Spring 2013

The portable sensor network: Conceptualization and development of a modular, upgradable, and reusable sensor system for the provision of offensive and defensive surveillance

Brandon Curtis Sanders
James Madison University

The Portable Sensor Network:

Conceptualization and Development of a Modular, Upgradable, and Reusable Sensor System for the Provision of Offensive and Defensive Surveillance

by Brandon C. Sanders

A thesis submitted to the Graduate Faculty of

JAMES MADISON UNIVERSITY

In

Partial Fulfillment of the Requirements

for the degree of

Master of Science

Integrated Science and Technology

May 2013

Table of Contents

List of Tables

List of Figures

Abstract

In the 21st century, law-enforcement, military, border patrol, and private companies all use a wide variety of surveillance equipment that is tailored to their specific needs. This equipment is expensive, typically requires an enormous capital investment, and often fails to live up to expectations; there must be a better way. The primary objective of this thesis is to conceptualize a new and more capable surveillance system, dubbed the Portable Sensor Network (PSN), which can either augment or entirely replace existing systems. The core concept of the PSN demands that it must affordable, portable, modular, and based on existing, commercially available technology. To achieve this goal a four step methodology has been developed: analysis of customer's needs, analysis of the capabilities and features of existing systems, development of the PSN based on that analyses, and finally, analysis of the fully developed PSN's effectiveness via analytical methods borrowed from the field of intelligence analysis. By the end of this thesis, it should be clear to the reader which surveillance system(s) are most effective in a given scenario and how the PSN can augment or replace that system(s).

Introduction

Background

Various electronic sensors have been utilized for decades in surveillance systems designed to provide intrusion detection for everything from national borders to prison walls. Modern surveillance systems are required to provide border intelligence for three classes of geographic regions: geopolitical borders, localities (e.g., cities, ports, small islands, etc.) under strict military or police observation (perhaps even quarantine), and fixed installations (e.g., power plants, military bases, airports, etc.). While these systems have evolved significantly from their original incarnation, they have been proven insufficient to cope with the 21st century threats facing the United States at home and abroad. The failure of the U.S. to secure neither the U.S.-Mexico border nor the Afghanistan-Pakistan border are two of the most egregious and well-known failures to successfully implement an affordable system to monitor geopolitical borders.

One of the biggest problems facing those whose task it is to address the problem of insufficient surveillance is cost. The cost of a surveillance system can be broken down into four categories: development, procurement, operational, and maintenance. In the case of the U.S. – Mexico and Afghanistan – Pakistan borders, the cost of border surveillance has been a topic of great debate. Successful monitoring of the U.S.-Mexico border is an essential step in reducing the flow of illegal narcotics and undocumented immigrants into the U.S; a task which has required enormous capital investments. Unfortunately the border is still insecure despite the fact that the U.S. has invested billions of dollars into new technology, technology that has been augmented by a two fold increase in the number of border patrol agents (since 2004) and deployment of 1,200 National Guard troops along the border.[12] With respect to the surveillance needs of the U.S. –

[1] "Napolitano Cancels Virtual Border Fence Project, Proposes Alternative." Fox News, January 14, 2011.

Mexico border, the problem is both a lack of funding and the allocation of that funding. One such example is the choice made by the DHS to fund the Secure Border Initiative (SBI)[3], a multi-billion dollar program that was cancelled in 2011 because it both ran over budget and failed to live to live up to expectations.

Attempts to properly monitor the Afghanistan – Pakistan border have had failures not unlike those encountered by DHS. Here to the problem is not a lack of funding, it is how that funding has and continues to be appropriated. Given these facts, the question becomes: how should current funding be allocated so that it both maximizes effectiveness and reduces cost? Secretary Janet Napolitano addressed this question in January of 2011. The following statement was made by the Secretary elaborating as to why DHS cancelled the SBI in favor of a less expensive program known as the Alternative SBI[4]:

> "There is no 'one-size-fits-all' solution to meet our border technology needs, and this new strategy is tailored to the unique needs of each border region, providing faster deployment of technology, better coverage, and a more effective balance between cost and capability."[5]

Farley, R. (2011). Obama Says Border Patrol Has Doubled the Number of Agents Since 2004. Politifactcheck.com, May 2011.

[2] According to the U.S. Drug Enforcement Agency, the Southwest Border remains the primary gateway for moving illicit drugs into the United States. This is estimated to be between a $50 and $60 billion business that relies on smuggling in two directions: immigrants and narcotics are smuggled into the U.S. while drug money, weapons, and ammunition are smuggled out.
Molzahn, Rios, and David A. Shirk. *Drug Violence in Mexico: Data and Analysis Through 2011*. University of San Diego, Trans-Border Institute: Joan B. Kroc School of Peace Studies.

[3] *SBInet Program: Program-Specific Recovery Act Plan*. U.S. Department of Homeland Security: Customs and Border Protection, May 15, 2009

[4] Zuckerman, Jessica. "The 2013 Homeland Security Budget: Misplaced Priorities." The Heritage Foundation, March 23, 2012.

[5] "Napolitano Cancels Virtual Border Fence Project, Proposes Alternative." Fox News, January 14, 2011.

Secretary Napolitano's statement reflects DHS's new approach to border security, an approach that is the antithesis of the one embodied by the original SBI. This approach calls for the recalculation of available funds towards programs that provide faster deployment of technology, better coverage, and achieve a more effective balance between cost and capability. To date, this plan has proven a more effective use of resources than was achieved under the prior initiative. Despite this success, there is room for further optimization, optimization that challenges the Secretary's statement that there is no 'one-size-fits-all' solution. There may not be a one-size-fits-all system, but there may very well be a one-size-fits-all solution – a solution that not only addresses the surveillance problems of DHS but those of other organizations as well.

Foundation of the Solution

The solution to the problem posed by over-budget and insufficient surveillance systems is three-fold. First, the solution, or asset(s) implemented, must be budget friendly. Any economist will tell you that, all things being equal, as the production of a given product increases the cost to produce that product decreases. In this case, the product that is being considered is surveillance equipment designed to monitor geopolitical borders. As the production of a single surveillance product increases, its cost decreases. The problem with the SBI is that the technology being produced was in the form of large and very expensive installations that contained the latest technology available such as advanced, long-range radar.[6] Development and research cost remain the same regardless of how many assets are purchased, a cost that is shared in the per unit price of the final asset. As the number of assets produced decreases the development and research cost shared by each of those assets increases, driving up the final price of each (e.g., the

[6] *SBInet Program: Program-Specific Recovery Act Plan*. U.S. Department of Homeland Security: Customs and Border Protection, May 15, 2009

B-2, F-22, and DDG-1000 programs)[7]. No matter how many of these 'products' DHS purchases they will always remain relatively expensive. An alternative to this approach is investing in smaller hardware that can be mass produced, a concept DHS has begun to adopt with the implementation of the alternative SBI. With that in mind, the alternative SBI is based around the acquisition of hundreds of surveillance assets as opposed to only a dozen. Though a step forward, there is room to take this concept even further. In place of adopting assets produced by the hundreds, DHS could invest in the acquisition of less expensive assets numbering in the thousands, thereby reducing the per-unit (and total program) costs that much more. This however is not the only way to reduce costs.

In an effort to further reduce the costs, any new surveillance assets employed should be developed in such a way that they appeal to a wide variety of organizations. As the number of organizations interested in a new asset increase the capital investment required by a single organization to develop that asset decreases. Unfortunately, achieving this is no small task. Doing so requires the development of an asset that is the solution to a problem shared by every organization for which the asset, or solution, is intended to appeal. This is a difficult task given the organizations covered in this thesis: DHS, the owners of critical infrastructure, and the military. Nonetheless a problem has been found, the identification of items of interest (IOI).

The second part of the solution relates to the actual design of the asset(s) itself. DHS's decision to invest, via the implementation of the alternative SBI program, in surveillance assets that use off the shelf technology was a step in the right direction but one that, as was the case with the acquisition of new assets, can be taken even further. It is one thing to use off-the-shelf technology, it is another thing entirely to use 100%, commercially available components, the

[7] "Planned stealth destroyer could underpin U.S. Navy's China strategy." Fox News, June 4, 2012.

type of components marketed to every day citizens. The more these types of components are used, the greater the savings. The potential savings may be so great and the development cost so low that private companies take it upon themselves to develop the asset without first being contacted by customers to do so.[8] Another advantage of using off-the-shelf components is that it reduces the time required to go from concept to production. While it may take additional time to implement these assets, doing so can be reduced if the contractor used to develop and produce them is the same contractor responsible for the production and development of existing assets.

The third and final part of the solution proposed addresses the inability of existing surveillance systems to identify IOIs. The three key components to surveillance are detection, identification, and tracking of IOIs. Nearly all surveillance systems are designed to detect and track IOI's, but very few have the capability to identify them. Even fewer have the capability to distinguish between objects of the same class (e.g., a pleasure craft vs. a smuggler's go fast boat, a narcotics smuggler vs. an illegal immigrant, etc.). If an asset can be developed that addresses this problem it has the potential to replace or augment existing surveillance systems in service with all three organizations. This asset is the Portable Sensor Network (PSN).

In addition to addressing the above deficits, the core concept of the PSN requires it to be portable, modular, upgradable, and reusable. Although these requirements place additional restrictions on the final design of the PSN, those restrictions are nowhere near as restrictive as the final and most difficult requirement: the design of the PSN must be original. Original means just that, a system that, to the best of anyone's knowledge (the knowledge possessed by individuals whose domain is surveillance equipment, not your average bystander), has never

[8] Reference showing when this has happened in the past.

been designed. The PSN cannot simply imitate the design of current systems by either improving the capabilities of those systems or reducing the cost of acquiring them.

Methodology

The PSN is a fully integrated, portable, modular, upgradable, rapidly deployable, and inexpensive sensor system that fulfills the needs expressed in the preceding paragraph. The primary objective of this thesis is to conceptualize a new and more capable surveillance system, dubbed the Portable Sensor Network, which can either augment or entirely replace existing systems. A four step process has been developed to accomplish this objective: analysis into whether or not demand for the PSN exist (or a surveillance system similar to it), development of a working concept off of which a tangible product can be modeled, analysis of the proposed system's performance against existing ones, and to provide proof of concept by actually constructing one of the sensors the PSN would employs. This four step process is the methodology on which this thesis is based. If successful, it should be clear to the reader which surveillance system(s) are most effective in a given scenario and how the PSN can augment or replace that system(s). The first step towards achieving this task is to determine to whether or not and to what extent demand for the PSN exist. Demand, in this case, is the main discourse of the first two chapters.

Summary Introduction to Each Chapter

Each of the chapters in this thesis is part of the four step process described in the previous paragraph. The following is an introduction to these chapters and how each of them contribute to the overall methodology.

Chapter 1: Surveillance Demands in the 21st Century

In Chapter 1, surveillance demands are broken down by the three organizations analyzed in this thesis. Each organization has its own subchapter which itself is broken down into four sections: review, criteria/condition, summary, and mission/scenario table. The majority of the material presented in each subchapter is done so in the review. The review section contains information detailing the background and various missions each organization performs. This information is broken down according to the type of surveillance, offensive or defensive, and the specific missions performed within each surveillance type. Following the review is list of each organization's criteria and condition. Criteria and condition are gathered based on an analysis of the review. Criteria determine what capabilities an organization must possess in order to fulfill its mission. Condition is the actual ability that organization possesses. The criteria examined in this chapter came from several sources, including: legislation, contracts, white papers, and criteria based on a stated objective (e.g., a public affairs statement regarding the goals of an organization). As part of this examination a gap analyses is performed. This analysis assesses the gap, if any, that exist between an organization's surveillance capabilities and their designated criteria. Both this gap and the criteria from which it is derived are crucial details to consider when determining whether or not the PSN is a viable solution for the needs of a given organization. Immediately following the criteria and condition list is a summary. This primary purpose of this summary is to create an abridged list of an organization's criteria that includes mention of what criteria on that list is not satisfied by that organization's current surveillance system(s). Following the summary is a scenario specific requirements table.

This table takes the information obtained in the review of an organization and translates it into a table that quantifies that organization's surveillance demands. These demands are quantified

according to the different surveillance missions performed by an organization and the conditions under which those missions are performed. At the end of the chapter, the data contained in each organization's table is assembled into a master one. The master table serves as a reference for determining the needs of one organization versus the needs of another. It also highlights the specific surveillance needs according to external variables such as terrain and climate. Ultimately, this information is analyzed with respect to a similar table located at the end of Chapter 2.

Chapter 2: Analysis Existing and Proposed Surveillance Systems

Once it can be determined what customers want and need in a surveillance system attention is turned towards existing and emerging surveillance systems against which the PSN would compete. Chapter 2 of this thesis does just that, it analyzes the features and capabilities of existing and emerging surveillance systems. All of the major existing surveillance systems, particularly those in wide spread use by U.S. organizations, are analyzed to determine their key features, capabilities, strengths, weaknesses, and operators (organizations). This data is then compiled at the end of each surveillance system's analysis as an abridged summary. Following each system's summary is a table similar to those constructed in Chapter 1, and like Chapter 1, a master table is created from them and placed at the end of the chapter. This table assists in determining what features the PSN must possess to be competitive with existing systems and what shortcomings those systems have that the PSN can address. It is crucial that this analysis yield useful data that can be applied to the development of the PSN if it is ever going to be viewed as a viable alternative or augmentation to existing, already proven hardware. Moreover, this table helps to assess what features existing systems possess that are transferrable to clientele

who have yet to take advantage of them. With this information in hand the development of a better and more capable system can proceed.

Chapter 3: Conceptualizing a Better System

The major objective of Chapter 3 is to analyze the tables constructed in the first two chapters. Analysis of these tables is performed to determine what surveillance system(s) are best suited to fulfill the scenario specific surveillance demands of an organization on a mission by mission basis. This analysis also highlights scenarios in which two or more organizations have overlapping surveillance demands. Knowing this information helps to determine what components (certain capabilities are directly related to the components installed, others are not) of the PSN should have a modular design. Taking this approach enables the development of a system whose variants share the maximum number of unique components, reducing overall cost of each PSN unit. Next, analysis of the tables from Chapters 1 and 2 is conducted to reveal which scenario-specific missions have surveillance demands that have not been satisfied by existing surveillance systems.

Following this analysis the tactics and operational use of existing surveillance systems are examined on a scenario by scenario basis. Understanding how an organization employs their surveillance systems and the contribution those systems have with respect to that organization's broader mission is crucial to the development of the PSN. This examination makes use of the Scenario-Specific Optimization Asset (SOSA). SOSA is used, in this chapter, to generate some of the images used to illustrate specific scenarios and the organization-specific tactics used in them.

Chapter 4: Design of the Portable Sensor Network

Chapter 4 begins with a quick review of the analysis and examination conducted in chapter 3. This information is then applied to the requirements imposed on the design of the PSN (e.g., portable, modular, cheap, original, etc.). This examination and all of the research conducted prior to it is taken and used to create a preliminary design for the PSN. This design is the product of multiple, unsuccessful versions of the PSN that preceded it. For that reason, the design history of the PSN is discussed prior to introducing the final design itself. Using this approach explains how and why the final design came in to being, an excellent method of introducing the final designs itself.

Next, the various features of the PSN are discussed. While many, but not all, of these features are taken from the table at the beginning of the chapter, the discussion of them in this section is in greater detail and in the context of their specific application to the PSN. There are however some features and capabilities that require further elaboration. These features and capabilities, due to their originality, will no doubt be scrutinized more than those which are already considered to be proven technologies. As a result, they are explained in greater detail than those covered earlier in the chapter. At the conclusion of this chapter the actual design of each variant of the PSN can begin.

Chapter 5: Variants and Deployment of the PSN

The preliminary design, features, and scenario-specific use of the PSN is used in this chapter to determine how many versions of the PSN are required and what features those versions require. This information is then taken and used to determine the approximate cost of each version. Next, the individual variants are deployed in mock scenarios. This is intended to show how these

sensors are both deployed, operated, and maintained in the field. The majority of the mock scenarios performed in this chapter will be similar to those from chapter 3. The only exception is that in this chapter the PSN is used in lieu of real-world systems. The purpose of this is to determine whether or not the PSN provides any benefit over existing systems and whether or not the capabilities of the PSN can be utilized without modifying the tactics used in those scenarios. Any scenario that requires and/or allows for the use of different tactics when the PSN is deployed is examined to determine the costs and/or benefits of using those tactics, a task that is made much easier via the use of SOSA. Although SOSA is used to generate illustrations similar to those in chapter 3, it is used to its full extent in this chapter to both compare different systems and optimize the placement of them.

Chapter 6: Analysis of the Proposed System

Once the operation of each sensor system has been established an analysis of each variant of the PSN is conducted. These analyses compare the PSN against existing sensor systems as well as judge its ability to handle various scenarios which it may encounter (scenarios derived from historical precedence and those which are entirely hypothetical).

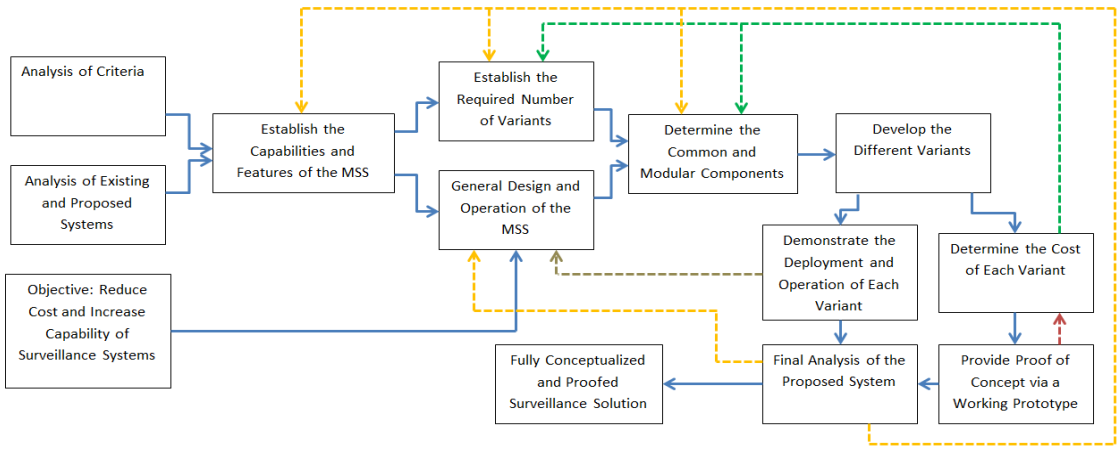

Figure I.1: Methodology behind the development of the PSN

It is important to acknowledge that the process outlined by the steps in the methodology above is an active one. For example, if analysis conducted in chapter 5 reveals a weakness in the operation of the PSN, that weakness will be addressed, if possible, by rethinking the design and operation of a specific sensor, component, or sub-component. The overall methodology and the active process of break analysis that supports it is summarized in **Figure I.1**.

Chapter 1: Surveillance Demands in the 21st Century

Condition and Criteria

The surveillance demands of any given organization can be determined from three sources: those that are explicitly stated by that organization or any organizations to which it is subservient; in-house and third party audits of an organization that reveal gaps in that organization's surveillance capabilities; and those needs which can be derived from an organization's mission statement, stated objective, and/or responsibilities. These three sources of an organization's surveillance demands are known as the 'criteria'. Criteria are the litmus test against which the surveillance capabilities of an organization are judged.

On its own, criteria is nothing more than a statement of the ideal surveillance capabilities an organization possesses. In the real world the capabilities of an organization rarely meet or exceed those expected of it. The current state of these capabilities is called the 'condition', a statement of what is. Condition refers to the total surveillance capability surveillance of an organization, not the capability of any single component or system (some organizations have multiple surveillance systems, each of which has components of its own). At this point it is important to note that surveillance related condition and criteria are not always explicitly stated as surveillance specific. Any criteria or condition which has a surveillance component or depends implicitly upon surveillance is also a possible source of both criteria and condition.

