a one-way ticket and pays cash, this is considered atypical and could cause the computer to flag that person. When this happens, that person's checked bags are immediately sent through the CT scanner, which is usually located somewhere near the ticketing counter.

In most other countries, particularly in Europe, all baggage is run through a scanning system. These systems are basically larger versions of the X-ray system used for carry-on items. The main differences are that they are high-speed, automated machines integrated into the normal baggage-handling system and the kVp range of the X-rays is higher.

While most of the things that you can't take on board an airplane are fairly obvious (guns, knives, explosives), there are some things that most people wouldn't think about. Who would have thought that a smoke detector could be considered hazardous? If you do transport a hazardous material on a passenger plane without declaring it, you could face a fine of up to $27,500.

Because terrorism is a constant and very real threat, this means that any mention of certain words, such as "bomb," "hijack" or "gun," can lead to your immediate removal from the plane and quite possibly your arrest, even if the word is said in an innocent manner. Everyone who works in aviation, from flight attendants to security personnel, is trained to react immediately to those words.

There are a number of items that you cannot carry on a plane, and some of that can't be packed in your bags, either:

- Explosives: Fireworks, ammunition, sparklers, matches, gunpowder, signal flares
- Weapons: Guns, swords, pepper spray, mace, martial arts weapons, swords, knives with blades of any length
- Pressurized containers: Hair spray, oxygen tanks, propane tanks, spray paint, insect repellant
- Household items: Flammable liquids, solvents, bleach, pool chemicals, flammable perfume in bottles 16 ounces or larger
- Poisons: Insecticides, pesticides, rat poison, arsenic, cyanide
- Corrosives: Car batteries, acids, lye, drain cleaner

2.2.4 Air marshals

If everything else fails and a terrorist still gets onto a flight with a weapon, an armed air marshal can take control of a situation and restrain the attackers. Although the air marshal program has existed since the 1970s, it has never had as high of a profile as it has in the post-911 era.

An air marshal is a federal agent disguised to look like regular passenger. Each air marshal is authorized to carry a gun and make arrests. There are not enough air marshals to cover every flight, so their assignments are kept secret. No one knows which passenger is the air marshal, or even if an air marshal is present on the flight at all. Although their exact numbers are kept classified, airline insiders estimate that only five percent of U.S. flights have an air marshal on board. This is still a major increase; in the years before 911, a handful of marshals guarded just a few international flights.

2.3 Attack summary

With the numerous internal security measures in place, restricting all aspects of entry into an aircraft, selecting this method of attack would be very risky and would most likely result in marginal results at best. Looking at the history of airbase assaults, a Rand study summarizes the attacks stating, "the most common air base attack objective was to destroy aircraft. Seventy five percent of such attacks used standoff weapons, and the standoff attacks were very difficult to counter. The standoff threat is the most worrisome. Attackers using relatively crude techniques, unadjusted mortar or rocket fire have destroyed hundreds of aircraft on air bases. Defeating this threat is not a matter of guarding perimeter fences or flight lines; it cannot be handled without vigorous surveillance outside the wire."[40] Additionally, an internal attack would violate several of the applicable principles of war, specifically endurance and economy of force. This exclusion of the option of an internal attack will lead to an evaluation of the possible external attack methods.

Once again applying the principles of war we can exclude several methods of external attack also. The use of IEDs or VBIEDs would require the breaching of the outer perimeter and would most likely result in contact with roving patrols and deadly force. The small covert cells may want to strike and disappear without a chance of being captured. This leads us to the need to defend against the use of stand off weapons to engage an aircraft.

Chapter 3: Weapon Selection

Determining the weapon to defend against is a required step in the solution recommendation process. The weapon type will dictate the further planning of defenses. The airline industry may be chosen for attack. The internal vs. external attack evaluation has been made, and the external attack abides by the principles of war. The next step in the process is determining the enemy's most likely weapon selection. This section will provide discussion on the various classes of weapons available for possible aircraft attack. Each weapon class will be evaluated for its capability, availability, and training. Additional weapon classes may be discussed briefly but will be omitted for various reasons. All specific data regarding weapons were obtained through www.howstuffworks.com.

3.1 Shoulder launched missiles (MANPADS)

3.1.1 MANPADS capabilities

The most famous U.S. Manned Portable Air Defense System (MANPADS), the Stinger missile officially known as the FIM-92A, is designed to give ground troops a way to deal with low-flying airplanes and helicopters. The foreign models of this missile, SA-7/14/16/18 are very similar and will not be discussed individually, other than some basic capability differences. From the perspective of soldiers on the ground, low-flying enemy aircraft are normally a problem because they are bombing or strafing, doing surveillance work or inserting, extracting and re-supplying enemy troops. Shooting down these aircraft is the easiest way to eliminate the threat. There are several things that make the Stinger such an effective weapon for ground troops and terrorists alike. The Stinger is a lightweight, portable weapon. The missile and its launcher weigh about 35 pounds, the launcher is reusable, and it is a shoulder-launched weapon. One person can launch a Stinger missile, it uses a passive infrared seeker, and it is a fire-and-forget weapon.

The infrared seeker is able to lock on to the heat that the aircraft's engine is producing. It is called a "passive" seeker because, unlike a radar-guided missile, it does not emit radio waves in order to "see" its target. To fire the weapon, the soldier aims the missile at the target. When the seeker locks on, it makes a distinctive noise. The soldier pulls the trigger, and two things happen, a small launch rocket shoots the missile out of the launch tube and well clear of the soldier who is firing it and the launch engine falls away and the main solid rocket engine lights.

This rocket propels the Stinger to approximately 1,500 mph (2,400 kph, Mach 2). The missile flies to the target automatically and explodes via a contact fuse. The Stinger missile can hit targets flying as high as 11,500 feet (3,500 m), and has a range of about 5 miles (8 km). This means, in a general way, that if an airplane is less than 2 miles high and it is visible as a shape, rather than a dot, then it is likely that the Stinger can hit it. Stinger missiles are extremely accurate.

MANPADS have received much of the media attention recently with multiple studies done on the possibility of putting self protective systems on airliners. A Jane’s Intelligence review states, “the most recently deployed of these missiles can be very difficult to counter. For example, during the Gulf War, 12 of the 29 U.S. aircraft lost to Iraqi air defenses were shot down by SA-14 and SA-16 man portable missiles."[41] From airport diagrams and typical approach patterns it is possible to deduct a rough order of magnitude for the square mileage of area within which a terrorist armed with a MANPADS could pose a threat to civilian airliners. With an SA-7 and an approximate maximum engagement altitude of 10,000 ft a terrorist could launch while situated anywhere within an 800 square mile area. With a more modern missile, for example an SA-18, with the capability to engage up to 18,000 ft the engagement area is in excess of 4,000 square miles.

3.1.2 Availability

"The former Soviet Union provided tens of thousands of their SA-7s to various client countries, and the United States has sold or given thousands of Redeye and Stinger SAMs to its allies as well. According to RAND published report, MANPADS missiles are available on the black market for under $100,000. Indeed the U.S. General Accounting Office alleges the inventory control over U.S. stockpiles of such weapons has been so shoddy that hundreds, if not thousands might be unaccounted for."[42] "With the increase in collaboration among terrorists groups, one may expect the transfer of a variety of MANPADS types among them. A Jane's Intelligence Review, Table 1, provides an overview of non-state groups known or thought to be in possession of MANPADS today."[43] "Al Qaeda in particular has at least first generation MANPADS, has the ability to move them internationally, and has decided to employ MANPADS attacks as part of its terror campaign.

Table 1: Proliferation of MANPADS among Selected Non-State Groups[44]

Non-State Groups	1st Gen infrared Retical Scan SA-7	2nd Gen IR Conical Scan Sa-14, 16 Basic Stinger	3rd Gen IR Pseudo Imaging SA-18	CG Command Guided Blowpipe
Al Qaeda	Confirmed	Confirmed	Probable	Probable
Chechen rebels	Confirmed	Confirmed	Confirmed	Possible
Taliban	Confirmed	Probable	Probable	Probable
Tamim Tigers	Confirmed	Confirmed	Possible	Possible
Hezbollah	Confirmed	Probable	Possible	Possible
FARC	Confirmed	Possible	Possible	Possible

That was shown, for example, by the November 2002 attempt to use two MANPADS missiles to bring down an Israeli charter airliner departing Mombassa, Kenya."[45] "The difficulties associated with getting the assets in place are certainly not insurmountable for an organization such as Al Qaeda. The difficulties and risks associated with smuggling a handful of man-portable weapons and a few trained operators into the United States are probably commensurate with those of training, indoctrinating, and positioning the four teams of men who commandeered and flew the aircraft involved in the attacks of September 11, 2001."[46]

3.1.3 Training

Training, as depicted in Figure 8, would be a challenge for a covert cell attempting to adhere to the principle of surprise. There is no place in the U.S. where you could brandish and be seen with a MANPAD without raising suspicions. Even if extra missiles were available, the only type of training that could be done is dry fire training, where the operator just assembled the unit, simulated aiming and simulated firing. This amount of simulation would cause U.S. military training experts to

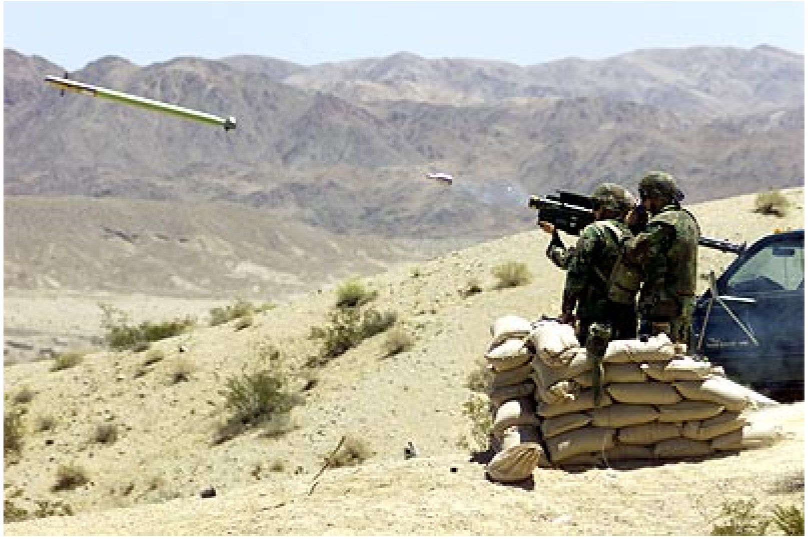


Figure 8: Marines launch a Stinger anti-aircraft missile

question the capability of their forces to actually perform the assigned tasks, and it should be no different for an adversary.

3.2 Rocket propelled grenades (RPG)

3.2.1 RPG capabilities

Rocket propelled grenades, Figure 9, were first introduced into combat in the form of a bazooka in 1941.

The RPG was based on simple principles where a hand held grenade could be thrown 100 feet or less, a RPG can fire with some accuracy out to 2000 feet. The RPG operator takes a propelling charge and screws it onto the end of a warhead. The operator then takes this assembled artillery and loads it into the front end of the RPG launcher so that it lines up with the trigger mechanism.