When condition and criteria are combined they paint a picture that reveals both an organizations surveillance demands and where those demands are not met. The difference between condition and criteria is known as the 'gap'.[9] Most criteria are either explicitly stated by an organization or

[9] **Note:** Condition and criteria are commonly used terms in the auditing process. The Government Accountability Office (GAO), the preeminent auditing agency for the U.S. federal government, uses this technique as standard procedure when conducting its own audits. The complete auditing process involves determining the condition,

can be derived from that organization's goals/objectives. Condition on the other hand is most often found in reviews and/or audits of an organization's surveillance capabilities. The following chapter examines major organizations in the U.S. and abroad that rely on surveillance to fulfill their mission. This examination further breaks down the mission of each organization by defining the type of perimeter each of these organization monitors. Since no formal definition of perimeters exist that is common to each, a three tier system has been developed: hard, soft, and dynamic. Hard perimeters are perimeters that have a static outer edge defined by a physical barrier (e.g., an Army fort, Air Force base, Naval port, prison, etc.). Soft perimeters are static perimeters which have no physical barriers (i.e., a coast line or geo-political border, small, circular forest with 'private property, do not enter' signs every 50 ft, etc.). A dynamic barrier on the other hand is more ethereal than its counterparts. Any surveillance asset serving in support of a dynamic barrier must be able to adapt according to the day to day needs of its operators. Moreover, dynamic barriers are not really barriers at all; they are more or less regions of surveillance that encircle a semi-permanent or newly established installation (e.g., a forward operating base, tactical airfield, etc.)

Due to the variety of surveillance demands that exist across the whole of the whole of the organizations covered in this chapter, each sub-chapter is organized according to both the aforementioned perimeter but also the type of surveillance (mission type) being performed: offensive or defensive.

---

criteria, cause, and effect of whatever capability is being audited (in this case surveillance). In this thesis, the final two steps in the audit process are implicit in the analysis of the organizations themselves, not explicitly stated like condition and criteria.

Defensive Surveillance

Defensive surveillance applies to surveillance that is conducted for the purpose of detecting intruders who approach and/or cross the perimeter of an asset whose perimeters may be protected by any one of the three perimeters discussed earlier: hard, soft, and dynamic. The protection of these assets is made all the more difficult by the vast array of assets that fall into one of these three categories. This is especially true in the case of military assets. Consequently, the military has a greater number of missions unique to each type of perimeter. The vast majority of missions performed by all three of the organizations reviewed in this chapter are defensive, and the majority of those are in the defense of hard borders.

Offensive Surveillance

For the purpose of this thesis, offensive surveillance is classified as surveillance conducted to gather intelligence not directly linked to the security of a perimeter or installation. Offensive surveillance is not always conducted in support of immediate, offensive military action; it may be conducted for the sole purpose of gathering intelligence useful to individuals making key decisions related to U.S. national security or foreign policy.

Following the detailed review of each organization there is summary which lists the major criteria and condition(s) of that organization. Each criteria and condition are broken into two parts which are separated by a hyphen. The first part is the official criteria/condition that more often than not surveillance specific, the second describes specifically how that criteria/condition relates surveillance.

In addition to the review and summary there is a surveillance table that quantifies the various surveillance needs of an organization. Depending on the number of unique missions and the

number of scenarios per mission, each of which has its own surveillance requirements, an organization can have a table with multiple rows, with one mission-scenario combination per row.[10] There are however thousands of possible combinations per mission. In an effort to reduce the number of rows in the final table (to a manageable number), a maximum of five scenarios have been logged per organization. These five mission-scenario combinations are modeled after a real life mission-scenario combination.[11] Depending on the scenario, surveillance assets currently in use may be declared in the scenario title. The following list contains the name and description of the variables used in these tables to quantify the surveillance requirements of each organization's mission-scenario combination(s)[12]:

Scenario Title: The specific title of the scenario. This title is typically named based on the real world scenario on which it was modeled.

Operator: The name of the organization represented in that row's mission-scenario combination. This field has two parts that are separated by a hyphen. The first part is the organization or mission itself, the second is the parent organization and/or class of organization to which the first belongs (e.g., CBP/DHS, Army/Military, Air Force/Military, etc.)

Surveillance Mission: Indicates whether the surveillance conducted in this row is offensive or defensive

Objective: Indicates how the surveillance assets are with respect to the broader mission. Assets implemented can be used to deter, detain, overtly survey, or covertly survey IOIs.

Preconditions: Not used until chapter 3. This is a variable similar to scenario title but is only used in custom scenarios, and is therefore N/A to the scenarios outlined in this chapter

---

[10] The number of rows can vary for many reasons. The first and most obvious reason there may be additional rows is because a particular organization has multiple surveillance needs (e.g., multiple offensive and/or defensive missions each with their own requirements, etc.). However, an organization may also have additional rows if characteristics within that mission vary based on certain criteria, in which case there are multiple 'scenarios' for a single mission. For example, an organization may have defensive requirements based on the type of a perimeter used in a particular scenario. If that same mission has different surveillance requirements when the perimeter is changed (e.g., soft to hard) then that scenario will be added to the matrix as a new, independent row.

[11] For example: if there was a real nuclear power plant needing defensive surveillance, that piece of critical infrastructure and the surveillance requirements demanded by it would be translated via the use this rating system into a mission-scenario combination.

[12] Some of the variables listed in this section are rated on a scale from 1 to 5 or 1 to 10. Each value of a rating has a unique description attached to it, a description which varies from variable to variable. Appendix A has a list that describes the meaning behind the values attached to each variable

Type of Perimeter: Indicates the type of perimeter surrounding an installation requiring defensive surveillance. The three types of perimeters are hard, soft, and dynamic. All scenarios with an offensive surveillance mission are designated as having a dynamic perimeter

Perimeter Length: Perimeter length is the length, in meters, of the perimeter requiring surveillance. In the case of a border, the perimeter length is the length of the border needing surveillance. Some scenarios are a microcosm of larger ones. Scenarios of this type are denoted with an asterix and, if known, the length of the actual perimeter

Required Portability Rating: The portability requirements associated with a specific scenario. These requirements represent the maximum size and weight of surveillance assets that can be used in a particular scenario. These requirements are rated on a scale from 1 to 10 with 10 being the most portable

Required Setup and Teardown Rating: The time and manpower requirements associated with a specific scenario. These requirements represent the maximum time and manpower allotted to initially setup and then later repackage a particular scenario's surveillance assets. These requirements are rated on a scale from 1 to 10 with 10 requiring the least time and manpower

Required Endurance: The endurance requirements associated with a specific scenario. Endurance is rated according to the number of days (and fractions of a day) an asset must remain operational without service of any kind. Most scenarios do not require (hence the word must) assets with specific endurance requirements since those scenarios take place under conditions where resupply is not an issue (e.g., along a border that is frequented by personnel on a daily basis). Scenarios with no endurance requirements are designated N/A

Terrain Rating: Terrain rating is used to quantify the type of terrain in which a particular scenario takes place. The terrain quantified is only that terrain which falls within the scope of that scenario (e.g., terrain beyond a given scenario's required distance of detection or identification is irrelevant). This rating varies on a scale from 1 to 5 with 5 being the most uneven

Foliage Rating: Foliage rating is used to describe the type and density of vegetation in which a scenario takes place. Both the type and density of foliage are represented by a single variable. In addition to describing type and density, this rating defines how much the foliage present inhibits the operation of surveillance assets. Foliage is rated on a scale from 1 to 5, with 5 being the most surveillance inhibiting

Required Low Observability Rating: Low observability requirements rating is used to quantify how important it is that the surveillance assets used in a particular scenario are and remain covert. Low observability is rated on a scale from 1 to 5, with 5 being the most covert

Required Detection Range of Vehicles[13]: The distance from the perimeter a vehicle must be detectable

[13] All detection, identification, and tracking requirements are under nighttime conditions. Although many surveillance missions are conducted during the day, the majority of those missions have are conducted both day and night. The rational for choosing nighttime is three-fold. First, conditions at night are far more stringent than during the day (including thermal since nearly all are equipped with daytime optics), any surveillance asset will perform equally or better during the day. Second, it would be much more difficult to rate requirements for both

Required Detection Range of Humans: The distance from the perimeter a human must be detectable

Required Class-Specific Identification Range of Vehicles (see footnote 13 below)**:** The distance from the perimeter at which surveillance assets are required to identify vehicles as belonging to a particular sub-class (e.g., a car vs. a truck or an ultra-light vs. a Cessna)

Required Class-Specific Identification Range of Humans: The distance from the perimeter at which surveillance assets are required to identify the number of individuals traveling in a single group on foot

Required Recognition Range: The distance from the perimeter at which surveillance assets are required to recognize the intent of a vehicle or human. A single variable is chosen since it is equally as difficult to discern the intent of individuals in a vehicle (e.g., a truck load of illegal immigrants vs. some ranchers in their pickup) as it is individuals on foot humans (e.g., a smuggler versus a terrorist versus an illegal immigrant)

Required Tracking Depth of Detected Vehicles: This distance from the point of detection that surveillance assets are required to maintain constant surveillance contact with vehicles. The vector of this distance, or depth, depends on the mission type. If the mission is defensive surveillance of any kind or offensive surveillance of a border, the required tracking depth is oriented with respect to the border/perimeter. If the mission is offensive surveillance of a fixed perimeter, the tracking depth oriented with respect to the center of the installation/perimeter being surveyed. **Figures 1.1** through **1.5** at the end of this list provide a graphical depiction of these measurements, measurements which apply to all tracking variables

Required Tracking Depth of Detected Humans: This distance from the point of detection that surveillance assets are required to maintain constant surveillance contact with humans

Required Tracking Depth of Class-Specific Vehicles: This distance from the point of identification that surveillance assets are required to maintain constant, class-specific contact with vehicles

Required Tracking Depth of Class-Specific Humans: This distance from the point of identification that surveillance assets are required to maintain constant, class-specific contact with humans

Required Tracking Depth of Recognition for IOIs: This distance from the point of identification that surveillance assets are required to maintain constant, recognition contact with IOIs

Surveillance Budget: The surveillance budget is the total, scenario specific, funding, in U.S. dollars, allotted for the acquisition of surveillance assets. In many cases the surveillance budget will be N/A (the scenarios in this chapter are modeled after equipment that is already in place, not equipment up for purchase. This variable is used more extensively in chapter 3

---

day and night. Finally, it is unlikely that the surveillance requirements for a particular scenario change from day to night, only the capabilities of a particular asset.

All detection and identification ranges, in meters, are positive if the range is outside the perimeter, negative if inside.

Important notes regarding the variables above:

Later in this thesis the detection, identification, and tracking variables are all graphed. The large number of them makes it very difficult to both first create and afterwards view a graph that large (particularly since those variables apply to individual surveillance assets as well). To make the graphing of data used in this and later chapters easier to handle, the required detection range of humans and the required class-specific identification range of vehicles are given the same value. Similarly, the class-specific identification range of humans and the recognition range of IOI have been combine into single table as well. For the purposes of the table below, the table at the end of this chapter, and all graphs created in this thesis, the two combination variables described above are named 'Required Range of Vehicle Human Detection' and 'Recognition Range of IOI' respectively.[14] The same logic has also been applied in similar manner to the tracking variables which have been combine to form the variables 'Required Tracking Depth of IOIs' and 'Required Tracking Depth of Recognition IOIs'

The following figures are a graphical depiction of the different tracking depths and detection ranges described in the list above. It is important to remember that **Figures 1.2** through **1.5** are only representative of an airborne asset's tracking depth**. Figures 1.2** and **1.3** only apply to installations with a fixed outer perimeter (does not matter the type of perimeter). First, **Figure 1.1**, a depiction of detection ranges with respect to a border.

Figure 1.1 depicts the all three of the detection ranges and tracking depths (vehicle, human, and recognition). In order to make this page image less burdening to look at the entire next page has been devoted to it.

[14] It was important to list all four variables in the list above despite the fact that only two are used. The reader now knows what variables where considered when creating each scenario and why those variables where chosen.

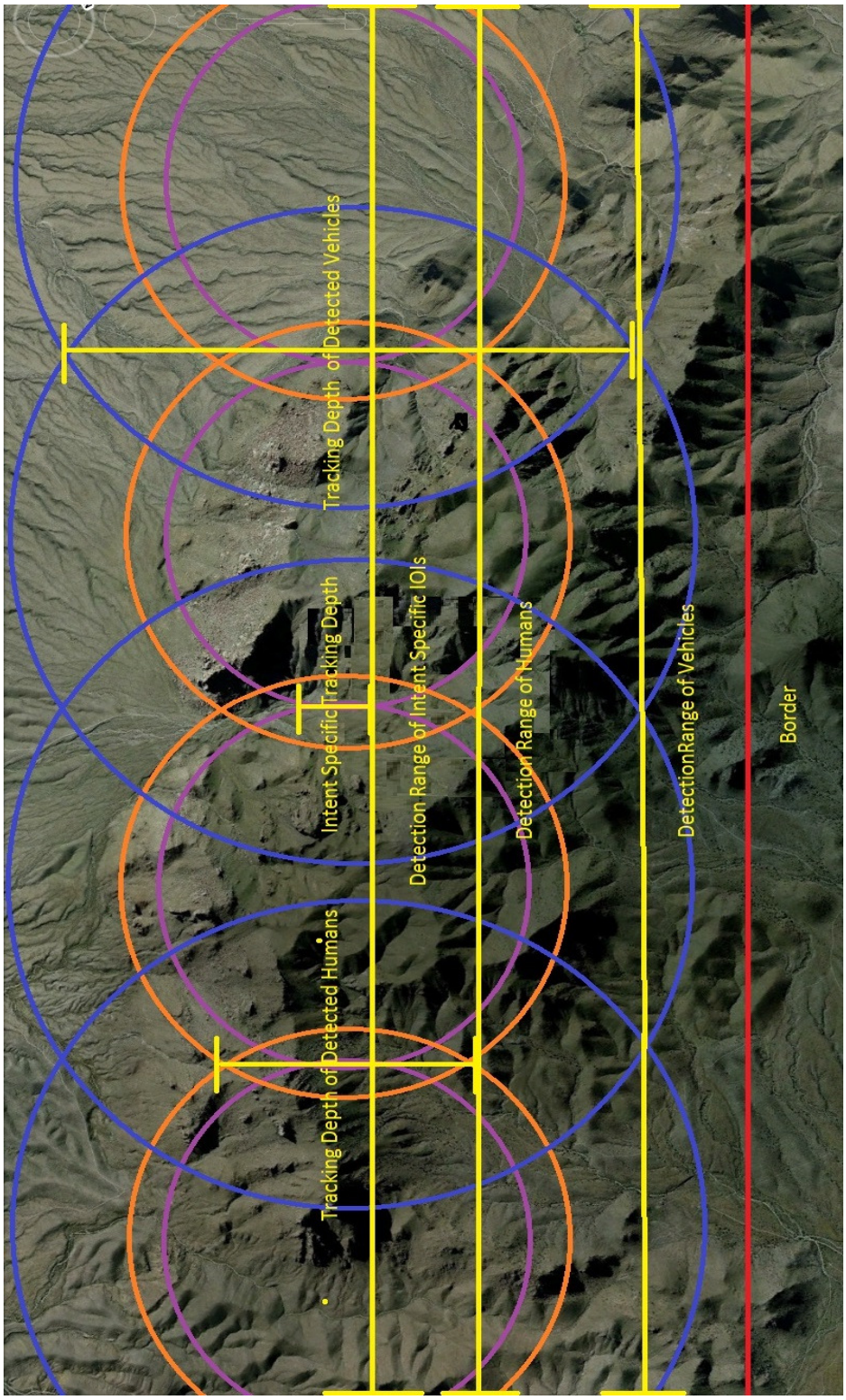

Figure 1.1: Detection ranges and tracking depths

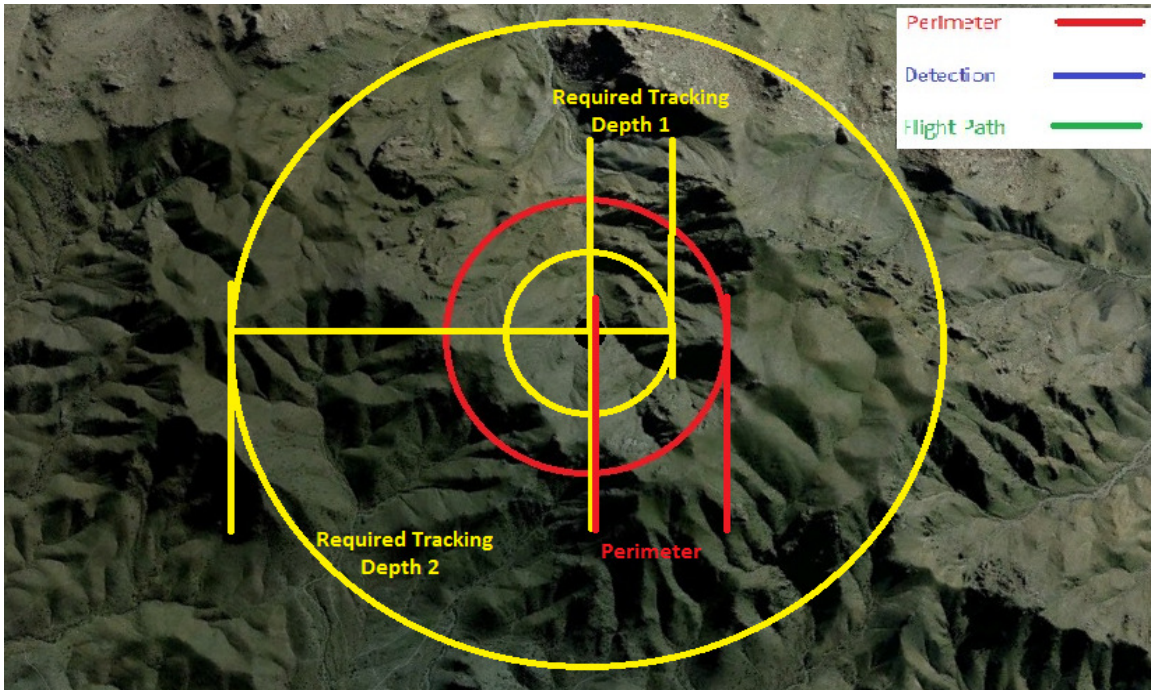

Figure 1.2: Offensive surveillance. All offensive surveillance assets must orbit the center of the perimeter so that their detection radius is tangent to it. As a result, the tracking depth is oriented with respect to the center of the perimeter