After the RPG operator pulls the trigger, Figure 10, a percussion cap ignites the primer, gases build up inside the launcher's chamber, thereby breaking apart the

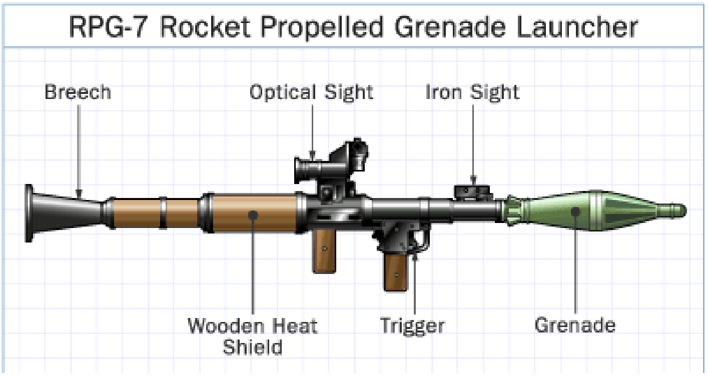


Figure 9: RPG Basic diagram[47]

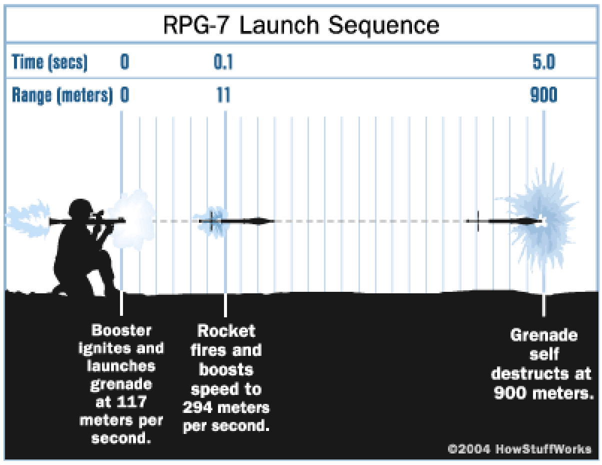

RPG-7 Launch Sequence
Time (secs) 0 0.1 5.0
Range (meters) 0 11 900
Booster ignites and launches grenade at 117 meters per second.
Rocket fires and boosts speed to 294 meters per second.
Grenade self destructs at 900 meters.
©2004 HowStuffWorks

Figure 10: RPG launch sequence[48]

cardboard container and propelling the grenade forward through the barrel of the launcher. The force of the built-up gases throws the grenade out of the tube at approximately 384 feet per second. As the grenade leaves the launcher the fins spread out, which along with the rocket motor, allow the grenade to travel at a potential speed of about 965 feet per second. The exhaust gases exit to the rear of the launcher unit and the operator is free to immediately reload the weapon. In practice, however, no RPG operator would ever remain stationary and spend the time to reload. The launching flash and whitish blue-gray smoke provides a clear indication to the enemy of the RPG launcher's location.

3.2.2 Availability

The availability of RPG's is similar to MANPADS in that they are available on the black market, but at a much lower price range. The ability to smuggle this class of arms into the U.S. would be the same as MANPADS in that they are about the same size and weight and are no less restricted. The difference between the highly technical aspects of MANPADS and RPG is that it is possible with a moderate amount of knowledge to create your own RPG type capability. Several web sites describe what it takes to build your own firing grenades but there is no way to validate the web site claims without actually attempting the act.

3.2.3 Training

Training with RPGs is actually worse than with MANPADS since with a MANPADS you can fire and forget the weapon since the guidance is automatic. This is not the case with an RPG. RPGs are point and shoot weapons that have no guidance. Each PRG round will fly out differently and hitting a target at distance would be very difficult if not impossible without significant live fire training. Live fire training with an RPG would most definitely raise suspicions.

3.3 Rifles

3.3.1 Caliber vs. capability

Aside from the discussion about what overall weapon to use against an aircraft is the secondary question about what caliber rifle to use in an attack to allow for a true capabilities comparison.

One glance at Figure 11 reveals the absolute size difference between the 50 caliber round and regular conventional rounds. When attacking an airfield and its aircraft with a rifle there is no comparison: a 50 caliber weapon would most likely be used. The 50 caliber is designed for that very purpose. The first and most widely purchased 50 caliber rifle is the Barrett Model 82A1. Early Barrett promotional material directly states the weapons usefulness against aviation threats. For example, an undated brochure, from about 1984, from the ATF's licensing file states:

> "The Model 82A1 is designed to provide extreme accuracy at extended ranges with standard military ammunition. The accuracy of the Model 82A1 makes possible the placement of the shot in the most vulnerable area of the target. The compressor section of jet engines or the transmissions of helicopters are likely targets for the weapon, making it capable of destroying multi-million dollar aircraft with a single bullet delivered to a vital area. The cost effectiveness of the model 82A1 cannot be overemphasized when a round of ammunition purchased for less then ten US dollars can be used to destroy a modern jet aircraft."[49]

"The same brochure boasts that the accuracy of the 50 caliber sniper rifle enables it to place more rounds on target in the same time than the M2HB machine gun firing full automatic while expending approximately one third the rounds. Inventor and manufacturer Ronnie G. Barrett elaborated on these capabilities of his company's 50 caliber anti-armor sniper rifles more recently in sworn testimony during a 1999 federal criminal trail. He testified that a shooter could empty his rifle's

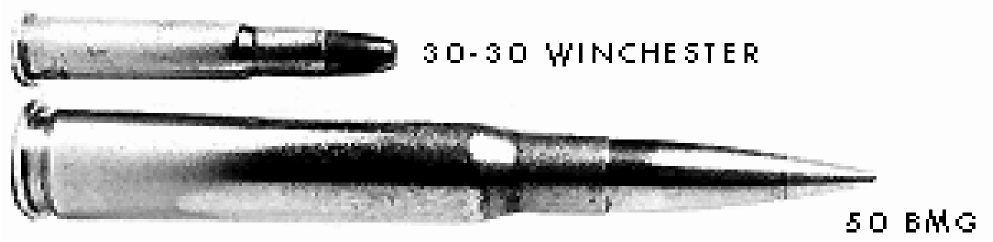


Figure 11: 50 Caliber BMG to 30 Caliber round comparison[50]

Table 2: 50 Caliber Armor Piercing Capability[51]

Material	***200 Meters*** ***(219 Yards)***	***600 Meters*** ***(656 Yards)***	***1,500 Meters*** ***(1,640 Yards)***
Homogeneous Armor Plate	1.0"	0.7"	0.3"
Face-Hardened Armor Plate	0.9"	0.5"	0.2"

standard 10-round magazine in less than a minute, even taking time to regain a sight picture of the target after every shot. Barrett also testified that at a distance of 1,000 yards the 50 caliber anti-armor sniper rifle could penetrate the fuselage, engines and cockpit windows of commercial aircraft, Table 2.”[52]

3.3.1.1 Ammunition

“The U.S. Army says that the basic 50 caliber armor-piercing incendiary (API) round is designed for use against armored aircraft and lightly armored vehicles, concrete shelters and other bullet resistant targets.”[53] The armor piercing effect is achieved by the bullet’s design, which wraps a hardened core of a substance like manganese-molybdenum steel with a softer metal jacket. The hardened core allows the round to penetrate armor plating until the core is pealed back and the incendiary material reaches its flash point and lights off causing a molten jet to form. This effect is devastating when placed in the vital locations on an aircraft specifically the engines or fuel tanks.

The range of the 50 caliber at which a terrorist can effectively take out hardened targets is greater than the maximum effective range of conventional police anti sniper rifles, Table 3. The 50 caliber weapon should be of grave concern for any police enforcement unit not ready to deal with it as a threat.

Table 3: 50 Caliber bullet maximum range and muzzle velocity[54]

Cartridge	Maximum Range (Meters)	Meter Trace	Average Muzzle Velocity (Feet per second)
Ball, M2	7400	-	2930
Tracer, M1 (with gilding metal jacket)	5575	1800	2860
Tracer, M1 (with clad steel jacket)	5450	1800	3030
Tracer, M17	5450	2450	3030
Incendiary, M1	6050	-	3090
Armor Piercing, M2	7400	-	2930
Armor Piercing-incendiary, M8	6470	-	3050
Armor Piercing-incendiary-tracer, M20	6470	300-1750	3050

The crown jewel of 50 caliber ammunition is the Raufoss multi-purpose round, developed by a Norwegian company and manufactured under license by several companies including Winchester. Designated the MK211 by the U.S. military, the round combines armor-piercing, explosive, and incendiary effects by using a "highly effective pyrotechnically initiated fuse that delays detonation of the main projectile charge until after initial target penetration. This delay moves projectile fragmentation and damage effect inside the target for maximum anti-personnel and fire start capability."[55]

According to its developer, Nordic Ammunition Company (NAMMO), the round can be used in "sniper rifles similar to the Barrett M82A1," has "the equivalent firepower of a 20mm projectile to include such targets as helicopters, aircraft, light armor vehicles, ships, and light fortifications, and can ignite JP4 and JP8 military jet fuel. "[56]

"According to the Marine Corps, the Barrett M82A1 fires the .50 caliber Raufoss ammunition, which contains a tungsten penetrator and a more powerful explosive charge than the API ammunition. The Raufoss round has penetrated an inch of steel at 2000 yards."[57] The devastating effects of the Raufoss round are realized by the combined armor piercing capabilities and the incendiary effects once inside the skin of the target, Figure 12.

3.3.2 Availability

Arms and ammunition are readily available in the U.S. Figure 13 reveals just how inexpensive and easy it is to purchase armor piercing incendiary rounds capable of absolute destruction of aircraft and air field vital facilities. A terrorist cell must decide if it wishes to purchase its 50 caliber rifles and ammunition openly and be subject to tracking by the Federal Bureau of Investigation (FBI) or the Alcohol Tobacco and Firearms agency (ATF), or to acquire the weapons through theft or black market purchase, which also has its risks.