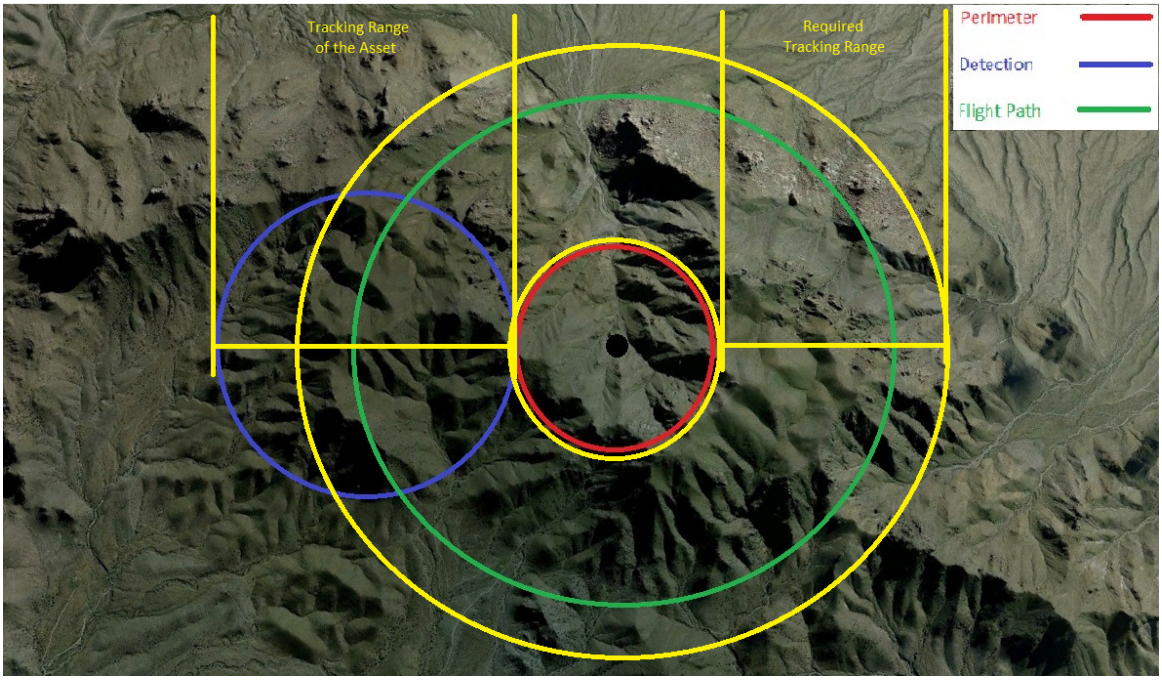

Figure 1.3: Defensive surveillance around a perimeter. All airborne defensive assets must operate such that the inner detection range is tangent to or inside the perimeter. The required tracking depth is measured outwards from the perimeter

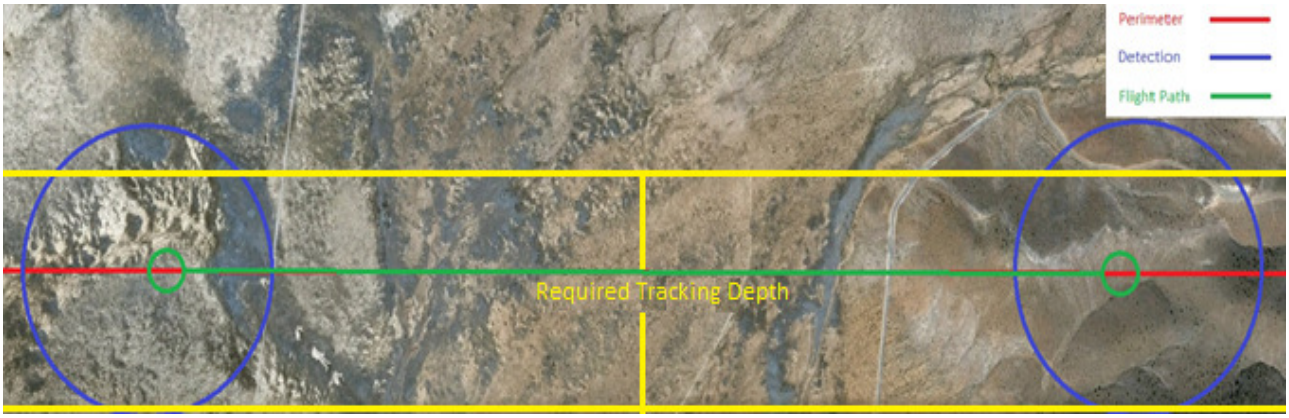

Figure 1.4: An example of offensive and defensive tracking depth along a border. The tracking depth is oriented with respect to the border

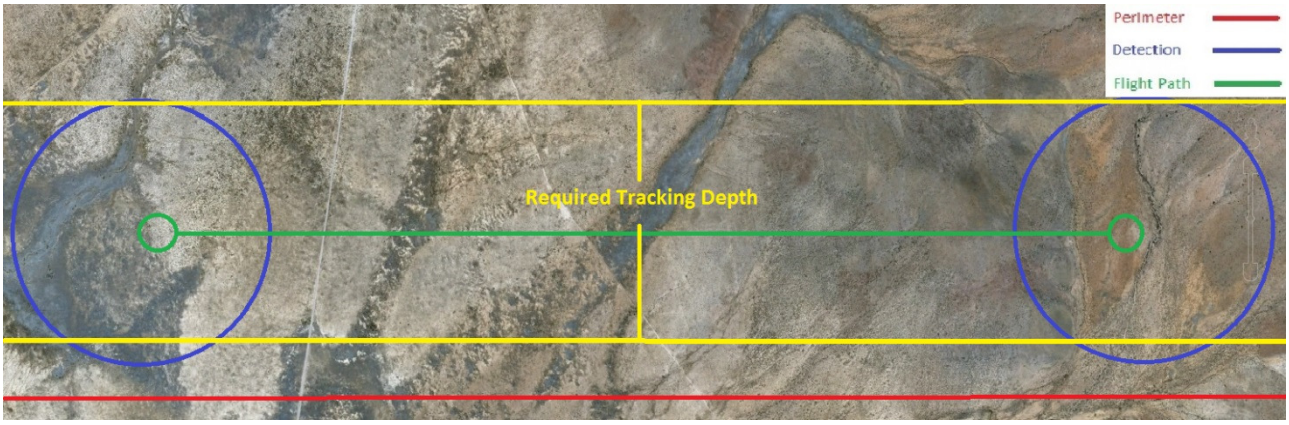

Figure 1.5: An example of purely defensive tracking depth. The tracking depth has an inner depth that inside or on the border itself. The tracking depth is oriented with respect to the border

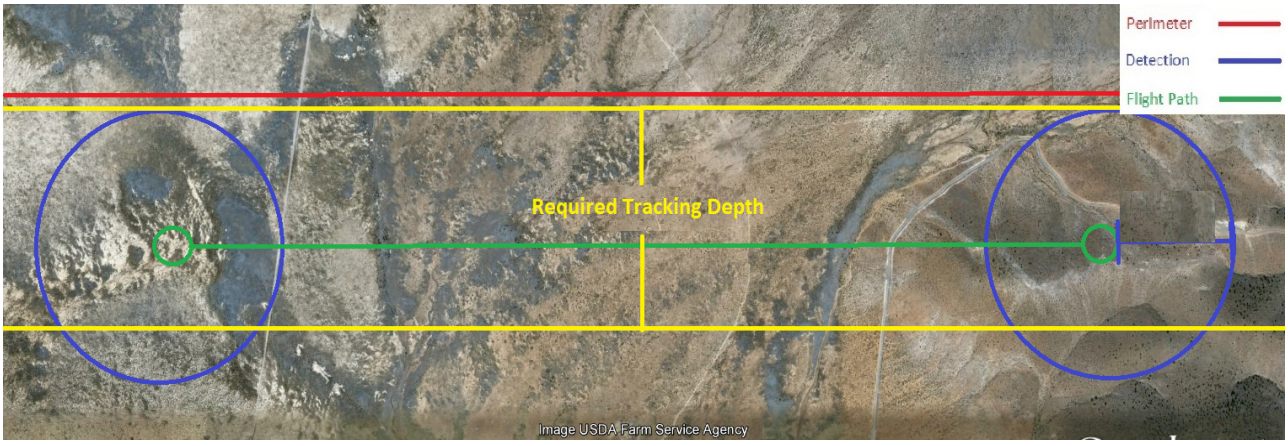

Figure 1.6: An example of purely offensive tracking depth along a border. The inner detection radius extends beyond the border. The tracking depth is oriented with respect to the border

When assembled, the variables above form a table identical to **Table 1.1** below (to make this table easier to read it was broken into two different rows. The tables following each organization are displayed in this method while the master table at the end of this chapter is arrayed horizontally on two pages):

Scenario	Operator	Surveillance Mission	Objective	Preconditions	Type of Perim.	Perim. Length	Required Portability Rating	Required Setup and Teardown Rating	Required Endurance

Terrain Rating	Foliage Rating	Required Low Observ. Rating	Required Detection Range of Vehicles	Required Detection Range of Humans	Recognition Range	Required Tracking Depth of Vehicles	Required Tracking Depth of Humans	Required Tracking Depth of Recognized IOIs	Surveillance Budget

Table 1.1: An example of the scenario tables used in this

At the end of this chapter there is a master table that contains the surveillance requirements of all three organizations. This table is used in chapter 3 to aid in the design and marketing[15] of the PSN.

The first agency to undergo examination is U.S. Customs and Border Protection, the organization that has the most to benefit from the development of the PSN.

U.S. Customs and Border Protection (CBP) – DHS

Defensive Surveillance of Hard and Soft Perimeters – Border Protection

CBP is one of 22 federal agencies that make up the recently formed DHS. DHS is tasked with fulfilling five distinct missions:[16]

- Prevent terrorism and enhancing security

[15] Not from a sales point of view but rather from a development one. This matrix will assist in determining what organizations might be interested in the PSN and what organizations / missions should be ignored during the development of it. Simply put, the surveillance requirements of these organizations exceed the surveillance capabilities of the PSN, capabilities which are limited by the underlying concept on which the PSN was founded.
[16] "Our Mission." U.S. Department of Homeland Security, February 2013.

- Secure and manage our borders
- Enforce and administer our immigration laws
- Safeguard and secure cyberspace
- Ensure resilience to disasters

Of these five missions, CBP is the primary agency responsible for both 'securing and managing our borders' and the 'enforcement and administration of our immigration laws'. It should also come as no surprise that, while not the lead agency, CBP also plays an important role in 'preventing terrorism and enhancing security'. These three missions place a high demand on CBP's limited resources, especially when considering the physical types and domain CBP is responsible for monitoring. This mission is conducted in the defense of both hard and soft perimeters, perimeters that are often defended by a combination of each (i.e., in some locations the U.S. – Mexico border is fenced while in other it is undefended). Regardless of the type of perimeter being defended, CBP's self-described mission remains the same:

"U.S. Customs and Border Protection is responsible for guarding nearly 7,000 miles of land border the United States shares with Canada and Mexico and 2,000 miles of coastal waters surrounding the Florida peninsula and off the coast of Southern California. The agency also protects 95,000 miles of maritime border in partnership with the United States Coast Guard."[17]

This undertaking requires a large surveillance network, without which the 61,000 employees of CBP would be unable to perform the task laid before them. These employees are divided amongst the various mission teams, the largest of which is the U.S. Border Patrol. Border Patrol,

[17] "Protecting Our Borders: This is CBP." U.S. Department of Homeland Security: Customs and Border Protection, September 2012.

founded in 1924, is an organization that has doubled since 2004[18] to a force of over 22,000 in 2013.[19] According to the CBP, the two-part mission of Border Patrol is:

"… preventing terrorists and terrorists weapons, including weapons of mass destruction, from entering the United States..."[20]

"… to detect and prevent the illegal entry of aliens into the United States… maintain borders that work - facilitating the flow of legal immigration and goods while preventing the illegal trafficking of people and contraband."[21]

These missions must be accomplished across vast land and seascapes. Border Patrol's domain, which is nearly identical to that of CBP, is described by them as being "…nearly 6,000 miles of Mexican and Canadian international land borders and over 2,000 miles of coastal waters surrounding the Florida Peninsula and the island of Puerto Rico."[22]

Due in large part to the size of this domain, it is the Border Patrol agents who benefit the most from the implementation of new, more effective surveillance technology. Unfortunately, recent attempts to implement new surveillance technology, particularly along the U.S. – Mexico border, have met with only mild success.

---

[18] Farley, R. (2011). *Obama Says Border Patrol Has Doubled the Number of Agents Since 2004*. Politifactcheck.com, May 2011.
[19] *Snapshot: A Summary of CBP Facts and Figures for 2012*. U.S. Department of Homeland Security: Customs and Border Protection, January 2013. p. 1
[20] *Border Patrol Overview*. U.S. Department of Homeland Security: Customs and Border Protection: Border Patrol, January 2011.
[21] Ibid.
[22] Ibid.

According to DHS' own assessments, in 2010 only half of the southern border and 2% of the northern border were deemed acceptably secure.[23] This is despite the fact that CBP has spent over $5 billion in new fencing and technology. The fencing alone has cost billions – approximately $3 million per mile less the cost of maintenance for the 649 miles that have been constructed to date.[24] Several billions more have been increasing the number of border patrol agents, expanding the force every year since 2001. There are currently 21,970 Border Patrol agents in CBP, of which nearly 18,000 are tasked with monitoring the U.S.-Mexico border. Although the border is only marginally more secure now than it was in 2010, DHS has recently classified the southern border as acceptably secure. It is important to note however that prior to

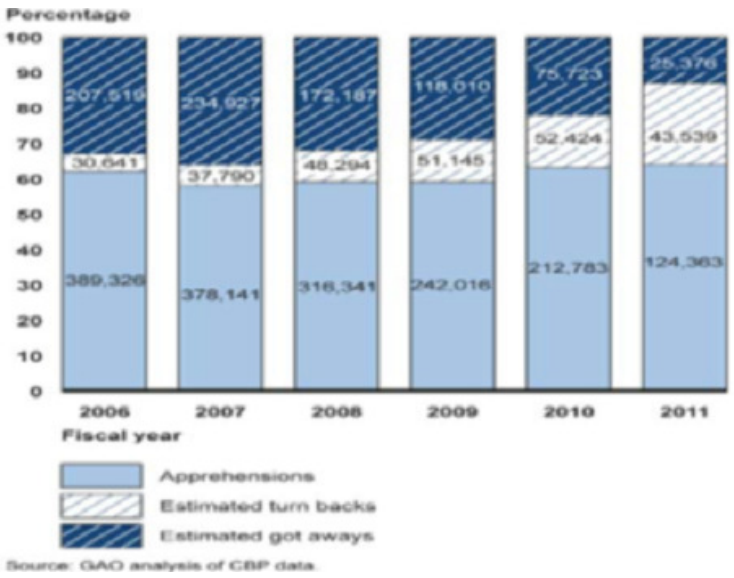

Figure 1.7: GAO analysis of CBP data[25]

[23] An acceptable level of border security is defined as possessing the capability detect, deter, and/or intercept violators at the border or shortly thereafter. There is no mention as to how effective these capabilities must be, only that they exist.
Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders. U.S. Government Accountability Office, March 2011. p. 2
[24] *Secure Border Initiative Fence Construction Cost.* U.S. Government Accountability Office, March 9, 2009. p. 4
[25] Border Patrol: Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs. US Government Accountability Office, December 2012. p. 29

the border being declared secure, DHS changed the criteria defining what is and what is not secure.[26] Nonetheless, issues remain. GAO analysis of CBP data (**Figure 1.7**) shows that attempts to cross the southern border have sharply decreased over the past 5 years. This same analysis states that the number of 'got aways' have declined as a percentage of total border violators, proof that the border is more secure[27]. Analysis conducted in association with thesis suggests that the actual cause behind the increase in apprehensions and got aways is more complex. In the same GAO report that quoted the DHS as having said the southern border was acceptably secure there was a comment from DHS acknowledging that part of their 'success' was a decrease in border violators, the suggested cause being the contraction of the U.S. economy.[28] The result is a scenario in which the number of detected border violators drops from 620,000 in 2006 to 193,000 in 2011 during which period the DHS increased the number of Border Patrol agents and pumped billions of tax payer dollars into surveillance programs. Analysis of the externalities/circumstances that contributed to a drop in the annual number of border violators is evidence enough to question the DHS's claim that the border is acceptably secure. At best, the circumstances surrounding DHS's claim make the statement itself premature; hard proof that DHS has acceptably secured the border would be for them to do so under the same conditions that have prompted illegal immigration to rise in the past. Once and

---

[26] *Progress Made and Work Remaining after Nearly 10 Years in Operation.* U.S. Government Accountability Office, February 2013. p. 1

[27] Despite the increase, less than 2/3rd of the known violators are intercepted and detained. 13% of violators successfully evaded Border Patrol agents and gained illegal entry while 20% avoided capture by re-crossing the border to Mexico. These figures do not take into account the unknown number of violators who were not detected by the Border Patrol.
Progress Made and Work Remaining after Nearly 10 Years in Operation. U.S. Government Accountability Office, February 2013. p. 1
Border Patrol: Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs. US Government Accountability Office, December 2012. p. 29

[28] Progress Made and Work Remaining after Nearly 10 Years in Operation. U.S. Government Accountability Office, February 2013. p. 1

only once this scenario is faced and successfully countered can CBP declare victory and the southern border 'acceptably' secure.

Far from being able to declare the border secure, there is in fact ample evidence to state just the opposite. One of the statistics often quoted by both CBP and DHS are drug seizures which, in some cases (i.e., depending on the specific narcotic), have more than doubled. What is often ignored is the production of narcotics, particularly in areas that commonly ship their product to the U.S. via the southern border. The figures below highlight exactly that fact. **Table 1.2** shows

Potential Pure Heroin Production in Metric Tons, 2005–2009

	2005	2006	2007	2008	2009
Afghanistan	526.0	664.0	947.0	650.0	630.0
Burma	36.0	22.0	26.0	32.0	24.0
Colombia	NA	4.6	1.9*	NA	2.1
Laos	2.7	0.8	0.5	2.0	1.0*
Mexico	8.0	13.0	18.0	38.0	50.0
Pakistan	3.8	4.2	NA	3.0	NA

Source: U.S. Government estimate.
*Estimate is based on partial data.
NA–Not available

Heroin Seized at Southwest Border Area and Commercial Air POEs, in Kilograms, 2004–2010

	2004	2005	2006	2007	2008	2009	2010
Southwest Border Area	386	228	489	365	557	798	945
Commercial Air POEs	909	739	529	424	469	321	660

Source: El Paso Intelligence Center, National Seizure System.

Table 1.2: from DEA National Drug Assessment for 2011[29]

heroin production and seizure from 2004 to 2010. While a first glance at production would have one think that, since the total amount of heroin produced has not risen sharply, heroin entering the U.S. has also not risen. This could not be further from the case. The majority of Afghani heroin is bound for Europe or Asia. The major source of U.S. heroin is Mexico which has risen in production from 8 metric tons in 2004 to 50 in 2010, an increase of more than six fold, while

[29] *National Drug Threat Assessment for 2011*. U.S. Department of Justice: Drug Enforcement Agency, August 2011. p. 27

seizures of heroin (total, POE and border) have risen by only about 30%. Even if one just looks at the border, seizures have only risen 250%, marginal when compared to the 650% rise in production. Marijuana seizures are another example of how CBP and DHS have lured themselves into developing a false confidence in their ability to interdict narcotics. **Tables 1.3** and **1.4** show the production of marijuana and the seizures of various drugs from 2005 through 2010 (tables overlap from 2006-2009).

Cannabis Cultivation and Potential Marijuana Production in Mexico, 2005–2009

	2005	2006	2007	2008	2009
Net Cultivation (hectares)	5,600	8,600	8,900	12,000	17,500
Potential Production (metric tons)	10,100	15,500	15,800	21,500	NA

Source: United States Government estimate.
NA–Not available

Table 1.3: Marijuana Production[30]

Total U.S. Seizures,* by Drug, in Kilograms, FY2006–FY2010

	2006	2007	2008	2009	2010
Cocaine					
Southwest Border Area**	27,361	24,780	17,459	18,737	17,830
Northern Border	2	<1	<1	18	23
Rest of U.S.	42,198	33,177	28,547	29,629	26,210
Total U.S.	**69,561**	**57,957**	**46,006**	**48,384**	**44,063**
Methamphetamine					
Southwest Border Area	2,706	2,128	2,221	3,278	4,486
Northern Border	<1	1	135	0	11
Rest of U.S.	2,872	3,100	3,696	3,323	4,202
Total U.S.	**5,578**	**5,229**	**6,052**	**6,601**	**8,699**
Heroin					
Southwest Border Area	449	358	496	737	905
Northern Border	5	<1	0	28	20
Rest of U.S.	1,719	1,631	1,404	1,485	1,637
Total U.S.	**2,173**	**1,989**	**1,900**	**2,250**	**2,562**
Marijuana					
Southwest Border Area	1,046,419	1,459,162	1,242,758	1,730,344	1,545,138
Northern Border	5,455	3,084	2,369	3,784	2,194
Rest of U.S.	237,330	263,904	227,948	241,000	262,164
Total U.S.	**1,289,204**	**1,726,150**	**1,473,075**	**1,975,128**	**1,809,496**
MDMA***					
Southwest Border Area	17	43	69	77	216
Northern Border	271	316	440	506	557
Rest of U.S.	1,150	1,444	2,069	1,896	1,351
Total U.S.	**1,438**	**1,803**	**2,578**	**2,479**	**2,124**

Source: National Seizure System.

Table 1.4: Narcotics seizures, 2006-2010[31]

[30] Ibid. p. 29

A recognizable trend appears when comparing the production and seizure of marijuana between the years 2006 and 2009. During this period the seizure of marijuana has increased by roughly 50% while the production has increased by 300%. Both of these statistics suggest that the U.S. southern border may not be as secure as DHS and CBP claim.

Regardless of whether DHS chooses to declare the southern border secure or not, there are still tens of thousands of border violators who go uncaught. As long as this remains the status quo the southern border can never truly be declared secure. There is however a much larger problem that, in the future, could present a greater problem to CBP than that which it now faces along the southern border.

As the percentage of border violators successfully intercepted rises, those that can afford to enter via an alternate route will increasingly choose to do so. Unfortunately, a disproportionately large number of those that have the financial freedom to do so are the worst of the worst – drug smugglers and terrorists.[32] The lack of surveillance along the northern border will make it difficult to counter the problem of a shift in smuggling routes since the majority of the technology in use today is static, requiring months to years to erect. Even worse is the fact that the northern border is significantly more difficult to monitor than the southern. Not only is the northern border longer than the southern, it also contains thick foliage. This foliage further inhibits the ability of both UAVs and long range border installations (e.g., SBI*net*[33]) to detect violators. Finally, these individuals are much more adept at smuggling than the average border violator. Despite a noticeable drop in total border incursions, the total amount of drugs

---

[31] Ibid. p. 50
[32] A Line In The Sand: Countering Crime, Violence And Terror At The Southwest Border. U.S. Congress: House Committee on Homeland Security, November 2012. p. 4
[33] SBI*net* is the single largest and most recognizable component of the SBI. A detailed review of this system is conducted in Chapter 2.

smuggled across the border has risen – more so than many agencies responsible for stifling the flow of narcotics are acknowledge These statistics are supported by U.S. citizens living along the border who report that, although the overall number of violators has decreased, encounters with smugglers have remained constant, if not increased.[34]

Although CBP's past attempts to secure U.S. borders have had mixed results, the organization may be at a crossroads. With the cancellation of the SBI*net* program, CBP has been forced to implement an alternative program known as the alternative or post-SBI program. This program is marked by the introduction of six contracts for assets developed around proven technology. These assets are:[35]

- Mobile Security System (MSC)
- Mobile Video Surveillance System (MVSS)
- Air Support via the Unmanned Aircraft System (UAS)
- Long Range Handheld Thermal Imaging System
- Agent Portable Surveillance System (APSS)
- Remote Video Surveillance System (RVSS)

Each of these technologies, though still being tested by CBP, has so far proven effective. With that in mind, only time will tell how effective they really are – every system has its pros and cons.

[34] "DHS Napolitano' Touts Border Security." CBS News, February 2013.
[35] *Arizona Border Surveillance Technology: More Information on Plans and Costs Is Needed before Proceeding.* U.S. Government Accountability Office, November 2011. pp. 37-43

Offensive Surveillance – Interdiction of Maritime and Airborne Smugglers

The missions conducted by CBP that qualify as offensive surveillance are those which are in support of enforcement assets that intercept smugglers before they enter U.S. territorial waters. This mission also applies to surveillance assets operated by the CBP that monitor the territorial waters (and open water around those waters) of nations cooperating with the U.S. to combat the international narcotics trade.[36] While some of the assets used in this role are dedicated to it (surveillance), others perform both surveillance and enforcement. The organization within CBP that is tasked with the operation of aircraft and maritime assets is the Office of Air and Marine (OAM). As of January 2011, OAM operated 267 aircraft and 301 marine vessels in support of their mission which is to:[37]

- provide support to CBP's anti-terrorism mission at U.S. borders including, air-to-ground interception of people and contraband illegally crossing land borders, air-to-air interception of aircraft, and air-to-water interception of transportation vessels.
- provide support for CBP's traditional work, such as border interceptions unrelated to terrorism and other DHS missions as well.
- conduct air operations to support other federal, state and local needs, such as disaster relief

[36] "CBP Intercepts Cocaine Smugglers in Open Water" U.S. Department of Homeland Security: Customs and Border Protection, January 2013.
[37] *Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets*. U.S. Government Accountability Office, March 2012. p. 1

In 2011 OAM logged 94,968 flight hours and 133,374 maritime hours, an average of 352 hours per air asset and 476 hours of maritime asset annually.[38] This is an operation tempo that is a credit to OAM and CBP. However, the operation of these assets comes at an annual cost in excess of $815 million on top of the $1.3 billion spent between 2006 and 2011 to modify OAM's assets.[39] Moreover, analysis of the capabilities provided by OAM assets revealed that, despite being a highly a potent surveillance system, it was unable to meet its 2011 operational goals.[40] More often than not, these goals were not met because of extreme environmental conditions that prohibited OAM assets from either deploying in the first place or negated their effectiveness after having arrived on location. Finally, although OAM is increasing its use of advanced UAVs, these aircraft accounted for only 4,406 of the 94,968 hours flown in 2011.[41]

Summary Analysis

DHS has tasked the CBP with safeguarding the borders of America as well as points of entry (POE) inside U.S. borders. Although CBP has increased its surveillance assets it still lacks the ability to sufficiently monitor the southern border, where it spends $4 billion of its $12 billion budget, and all but lacks the capability to effectively monitor the northern border (aside from POE's).[42] The CBP is pursuing the GAO's recommendation of acquiring more mobile surveillance equipment (through the Mobile Surveillance Capabilities Program, or MSC) but that equipment has not yet been employed en mass nor has it been in the field long enough to be

---

[38] "2011 Air and Marine Milestones." U.S. Department of Homeland Security: Customs and Border Protection: Office of Air and Maritime, December 2011.
[39] *Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets*. U.S. Government Accountability Office, March 2012. p. 1
[40] *Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets*. U.S. Government Accountability Office, March 2012. p. 9
[41] *Fact Sheet: Office of Air and Marine*. U.S. Department of Homeland Security: Customs and Border Protection: Office of Air and Marine, January 2011.
[42] *Border Patrol: Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs.* US Government Accountability Office, December 2012. p. 1

considered a long term solution for CBP's intelligence and surveillance gap. This program is a diversion from prior trends, one that, despite not yet having been proven, is likely to be very successful. Quotes related to CBP's ability to seize narcotics are overstated. CBP needs to expand its surveillance capabilities to include borders (e.g., northern and coastal) not currently monitored (via sensors that are capable of providing real-time, actionable intelligence). It is however important to note that CBP has established a program, the Mobile Surveillance Capabilities Program, in an effort to utilize off the shelf, existing

Criteria

Based on audits, mission statements, and analysis of agency responsibilities, the CBP must possess:

- surveillance assets capable of detecting border violators immediately upon entry, yielding actionable intelligence
- surveillance assets capable of tracking border violators from the point of entry until the point of interception, a distance that in some areas along the southern border stretches for over 50 miles
- surveillance assets capable of identifying border violators with enough detail to determine the nature of their incursion (i.e., determine whether they are smugglers or illegal immigrants)
- the ability to quickly communicate the intelligence gathered via surveillance to enforcement assets that intercept border violators and potential violators in time to deter or detain them
- surveillance assets that are inexpensive, mobile, and use off the shelf technology

- the capability to effectively monitor both the northern and southern borders simultaneously
- operate across multiple Border Patrol sectors more effectively, using common surveillance and enforcement assets

Condition

CBP possesses:

- surveillance systems that are mobile and capable of providing surveillance via ground radar, high-end day time and low-light optics, thermal imaging, and night vision that utilizes various types of infrared (IR) optics
- high-end, ground based surveillance systems that, with a single asset, are capable of detecting items of interest (IOI) at great distances, an example of which is the now cancelled SBI*net*
- an extensive number of airborne and maritime assets including a small number of unmanned aerial vehicles (UAV's), many of which are equipped with forward looking infra-red (FLIR), thermal imagining, and radar
- an increasingly large number of Border Patrol agents themselves providing mobile and fixed surveillance (Border Patrol sectors with advanced surveillance assets use a smaller percentage of their available agents in the classic role of mobile surveillance and border enforcement, less equipped sectors use more (39% versus 63% or more)[43]

[43] Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders. U.S. Government Accountability Office, March 2011. p. 15

- the ability to intercept border violators with varying degrees of success, success that is by the surveillance assets deployed and the location of the incursion (e.g., in limited, high traffic portions of the southern border that have excellent detection and enforcement capabilities IOI can be intercepted with high degree of confidence while IOI using tunnels constructed in urban areas are considerably more difficult to detect)
- an annual budget of approximately $12 billion[44]

Scenario Table – Customs and Border Patrol

Scenario	Operator	Surveillance Mission	Objective	Preconditions	Type of Perim.	Perim. Length (m)	Required Portability Rating	Required Setup and Teardown Rating	Required Endurance
Nogales Arizona: 8 FLIR equipped SkyWatch towers guarding 10 miles of the southwest border (16.1 km)	CBP	Defensive	Deter/Overt Surveillance/ Active Intercept	N/A	Soft	16100	3	3	N/A
Single SkyWatch tower along the southern border equipped with STS 12000 radar	CBP	Defensive	Overt Surveillance/ Active Intercept	N/A	Soft	12000	3	3	N/A
Three FLIR equipped SkyWatch towers, east of El Paso, between Quitman mountain and the border	CBP	Defensive	Overt Surveillance/ Active Intercept	N/A	Soft	9000	3	3	N/A
Three FLIR equipped SkyWatch towers west of El Paso	CBP	Defensive	Overt Surveillance/ Active Intercept	N/A	Soft	9000	3	3	N/A

Terrain Rating	Foliage Rating	Required Low Observ. Rating	Required Detection Range of Vehicles from Border	Required Detection Range of Humans from Border	Required Recognition Range from Border	Required Tracking Depth of Vehicles	Required Tracking Depth of Humans	Required Tracking Depth of Recognized IOIs	Surveillance Budget
1	1	2	1000 m	1500 m	2000 m	3000 m	300 m	10 m	N/A
1	1	2	-200 m	5000 m	7000 m	4000 m	2000 m	10 m	N/A
5	1	2	500 m	1500m	2000 m	2000 m	500 m	10 m	N/A
3	1	2	500 m	1000 m	2500 m	2000 m	300 m	10 m	N/A

Table 1.5: CBP scenario table

[44] "DHS Napolitano' Touts Border Security." CBS News, February 2013.

Protection of Critical Infrastructure – DHS

Defensive Surveillance of Hard and Soft Perimeters – Critical Infrastructure

Critical infrastructure is defined by DHS as: "…the physical and cyber systems and assets so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[45] These assets provide services in the following public and private sectors:[46]

- Food and Agriculture
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation Systems
- Water

Since its founding in 2002, the protection of critical infrastructure has been one of DHS's primary responsibilities. This responsibility was clarified in December 2003 when President George Bush released HSPD-7, a presidential directive outlining DHS's mission and responsibilities as they pertain to safeguarding America's critical infrastructure.[47] Among other things, this directive stated that it was the responsibility of the Secretary of DHS to: "…serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect

[45] "Critical Infrastructure Protection." Department of Homeland Security, February 2013.
[46] Ibid.
[47] "December 17th 2003, Homeland Security Presidential Directive/HSPD-7." White House, December 2003.

critical infrastructure and key resources."[48] This means that in some cases DHS can only assist in the protection of certain assets through collaboration, not take unilateral action to secure them. Nonetheless, DHS has made steps towards securing the assets in all 18 sectors outlined above through: the institution of new regulation, the formation of public-private partnerships, risk-management, and the use of grants designed to assist private companies whom the DHS deemed 'worthy'.[49] These tasks have been assigned to various organizations within DHS, each of which is responsible for various program(s) and/or grant(s). The following are just a few of the programs and grants DHS has created since 2002:[50]

- Buffer Zone Protection Program (BZPP)
- Urban Security Initiative (USI)
- State and Regional Preparedness Program (SRPP)
- Regional Resiliency Assessment Program (RRAP)
- Port Security Grant Program (Federal Emergency Management Agency (FEMA))

These programs provide many services, two of which are funding and vulnerability assessment. The latter is a service provided by the DHS which assesses the vulnerability of an asset. Based on that assessment the vulnerability and assessment team (VAT) makes recommendations to the owner/operator on how to reduce their vulnerability. The owner/operator then decides whether or not to act on the recommendations made, usually basing their decision on available funding. In order to make sure that more recommendations made are actually implemented, DHS provides financial assistance through one of its many grant programs. This funding is traditionally

---

[48] Ibid.
[49] "Critical Infrastructure Protection." Department of Homeland Security, February 2013.
[50] *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure.* U.S. Government Accountability Office, December 2005. p. 60

allocated based on the criticality of the asset and the financial contribution the owner of the asset is willing to make with respect to the overall cost of implementing the recommendation. One of the most common recommendations made by VATs is the installation of additional surveillance equipment in the form of sensors and cameras.

Providing surveillance services have never been a task explicitly assigned to DHS, it has however been an implicit part of the services they provide. When making their recommendations, a VAT has the liberty to recommend specific technologies (e.g., thermal, IR, etc.) but not manufactures. Their clients however are not required to use the technologies recommended by VATs. As a result, those owners/operators who do implement the recommendations made use a variety of different surveillance devices, driving up the cost of doing so. To make matters worse, there are not only different organizations providing grants and assessments for each type of critical infrastructure, there are multiple organizations providing grants within each class of infrastructure. An example of this chaos is the fact that there are three different organizations providing grants to the owners/operators of ports. In this case, the three organizations are: the Coast Guard, Office of Domestic Preparedness (ODP), and Information Analysis and Infrastructure Protection Directorate (IAIP). Making this a particularly bad scenario is the fact that these three organizations each have their own criteria defining how they allocate grants, leading to a situation in which the most significant security needs are not addressed.[51] Nonetheless, vulnerability assessments are performed, grants awarded, and the surveillance capabilities of critical infrastructure assets improved.

[51] In the case of the ODP, the criteria that determined how grants are awarded have changed significantly over the past decade. In the past, a private company was awarded a security grant based on the priority of that request as it was assigned by DHS (use of a ranking system) and the amount that company was willing to contribute. As of 2006, a company's worth is now taken into account. The more a company is worth, the more that company is expected to pay, which in some cases is 100%.

Unfortunately these improvements, in addition to being costly, have yielded mixed results. In one case a chemical plant was equipped with cameras that were linked via the internet to both the installation's internal security and/or local law-enforcement (LE).[52] This highly sensible and effect use of cameras is contrast by the use of insufficient thermal cameras at ports. In 2011 the GAO reported that some organizations who have implemented thermal cameras as part of their port's surveillance package did not install units that were capable of detecting small watercraft, the type of vessel most likely to be used by both terrorists and smugglers.

Summary Analysis

Various agencies and programs within DHS (e.g., FEMA, BZPP, etc.) and other, independent agencies (e.g., Coast Guard) have been tasked with addressing the vulnerabilities of U.S. critical infrastructure through mutual cooperation, and the provision of grants and vulnerability assessments. A key element in the success of their mission is ensuring that the surveillance needs of these assets are met. This task has only been met with mild success due to the massive number of government programs involved and the inconsistent allocation of resources towards the most critical of assets.

Criteria

Based on audits, mission statements, and analysis of the responsibilities assigned to DHS, DHS is required to:

[52] *Homeland Security: DHS is Addressing at Chemical Facilities, but Additional Authority is Needed*. U.S. Government Accountability Office, June 2006. p. 9

- serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources
- support risk management; enhanced domain awareness; training and exercises; expansion of recovery and resiliency capabilities; and further capabilities to prevent, detect, respond to, and recover from attacks involving improvised explosive devices and other non-conventional weapons; and competitively award grant funding to assist critical infrastructure in obtaining the resources required to support the National Preparedness Goal's associated mission areas and core capabilities[53] - conduct security assessments via VATs that assist the public and private sectors in determining their surveillance needs
- ensure that the vulnerabilities of critical infrastructure are addressed by providing both grants and vulnerability assessments – funding to help both the public and private sectors pay for their surveillance needs in accordance with the VAT's recommendations

Condition

DHS:

- is continuing to foster communication between local law-enforcement, federal agencies, and the owners/operators of critical infrastructure assets
- is providing vulnerability assessments that make specific recommendations on how to decrease the vulnerability of a critical infrastructure asset via the installation or upgrade of surveillance equipment

[53] "FEMA: Port Security Grant Program." U.S. Department of Homeland Security: Federal Emergency Management Agency, June 2012.

- has instituted grant programs that award hundreds of millions of dollars per year in financial assistance to the owners of critical infrastructure, assistance which used to encourage owners to implement the recommendations made by VATs
- is not overseeing the process of implementing recommendations as well as they could, leading to scenarios in which some of this nation's most critical assets are left with considerable vulnerabilities (to include surveillance)
- is not allocating grants based purely on the criticality of an asset but instead with respect to the capability of an asset to provide for its own defense, leaving many of this nation's most critical assets highly vulnerable to attack and/or penetration (by terrorists and smugglers respectively)

Scenario Table – Critical Infrastructure

Scenario	Operator	Surveillance Mission	Objective	Preconditions	Type of Perim.	Perim. Length	Required Portability Rating	Required Setup and Teardown Rating	Required Endurance
Civilian Port Complex	DHS	Defensive	Deter/ Detain	N/A	Soft	16100 m	3	3	N/A
	DHS	Defensive	Deter/ Detain	N/A	Soft	12000 m	3	3	N/A
Three FLIR equipped SkyWatch towers, east of El Paso, between Quitman mountain and the border	DHS	Defensive	Deter/ Detain	N/A	Soft	9000 m	3	3	N/A
Three FLIR equipped SkyWatch towers west of El Paso	DHS	Defensive	Deter/ Detain	N/A	Soft	9000 m	3	3	N/A

Terrain Rating	Foliage Rating	Required Low Observ. Rating	Required Detection Range of Vehicles from Border	Required Detection Range of Humans from Border	Required Recognition Range from Border	Required Tracking Depth of Vehicles	Required Tracking Depth of Humans	Required Tracking Depth of Recognized IOIs	Surveillance Budget
1	1	2	1000 m	1500 m	2000 m	3000 m	300 m	10 m	N/A
1	1	2	-200 m	5000 m	7000 m	4000 m	2000 m	10 m	N/A
5	1	2	500 m	1500m	2000 m	2000 m	500 m	10 m	N/A
3	1	2	500 m	1000 m	2500 m	2000 m	300 m	10 m	N/A

Table 1.6: Critical Infrastructure scenario table

Military – Department of Defense (DoD)

The organizations that compose the U.S. military are referred to as "departments", which when combine form the DoD.[54] These three departments are the Air Force, Army, and Navy. The Marines, despite commonly thought of as a forth department, are a subdivision of the Navy. All three of these departments have extensive surveillance demands that are an implicit part of the mission each department is required to perform. These demands require the use of surveillance assets capable of capable of detecting a variety of rapidly evolving threats, making the job of countering them far more difficult, at least on paper, than those of facing DHS and CBP. Fortunately for the military, the type and quality of surveillance assets available to them far outpaces those in use by CBP and DHS, assets which are available (by comparison) on a moment's notice. While the military does perform a wide variety of missions, one of the most common is the defense of static installations, a mission that requires the use of surveillance assets nearly identical to the ones used in the defense of critical infrastructure. With that in mind, the first topic discussed is the defensive surveillance of permanent installations.