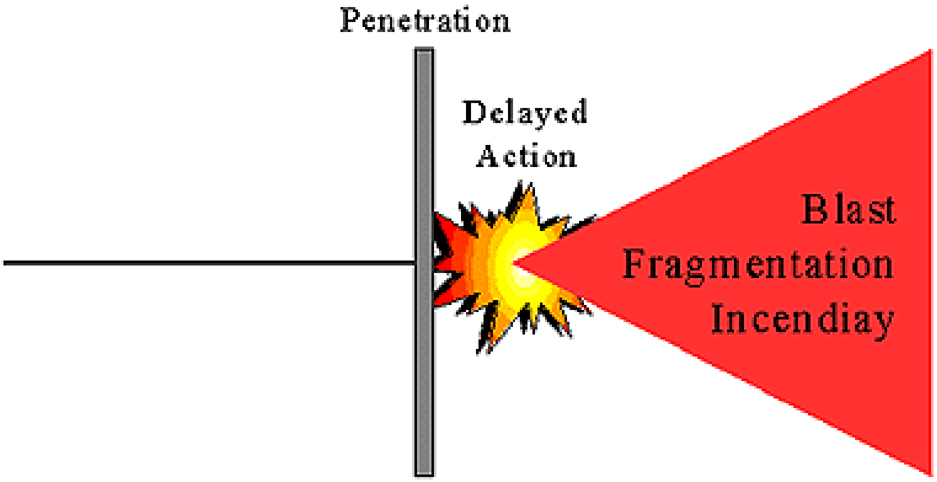
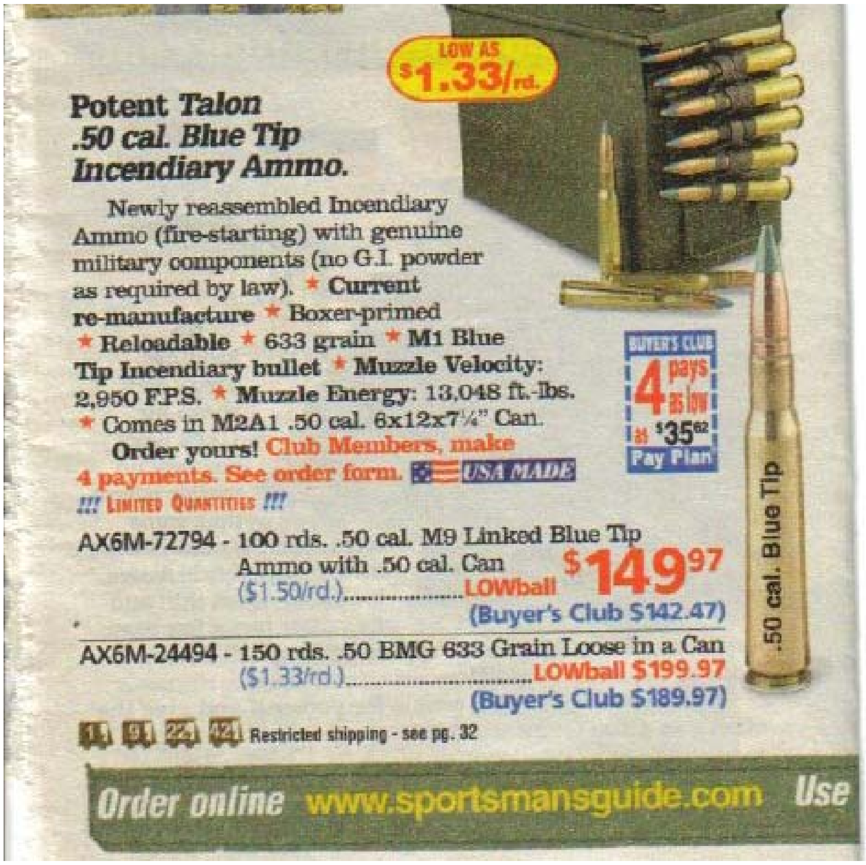


Figure 12: Raufoss Round Effects[58]



Potent Talon .50 cal. Blue Tip Incendiary Ammo.

Newly reassembled Incendiary Ammo (fire-starting) with genuine military components (no G.I. powder as required by law). * Current re-manufacture * Boxer-primed * Reloadable * 633 grain * M1 Blue Tip Incendiary bullet * Muzzle Velocity: 2,950 F.P.S. * Muzzle Energy: 13,048 ft.-lbs. * Comes in M2A1 .50 cal. 6x12x7¼" Can.

Order yours! Club Members, make 4 payments. See order form. USA MADE

!!! LIMITED QUANTITIES !!!

BUYER'S CLUB 4 pays as low as $\$35^{62}$ Pay Plan

AX6M-72794 - 100 rds. .50 cal. M9 Linked Blue Tip Ammo with .50 cal. Can ($1.50/rd.)........................LOWball $\$149^{97}$
(Buyer's Club $142.47)

AX6M-24494 - 150 rds. .50 BMG 633 Grain Loose in a Can ($1.33/rd.)........................LOWball $199.97
(Buyer's Club $189.97)

Restricted shipping - see pg. 32

Order online www.sportsmansguide.com Use

Figure 13: 50 Cal API bullet advertisement from Sportsman guide

"Arms and ammunition, including such destructive items as M-16 assault rifles, machine guns, TNT, dynamite, plastic explosives, land mines, and hand grenades, are regularly stolen from U.S. military armories."[59] **"**A recent U.S. Department of Justice Inspector General report revealed that even the FBI cannot account for hundreds of missing firearms. The implications of the potential uses against civilian aviation facilities to which a terrorist might put 50 caliber armor-piercing, incendiary or Raufoss ammunition can only be described as frightening. Yet all of these types of ammunition are available on the U.S. market."[60] Large caliber sniper rifles are legal in the U.S. and can be purchased for around $7,000 new in the box, Figure 14.

3.3.3 Training

Training for "small arms proficiency" is quite simple. There are indoor ranges in every city across the country, and outdoor ranges within miles of most urban areas. There is no expertise required to become relatively proficient with a rifle. Practice and some investigation is all that is required to begin. Any search on the World Wide Web for the term "sniper" brings up a plethora of books and training manuals. Some of the best and most readily available are Army and Marine Corps manuals on urban warfare, concealment, and sniping techniques. Army Field manual 3-23 is titled Marksmanship. The manual goes into specifics on terminology, aiming, breathe control, trigger control, ballistics, wind classification, and techniques for hitting moving targets.

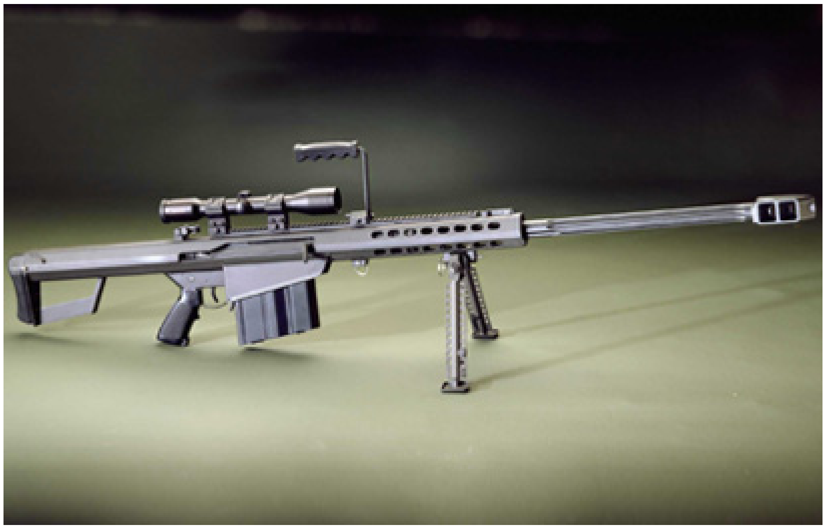


Figure 14: Barrett M82A1 with 10 round clip

It is easy to see that studying available material and practice would enable most anyone to become proficient in hitting targets with a high powered rifle.

3.4 Other weapons

3.4.1 Precision mortars

A traditional mortar is an aiming tube that adjusts its elevation angle to lob grenades in a ballistic trajectory toward its target. "Armed with traditional bombs, a skilled mortar man in radio contact with a forward observer can lay down extremely accurate fire, but doing so takes time. A few rounds are needed to set the mortar base plate firmly in the ground, and then individual shots are adjusted onto the target by the forward observer. This allows the defender to determine the location of the mortar team and return fire relatively quickly. In contrast, a global positioning system (GPS) guided round could achieve first round kills, allowing targets to be killed within seconds, and the attacker much better chances of escaping."[61] The advantage to having GPS guided mortars would be immense, allowing an attacker to accurately place rounds at selected locations on a civilian airfield just based on commercially available coordinates. This would be possible while not even in view of the airfield and any security forces. The precision mortar threat is a real possibility for an attack of an airfield and static targets in the future. The development of these weapons is ongoing and should be watched closely. Their developmental status and lack of availability will prevent them from being a viable option at this time, and thus will not be considered in our solution recommendation.

3.5 Weapon Comparison

3.5.1 Capability

Figure 15 depicts an airport diagram with weapon engagement zones overlaid on top for an easy reference for weapon range capability comparisons. The increased ranges and capabilities of MANPADS and mortars alone would make them obvious choices for attack of an airfield or aircraft. The current imprecise nature of current mortar systems would remove them from selection. If taking down an aircraft in flight is the goal then capability wise there is no better choice for a weapon than the MANPADS.

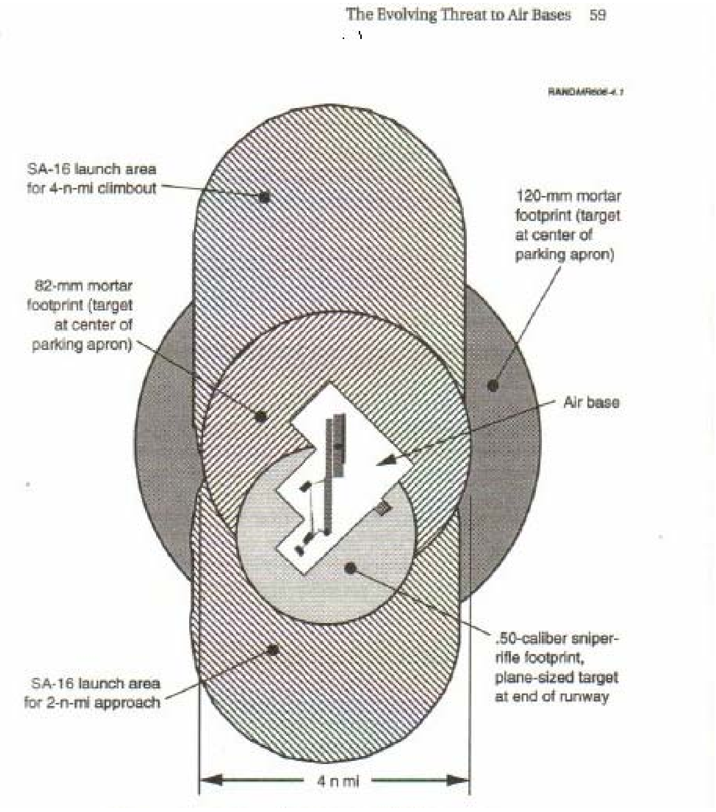

The Evolving Threat to Air Bases 59
RANDMR606-4.1
SA-16 launch area for 4-n-mi climbout
120-mm mortar footprint (target at center of parking apron)
82-mm mortar footprint (target at center of parking apron)
Air base
.50-caliber sniper-rifle footprint, plane-sized target at end of runway
SA-16 launch area for 2-n-mi approach
4 n mi

Figure 15: Weapon Engagement Zones[62]

The selection of an RPG as the attack weapon would be very restrictive. With a maximum range of 900 meters and no possibility to guide to the selected target, the RPG would not provide the capability required to execute a covert attack. The principle of surprise or secrecy alone would prevent the use of an RPG with its visible smoke trail.   As already discussed the airport is filled with targets that would be suited for attack. MANPADS are extremely capable weapons against flying aircraft but have no capability against other targets.

With the possible selection of a 50 caliber anti-armor sniper rifle and armor-piercing incendiary ammunition the whole thought process of what to attack begins to change. Shooting an aircraft in flight with a rifle can be a challenging endeavor especially if you are a self taught sniping team. The covert team may transition from attempting to take down an aircraft in flight to attacking all the available targets within range of their firing position. Once analysis is done on the possible outcomes and the desired effect, taking out many targets in an airport complex in an urban environment may receive much more media coverage.

3.5.2 Availability

The availability of MANPADS on the black market makes them a good choice in foreign areas where restrictions to travel and minimal general population reporting of suspicious activities occurs. However, in the U.S. these weapons are very hard to smuggle into the country and distribute to multiple teams without an extensive network of operatives. The possibility of being caught while committing so many illegal activities is very high. RPGs are more readily available on the black market and also cheaper than MANPADS but their transportation and distribution would be equally as risky as MANPADS.

The covert teams may weigh the illegal acquisition methods with the legal methods and possibility of being tracked or identified by the procedures in place. The overall attack coordinator may risk one team in an effort to steal several 50 caliber weapons at one time. This would remove the risk to all the other teams in that they would have no connection or paper trail to their weapon. The same or similar procedure may be done with the API ammunition, but there is currently no tracking or special procedures to purchase this ammo other than proving you are 18 years old. Availability wise there is no comparison to the possibilities and ease of acquiring 50 caliber rifles.

3.5.3 Training

Training may actually be the determining factor in weapon selection. Both MANPADS and RPGs would be extremely hard if not impossible to train with before an attack. That means the first live firing of the weapon could be during the actual attack. The stress associated with an attack and the fear of failure would all need to be evaluated also. It is very hard to believe a covert team would go through months of recruiting, training, and planning to leave the chance for success contingent upon a single live shot of a weapon system.

Rifle training is absolutely simple and all very similar. If you are a proficient shot with a high power rifle in 30 caliber then transitioning to 50 caliber on attack day is not that difficult. By many accounts the 50 caliber is simpler to use. For the first several thousand feet the 50 caliber is virtually a point and shoot weapon since its trajectory is extremely flat.

3.6 Weapon selection

Based on the capability, availability, and training of the selected weapons for attack of an aircraft and its associated vital surroundings the 50 caliber sniper rifle is by far the most logical choice. There is no other weapon that will allow the covert team to remain within the bounds of the Principles of War, and yet still possess an incredibly powerful destructive capability. There exists an extreme threat within this country in that a hostile adversary could legally acquire such weapons and covertly plan an offensive without breaking any laws or leaving any clues. Our solution recommendation must in some way neutralize this threat and prevent an extended terror campaign that may include attacks on the airline industry within the United States.

3.7 Attack final planning

Once the 50 caliber rifle is highlighted as the most likely weapon choice for the covert cell, the remaining portions of the attack must be analyzed before solution investigation. The answers to where and what may be attacked will provide insight and guidance to a viable solution.

3.7.1 Where?

There are several aspects to the answer of where an attack may come from. The first is the answer of what airports and surrounding communities the covert teams might be placed for initial attack planning and reconnaissance. The second is the answer of where they may attack from, meaning the actual firing position from which targets will be engaged. The third is where inside the airport are the targets they wish to engage, the what to shoot at?

3.7.1.1 Airport and community selection

The answer of what individual airports may be attack is a very complex issue. The covert cell must adhere to the principles of war and attempt to attack an airfield and then disappear without a trace. There are several schools of thought when it comes to airport and community defenses. From a traditional sniping point of view a wide open space in a rural area might be the best option for clear lanes of fire, and less chance of being observed. For this type attack the covert cell would use more traditional sniping tactics of a slow unobserved approach and departure from the firing location. This would be more suited if the covert team were to attempt to take down an aircraft in flight and there were no risk of a police force surrounding the position. The problem with the airports that are located in rural areas is that they are very expansive. The vital targets within them are spread out and not easily engaged from a single firing location. As already stated, many more targets are available and more media attention would be realized if the covert teams were to destroy multiple targets. For this reason and many others, airports that are tucked closely to urban environment require better defensive postures with ramps, taxiways, fuel storage, and control towers all closely spaced. Viewing the airport diagram and imagery of each airfield is required for proper defensive planning. Major highways and access to firing positions should be initially evaluated with overhead imagery, Appendix A, and topographic maps. Once the list of all city/airport combinations was reduced a further refinement of the defensive possibilities would take place considering many other factors. The range at which the shooting will take place is directly related to the airport and urban environment physical layout. There are innumerous other factors in determining what actual cities to attack but additional factors are beyond the scope of this investigation and will not be considered.

3.7.1.2 Where to shoot from?

Once the actual city that a covert sniper team may be assigned was determined a reference to Army FM 4-1 would provide a plethora of defensive guidance. The following is a loose translation and reference to FM 4-1, with author injects and interpretations where needed.

Figure 24 in appendix A depicts a satellite overhead image of Los Angeles International airport (LAX) with a map overlay for easy orientation and initial observation point selection. This simple google.com image allows the covert cell to visualize the runways and vital area orientation with respect to highways and major routes in and out of the area. Additionally, the scale at the bottom of the map allows security teams to limit the search for possible firing positions, based on their knowledge of the capability required to hit different size targets at various ranges. A proficient 50 caliber sniper could hit aircraft and vital buildings at LAX from anywhere within Figure 24!

The covert sniper team must ensure the firing position provides an optimum balance between the following considerations: maximum fields of fire, concealment from enemy observation, covered routes into and out of the position, located no closer than 300 meters from the target area, and a natural or man-made obstacle between the position and the target area. A sniper team must remember that a position that appears to be in an ideal location may also appear that way to the enemy. Therefore, the security forces should look for locations that are not on a point or crest of prominent terrain features, close to isolated objects, and at bends or ends of roads, trails, or streams. The security force must use its imagination and ingenuity in attempting to identify good locations for sniping.

Positions in urban terrain are quite different than positions in the field. The enemy normally has several places to choose. These can range from inside attics to street level positions in basements. When an enemy constructs an urban position common sense and imagination are their only limitation. Urban hide positions that can be used are the room hide, crawl space hide, and rafter hide. The enemy team may construct and occupy one of these positions or a variation thereof.

In a room hide position, the sniper team uses an existing room and fires through a window or hole in the wall, Figure 16. Weapon support may be achieved through the use of existing furniture.

When selecting a position, enemy teams may notice both front and back window positions. To avoid silhouetting, they may need to use a backdrop such as a dark colored blanket, canvas, carpet, or a screen. Screens, common screening material, are important since they allow the sniper teams' maximum observation and deny observation by the enemy.

Sniper teams use the technique best suited for the urban hide position. The second floor of a building is usually the best location for the position. It presents

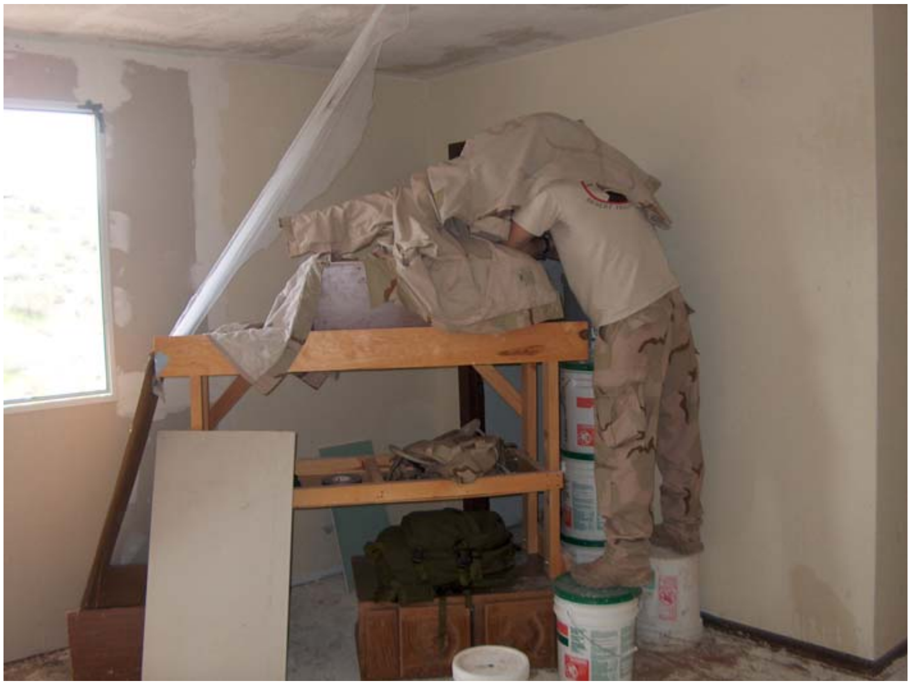


Figure 16: Room hide position[63]

minimal dead space but provides the team more protection since ground level traffic cannot easily spot it. Normally, a window is the best viewing aperture. Lace or net-type curtains can be seen through from the inside, but they are difficult to see through from the outside. Firing a round through a curtain has little effect on accuracy however; one should ensure the muzzle is far enough away to avoid muzzle blast. The enemy may set up well away from the window while ensuring effective coverage of the assigned target area. Firing through glass may be avoided since more than one shot may be required.

The enemy may have multiple firing positions; flexibility may be the key factor in a successful defensive plan.

3.7.2 What to shoot at?

An airbase is a classic target rich environment. “A book on 50 caliber sniper rifles published by a former U.S. Army Officer, “The Ultimate Sniper”, describes in detail how a sniper mission would be carried out against parked military aircraft. The description includes drawings and diagrams. The book has received wide praise from within the sniper enthusiast community.”[64] Besides the aircraft themselves, air bases offer storage facilities, control tower, operations center, navigation aids, handling crews, maintenance facilities, and ground equipment. With so many targets available and the difficulty engaging a flying aircraft, thought must be given to the fact that the terrorist might not target an aircraft in flight at all. The same effect and even more may be achieved if the covert cell attacks the entire vital infrastructure within an airport complex.

From earlier Barrett testimony it is not beyond the realm of the possible for a sniper team to take ten well placed shots in a span of one minute and ten more shots in rapid succession. The total attack could be complete in less than two minutes.

The enemy sniper team may consider what effect the elimination of the target will have on the enemy's center of gravity. Attacking aircraft will most likely result in the largest casualty possibilities. Attacking fuel storage tanks may have the largest media effect. Attacking the control towers may actually have the longest lasting effect in the time it would take to rebuild and repair that facility.

Chapter 4: Solutions

The solutions search will begin where attack analysis left off. An attack on the airline industry with 50 caliber rifles is a very real possibility based on the 50 caliber's capabilities, availability, and training possibilities. There are several technologies and evolving systems available that provide a basis for solution recommendations for a rapidly deployable and flexible solution.

4.1 Technology Overview

4.1.1 Gunshot Detection

There are several different approaches to detecting weapons fire. All of them relate in some way to the distinct events which take place when a gun is fired. When firing a projectile a gun explodes a propellant, and the explosion propels the projectile through the barrel towards the target. In the process, a loud explosion (called the *muzzle blast)* radiates out from the weapon in all directions. The light from the explosion (called the *muzzle flash)* can also be seen. Depending on the weapon type, the projectile may or may not be audible as it travels. If the projectile travels faster than the speed of sound, a sonic boom will propagate out behind the projectile. Finally, when the projectile reaches the target its impact will have its own noise, the *impact noise*.

Some systems focus on detecting the sonic boom of a bullet as it passes by. Such systems are generally referred to as "counter sniper" systems. In order to hear the sonic boom, the system must be downrange of the weapon and within a fairly

narrow cone swept out by the sound waves. Sonic boom counter sniper systems must basically be shot at or have the bullet pass close by in order to be effective.
Other systems detect either the muzzle flash or the heat from the explosion of the propellant with Midband IR detectors. Such systems require line of sight between the weapon and the detector and cannot be used to detect gunfire which can be heard but not seen.