Defensive Surveillance of Hard Perimeters – Permanent Installations

Permanent installations with hard perimeters are common to all three departments. In most cases, these installations have very similar, if not nearly identical, surveillance needs. The individuals responsible for making sure the surveillance needs of their installation are met are the commanders of the installations themselves. These commanders face many of the same limitations facing the owners of civilian infrastructure, the two most prominent being adequate

[54] Departments are different from branches. There are five branches: Army, Navy, Air Force, Marines, and Coast Guard. The Marines report to the Department of Navy. The Coast Guard, which is not a DoD organization, reports to DHS.

assessment to determine the vulnerabilities of a given installation and the funding to implement changes that adequately address those vulnerabilities.

When it comes to the DoD, the most pre-eminent organization that conducts vulnerability assessments is the Defense Threat Reduction Agency (DTRA). The DTRA sends out balance survivability assessment teams (BSAT) that provide a service similar to the one provided by DHS's VATs. These teams conduct what they refer to as a balance survivability assessment (BSA): a comprehensive review of an installation's vulnerabilities to physical and cyber-attacks. In addition to the run of the mill assessment conducted by VATs, BSATs will typically conduct a red team assessment – a type of assessment in which the vulnerabilities of an installation are test by having a red team (friendly units/personnel posing as the enemy) attempt to breach or otherwise defeat the defenses of that installation. After having conducted these assessments, the BSAT makes recommendations to the installation's commander on how to reduce the installations vulnerability. More often than not, surveillance is one of the recommendations made by BSATs. Though they are not required to act on these recommendations, most commanders who request a BSA of their installation do the best they can to do so (George C. Baker, personal communication, March 9, 2013) [1].[55]

Acquiring the funding needed to implement the recommendations made by BSATs is always an issue. Commanders have very little control over their installations budget, leaving those commanders who do wish to implement recommendations made by BSATs with one of two choices: apply for DoD grants or pay for it themselves. If no financial aid is awarded, the commander of an installation must either allocate money from their pre-existing budget or

[55] All of the facts contained within this paragraph were obtained via an interview with Dr. George C. Baker that was conducted on March 9, 2013

choose not to implement the BSAT's recommendations. The cost to implement these recommendations can vary wildly depending on the specifics of the recommendation itself (George Baker, personal communication, March 9, 2013) [2].[56]

Standard surveillance recommendations made by BSATs can be broken down into two broad categories: personnel and hardware. Personnel recommendations deal with the use of manpower to reduce an installation's vulnerability by increasing the number, route, and outfitting of patrols (e.g., increase the number of security guards, increase the frequency of patrols, utilize canines, modify procedures to increase accountability for security guards, etc.). Hardware recommendations, with respect to surveillance, deal specifically with the installation, upgrade, re-allocation, and integration of surveillance hardware. The types of hardware recommended ranges from increased lighting to the installation of ground based radar and thermal cameras. This hardware can either be fixed (e.g., security camera mounted on the wall of a building) or mobile (mobile, man-portable ground radar). The upside to using fixed hardware is that the surveillance assets installed provide useful intelligence that mobile assets cannot. For example, an installation's POE (for vehicles) can be equipped with a remotely operated, under vehicle inspection system. These systems consist of multiple cameras embedded in the pavement that are capable of detecting smuggled and potentially dangerous devices (e.g., a bomb, weapons, computer hacking hardware, etc.).[57] Using cameras such as these allows an installation's security personnel to conduct an otherwise risky search from the safety of their guard house, far from the suspect vehicle. Largely because of their cost, immobility, and the time required to install, assets like the under vehicle inspection system are only implemented at fixed installations.

---

[56] Ibid.
[57] "Gatekeeper – Automatic and Under Vehicle Inspection Systems." Army-Technology.com, 2012.

Another way of reducing an installation's vulnerabilities is to increase the effectiveness of surveillance assets by making those assets more intelligent. Making them more intelligent refers to improving their identification and communication capabilities. Intelligent identification refers to a whole class of capabilities, nearly all of which are software related, that aid in managing the operator's workload and identifying IOIs. For example, one of the capabilities intelligent identification adds is the ability to identify IOIs it detects as being relevant or irrelevant to the human operator/security personnel. If relevant, the system would alert a human operator, if irrelevant the system would simply ignore the IOI it detected. The second capability that is an essential component of an intelligent surveillance system is improved communication between the different components of that system, communication which requires networking. A modern, intelligent, and networked surveillance system is capable of:

- motion detection
- classifying an IOI detected (e.g., person, animal, car, etc.)
- discerning between IOIs of interest to the operator and those which the operator would deem 'false alarms'
- discerning between IOI that are within the installation's perimeter and those outside of it (e.g., a camera mounted on the rooftop of an embassy that points towards the outer wall and main gate, outside of which is a sidewalk and busy street. The system needs to ignore any IOI detected outside of the wall and gate despite the fact that people and vehicles outside the gate are visible to the camera 24/7)
- communicating from one sensor to another that an IOI has been detected, after which all surveillance equipment capable of viewing that IOI automatically pan and tilt to do so (known as smart surveillance)

- tracking a single IOI from one sensor to the next, ideally doing so on a 2D overlay of the installation and surrounding area
- linking an installation's sensor feed in real time from the installation itself to nearby security or LE assets

All of the features and capabilities above can be easily implemented as part of an installation's surveillance package so long as that installation has either a hard or soft perimeter. While some of these features and capabilities cannot be used to monitor a dynamic perimeter, some can. Unfortunately, doing so would require the development of a system that is much more flexible and easy to setup than that which is required for a use in an installation that has either a hard or soft perimeter. Further complicating matters is the fact that an intelligent surveillance system monitoring an installation with a dynamic border must also be equipped with wireless power and communication.

Defensive Surveillance of Soft and Dynamic Perimeters – Tactical Airfields and Forward Operating Bases (FOB)

The Air Force operates almost exclusively from permanent installations while the Army and Marines operate extensively from installations with hard, soft, and dynamic perimeters. There is however one instance in which all three services perform a similar mission – the establishment of tactical airfields and FOBs. These are temporary installations typically constructed close to the front lines, and in some cases, behind enemy lines. Tactical airfields, like the one shown in **Figure 1.10**, allow transport aircraft to insert large numbers of troops and their heavy equipment where the enemy least expects it. They may also be used as a temporary airfield from which short-range attack and close air support aircraft and helicopters operate. FOBs are similar to

tactical airfields in that they sometimes have an airfield or helipad. What makes them unique is that they perform a wider variety of missions than tactical airfields. It is common for FOBs fulfill the role of a: command and control station, staging area for ground forces and close air support (CAS), fire support base (artillery), and resupply depot. A good way of think about tactical airfields vs. FOBs is that a tactical airfield can morph into a FOB. A FOB on the other hand cannot morph, via the addition of an airfield, into a tactical airfield; it simply becomes a FOB with an airfield. This is not a text book definition and others may disagree with it. It is based on the author's time in the Air Force as a loadmaster on C-5 aircraft[58].

Figure 1.8: C-130 Hercules landing on a tactical airfield[59]

[58]Several of the loadmasters the author served with have operated from tactical airfields in support of Tanker Airlift Control Elements (TALCE). TALCE is defined as a "…composite organization tailored to support airlift missions transiting locations where command and control, mission reporting, or support functions, as required, are nonexistent or require augmentation".
Global Security: Glossary I, Abbreviations and Acronyms. Global Security.org, March, 2013.
[59] "Tactical airfield landing" Wyoming Air National Guard: 153rd Airlift Wing, Cheyenne, WY, March 2013.

Both of these installations require ground forces to establish and maintain. The Army and Marines can and do establish both without assistance whereas the Air Force requires assistance to do so. Regardless, when either installation is initially established it will have a soft perimeter. If the airfield or FOB in question becomes semi-permanent it may transition towards having a hard or soft perimeter. Regardless of the scenario, tactical airfields and FOBs established using only airborne assets (ground troops and their equipment that are inserted via helicopters and/or aircraft) have nearly identical surveillance requirements.

FOBs and tactical airfields can and have been established in a variety of environments ranging from deserts to thick forests, each of which challenge surveillance systems operating in them with unique atmospheric and climatological challenges. A truly capable surveillance system should be easily transportable and capable of functioning, day and night, in any environment. With this in mind, any surveillance package used by airborne troops to establish the initial perimeter of a FOB or tactical airfield should:

- be capable of functioning day and night in all environments for a predestinated length of time[60] without (e.g., forest, desert, tundra, etc.) and atmospheric conditions (e.g., fog, rain, sandstorms, etc.)
- consist of individual components/assets that are lightweight and man-portable[61]
- consist of sensors designed with an emphasis on the detection[62] of IOIs (as opposed to the identification of them) regardless of the environment [63]

[60] Those sensors that are deployed several kilometers from the airfield will need to operate without maintenance or resupply until supplies are delivered. The time taken before these supplies are delivered could range from a single day to more than a week (data is approximated, no published timeframe could be found)..

[61] Installations established in a 'hot zone' are initially secured by troops who likely have limited or no supply lines, particularly if the installation being established is done so behind enemy lines. Either way, there is a premium placed on both the volume and weight of any gear carried by these troops.

- be capable of using existing military power sources and support/maintenance equipment

Although similar to FOBs without an airfield, any installation with an airfield must take into account additional considerations. A typical airfield will have a runway that is 3,500-4,500ft long with enough space for one or two large aircraft (if the airfield is used for transports, if not it may be much smaller, particularly if it only operates helicopters or vertical or short takeoff and landing (VSTOL) aircraft). When establishing an airfield, both the security of the airfield and that of the aircraft must be taken into account. To do so requires the establishment of a very large perimeter, particularly along the route taken by aircraft during takeoff and landing. Ideally, the surveillance system employed should be able to detect IOIs out to a range that completely prohibits the use of man portable air defense systems (MANPADS). This is a fairly large area considering the fact that most MANPADS have a range of 3.2 miles.[64] These conditions require any surveillance system deployed by airborne troops in support of a newly established installation with airfield should:

- be capable of detecting IOIs well beyond the maximum range, relative to the airfield, of any MANPADS believed to be deployed in the area
- be able to be quickly deployed, ideally before the airfield itself becomes operational

The requirements for newly established airfields and FOBs not constructed by airborne troops have nearly identical requirements to those above. The primary difference between the two is

---

[62] Detection is more important when establishing an FOB or tactical airfield due to the rural environment in which most of these installations are established. The potential threat posed by any IOI will require enforcement assets to intercept all IOI detected, regardless of their intention (think of the perimeter of a tactical airfield as that of any permanent military installation – visitors are not welcome!).

[63] The sensors deployed will vary depending on the environment (e.g., a desert airfield may use ground based radar while an airfield established in the jungle may rely on thermal cameras). Regardless of the environment and sensors employed, every non-sensor component should be generic (e.g., interface, networking, setup and teardown, etc.).

[64] "MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems" U.S. Bureau of Political-Military Affairs, July 27, 2011.

the fact that ground forces are not nearly as limited by or concerned about the weight and size of the surveillance system being deployed. Nonetheless, any surveillance system used to secure a dynamic perimeter will need to be extremely mobile, easy to setup, and easy to tear down.

When an installation transitions from having a dynamic perimeter to a soft or hard one, the requirements of that installation's surveillance system change as well. As the perimeter of an installation becomes permanent, less of an emphasis is placed on the mobility of that system. There is however a tradeoff. The more permanent an installation is the more likely an enemy is to know the location and vulnerabilities of it. Because of this, surveillance systems monitoring soft and hard perimeters must be more capable than those monitoring dynamic ones. For example, the longer an installation's perimeter is in place the more important it is to have quality surveillance – surveillance which can detect, identify, and classify IOIs at the same range previous, more tactical, systems could only detect them.

Defensive Surveillance of Hard and Soft Perimeters – Geopolitical Borders

Depending on whether or not it has a physical barrier, geopolitical borders may have either a hard or soft perimeter. The defense of geopolitical borders has always been one of the U.S. military's primary missions, a mission which had an early emphasis on the protection U.S. borders. This mission has evolved over the course of the 20th and 21st centuries to such an extent that, at present, most of the focus is now centered on the protection of foreign borders. Regardless of the border protected, the overall mission remains the same. Unfortunately this mission is not explicitly stated by the military; it is however a mission that can be derived based

on historical precedence.[65] Analysis of this precedence suggests that the mission of the military is to:

- prevent contraband, border violators, terrorists and terrorists weapons (including weapons of mass destruction) from crossing borders
- enhance border security
- secure and manage borders
- deter the enemy from taking offensive military action
- repel attacks made by the enemy
- defend friendly assets within the designated border from airborne attacks, whether those attacks are made by aircraft or missiles (e.g., the use of Patriot missile systems to shoot down Scud missiles fired at Israel during the first Persian Gulf War)[66]

As it was with DHS, surveillance an integral part of the broader mission of border protection. The major difference between the two is that military forces are far more concerned than their DHS counterparts with the detection, tracking, and identification of IOIs long before they cross or even approach the border. While there are a few DHS assets, such as maritime patrol aircraft and vessels, that attempt to detect, identify, and track IOIs before they enter U.S. territorial waters and/or airspace, there are no DHS assets that do so when monitoring land borders. Like the DHS, the military also attempts to detect, identify, and track maritime and airborne IOIs approaching a maritime perimeter; the military however must do the same for land borders. Unlike the DHS, military assets must also protect against the threat of rapidly approaching

[65] The specific cases analyzed are the protection of: the Saudi Arabian and Israeli borders during the first Persian Gulf War, Afghan-Pakistan border currently still under protection, the Korean Demilitarized Zone still under protection, and U.S. air and maritime 'space' during the Cold War.

[66] The reason for a distinction between this mission and the one above it is that this mission specifically applies to attacks made against assets within the perimeter that can be intercepted by or with the assistance of border defenses.

enemy aircraft and ground forces. Fortunately for the DoD, their budget is considerably larger than that of the DHS ($553.0 vs. $43.2 billion)[67]

The ability of the military to secure a border depends on the border in question, the number of friend forces deployed along that border, and the surveillance technology in use by those forces. The sheer number of troops that are often deployed to a warzone gives them a decisive edge over the DHS. Despite this, the military is not all that more effective in securing borders than DHS. One way to demonstrate this fact is to examine the narcotics imported to the U.S. from Mexico versus the narcotics exported from Afghanistan to Pakistan (in this case, smuggling is used as a gauge from which the relative surveillance capabilities of each organization can be approximated). Although the DHS has made progress towards securing the southwest border, it has failed to secure other POE, including seaports and airports. By comparison, military forces in Afghanistan have no ports and fewer airports to monitor, have access to more advanced technology, and have many times the personnel at their disposal. Despite these advantages, Afghanistan remains the world's leading producer of opium, most of which is smuggled across the border to Pakistan.[68] This comparison gives rise to the question: why is the military, in certain cases, less capable of securing land borders than the less equipped DHS?

There are many scenario specific reasons as to why the DHS is capable of doing more with less, but only one reason that is directly related to the surveillance equipment employed by each organization.[69] The surveillance equipment used by the DHS is larger, more robust, and in many

---

[67] "Department of Defense Federal Budget: Fiscal Year 2012." Office of Management and Budget, 2012. "Department of Homeland Security Federal Budget: Fiscal Year 2012." Office of Management and Budget, 2012.
[68] *National Drug Threat Assessment for 2011*. U.S. Department of Justice: Drug Enforcement Agency, August 2011. p. 27
[69] Some of the scenario specific reasons are: DHS personnel have more knowledge and experience, particularly in the case of CBP, than soldiers deployed to Afghanistan; DHS stationed along the southern border are monitoring more level terrain; the region along the southern border is much easier to navigate, largely due to the roads, than the

cases more, more capable than that used by the military. Why? Although their equipment is less advanced, the surveillance equipment possessed by DHS is not designed for universal deployment along a variety of borders[70], nor is not limited by its size and weight. As a result, the DHS can build permanent installations while the military is forced to use more tactical and mobile equipment. Moreover, military objects defended by soft perimeters do not benefit from the installation of infrastructure/defenses that have a symbiotic relationship with surveillance assets (e.g., triple layer fencing along the southern border allows surveillance assets to focus on the border's more permeable segments). This (symbiotic) relationship maximizes the capabilities of surveillance in two ways. First, it enables an installation's surveillance assets to provide more extensive surveillance of high threat regions via the installations of a greater number of fixed assets in those locations. Second, these barriers slow the advance of intruders, allowing mobile surveillance assets to cover greater ground than they otherwise would. However, as was stated above, the relationship established by the deployment of both barriers and surveillance assets is a symbiotic one. Regions in which surveillance assets saturate the landscape will require the establishment of far fewer barriers. As a result, those regions of the perimeter can be defended more extensively by them, increasing their effectiveness (i.e., assuming the availability of barriers remains constant, less barriers in one region allows for the greater use of them in another). More importantly, the installation of multiple barriers in a single location can act as a force multiplier. The imposing site of so many barriers in one location can act as a deterrent to would be intruders, reducing the total number of threats

---

rural region between Afghanistan and Pakistan; soldiers are required to work with their Afghan counterparts who have proven to be extremely corrupt; interdicting narcotics smugglers has become less of a goal given the dependency southern Afghans have on the harvesting of it (doing so only encourages them to support the Taliban more fervently).

[70] DHS has equipment specifically developed for use along the U.S-Mexico border. Military equipment is most often not tailored to function in specific location; rather it is designed to be flexible, allowing for its deployment in multiple theatres.

attempting to breach that installation over time. Finally, the establishment of a critical number or mass of barriers may effectively neutralize any possibility of threats breaching them, enabling the security personnel and surveillance assets defending that installation to concentrate their efforts along other regions of the perimeter (as the adage goes "he who defends everything defends nothing" (Fredrick II, aka Fredrick the Great)).

Defensive Surveillance of Dynamic Perimeters – Fleet Defense

The Navy has very unique surveillance demands that are tied to the mission of fleet defense. Both while in port and when at sea, naval fleets depend on surveillance systems to provide the intelligence necessary to take pre-emptive action against would be threats. Some of the assets used to provide intelligence in the defense of a naval fleet include radar, sonar, manned aircraft and helicopters, and UAVs. However, most of these assets are used in defense of the fleet while it is underway. There are scenarios in which the ships are not underway but those scenarios are few and far between. One such example is the use of thermal imaging equipment to monitor the waters around ships that are either in port or in the close proximity of one. This type of equipment can be used to detect personal watercraft and/or small boats approaching naval ships that may be, as was the case with the USS Cole, terrorists armed with high explosives. This is one of the few examples of video surveillance aiding in fleet defense, and in this case, an example of surveillance that could be performed by surveillance assets stationed at the port itself or onboard maritime security vessels (e.g., port security, Coast Guard, etc.). With this in mind, it is clear that the mission performed by naval assets at sea fall outside the scope of this chapter (surveillance provided when in port is more closely related that of critical infrastructure, not fleet defense). Moreover, the surveillance equipment used by naval vessels at sea are in an entirely

different class than those examined so far and are designed to fulfill a mission that is very different from that of the PSN).

Defensive and Offensive Surveillance of Dynamic Perimeters – Special Forces (SF)

SF is a very broad term that describes a whole range of groups that engage in special operations missions. The personnel who operate within these groups under take the most covert, high risk, and high reward missions there are. Some of examples of U.S. groups designated as SF are: Navy Seals, Army Green Berets, and the CIA Special Operations Group.[71] The surveillance requirements demanded by SFs, in this subsection, are broken down into two familiar categories: Offensive and Defensive.