Other systems use an acoustic detection of muzzle blast and, depending on the circumstances, the sound of the projectile while it travels. Unlike optical (muzzle flash) detection techniques, acoustic techniques do not require the shooter to be located in the field of view of a sensor. An acoustic system can cover a much larger area than an optical system and is thus most appropriate for covering large areas.
But, unlike counter sniper systems, acoustic systems can detect gunfire which is not fired towards its sensors, because they use muzzle blasts (which radiate in all directions).

Any system which uses acoustic impulses (muzzle blasts, sonic booms, or a combination of the two) must necessarily be capable of differentiating real events from false alarms. Many things sound like the muzzle blast of a weapon, including car backfires, people hammering nails and even basketballs bouncing. For these reasons most acoustic sensors need to be linked not only to other acoustic sensors for a triangulation, but also to a processing system which runs algorithms to reduce false alarms.

Finally, there are emerging technologies that can detect optical lenses which could identify an aiming or reconnaissance system. These solutions will be presented in a general discussion format and no system names or technical capabilities numbers will be mentioned.

4.2 Acoustic Sensors

As previously discussed there are two basic types of acoustic gun shot detectors. The first type of system is focused on detecting the sonic boom of a bullet as it passes by. Such systems are generally referred to as “counter sniper” systems, and they have one key shortcoming: in order to hear the sonic boom, they must be downrange of the weapon and within a fairly narrow cone swept out by the sound waves. Thus, sonic boom counter sniper systems must be shot at in order to be effective. This enormous limitation restricts the usefulness of this type of system in large area coverage situations. For this reason counter sniper systems will not be considered as a viable option for airport area security reasons, although their merit in the security force protection realm cannot be overlooked.

4.2.1 Shot Spotter

The second type of system is based on the propagation of sound in all directions from a gunshot. The following description of ShotSpotter’s capabilities, an acoustic gun shot detection system, and uses is from ShotSpotter’s website. It should be noted that for privacy, security and safety reasons, ShotSpotter does not make photographs of its sensor enclosures or roof-mounting equipment. Additionally, the ranges, alert times, gun type classification and exact position reporting capabilities of ShotSpotter are all classified and the numbers reported in its advertising material are declassified for military and police force security reasons.

4.2.2 Shot Spotter Overview

The ShotSpotter Gunshot Location System uses the principle of acoustic triangulation to locate gunfire across wide areas. Sensors are placed throughout an area of interest and linked together. Each sensor includes a sophisticated, self-surveying GPS engine, which the sensor also uses as a highly-accurate time source during triangulation. Each sensor has a plotted position or a current GPS position if wireless and mobile. As a significant sound event takes place, the individual sensors record the audio signature of the event and the GPS time of arrival at that location. This recording is linked real time back to a central processing unit that takes the time of arrival from different locations, matches the audio events and then triangulates an extremely accurate position and time stamp of the audio event.

Car backfires, bottle rockets, fire crackers, and even nail guns can confuse “ear” witnesses into thinking they heard gunfire. Every day, thousands of such false alarms are reported to police and first-responders nationwide. ShotSpotter uses sophisticated Acoustic Incident Classification (AIC) technology to separate the wheat from the chaff. Using a complex network of algorithms, data acquired over nearly a decade of deployments, and real-time processing, the ShotSpotter AIC separates incidents into gunfire and other categories, and then reports all of them.

Coverage areas can vary in size from roughly half a square mile all the way up to tens of square miles or hundreds of linear miles, with event notification and dispatch functionality provided either to single or multiple stations.

4.2.3 Deployment Options

The system consists of multiple redundant “layers” of protection. Each layer is equally capable of being deployed independently or in concert with other layers. The rapidly changing and dynamic nature of modern military combat motivated ShotSpotter’s decision to develop redundant protection layers which can interact with eachother.

4.2.3.1 Layer 1: Soldier-worn

Available now, this highly-sophisticated soldier-worn gunshot location system allows troops on the move to detect and locate gunshots and sniper-fire. Sensor devices weigh less than half a pound and are about the size of a PDA. The system immediately tells the small unit leader where a shot or multiple shots were fired from, and can deliver that information to others in the field.

4.2.3.2 Layer 2: Vehicle-mounted

A second layer of protection is provided by ShotSpotter designed specifically for vehicle protection, or security force situational awareness whether on the move or stationary. The system works seamlessly with both soldier-worn and fixed sensors. These sensors can be integrated with cameras mounted on the vehicles and aimed in the direction of enemy fire.

4.2.3.3 Layer 3: Wireless fixed installations

A third layer, for deployment around temporary or fixed locations consists of a rapid deployment wireless version of the ShotSpotter gunshot location system. Sensors can be quickly and easily installed on walls, posts and rooftops to form a complete grid that detects and locates gunfire and instantly relays that information to a visual display. The ShotSpotter technology is proven in difficult urban environments, and can be taken down and re-deployed as needed.

4.2.3.4 Layer 3 Option: Hard wired fixed installations

For long term deployment in fixed areas, nothing beats the cost and durability of wired sensors. With sensors deployed and still operational for over nine years in some locations, Shotspotter sensors are proven effective and sturdy. These sensors are FCC-certified to draw power from the telephone line to which they are connected. Wired sensors are self diagnosing when hooked up to the ShotSpotter base station server, and sensor status is automatically reported to system operators. They require a single telephone line and no special provisioning from the telephone company.

4.2.4 Advantages

ShotSpotter gunshot location sensors connect together either over wireless radio or wired telephone lines. It is easy to mix and match wired and wireless sensors and any ShotSpotter sensor will be compatible with future systems and developments.

In an urban environment, echoes can confuse the listener and mislead investigators. Echoes can be caused by virtually anything and they are capable of fooling locating systems. The ShotSpotter patented spatial filter technology, along with the array of redundant acoustic sensors, has an extremely low false alarm rate.

ShotSpotter sensors detect gunfire at a range of one to two miles away from the sensors. The systems have been shown to be accurate to less than 10 meters over one to two mile ranges. Accuracies within events are far greater, demonstrating an unprecedented intelligence and forensic capability.

ShotSpotter has flexible deployment options already discussed. The sensors are designed with a modular approach to radio frequency (RF) subsystems, and virtually any digital-capable RF technology has been used to connect sensors back to the base station, including 802.11a/b/g, 900MHz, 5.8GHz, and 800MHz. ShotSpotter systems generally use eight to fifteen sensors per square mile. Sensor density is critical for the speed and ease of installation as well as cost.

ShotSpotter holds patents on GPS-integrated gunshot detection sensors. This key advance allows ShotSpotter users to “install and forget” sensors, with no difficult surveyor’s tools, external GPS devices, or data entry required. Additionally, the clocks in GPS-enabled devices are accurate to 20 nanoseconds or less.

Figure 17, was taken from a drive-by shooting in Charleston, South Carolina. Using ShotSpotter’s forensic tool suite, investigators established both the precise location of the event and the shot-by-shot sequence of events. Individual shots were plotted and used by investigators to establish key facts. Two gunmen were in the car: the passenger fired first and the car kept moving at 9 mph throughout the incident. A total of eleven shots were fired. Police reports from citizens on the scene varied wildly, especially because the second gunman’s firing sounded like, but was in fact not, an echo of the first gunman.

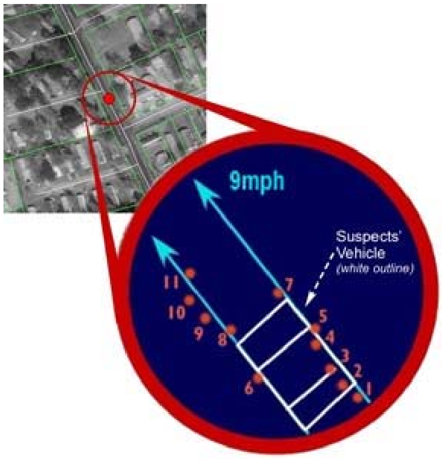


Figure 17: Forensic evidence from a drive-by shooting.
11 shots fired by two gunmen in vehicle moving NNW @ 9mph

4.2.5 Disadvantages

The numbers of sensors required to adequately cover an urban area around an air complex could be extremely difficult to manage. If we use a nominal maximum range of 2 nm for the weapon, a 50 caliber rifle, then we can make a rough sensor footprint. Using LAX as example approximately 2 x 4 nm in size we can estimate the number of sensors required. Extending out 2nm in all directions from the fence line we then would have a 6 nm by 8nm square, approximately 48 square miles. Subtracting out the 8 sq nm of the airfield itself, we must then provide coverage for 40 square miles. Using the minimum advertised density of 10 sensors per square mile we would have to place 400 sensors for adequate coverage. This is a large number to manage no matter how you break it down.

Another shortcoming of acoustic sensors in an urban environment is the result of multi-path or echoes. To adequately reduce multi-path effects you need higher sensor densities, and more processing power. This will increase the minimum densities required. Each environment would need to be evaluated and tested to ensure correct placement and reduction of blind spots. The final disadvantage would be the reduction in effectiveness when shielding of the acoustic signature was used. Shooting from within a house or from an enclosed car similar to the DC sniper vehicle, Figure 18, would pose a significant problem for acoustic sensors.

4.3 Midband IR Sensors

4.3.1 Overview

Medium wave infrared detectors are based on detecting light in the 8 to 12 micrometer range. This detection is a heat and light detection of the area being viewed. Figure 19 illustrates how medium wave detectors are ideally suited for gun flash and plume detection in daylight and night conditions.

4.3.2 Passive infrared detection of ordinance

The Tactical Electronic Warfare Division of the Naval Research Laboratory has been working with passive Infrared (IR) detection of small arms and ordnance since 1993.

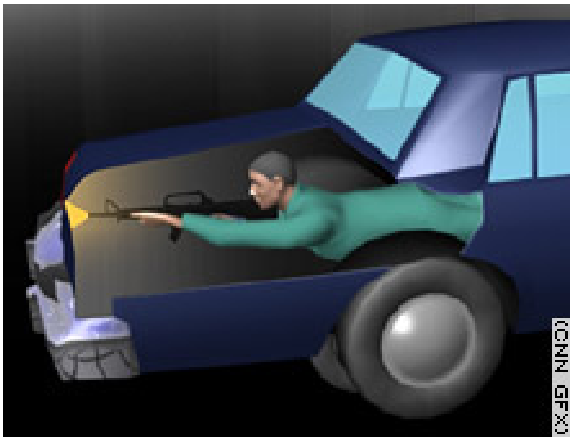


Figure 18: DC Sniper vehicle[65]

.

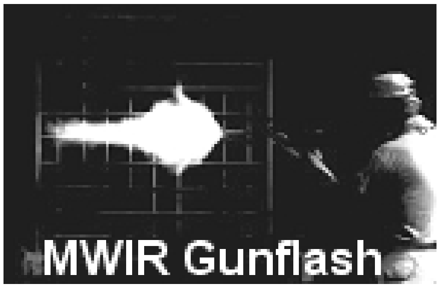


Figure 19: Medium Wave signature of small arms Gunflash

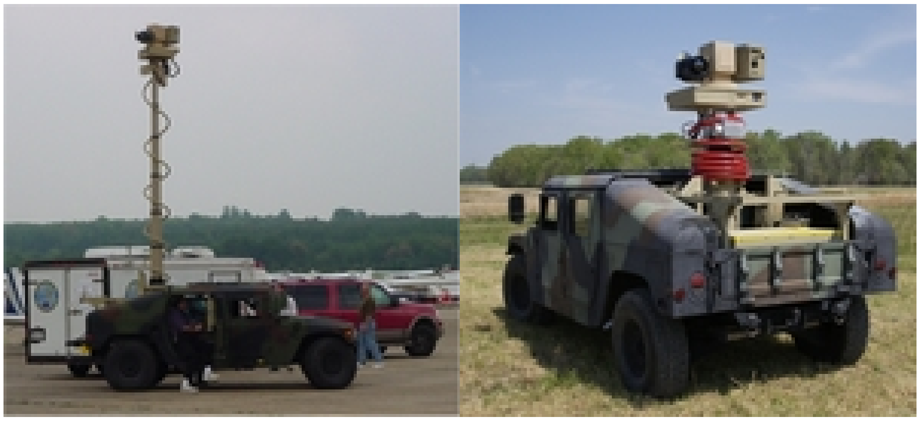


Figure 20: Viper system mounted on a HUMMWV with telescopic arm

The two main systems that have resulted are the Vectored Infrared Personnel Engagement and Return fire (VIPER) small arms detection and the Battlefield Ordnance Engagement-Network Centric Employment (BOUNCE) systems. The VIPER has many modes of operation. These include: static operations for protection of high value targets (embassies, etc.), mobile operations on vehicles (HUMMWV and LAV), Figure 20, networked mobile operations (dismounted troops near HUMMWV), and man-portable operation.

The VIPER has been integrated with gimbals and high resolution visual cameras for law enforcement purposes. It has been tested extensively against over

10,000 rounds from various small arms and works beyond the maximum effective ranges of the weapons.

VIPER provides both gun shot detection, within 70 ms, and geolocation of the firing event. A passive acoustic component (microphone) or a laser range finder can be incorporated to determine range to the gunfire.

The VIPER equipment consists of a mid-wave IR camera, with real-time signal processing, magnetic compass, and user display and alarm. The current field of view (FOV) of the Viper's IR sensor is 120 degrees. This would require three separate sensors for 360 degrees of coverage at a point location, like the roof of a control tower. If the sensors were place along a straight fence line, individual units at varying distances along the fence would be adequate. Based on the possible firing positions and the required coverage area the number of sensors could be kept to a minimum. When sensors are placed at the end of a runway typically two covering 240 degrees is sufficient.

Figure 21 is a picture of 120 degree width to illustrate the FOV of the VIPER if pointed down this airport perimeter road for surveillance. All of the capabilities other than basic pictures, videos and functional components of these systems are classified.

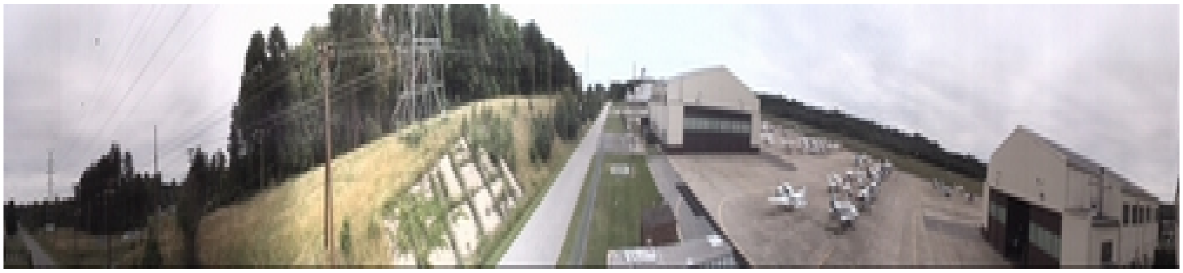


Figure 21: Field of view of current Viper system

The VIPER system can detect all small arms fire, including 50 caliber rifles out past the maximum effective ranges of the weapons. The VIPER will also detect any other plumes in its field of view like MANPADS and RPGs. The test data for these detections is also classified.

From video of a VIPER system at work at a Marine Corps firing range the system demonstrates its capabilities to handle rapid fire from multiple automatic weapons. The 70 ms detection speed is hard to visualize until you see the system at work. The VIPER detects gun fire, slews, auto zooms, focuses the camera onto the shooter and snaps several photos all before the rapport or acoustic muzzle blast reaches the detection unit. This capability to locate and ID a covert cell within a second of the first shot would be ideal in an airport protection scenario.

Figure 22 is a pictorial depiction of the capabilities of the VIPER system.

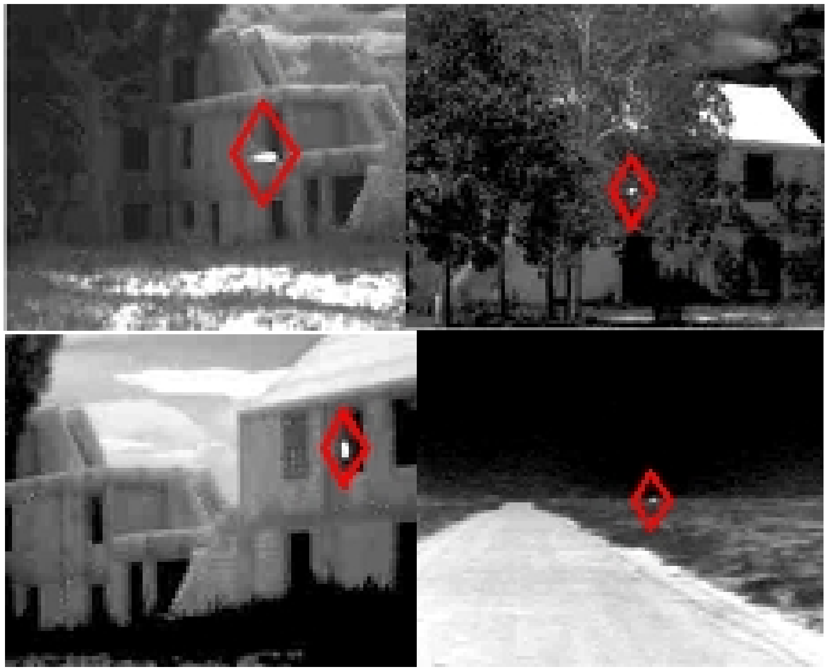


Figure 22: Gunflash detection from a window, through foliage, of reflection off inner wall, and at extended ranges

The top left is a rifle fired at the edge of a window. The top right is a rifle fired from behind several medium sized trees. The bottom left is a sniper using proper techniques of being back inside the room while firing, yet VIPER still picks up the reflected medium wave energy off the wall. The bottom right is detection at extreme ranges. These detections would be aided in geolocation by integrated laser range finders and high power zoom cameras for exact shooter positioning.

The BOUNCE system has been developed for use in tactical unmanned aerial vehicles which will be able to fly underneath clouds in order to locate and classify enemy ordnance. It consists of an IR camera, GPS, attitude sensors, image processing, gimbaled visible zoom camera with laser rangefinder, and ground and user stations. The UAV option is not relevant to the continuous airport security solution.

Advanced work in the passive IR gun and ordnance detection technology area is being pursued currently. The advanced development includes refinement of motion algorithms in order to operate in high clutter urban scenarios and development of lighter weight systems for dismounted war fighters.

4.3.3 Advantages

Midband IR sensors like VIPER provide wide area coverage with a minimal number of sensor units when the FOV is not blocked. Ideally suited for an airport like Logan International, Figure 26 in Appendix A, where a 50 caliber sniper shooter could position themselves in the town of Winthrop across the bay and yet still possibly take down an aircraft. Sensor placement inside the current perimeter of the airport complex makes installation and maintenance much simpler. Staring systems are ideally suited to be placed on the roof of the control tower for the best elevation advantage. Rapid and precise location of the firing event to include the floor fired from and even the exact window to narrow the security response is a distinct advantage. In an urban environment elevation indication may be a determining factor toward apprehension of a covert cell.

4.3.4 Disadvantages

Poor coverage in extremely tight situations like San Diego International Airport, Figure 25 in Appendix A, where the buildings are so close to the fence line that the sensors are blocked from seeing many lanes of fire. Additional sensors would be required to cover all the obscure firing lanes that are available in such a close building lay down.

4.4 Surveillance

If the U.S. desires to prevent an attack on the aviation industry preemptively, then the first two classes of solutions already discussed are wholly insufficient. A weapon must be fired and an attack already in place for acoustic and plume systems to provide intelligence on the perpetrators. There are many possible levels of intervention involved in preventing an attack. The final level "in countering the threat is to detect and defeat adversary forces in the standoff footprint outside of the airbase before those forces launch their attack. To do so requires surveillance of the entire footprint area of the suspected threat weapons. Depending on terrain and foliage a security force of the brigade size, approximately 3000 people, would be required to cover a several hundred square mile area."[66] Hiring massive security forces to protect airports from outside the perimeter fence is not a viable option. Some type of observation tool which must be automated in its search, classification, and notification of findings is required.

4.4.1 Video systems

Video monitoring systems are widely used in the security industry. Specifically, video systems are used to record certain vital areas and to identify the presence of objects or people. Video systems usually require an operator to slew the camera and classify threats off of a remote monitor. A single operator can observe multiple simultaneous displays in a benign environment. At Houston's International Airport a video system that uses regular video integrated with heat signatures is being installed due to the expansive nature of the airport with over 35 miles of perimeter. This system identifies heat sources in areas where nothing else of significance resides. When an object of significance appears somewhere it should not be, the mobile security force will be detached to investigate. In an urban environment where there are hundreds of independent objects moving about randomly a video observer would have difficulty picking out suspicious activity from the clutter of the normal surroundings. A thermal imaging system would be unable to classify individual personnel movements in such a complex heat signature environment. The largest disadvantage to video systems is that, while they are very inexpensive, they are not independently capable of scene recognition or intent determination.

4.4.2 Glint

The following discussion is a broad analysis of the limited unclassified information on several systems. Any and every sensor, your eye for example, gives off a signature in the frequency range it was designed to detect at. This can be used to the advantage of a security forces since you are able to see all sources of intelligence gathering taking place on your position. The defense of an airport would be very difficult. The system must detect the optical imaging sources present in its field of view and then catalog those reflections that currently exist. As the system scans, it compares the current image with its cataloged image and reports any difference in the glint signatures for investigation. When changes are present it may be someone using a scope, binoculars, or high power camera in an intelligence gathering mode. As discussed earlier a covert cell will do extensive planning before attack execution. Binoculars and high power zoom cameras may be used to locate firing positions and targets. This critical observation period would be the ideal time to gather counter intelligence data on a covert cell. An observation position, picture of a face, or ID of a vehicle that is watching an airfield could be the vital piece of intelligence needed to thwart a terrorist plot. Identifying the personnel that are watching airports in one way or another may be like looking for a needle in a haystack, but is it not worth preventing a large scale terrorist attack on a vulnerable industry?