Offensive surveillance is the type of surveillance undertaken either before an operation is launched or during an operation that is underway. However, surveillance gathered while an operation is underway can only be deemed offensive if that surveillance is directly related to the completion the successful completion of that mission (i.e., surveillance gathered for the sole purpose of gathering information and/or surveillance gathered by the SF's team in support of their assigned objective). An example of this would a SFs team conducting surveillance of a compound immediately prior to the storming of that compound. This type of surveillance can be provided via satellites, airborne assets, and personal surveillance equipment used by the SFs personnel themselves. The second type of offensive surveillance, that which is conducted prior to the launch of an operation, may be provided via satellite, airborne assets, and human intelligence (HUMINT) just to name a few. This type of surveillance can only be conducted prior to the launch of an operation but is surveillance that gathers intelligence which is critical to

[71] Washington, Douglas Waller. "The CIA's Secret Army." Time Magazine, February, 2003.
"Special Operations." Military.com, March 2013.

the planning and successful completion of that operation. The intelligence gathered prior to the launching of Operation Neptune Sphere is an excellent example. Prior to the launch of the U.S. Navy's SEAL Team 6, intelligence was gathered on Osama bin Laden's compound in Abbottabad, Afghanistan via three (known) sources: HUMINT provided by CIA operatives on the ground, satellites, and UAVs flying overhead.[72]

Defensive surveillance provided to protect SFs personnel is so closely related to offensive surveillance that the line between the two is blurred at best. For the sake of this thesis, defensive surveillance with respect to SFs is any surveillance which sole purpose is warning SFs teams of threats. This type of surveillance is the most dynamic of all surveillance covered in this chapter. The type of surveillance assets and scenarios in which those assets are used can vary from one operation to the next. With that in mind, an example would be the use of thermal cameras to guard the coastal region where SFs using ridged inflatables made landfall. The SFs that came ashore will want to hide their equipment, but even if they do so they it may be discovered. Even if it is not discovered, they may have been spotted coming ashore. Either way, the enemy may be waiting to ambush them upon return. The SFs team that came ashore could, theoretically, counter this ambush by detecting the enemy as they approach the region they came ashore via the use of concealed thermal cameras, cameras which are uplinked in real-time to the SFs team itself.

Offensive Surveillance using Mobile Assets

At first sight it would appear that offensive mobile surveillance assets (e.g., aircraft, satellites, unmanned ground vehicles (UGV), etc.) perform an entirely different mission than that of the

[72] Miller, Greg. "CIA flew stealth drones into Pakistan to monitor bin Laden house." The Washington Post, May 17, 2011.

PSN. However, as will be seen in chapter 5, there are variants of the PSN that provide a static form of offensive mobile surveillance that is capable of competing with its static brethren. Mobile or static, these assets fulfill a similar mission: the gathering of intelligence. Prior to the launch of any mission it is almost certain that attempts will be made to acquire intelligence; intelligence which can be used to assist in the successful completion of that mission. One form of gathering this intelligence is through the use of mobile assets capable of providing offensive surveillance. Airborne assets, both manned and unmanned, and satellites (though not technically airborne they are assets that provide similar capabilities from a similar 'perspective') are the two most common mobile assets used by the military to provide this type of surveillance (ignoring operational HUMINT). .

Of these two, satellites have the edge in terms of vulnerability. There are very few nations and organizations that are capable of taking out a satellite. An additional benefit of satellites is that they are capable of surveying large areas in a short time and at fairly rapid intervals.[73] This type of surveillance has its benefits but also its drawbacks. First, the resolution of the imagery provided by a satellite is not as high as that provided by assets closer to the ground (e.g., UAVs and manned aircraft). Second, the interval during which a satellite passes over a given region can be easily predicted by the enemy. This makes it much easier for the enemy to hide mobile assets. These are all deficits which can be overcome by the use of UAVs. UAVs can loiter over a single area for hours at a time, can take higher resolution pictures at shallower angles than satellites, and can arrive and depart the target area according to the operator's needs (as opposed to satellites and their predictable orbits).

Offensive Surveillance using Static Assets

[73] Depending on the type and altitude of orbit.

There are very few static assets used to provide offensive surveillance, particularly when the only ones examined in this chapter are assets against which the PSN can compete or augment (e.g., the PSN is designed to fulfill the same role or augment the capabilities of ground based radar spying on foreign aircraft as they take off and land hundreds of miles within an adversaries border). The only two that perform a mission remotely similar are micro-unattended ground sensors (UGS) and fixed surveillance cameras that are either operated on scene by covert personnel or remotely operated.

UGS come in many forms, but the ones that are most likely to provide offensive surveillance detect subtle sounds and/or movement around the sensors. Thousands of these sensors would be spread out behind enemy lines creating a large network. These sensors communicate amongst themselves and with friendly forces in friendly territory to determine the location of the approximate location of each sensor. A visual representation of this network would look like a fine mesh covering the area over which the sensors were dropped. When the data is gathered, it forms a network that can track objects (vehicles, personnel, etc.) as they pass through that network. This type of surveillance allows friendly forces to know the movement, location, and quite possibly the strength of enemy forces.

Although 100% fixed, remotely operated surveillance equipment is sometimes used behind enemy lines odds are they are micro-cameras that fulfill a different role than that of the PSN (or rather the concept on which the PSN is based). Man portable surveillance assets that are similar in size to the PSN do provide offensive surveillance, but the majority of those (that the author is aware of) are operated on scene. This use of surveillance equipment could be considered mobile or static, depending on how often it is moved. Ultimately there are only two attributes that determines whether or not a man portable and operated surveillance asset is classified as static.

First, the asset must be large enough to be considered as an alternative to the PSN (i.e., a mini, indoor sensor used to spy in the room next door doesn't count). Second, whether or not the asset in question gathers intelligence while it is in transit. Generally speaking, an asset designed to fulfill a role similar to the PSN is mobile if it gathers intelligence while on the move, static if it only gathers intelligence when fixed in place.

Scenario Table – Military

Scenario	Operator	Surveillance Mission	Objective	Preconditions	Type of Perim.	Perim. Length	Required Portability Rating	Required Setup and Teardown Rating	Required Endurance
Generic fixed base (Air Force base, Army fort, Navy base) equipped with long-range FLIR, Thermal Fence, and radar	All branches of the military	Defensive	Deter/Detain/Active Intercept	N/A	Hard	Varies, est. of 20000	2	2	N/A
Geopolitical border – Afghanistan / Pakistan	Army/ Air Force	Defensive	Detain/ Active Intercept	N/A	Soft	12000	4	5	N/A
Surveillance of a tactical airfield in the desert via the use of ground based radar and short-range FLIR	Air Force	Defensive	Detain/ Active Intercept	N/A	Soft/ Dynamic	Varies, est. of 9000	8	8	N/A
Surveillance in Afghanistan/ Pakistan via the use of UGS	Army/ CIA	Offensive	Covert Surveillance	N/A	Soft	8000	10	N/A	Varies, est. of 3650
Surveillance of SF during infiltration and exfiltration	SF	Defensive	Covert Surveillance/ Detain/ Active Intercept	N/A	Dynamic	Varies, est. of 500	10	10	Varies, est. of 0.1
Barry M. Goldwater Range Yuma, AZ Equipped w/ STS-12000 radar	Marine/ CBP	Defensive	Overt Surveillance/ Active Intercept	N/A	Hard /Soft	Est. 35000	1	1	N/A

Terrain Rating	Foliage Rating	Required Low Observ. Rating	Required Detection Range of Vehicles from Border	Required Detection Range of Humans from Border	Required Recognition Range from Border	Required Tracking Depth of Vehicles	Required Tracking Depth of Humans	Required Tracking Depth of Recognized IOI	Surveillance Budget
1	1	2	1000 m	1500 m	2000 m	3000	300	10	N/A
4	2	2	-200 m	5000 m	7000 m	4000	2000	10	N/A
1	1	2	500 m	1500m	2000 m	2000	500	10	N/A
4	2	5	500 m	1000 m	2500 m	2000	300	10	N/A
5	5	5	500 m	200 m	50 m	100	30	5	N/A
1		1	12000	6000	N/A	10000	8000	N/A	N/A

Table 1.7: Military scenario table

Scenario	Operator	Succ. Mission	Objective	Precond.	Type of Perim.	Perim. Length	Req. Port. Rating	Required Setup and Teardown Rating	Req. End.	Terrain Rating	Foliage Rating	Req. Low Observ. Rating	Required Detection Range of Vehicles from Border	Required Detection Range of Humans from Border	Req. Intent Specific Ident. Range from Border	Required Tracking Depth of Vehicles	Required Tracking Depth of Humans	Required Tracking Depth of Intent Specific IOI	Succ. Budget
Generic fixed base (Air Force base, Army fort, Navy base) equipped with long-range FLIR, Thermal Fence, and	All branches of the military	Defensive	Deter/ Detain/ Active Intercept	N/A	Hard	Varies, est. of 20000	2	2	N/A	1	1	2	1000 m	1500 m	2000 m	3000	300	10	N/A
Geopolitical border – Afghanistan / Pakistan	Army/ Air Force	Defensive	Detain/ Active Intercept	N/A	Soft	12000	4	5	N/A	4	2	2	-200	5000	7000	4000	2000	10	N/A
Surveillance of a tactical airfield in the desert via the use of ground based radar and short-range FLIR.	Air Force	Defensive	Detain/ Active Intercept	N/A	Soft/ Dynamic	Varies, est. of 9000	8	8	N/A	1	1	2	500	1500	2000	2000	500	10	N/A
Surveillance in Afghanistan/ Pakistan via the use of UGS	Army/ CIA	Offensive	Covert Surv.	N/A	Soft	8000	10	N/A	Varies, est. of 3650	4	2	5	500	1000	2500	2000	300	10	N/A
Surveillance of SF during infiltration and exfiltration	SF	Defensive	Covert Surv./ Detain/ Active Intercept	N/A	Dynamic	Varies, est. of 500	10	10	Varies, est. of 0.1	5	5	5	500	200	50	100	30	5	N/A
Nogales Arizona: 8 FLIR equipped SkyWatch towers guarding 10 miles of the southwest border (16.1 km)	CBP	Defensive	Deter/ Detain	N/A	Soft	16100	3	3	N/A	1	1	2	1000	1500	2000	3000	300	10	N/A
Single ~~SkyWatch~~ tower along the southern border equipped with STS 12000 radar	CBP	Defensive	Deter/ Detain	N/A	Soft	12000	3	3	N/A	1	1	2	-200	5000	7000	4000	2000	10	N/A
Three FLIR equipped ~~SkyWatch~~ towers, east of El Paso, between Quitman mountain and the border	CBP	Defensive	Deter/ Detain	N/A	Soft	9000	3	3	N/A	5	1	2	500	1500	2000	2000	500	10	N/A
Three FLIR equipped ~~SkyWatch~~ towers west of El Paso	CBP	Defensive	Deter/ Detain	N/A	Soft	9000	3	3	N/A	3	1	2	500	1000	2500	2000	300	10	N/A
Barry M. Goldwater Range Yuma, AZ Equipped w/ STS-12000 radar	Marine/ CBP	Defensive	Deter/ Active Intercept	N/A	Hard/Soft	Est. 37000	3	4	N/A	1	1	1	10000	8000	N/A	12000	6000	N/A	N/A

Figure 1.8: Chapter 2 master scenario table

Chapter 2: Analysis of Existing and Proposed Systems

Features, Capabilities, and Market

There are a whole range of surveillance systems currently in use by each and every one of the organizations examined in the previous chapter, most of whom operate multiple systems. Moreover, many of these organizations have one or more surveillance systems which have either been recently retired or are currently under development. Each of these systems typically employs a variety of different surveillance assets, assets which in some cases are used by more than one system. These assets are one of several components that, when combine, form a surveillance system. Over the course of this chapter these systems and their components will be analyzed to determine the features, capabilities, and market each of them possess. Some of the programs reviewed in this chapter are still under development, which means the contract for them has yet to be granted. In this case there are usually multiple manufactures submitting surveillance systems in hopes of winning the contract associated with that program. When this is the case, the first thing discussed is the program itself. Following this introduction, the various surveillance systems developed for that program are reviewed. Some of the assets and equipment reviewed in this chapter are sometimes employed both on larger assets as well as stand-alone systems/equipment. This type of equipment will be accounted for at the end of the assets chapter in two subsections entitled man-portable and standalone.

For reasons that are obvious, the surveillance assets and equipment reviewed in this chapter represent only a fraction of the total number of assets and equipment that are either in service, testing, or have been recently retired. The assets and equipment chosen for review have been selected based on the following criteria:

- the extent to which an asset is or has been used

- the impact resulting from the use of an asset
- the historical importance of an asset
- how the performance of an asset ranks relative like assets (e.g., the Predator and Darkstar are both large UAVs)
- the relationship between an asset and the condition/capability of an organization discussed in chapter 1 – assets eluded to or mentioned explicitly in chapter 1 are more likely to be reviewed
- how well an asset compares with another, already chosen asset (i.e., an asset may be selected for review primarily because it is in the same class as another, already chosen one; allowing for comparison between the two).

The need to develop a working database of assets and equipment has placed additional restrictions on which will be selected for inclusion and which will not. Originally, the hope was to develop a database that models a full range of surveillance assets, from UAVs to those that are man-portable. Recent research has numerous systems that are similar to the PSN, so numerous that even some of those will not be included. Based on this revelation, only those assets that are similar to the PSN (in both terms of cost and service) have been reviewed in this chapter. However, the variables and descriptions of them remain unchanged. This means that, if time allows, it is possible to add additional assets.

In addition to the criteria above, those assets and equipment designed by FLIR have been granted special consideration. FLIR, one of the largest manufactures of DoD and CBP assets and equipment, recently purchased ICx Technologies (ICx), another major manufacturer of assets

and equipment employed by the DoD and CBP.[74] The decision to give priority to FLIR and ICx assets and equipment is even more reaffirmed given the fact that FLIR was the major supplier of equipment used on/by ICx assets in the years preceding FLIR's acquisition of them.

Note: for the sake of this thesis, a distinction will be made between goods manufactured by these two companies despite the fact that ICx is a subsidiary of FLIR.

Conducting a thorough review of these systems is a necessary step in the design of the PSN. Depending on the surveillance asset being reviewed and the information that is available, the review of each will assist in determining:

- what features and capabilities customers expect in their surveillance systems
- what features can be harnessed for application onboard the PSN
- what capabilities the PSN must possess in order to succeed where current systems have failed
- whether existing systems are compatible with the PSN (i.e., co-operable)
- the ease with which an organization can transition from the use of their existing system towards that of the PSN
- how much organizations are willing to spend developing new surveillance systems
- the return, in terms of surveillance capability, customers expect from their financial investment

The review of surveillance systems in this chapter is broken down into two parts: surveillance assets and surveillance equipment.

[74] "FLIR Systems Announces Agreement to Acquire ICx Technologies." FLIR Investor Relations, August 16, 2010.

Surveillance Assets

The first part of the review process involves looking at the surveillance assets themselves. This review examines the chassis of the asset completely stripped of the actual surveillance equipment that can be or is installed on it. The review includes a general list of potential surveillance options, but nothing more. The review of each asset is concluded with a summary. Each summary is a condensed restatement of the most pertinent information within each asset's initial review.[75] Following the summary is a table that quantifies the data/capabilities of each. The variables quantified in this table are:

Name of Asset: The name of the surveillance asset or system being rated

Surveillance Mission: Indicates whether the surveillance conducted by an asset is offensive or defensive. If an asset is capable of both, both are listed in the table

Portability Rating: Indicates how portable an asset is. This rating is based on the size and weight of an asset. If an asset changes size and/or weight when it is being deployed, the size and weight of that asset in its stowed configuration is the data that should be entered. Finally, The portability of each system is rated on a scale from 1 to 10 with 10 being the most portable

Mobility Rating: The ability of an asset to traverse rough terrain based on the published capabilities of the asset in question and its design features (e.g., self-propelled vs. towed, wheel vs. tracked). This rating is takes into account the terrain rating of a particular scenario, rough terrains demand assets with higher mobility ratings. Mobility is rated on a scale from 1 to 5 with 5 being the most mobile

Note: Both mobility and terrain rating take are effected by the terrain rating from chapter 2. Moving forward, it is important to remember that 'required terrain rating' and terrain rating' are not exclusive to one another, as is the case with other, seemingly 'linked' ratings

Setup and Teardown Rating: This variable represents the maximum time and manpower required to initially setup and then later repackage an asset. Both the time and manpower to do so are rated on a single scale from 1 to 10 with 10 requiring the least time and manpower

Endurance Rating: The time, in days, that a surveillance asset can operate without resupply or maintenance

Low Observability Rating: Low observability rating is used to quantify how detectable, both when active and passive, a surveillance asset is with respect to other assets. Low observability is rated on a scale from 1 to 5, with 5 being the least detectable

[75] The information contained in the summary is not the only important information gathered from that review, merely a restatement of certain information in a different context. This information contained in the summary is not always explicitly defined in the review and/or features and capabilities. This information may be conclusions derived from the analysis of data contained in the review.

Ratio of Active to Inactive Service: The ratio between the time an asset is actively performing its mission versus total time (e.g., a UAV that can fly for 10 hours but needs 14 hours of service to redeploy has a ratio of 10/24, or 5/12. Another example is a system that can operate for 12 days but needs 2 days of service to redeploy has a ratio of 12/14, or 6/7). Assets that can operate continuously but require refueling and/or servicing to do so receive a rating of 1.0 as long as that asset can operate continuously while being serviced and/or refueled. Irregular service (e.g., repairs, upgrades, etc.) are not accounted for in this ratio

Operating Cost per Month: Total cost to operate an asset (e.g., manpower, maintenance, fuel, servicing etc.). This cost is calculated assuming the operational tempo of the asset under review is maximized. (e.g., a UAV takes off, lands, is serviced and/or receives regular maintenance, and takes off again without delay). Operating cost per month is rated on a scale from 1 to 10 with 10 representing the least expensive

Asset Cost: The cost of a single surveillance asset

Once all of the asset reviews are complete the review of surveillance equipment begins.

Surveillance Equipment

Whereas surveillance assets only looked at the chassis of assets, surveillance equipment only looks at the actual hardware that can be mounted on those chassis. The review of this equipment is broken down into sub-sections according to the type of equipment under review (e.g., thermal imaging vs. Radar). The reviews that follow are labeled according to their name and manufacturer. The reviews themselves are very brief. These reviews only contain information describing the strength, weaknesses and deployment for each piece of equipment. At the end of each review is a table that quantifies that equipment's capabilities. The variables quantified in this table are:

Terrain Rating: Terrain rating is used to quantify the effect terrain has on the capabilities of surveillance equipment. The main requirement that determines what terrain rating is required of a piece of equipment is 'required terrain rating' from chapter 2. This rating does not take into account how an asset's surveillance capabilities are inhibited on a terrain by terrain basis, only the general effect terrain has on an asset's surveillance capability relative to other assets. This rating varies on a scale from 1 to 5 with 5 representing the most capable of assets, those which are the least affected by terrain

Foliage Rating: Foliage rating is used to quantify the effect foliage has on the surveillance capabilities of surveillance equipment. As with terrain, the specific type and density of vegetation is not taken into account. Instead, this rating represents the extent to which any foliage inhibits the surveillance capability of an asset relative to other assets. Foliage is rated on a scale from 1 to 5, with 5 representing an asset whose surveillance capabilities are least affected by foliage

Detection Range of Vehicles: The range a surveillance asset can detect vehicles

Detection Range of Humans: The range a surveillance asset can detect humans

Identification Range of Vehicles: The range a surveillance asset can detect vehicles

Identification Range of Humans: The range a surveillance asset can detect humans

Identification of Recognized IOIs: The range a surveillance asset can identify vehicles or humans in enough detail to determine their intent (e.g., a smuggler vs. a farmer).by terrain

Equipment Cost: The cost for a single piece of surveillance equipment

Master Table – Surveillance Assets and Equipment in Harmony

At the end of this chapter there is a master table that contains a listing of the most common asset-equipment combinations. These combinations are labeled in this table under a column titled "Equipment Specific Asset" (e.g., a SkyWatch with STS-3000 radar and long-range FLIR would be titled "SkyWatch Equipped with STS-3000 and long-range FLIR". The capabilities recorded in the master table for each asset-equipment combination is based on the maximum capability of each piece of equipment used by that asset (e.g., if the STS 3000 radar has a detection range of 3 km and the FLIR only 2 km, the detection range recorded for that particular asset-equipment combination is 3 km. That said, since the radar has no ability to identify IOI, the value recorded in that row for identification is that of the FLIR). The unique surveillance qualities (e.g., the height of one asset vs. another) are accounted for in other asset-specific variables such as terrain rating. This table contains three additional variables that can only be quantified once an equipment specific asset has been chosen. The headings for these variables are:

Surveillable Area of Detection: The total area, in meters, an asset can provide full time surveillance capable of detecting and tracking of IOI. Area does not account for terrain (e.g., mountains limiting the coverage of ground radar). This variable applies almost exclusively to airborne assets[76], the surveillable area is calculated in one of two ways. Depending on the type of surveillance being performed, airborne assets will either fly a circular or linear

[76] Surveillable area of detection can also apply to other mobile surveillance assets but doing so would have much less of an effect. The reason behind having this object is to take into account the total area an asset can survey 'nearly uninterrupted'. The speed of airborne assets is substantially greater than that of ground or maritime assets, thereby allowing them to cover more ground in a short period of time (hence the 'nearly uninterrupted').

path. If an asset is providing either defensive or offensive surveillance around an installation or objective with a perimeter then the type of flight path flown is circular (i.e., orbital).

The surveillable area of detection is based on that assets detection range and the size of the perimeter being surveyed. If the mission performed is defensive surveillance, the surveillance asset flies a circular orbit that has a radius (from the center of the perimeter) that is equal to the radius of that perimeter plus that asset's detection range. The total surveillable area flown on a defensive mission is equal to: $A = \pi r^2 - \pi(a^2)$ where r is the orbital radius and a is the radius of the perimeter (see **Figure 2.1** for a visual). If the mission is offensive surveillance, the total surveillable area flown on a defensive mission is equal to: $A = \pi r^2 + b$where r is the orbital radius and b is the radius of the surveillance asset (see **Figure 2.2** for a visual).

If the asset is providing either offensive or defensive surveillance of a border, the total area that asset can survey is based on the asset's airspeed and detection range. The length of an assets detection range is based on the distance that asset, while flying a straight flight path that is parallel to the border, can fly before turning around and tracking along its path in such time that an IOI traveling at 50 km/h would only have travelled from the fringe of the assets detection range to a half way across the total width of the detection area (i.e., from the very border to just under the airborne asset). This calculation can be summarized as: $(((radius\ of\ detection)\ /\ (50\ km/h))\ /\ 2)\ *\ speed$ of the asset in km/h. For defensive surveillance, the asset flies so that its detection range just makes contact with the border (see **Figure 2.3** for a visual). For offensive surveillance, the asset flies along the border itself. (see the **Figure 2.4** for visual).

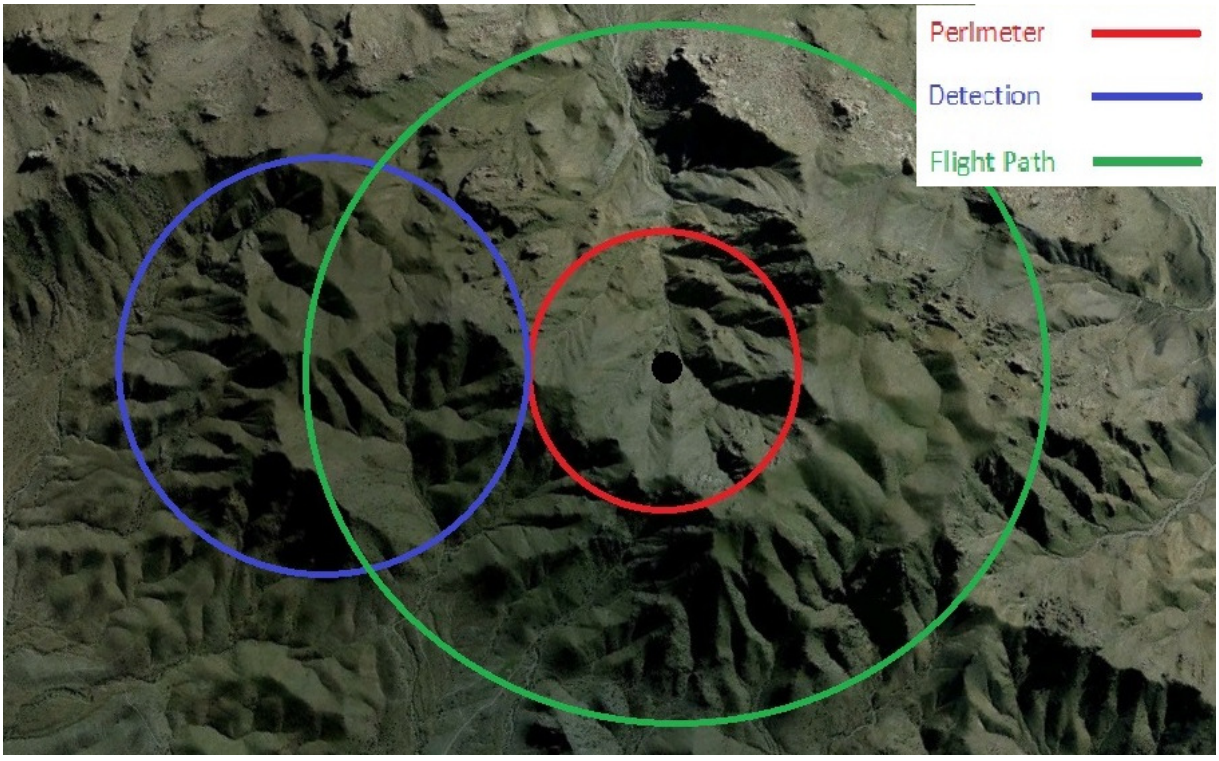

Figure 2.1: Defensive perimeter surveillance

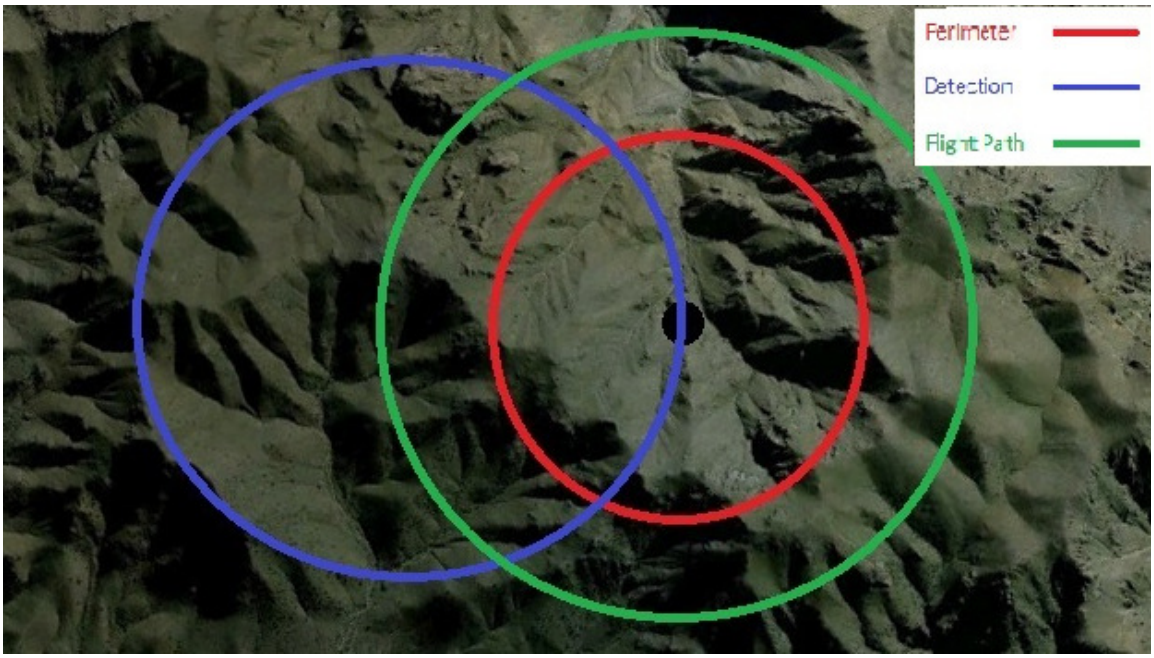

Figure 2.2: Offensive perimeter surveillance

Figure 2.3: Defensive border surveillance

Figure 2.4: Offensive border surveillance

Terrain Rating: Terrain rating is used to quantify the effect terrain has on the capabilities of surveillance assets. The main requirement that determines what terrain rating is required of an asset is 'required terrain rating' from chapter 2. This rating does not take into account how an asset's surveillance capabilities are inhibited on a terrain by terrain basis, only the general effect terrain has on an asset's surveillance capability relative to other assets. This rating varies on a scale from 1 to 5 with 5 representing the most capable of assets, those which are the least affected by terrain

Equipment Specific Asset Cost: The per unit cost of a single surveillance asset. Any systems that require more than one asset to operate must record the cost of each asset in its own row[77]

When assembled, the variables above form a table identical to the one below:

Equipment Specific Asset	Mission Type	Port. Rating	Setup and Teardown Rating	Endurance Rating	Detection Range of Vehicles	Detection Range of Humans	Recognition Range	Surveillable Area of Detection	Mobility Rating

Terrain Rating	Foliage Rating	Low Observ Rating	Ratio of Active to Inactive Service	Resiliency Rating	Personnel Cost Per Month	Estimated Maintenance and Resupply Cost Per Month	Total Operating Cost Per Month	Acquisition Cost Per Asset

Table 2.1: Sample performance table for surveillance assets

This table is the same one used to rate the capabilities of individual assets and equipment. Depending which is being reviewed, the unused columns are marked N/A.

Surveillance Assets

The reviews conducted in this chapter are limited to the generic platform of the asset itself. The features and surveillance equipment that can be or is installed are listed, but nothing more. Following the review of these assets is a table containing the data/capabilities of this equipment. The master table at the end of this chapter contains a listing of the most common asset-equipment combinations. These combinations are labeled in the scenario title (e.g., a SkyWatch with STS-3000 radar and long-range FLIR would be titled "SkyWatch Equipped with STS-3000 and long-range FLIR". The capabilities recorded in the final table for each asset-equipment combination is based on the maximum capability of each piece of equipment used by that asset

[77] This is referring systems that cannot operate without multiple components, but components that do not always share a set ratio between the two (or greater). For example, a system may require sensors an a communications uplink. If, in scenario one, the system uses 5 sensors per uplink the cost will be different than in scenario two which uses 15 sensors per uplink. To counter this problem, both the sensor and uplink must be logged as different surveillance assets. The uplink does not need to have all attributes filled out, only those which pertain to the complete system itself (in this case the range it can communicate with sensors and its per unit cost).

(e.g., if the STS 3000 radar has a range of 3 km and the FLIR only a detection range of 2 km, the detection range recorded for that particular asset-equipment combination is 3 km. That said, since the radar has no ability to identify IOI, the value recorded in that row for identification is that of the FLIR). The unique surveillance qualities (e.g., the height of one asset vs. another) is accounted for in other asset-specific variables such as terrain rating.

Mobile Surveillance Capabilities Program (MSC)

recently awarded contract: U.S. CBP

The MSC program is the first of two large contracts handed out by CBP after the cancellation of SBI. This contract, which was initially valued at $45 million, has risen in value of $102 million.[78] According to CBP, the goal of the MSC program is to develop and deploy assets that can:

"…provide area surveillance in rural, remote areas over a range of 8 to 12 kilometers. Capabilities are detection, identification, and tracking IOI until successfully ending in a law enforcement conclusion. Sensory equipment may include electro-optical/infrared cameras; ground surveillance radars; laser range finders; laser illuminators; global positioning systems; and command, control, and communication systems. The mobile nature of MSC allows Border Patrol to relocate surveillance assets based on changes in threat patterns and provides area coverage."[79]

This system employs the use of vehicles to rapidly deploy and redeploy advanced sensor equipment, equipment which is either towed behind or mounted on the delivery vehicle. This setup makes the MSC the most mobile, high-end surveillance asset CBP possesses – discounting

[78] Hock, Jessica. "FLIR Purchases ICx Technologies for $274 million." Oregon Business, August 16, 2010.
[79] *IT Program Assessment: Customs and Border Protection Mobile Surveillance System.* U.S. Department of Homeland Security: Office of the Chief Information Officer, March 2012. p. 1

their air and marine assets. A key distinction between the MSC and other surveillance assets deployed by CBP is the manned nature of the system. All but one of the potential contractors examined in this thesis put forward concepts which were manned, including the contractor who eventually won – FLIR. FLIR's entry, codenamed SkyWatch, is a derivative of the SkyWatch tower which has been manufactured by ICx for over a decade now.[80]

SkyWatch Manned Mobile Security System
developed by ICx

According to FLIR, there are currently 100 SkyWatch towers is service along the northern and southern borders, with additional towers in use with LE.[81] Unlike some of its competitors, SkyWatch is not a self-propelled system. It is towed to an area and then setup. Despite this shortcoming, SkyWatch is a proven, modular, upgradable, and mobile surveillance system. The only down sides to this system is that it is expensive, manned[82], limited in its ability to see over rough terrain, and difficult if not impossible to deploy on rough terrain. The core component of the SkyWatch system is the tower, one version of which can been **Figure 2.5** on the next page. These towers come in three models: generic, Sentinel and Frontier. The only major differences between the two final assets are that the Frontier is designed for longer deployments, can carry a wider variety of sensors, and is better equipped to function as command and control center (than the Sentinel).

[80] ICx is a recently purchased and now wholly owned subsidiary of FLIR, one of the world's premier manufacturer of military grade surveillance equipment.
[81] *White Paper: The Secure Border Solution*. ICx Technologies, February 2013. p. 4
[82] Some SkyWatch towers are manned, some are not. Based on research conducted into their use by CBP, I have come to the conclusion that the majority of the towers operated by CBP are manned.

Figure 2.5: SkyWatch towers in use by CBP. Note the second tower on the right, and what is likely a third even further down the road[83]

The generic SkyWatch towers have been in production for over 10 years. These towers are not equipped with the high-end sensors available on the other two nor were these the models that won the MSC contract. With that in mind, the Sentinel and Frontier did compete for it. These two towers are the same height (25ft), can be ordered with either a one or two person cab, and can be equipped according to the needs of the operator.[84] Some of the features typically found on the Sentinel and Frontier towers are:[85]

- short and medium range radar
- thermal cameras
- public address systems
- ability to record data from all monitoring devices
- ballistic resistant plating

[83] *White Paper: The Secure Border Solution*. ICx Technologies, February 2013. p. 1
[84] SkyWatch data sheet and brochure. FLIR, February 2013. p. 2
[85] Ibid. p. 2

- solar and diesel power
- command and control suite
- communications technology (e.g., Wi-Fi, cellular, satellite, etc.)

When equipped with the right combination of these features, the SkyWatch Frontier, the model that has been purchased by CBP, is an exceptionally effective system that should be capable of fulfilling the goals expected of it as winner of the MSC contract. Unfortunately, if **Figure 2.5** is any indicator, it appears that some of these towers have either not been equipped with the necessary features or the installed features are not being fully utilized.[86]

Figure 2.5 depicts several SkyWatch towers arrayed side by side along a rural road. The MSC program stated that a single MSC asset should have rural area surveillance capabilities that enable it to detect and identify IOI at a range of 8 to 12 km. This is clearly not the case with the CBP towers depicted in **Figure 2.5**. If this image is any sign of how these towers will be deployed in the future then their deployment is and will continue to be a misappropriation of resources. Finally, these towers are not cheap. It was reported that a LE version, which lacked both radar and FLIR cameras, was purchased for $119,000 by the San Diego Police Department using funds provided to them via a miscellaneous DHS grant.[87] Considering the type of sensor systems (e.g., radar, FLIR, etc.), armor, and communications employed on the CBP versions of SkyWatch Frontiers, it would not be surprising if the generic legacy towers cost $250,000 or more. One this is certain: the fixed price of each 'stripped' tower purchased by the U.S. government.

---

[86] It is not clear what type of tower is depicted in Figure 2.5. If these are the generic, legacy towers that have been around for over a decade, the deployed with which they have been deployed would make more sense. However, it does appear that these towers have been upgraded with high-end imaging equipment. It is important to acknowledge that this picture was taken from a 2013 ICx white paper on border surveillance, something that suggests these are the newer models.

[87] Davis, Katrina. "Police to buy mobile observation tower." U-T San Diego, March 2, 2009.

In 2005 ICx signed a contract with the General Services Administration (GSA). This contract fixed the acquisition cost of various ICx assets purchased by the government from 2006-2012. In this document there are several assets reviewed in this chapter, seven of which are different versions of SkyWatch towers:[88]

- SW - 1002 PLATFORMS SkyWatch Sentinel $73,171.28
- SW - 1003 PLATFORMS SkyWatch Frontier $87,770.78
- SW - 1005 PLATFORMS SkyWatch Frontier - Level National Instituted of Justice (NIJ) III Antiballistic Cab $139,806.17
- SW - 1006 PLATFORMS SkyWatch Frontier - Level NIJ IV Antiballistic Cab $165,149.50
- SW - 2003 PLATFORMS SkyWatch Frontier (two man cab) $110,402.78
- SW - 2005 PLATFORMS SkyWatch Frontier 2 Man - Level NIJ III $165,013.24

Examination of pictures taken clearly show that the type of towers purchased by CBP are the $165,013 2 man Frontiers with NIJ level III ballistic protection.[89] However, many of these could be legacy towers that have been upgraded with a new cab containing , which when outfit with various types of equipment, could run well over half a million dollars. The seventh and final 'version' of interest described in the previous paragraph is product MSS-MSP-LR PLATFORMS Mobile Sensor Platform $737,546.39. There is very little information surrounding this system which, since it is included in this document, predates the MSC contract. Nonetheless, the

---

[88] *GENERAL SERVICES ADMINISTRATION FEDERAL SUPPLY SERVICE AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST, CONTRACT NUMBER:GS-07F-0117U,* U.S. General Services Administration, 2005. p. 111

[89] **Figure 2.5** highlights the use of this ballistic protection. The standard Frontier cab is flush with the windows; cabs outfitted with ballistic plating are not flush and noticeably protrude from the cab.

additional info in this document confirms that a 2013 MSC equipped SkyWatch would cost at least $750,000, if not more.[90]

Summary

The SkyWatch has the potential to meet the criteria expected of it as the winner of the MSC contract, only time will tell. The cost of an individual SkyWatch tower is a major deficit. However, the fact that these towers are based on platforms already possessed by CBP should make their integration with other assets easier than it otherwise would be. In the long-term, the decade-old SkyWatch towers could be outfit to MSC standards for less than the cost of a new Frontier or Sentinel. When it comes to mobility, SkyWatch is the most mobile high-end surveillance system possessed by CBP. Unfortunately, its mobility and ability to provide surveillance over large areas has limitations, limitations which may inhibit or completely prohibit its use in mountainous terrain. Perhaps the most appealing feature of SkyWatch is its ability to act as a mobile command and control center, a capability that CBP did not possess before institution of the MSC program.

Features and Capabilities:

- mobile
- 1 to 3 person crew
- 8-12 km detection and identification radius (on relatively level terrain)
- 2-3 km detailed identification radius (est., on relatively level terrain)
- capable of operating for 300 hours without resupply[91]

[90] The cost estimate of $750,000 is based on an in depth review of the ICx/GSA contract. This contract includes all options, including sensors and communications equipment that would be used on an MSC equipped SkyWatch.
[91] The actual endurance of all assets reviewed in this chapter depend on what sensors are equipped.