4.4.3 Surveillance advantages

The most obvious advantage to additional surveillance aimed outside the bounds of the airport perimeter is the opportunity to prevent an attack before it takes place. Constant observable presence in and around an airport may make that airport a high risk attack for a covert cell, effectively preventing the planning of an attack. Video and heat signature monitoring of expansive open areas will significantly reduce the security force requirement to patrol expansive areas. Nevertheless, there must still be enough security in place to deal with a threat should it emerge. A significant advantage of optical augmentation techniques is a form of intent recognition. The identification of high optical zoom lenses allows early recognition of intelligence gathering and possible strike planning or imminent attack execution.

4.4.4 Surveillance disadvantages

Based on the maturity of the algorithms used with heat and glint signature recognition, the false alarm rate may be excessive or the detection rates may be low. This will either reduce the confidence in reporting or the effectiveness of the system. Video and heat based staring systems have a difficulty in urban environments in dealing with the associated clutter and shear volume of objects to classify. Glint systems have trouble identifying optics that are not pointed directly at them. Glint systems also have difficulty with moving systems, since the glint from a moving car for example will be a blur across the image. A highway would just be a group of blurs similar to a night photo of a highway with an open aperture.

4.5 Solution summary

The two major levels of security discussed are pre and post attack systems. The pre attack systems are best for wide area surveillance but are limited in urban clutter. In an urban setting these video and glint systems would be limited in their usefulness with the current state of algorithms and sensor densities required. The post attack systems are then broken down into acoustic and midband IR systems.

An acoustic system can cover a much larger area than an optical system at the cost of many times the sensors. Acoustic sensors do not require line of sight between the weapon and the detector and can be used to detect gunfire which can be heard but not seen. Acoustic sensors are much better in a tight urban setting around the airport. Acoustic sensors will have difficulty with shielded or muffled shots from inside buildings or vehicles.

Midband IR systems can detect many types of weapons and not just gun shots, including MANPADS and RPGs. Midband IR systems can be placed inside the perimeter of the airfield reducing installation and maintenance concerns. Midband IR sensors can see shots through foliage and from reflections off of buildings.

Both post attack systems will require significant processing power and the ability to slew high power cameras to the suspect location if within the FOV. Both systems will need to be automated for attack recognition, attack location reporting, and image capture.

Conclusion

When a covert operative group, that desires to attack or engage the United States in war on its home land, adheres to the *Principles of War* the aviation industry may become a target. The airline industry of the United States is a fragile multi billion dollar enterprise that must be protected with the limited resources available. Analyzing all avenues of attack on the aviation industry highlights the capabilities and availability of the 50 caliber sniper rifle as the most viable threat. Possible solution analysis of currently available acoustic, mid wave infrared and optical augmentation systems reveals the advantages of each of these approaches. The conclusion is that an open system architecture should be used to tailor the sensor suite around each airport. Based on the advantages of each system type, sensors should be selected with respect to the vital area locations and the urban layout. An integration of the best sensors for each environment will lead to a multi-layer and multi-system defensive posture around each airport. The synergy derived from the advantages of each system will significantly reduce the risk of a drawn out terror campaign which involves the airline industry.

References

[1] "Principles of War for the 21st Century", USJFCOM internal memo, January 2003

[2] NORTHCOM, Northern Command is the single point of command for homeland security and home land defense efforts, December 2005

[3] USJFCOM Definition from the USJFCOM Portal Website at WWW.jfcom.portal.mil, December 2005

[4] ARMY Field Manual 3-0, paragraph 4-35, p. 4-12, December 2005

[5] Griffin, Samuel B. Sun Tzu: the Art of War, Oxford University Press, 2002, page 84

[6] Joint Operations Concepts, JCS version 1.0, 3 Oct 03, p. 10

[7] Marine Corps Doctrine Publication 1, Warfighting. 20 June 1997, p. 40-41

[8] Clausewitz, Carl Von. "On War", New Jersey: Princeton University Press. 1976, p. 119

[9] Leonhard, Robert, "The Art of Maneuver", Novato: Presidio Press, 1991, p. 127

[10] Clausewitz, Carl Von. On War. New Jersey: Princeton University Press. 1976, p. 119

[11] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999

[12] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 11

[13] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 6

[14] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 19

[15] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 19

[16] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 22

[17] Qiao Liang and Wang Xiangsui, "Unrestricted Warfare", Beijing: PLA Literature and Arts Publishing House, Feb 1999, p. 46

[18] "Transformation for what?", December 2005, John P. White, Strategic Studies Institute report, p. 6

[19] Washington Post Article,"Bin Laden Speaks", 20 Jan 2006

[20] David A. Shlapak and Alan Vick , RAND, "Check Six begins on the ground": Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 19

[21] From en.wikipedia.org, Damadola airstrike From Wikipedia, the free encyclopedia, 20 Jan 2006

[22] "Bin Laden threatens attacks, offers truce", 20 Jan 2006, By Lee Keath, Associated Press Writer

[23] David A. Shlapak and Alan Vick , RAND, "Check Six begins on the ground": Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 18

[24] FBI Definition from FBI website, December 2005

[25] USJFCOM Definition from the USJFCOM Portal Website at WWW.jfcom.portal.mil, December 2005

[26] Airforce Effects Based Operations White Paper, 2002

[27] From jameshunall.com, key word Twin Towers Sept. 11, December 2005

[28] From CNN.com, key word DC Snipers, December 2005

[29] "The DC Sniper Nest: None Dare Call it Terrorism", 10 July 2002, Analysis by J.J. Johnson, Associated Press Writer

[30] From CNN.com, "Ballistics match rifle to sniper attacks", 25 October 2002

[31] From CNN.com, "Two split reward in D.C.-area sniper case, $350,000 to one tipster, $150,000 to other", 6 May 2004

[32] "Just Like Bird Hunting", The threat to civil aviation from 50 caliber sniper rifles, Violence Policy Center, 2003, p. 14

[33] David A. Shlapak and Alan Vick , RAND, "Check Six begins on the ground": Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 18

[34] "Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat", Rand Study, 2005, p. 9

[35] James Chow and Paul Dreyer , RAND, "Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat", 2003, p. 15

[36] Taken from www.dakotakid.us, LAX approach jpeg, December 2005

[37] Photo courtesy L-3 Communications, www.howstuffworks.com, December 2005

[38] Photo courtesy L-3 Communications, www.howstuffworks.com, December 2005

[39] Photo courtesy L-3 Communications, www.howstuffworks.com, December 2005

[40] David A. Shlapak and Alan Vick , RAND, "Check Six begins on the ground": Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 35

[41] Steven Zaloga, "Russian Man portable Surface-to-Air Missiles," Jane's Intelligence Review, April 1994, p. 147-153

[42] David A. Shlapak and Alan Vick , RAND, "Check Six begins on the ground": Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 52

[43] D. Kuhn, “Mombassa Attack Highlights Increasing MANPAD Threat”, Jane’s Intelligence Review, Vol. 15, No. 2, 2003, p. 26-31

[44] D. Kuhn, “Mombassa Attack Highlights Increasing MANPAD Threat”, Jane’s Intelligence Review, Vol. 15, No. 2, 2003, p. 26-31

[45] James Chow and Paul Dreyer , RAND, “Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat”, 2003, p. 5

[46] James Chow and Paul Dreyer , RAND, “Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat”, 2003, p. 5

[47] Taken from www.howstuffworks.com, keyword Military/Weapons/RPG, December 2005

[48] Taken from www.howstuffworks.com, keyword Military/Weapons/RPG, December 2005

[49] “Just Like Bird Hunting”, The threat to civil aviation from 50 caliber sniper rifles, Violence Policy Center, 2003, p. 17

[50] “Voting From the Rooftops”, Violence Policy Center Publication, 2001

[51] “Voting From the Rooftops”, Violence Policy Center Publication, 2001

[52] “Just Like Bird Hunting”, The threat to civil aviation from 50 caliber sniper rifles, Violence Policy Center, 2003, p. 17

[53] US Department of the Army, Field Manual 23-65, Browning Machine Gun Caliber .50 HB, M2, June 1991, Chapter 1-7

[54] “Voting From the Rooftops”, Violence Policy Center Publication, 2001

[55] “Winchester/Olin Corporation-Small Calibre Ammunition,” downloaded from “Army Technology” at http://www.army-technology.com/contractors/ammunition/winchester, December 2005

[56] NAMMO Raufoss AS, “12.7 mm Ammunition Family,” downloaded from http://nammo.com/mediumcalibre/12,7mm/127mm.htm, December 2005

[57] U.S. Marine Corps, Department of the Navy , Marine Corps War fighting Publication 3-35.3, Military Operations on Urbanized terrain, Appendix B, “Employment and Effects of Weapons,” 2002, p. B-8

[58] “Voting From the Rooftops”, Violence Policy Center Publication, 2001

[59] “Theft of weapons from army bases continue at high rate,” Cox news service, 20 December 1997

[60] Justice Dept. Details its loss of weapons and computers, The New York Times, 6 August 2002

[61] David A. Shlapak and Alan Vick , RAND, “Check Six begins on the ground”: Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 50

[62] David A. Shlapak and Alan Vick , RAND, “Check Six begins on the ground”: Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 59

[63] Taken from, WWW.sniperschool.org, urban hide position/training, July 2006

[64] “Just Like Bird Hunting”, The threat to civil aviation from 50 caliber sniper rifles, Violence Policy Center, 2003, p. 19

[65] Taken from CNN.com, keyword DC Sniper vehicle, January 2006

[66] David A. Shlapak and Alan Vick , RAND, “Check Six begins on the ground”: Responding to the evolving Ground Threat to U.S. Air Force bases, 1995, p 70

Appendix

Appendix A- Airfield Diagrams & Imagery

The following appendix is the type of information that is readily available online. The airport diagrams and approaches were taken from an FAA web site and the overhead imagery was obtained from Google.com.

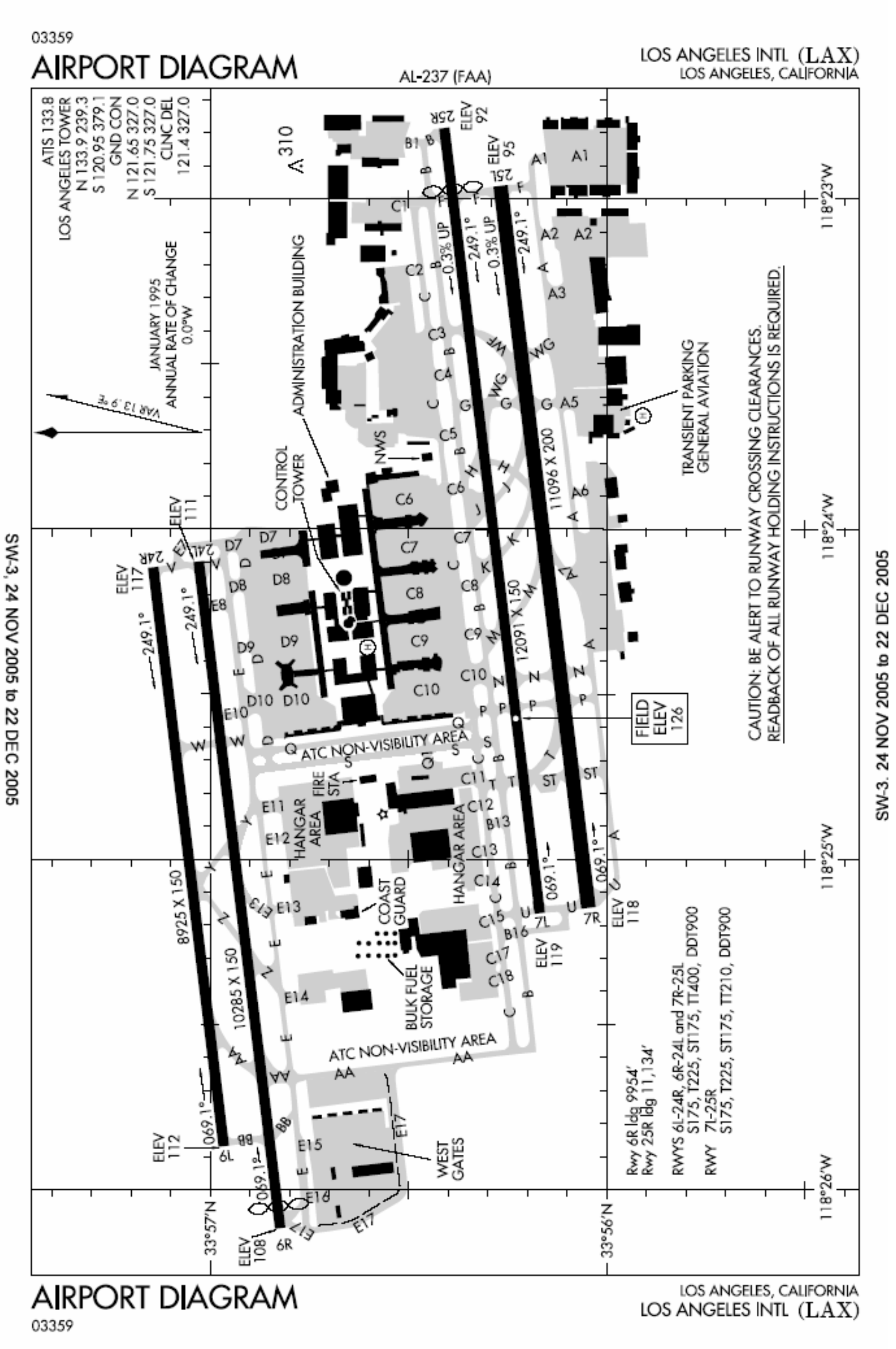


Figure 23: Los Angeles Intl Field Diagram

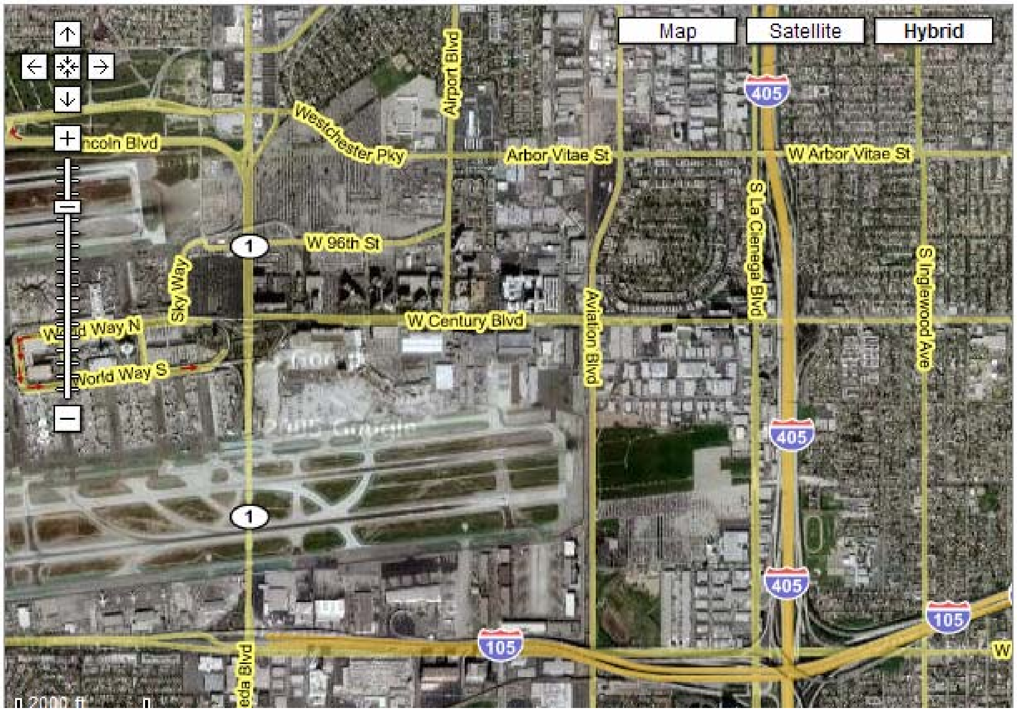


Figure 24: Google overhead imagery of Los Angeles Intl with Map overlay

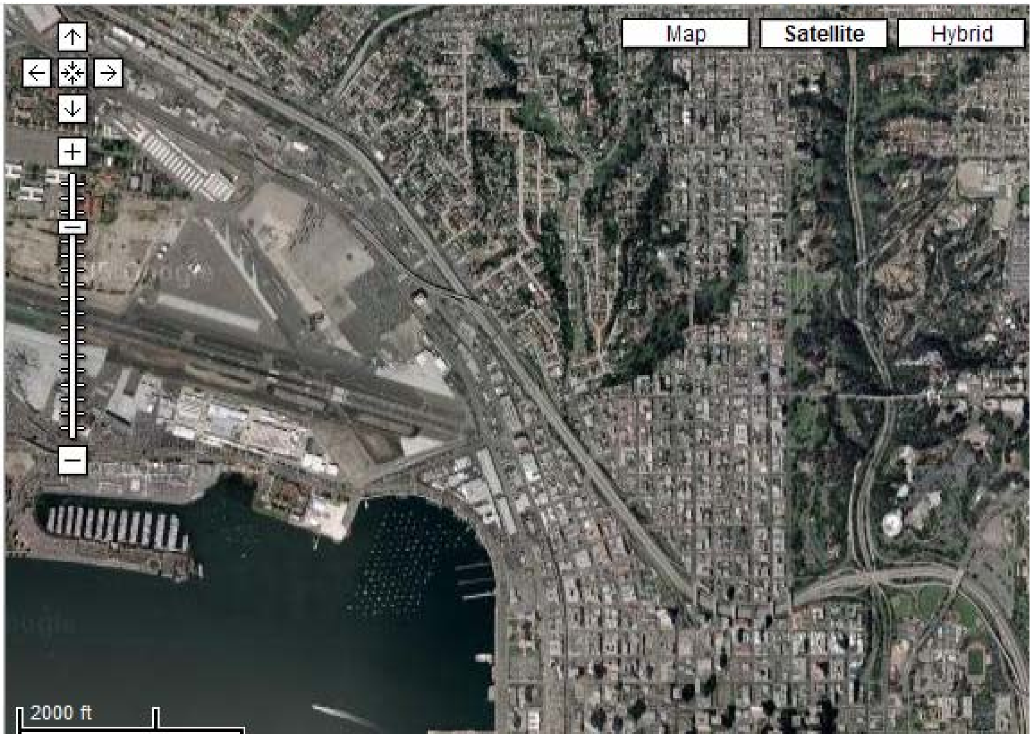


Figure25: Google overhead imagery of San Diego Intl

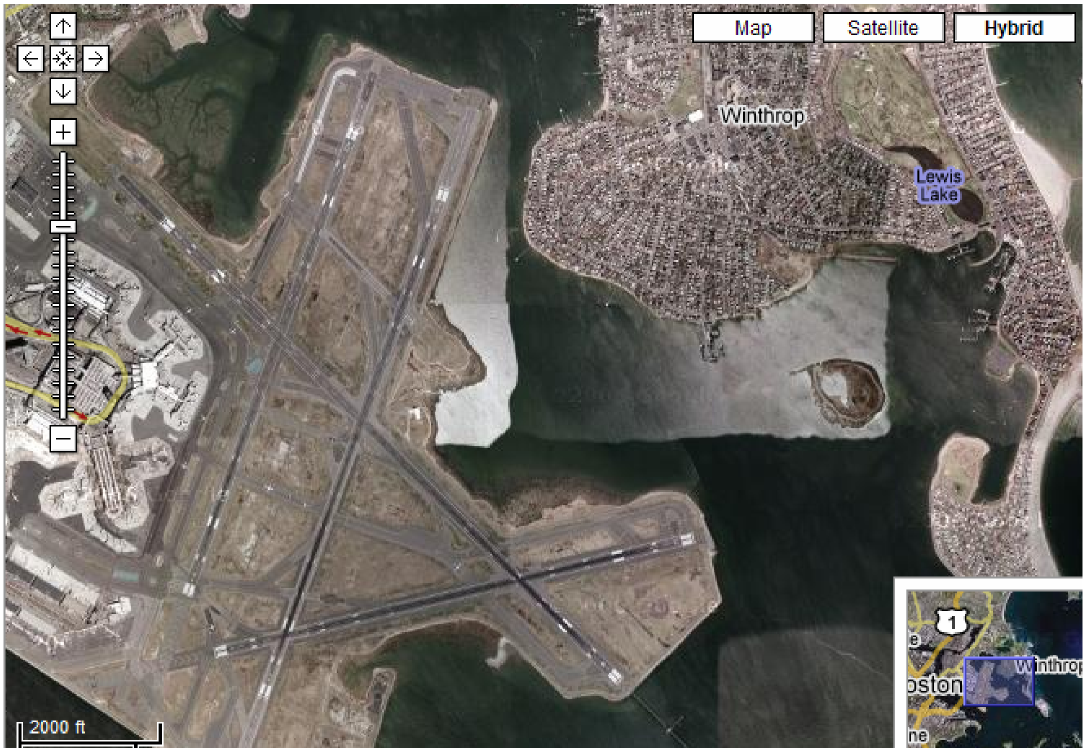


Figure 26: Google Overhead Imagery of Logan Intl with map overlay

Vita

David Thomas Ramsey Jr. was born in Portsmouth, NH on March 21, 1969. He was raised in Newmarket, NH and went to Newmarket public schools graduating from Newmarket Central High School in 1987. From there he attended the Naval Academy Preparatory School in Newport, RI. He graduated from the Naval Academy in 1992 with a B.S. in Aerospace Engineering.

After earning his wings of Gold in 1995 he was assigned to fly FA-18 "Hornets." After replacement pilot training LCDR Ramsey was assigned to the 'Fist of the Fleet', VFA-25, and flew combat operations in support of OPERATION SOUTHERN WATCH. LCDR Ramsey attended the United States Naval Test Pilot School in 2000 and was assigned to VX-31 Weapon Test Squadron China Lake for his test pilot tour. At VX-31 he served as the FA-18 Electronic Warfare and AESA (Active Electronically Scanned Array) project officer, and began his studies at UTSI's China Lake Campus.

In 2003 he was assigned to the 'Wildcats' of VFA-131 as a department head. He served as the Quality Assurance, Administration, Maintenance, and Operations Officer. He flew combat operations in support of OPERATION IRAQI FREEDOM, and participated in Fallujah I.

In 2005 he was assigned to the United States Joint Forces Command, J9 Joint Experimentation, and has served as the Joint Fires Team lead in the prototyping path way.

David began his Master studies at the United States Naval Test Pilot School in 2000 and is pursuing his M.S. from the University of Tennessee with a major in Aviation Systems.