- short-range radar (capable of detecting both individuals, ground vehicles, and ultra-lights)
- thermal, IR, and conventional cameras
- public address systems
- ability to record data from all monitoring devices
- ballistic resistant plating
- solar and diesel power
- command and control suite
- communications technology (e.g., Wi-Fi, cellular, satellite, etc.)
- per unit cost: $80,000 to $750,000

Performance Matrix:

Asset or System	Mission Type	Port. Rating	Setup and Teardown Rating	Endurance Rating	Detection Range of Vehicles	Detection Range of Humans	Recognition Range	Surveillable Area of Detection	Mobility Rating
SkyWatch	Def.				N/A	N/A	N/A	N/A	

Terrain Rating	Foliage Rating	Low Observ Rating	Ratio of Active to Inactive Service	Resiliency Rating	Personnel Cost Per Month	Estimated Maintenance and Resupply Cost Per Month	Total Operating Cost Per Month	Acquisition Cost Per Asset
								N/A

Table 2.2: Performance matrix for SkyWatch

ThreatSTALKER Surveillance System (TSS)

developed by Telephonics

The TSS, see **Figure 2.6** below, is an evolved version of the system developed by Telephonics Corp. in its bid to win the MSC contract. The first noticeable difference between this system and

Figure 2.6: ThreatSTALKER with partially retracted sensor suite[92]

SkyWatch is that TSS is self- propelled. This system has the capability to be outfit with all of the same sensors used by the SkyWatch.[93] It does however lack some of the command and control capability[94] and cannot remain on sight as long without resupply (diesel tank is not as large). The entire system, which weighs 3,800lbs, sits on a two axle, flatbed truck that itself weighs 6,500lbs. Although Telephonics lost the MSC contract, the TSS's comparatively low weight and extreme mobility make it an excellent choice for operators who work in a more dynamic environment, such as the U.S. military.[95]

The second major difference between the TSS and SkyWatch is that TSS is only designed to accommodate two operators. These operators are required to work from a 15" display that can

[92] *Telephonics: Ground Surveillance Radar and Long Range Systems.* Armed Forces International, 2012. Accessed March 3, 2012 from: http://www.armedforces-int.com/suppliers/air-traffic-control-systems.html
[93] *Mobile Surveillance Capability.* Telephonics Corporation, 2012. p. 2
[94] ThreatSTALKER still has the ability to act as a command and control vehicle, one that could be equipped to mirror the capabilities of SkyWatch. However, SkyWatch's superior ergonomics and its ability to sustain long-term deployments make it a better choice for use as a command and control asset
[95] Oddly enough, different variants of the SkyWatch towers are already in service with the military while no information exist that suggest the military has purchased a single TSS. One possible explanation of this phenomena is that the military already has multiple contracts with both FLIR and ICx.

be used from inside or outside the vehicle.[96] By comparison, the SkyWatch system can carry up to three operators in a much larger space, all of whom interface with a display much larger than that equipped on TSS. Moreover, these operators are able to use their own eyes to survey the terrain, a feature not found on the TSS.

Summary

TSS is a system that fulfills the gap between semi-mobile assets like SkyWatch and completely mobile, less equipped assets. Although not the ideal asset for sustained surveillance, it is ideal for scenarios in which a more mobile, yet still very capable, surveillance asset is required.

Features and Capabilities

- highly mobile
- 2 person crew
- 8-12 km detection and identification radius (on relatively level terrain)
- 2-3 km detailed identification radius (est., on relatively level terrain)
- short-range ground radar
- thermal cameras
- electro-optical cameras
- ability to record data from all monitoring devices
- ballistic resistant plating
- solar and diesel power
- 150 hour endurance without resupply
- command and control suite

[96] "Telephonics: Ground Surveillance Radar and Long Range Systems." Armed Forces International, 2012.

- communications technology (e.g., Wi-Fi, cellular, satellite, etc.)
- per unit cost: not available, likely $200,000 or more

Performance Matrix:

Asset or System	Mission Type	Port. Rating	Setup and Teardown Rating	Endurance Rating	Detection Range of Vehicles	Detection Range of Humans	Recognition Range	Surveillable Area of Detection	Mobility Rating
TSS	Def.				N/A	N/A	N/A	N/A	

Terrain Rating	Foliage Rating	Low Observ Rating	Ratio of Active to Inactive Service	Resiliency Rating	Personnel Cost Per Month	Estimated Maintenance and Resupply Cost Per Month	Total Operating Cost Per Month	Acquisition Cost Per Asset
								N/A

Table 2.3: Performance matrix for the TSS

Cam-V Mobile Security System

developed by Advanced Security Products (ASP)

The Cam-V, developed in Texas by ASP, stands out from its competitors, SkyWatch and TSS, in that it is entirely unmanned. Indications are that the Cam-V was ruled out as a potential candidate for the MSC contract early on, but this in no way diminishes the worth of the system. It is however considerably less capable than both the SkyWatch and TSS. Moreover, there is the possibility that the Cam-V will win or at least be considered for another one of CBP's outstanding contracts, the Integrated Fixed Tower program (IFT).

The Cam-V can be outfit with an array of sensors from static, long distance IR cameras to FLIR cameras. These cameras are mounted on a 23ft mast (see **Figure 2.6** below), not far off the 25ft mark set by TSS and SkyWatch.[97] Unfortunately, the Cam-V cannot be equipped with either radar or high-end FLIR. This limits its nighttime detection of IOI to roughly 2,000ft and identification to only 500ft.[98] It also lacks the command and control capabilities of the other two systems. Despite these drawbacks, the Cam-V

[97] *Cam-V Mobile Security System Spec-Sheet*. Cameras Onsite, 2013 p. 2
[98] Ibid. p.2

does have two distinct advantages over both the TSS and SkyWatch: endurance and cost.While TSS and SkyWatch measure their endurance by the hour (30 to 150), the Cam-V can operate a full month without support.[99] This makes the Cam-V an ideal choice in regions that require considerable effort to setup, maintain, and take down a surveillance system. Unfortunately, being unmanned the Cam- V may be a more tempting target for vandals than its competitors. The system is equipped with an automated alarm and motion detection that, when triggered, audibly warns those who approach with either a siren, pre-recorded message, or a live message sent from an off-site operator. However, if vandals/threats ignore this warning it may only give them further cause to take out the system (particularly at night when it may otherwise be hard to see).[100] With this in mind, the Cam-V cost between $39,000 and $70,000[101], considerably less expensive than both the TSS and SkyWatch.[102]

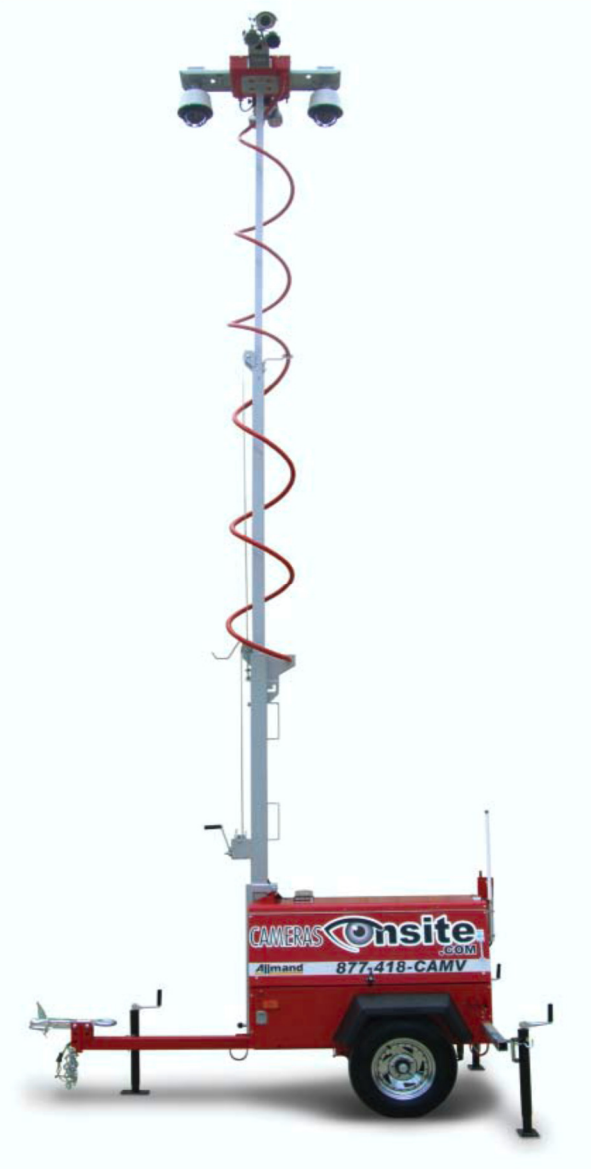

Figure 2.7: Cam-V fully deployed[103]

[99] Gunter, Ford. "Local Firms Mobile Surveillance System Could be Border Solution. Houston Business Journal, 2012.
[100] Ibid. p. 2
[101] When considering cost it is more reasonable to presume that CBP would purchase the highest trim Cam-V possible since it is the only one that has capabilities remotely approaching those of either the TSS or SkyWatch.
[102] Gunter, Ford. "Local Firms Mobile Surveillance System Could be Border Solution. Houston Business Journal, 2012.
[103] The Cam-V in the picture is equipped with defensive dome security cameras, low-equality thermal imaging equipment, and standard (high-quality) long-range day time optics.
Cam-V Mobile Security System Spec-Sheet. Cameras Onsite, 2013 p. 1

Summary

The Cam-V is an excellent choice for mobile surveillance in almost any terrain. Its most defining and appealing feature is also the one that is the most inhibiting: like the SkyWatch, it is not a self-propelled. The advantage the Cam-V has over the SkyWatch is that it is smaller, a quality that makes it less expensive, easier to transport, and easier to deploy. The size of the Cam-V means that nearly any vehicle operated by the military, public, or private sectors is capable of transporting it from location to location.

Performance Matrix:

Asset or System	Mission Type	Port. Rating	Setup and Teardown Rating	Endurance Rating	Detection Range of Vehicles	Detection Range of Humans	Recognition Range	Surveillable Area of Detection	Mobility Rating
Cam-V	Def.				N/A	N/A	N/A	N/A	

Terrain Rating	Foliage Rating	Low Observ Rating	Ratio of Active to Inactive Service	Resiliency Rating	Personnel Cost Per Month	Estimated Maintenance and Resupply Cost Per Month	Total Operating Cost Per Month	Acquisition Cost Per Asset

Table 2.4: Performance matrix for the Cam-V

Important Information Regarding the Reviews of the Remaining Assets

The task of rating surveillance assets required far more time than initially expected. As a result, the only assets that have undergone intense review are those above. The following assets and programs are brief descriptions that, at most, include a picture of the system. In most cases however there is only a sentence or two for each.

Integrated Fixed Tower Program (IFT)

outstanding contract: CBP

IFT is the second of two large, outstanding contracts up for award by CBP as part of the post-SBI initiative. The driving force behind the acquisition of these towers as described by DHS is:

> "…to provide commercial-off-the-shelf/government-off-the-shelf solutions for deployment at fixed, elevated sites, hereafter referred to as integrated fixed towers that would provide automated, persistent, wide area surveillance, the detection, tracking, identification, and classification of illegal entries."[104]

The concept behind the IFT is the use of unmanned towers, towers which are almost exclusively equipped with radar, and in most cases radars manufactured by ICx. The exact range and cost of an individual IFT system depends on the asset's manufacturer and equipment installed (e.g., STS-350, STS-1400, STS-12000, etc.) on it, but the current contract is for $98.1 million[105]. The following are a few of the entries submitted for consideration by CBP (Cam-V is not included in this review but is a possible contender):

Integrated Fixed Tower Border Surveillance System (IFTBSS)

developed by Telephonics

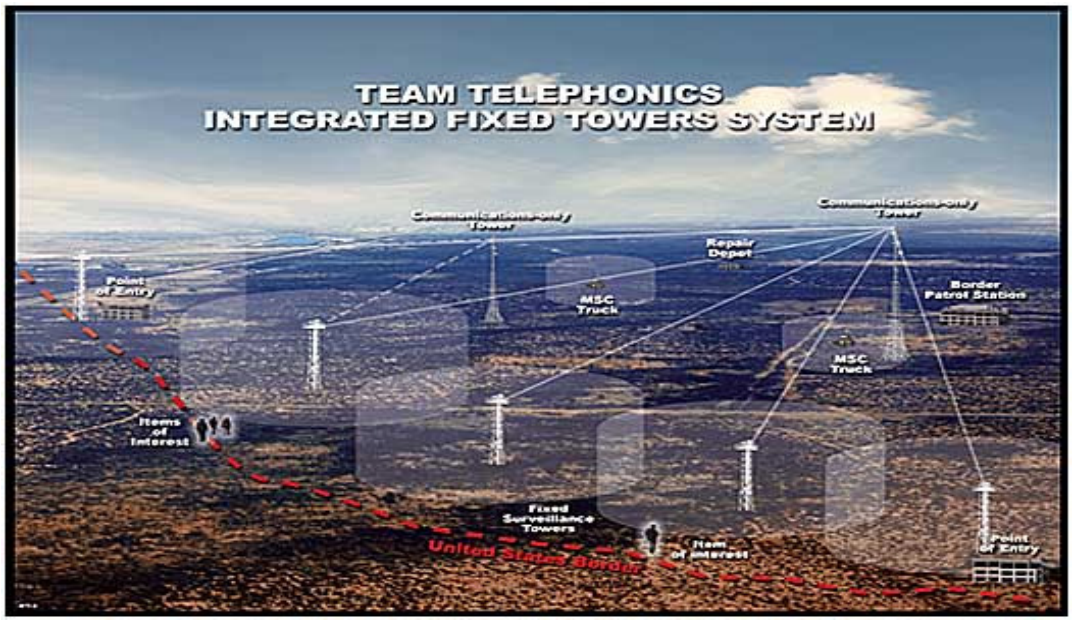

Figure 2.8: Telephonics IFTBSS network demonstration[106]

[104] "Integrated Fixed Towers." Federal Business Opportunities Office, January 2011.
[105] Ibid.
[106] "Ground Surveillance Systems IFT" Telephonics, March 2013.

Cerberus Unmanned Surveillance Tower System

developed by ICx

Figure 2.9: Cerberus IFT in the deployed position[107]

Summary

The IFT contract is similar to the MSC but may be an even more valuable and effective surveillance asset, particularly when the scenario requires a rapidly deployable system that can be delivered via a medium sized transport aircraft (e.g., C-130).

[107] "ICx Technologies Inc." Security Technology News, April 2013.

Remote Video Surveillance System (RVSS) and Agent/Man Portable Security System (APSS)

Both the RVSS and APSS are contracts that CBP funded as part of the alternative SBI program. The primary difference between the two is that one is man portable while the other is remotely operated. Both assets are intended to provide surveillance via the use of electro-optical cameras (e.g., thermal, image intensifying, simple low-light digital).

Unmanned Aerial Vehicles (UAVs)

The use of UAVs by both CBP and the military has risen considerably over the past decade. Current use of UAVs in places like Afghanistan outpaces the manufactures ability build them, a fact which has taken what was once a low production asset and turned it into a virtual assembly line of relatively inexpensive surveillance assets.[108] Not only are UAVs less expensive to purchase, they are also far less expensive to operate than manned aircraft. The cost of acquiring and operating them has dropped low enough to allow for their use by organizations, like CBP, that have been traditionally unable to acquire the same expensive, high-end surveillance assets used by the military. The surveillance capability of UAVs varies widely depending on the type of asset and the equipment installed on it. The UAVs presented in the next few pages are from more than one 'class' of asset; some of them cost less than a million dollars while others that are far more capable and survivable cost tens of millions of dollars and are capable of both detecting, tracking, and engaging IOIs. The first of these unmanned aircraft to be introduced is that which has become the most recognizable in the world, the Predator.

[108] Cost is relative to that of a manned aircraft capable of delivering a similar level of surveillance.

General Atomics RQ-1 (AKA MQ-1A) Predator

Figure 2.10: RQ-1 taking off in Afghanistan[109]

General Atomics MQ-9 (AKA the MQ-1B) Predator

Figure 2.11: MQ-9 armed with laser guided bombs[110]

[109] "Factsheet: MQ-1 Predator Unmanned Aerial Vehicle." U.S. Air Force, November 5, 2008.

Lockheed Martin RQ-170 Sentinel

Figure 2.12: RQ-170 rendering based on images of a RQ-170 shot down over Iran[111]

Manned Surveillance Aircraft and Helicopters

Similar to UAVs, many models of manned aircraft have been developed by multiple manufactures and are in service with multiple organizations. The aircraft and helicopter presented on the next page represent only a small fraction of those currently in service.

[110] "Factsheet: MQ-9 Reaper." U.S. Air Force, January 5, 2012.
[111] "Iran Shows Film of Captured US Drone." BBC World News, December 8, 2011.

Lockheed Martin P-3 Orion

Figure 2.12: P-3 at Lockheed Martin's Greenville facility[112]

UH-60 Blackhawk

Figure 2.13: CBP UH-60 at Dover Air Force Base Dover, DE[113]

[112] "Greenville Operations." Lockheed Martin, April 2013.
[113] "Customs Blackhawk from Tucson Air Branch at Dover A.F.B. to provide air security." Customs and Border Protection, April 2013.

Additional Surveillance Assets

The surveillance assets below are either platforms that do not fall within one of the prescribed categories or they are assets which augment other assets in an indirect manner.

Micro-UGS

FLIR Thermal Fence

ICx Deployment Rapid Deployment Software

Micro-UAVs

Reviews of Surveillance Equipment

Preliminary Introduction to Surveillance Technologies

The surveillance equipment reviewed in this chapter are organized into sections based on the type of technology each them uses. Prior to a review of the individual pieces of surveillance equipment is a brief introduction to the parent class to which that equipment belongs. First however is an introduction to some broader technologies that apply across the board to two or more of these sections.

Generic Technologies:

Optical Zoom: This is the type of magnification used by most of the daytime optics sold to consumers. It functions by adjusting the focal length. The quality/resolution of the image generated by this type of camera is the same regardless of whether it is zoomed or not. The only things that reduce the quality of a camera using optical zoom is the size of the lens, the quality of the lens, and atmospheric conditions.[114]

[114] There are other limitations that could be taken into account if using optical zoom in a place like space. These however are the variables that most affect optical zoom under standard atmospheric conditions (on or close to the Earth's surface).

Digital Zoom: This is the type of zoom used on commercial cell-phones. The image being magnified has a preset resolution that is defined by the number pixels in that image. Digital zoom does not sharpen the overall image itself, it only magnifies the individual pixels that make up the larger image. As the digital zoom of an image increases the quality/resolution of that image decreases.

Surveillance Equipment

Forward Looking Infrared (FLIR)

This technology is used in surveillance components to generate an image day or night. FLIR is synonymous with thermal imaging. Cameras that employ this technology create an image based on the subtle differences in temperature of the objects in that cameras field of view (FOV).[115] This technology is excellent at detecting and identifying objects at night or in cooler regions. The closer the temperature of the surrounding terrain is to that of the IOI the more difficult it is to detect and identify that IOI.[116] FLIR cameras range in price from several thousand to over a hundred thousand dollars, depending in large part on the resolution of the camera (which is directly related to the number of thermal reflectors, the truly expensive part of thermal cameras). Since FLIR cameras create an image without needing to generate their IR light they are extremely energy efficient.[117]

Some examples of FLIR equipment and their cost are:

FLIR 432-0010-01-00 MD-324 Static Thermal Night Vision Camera - $3,036

[115] "What's The Difference between Thermal Imaging and Night Vision?" FLIR Systems, Inc., 2013.
[116] Email correspondence with PTZ systems.
[117] "What's The Difference between Thermal Imaging and Night Vision?" FLIR Systems, Inc., 2013.

PTZ M-1D - $4,000-$15,000

Pelco / Schneider Electric - ESTI335-5N - Ip/analog P/t Thermal Camera 384x288 Res, 120/230vac, 35mm Lens, Pedestal Mount - $16,327

Samsung Techwin - SCB-9051 - Analog Thermal Imaging Camera, 20x240 - $8,721

Samsung SCB-9080 50mm Lens 1.2Km Range Weatherproof - $7,479

US Night Vision ATAC 360º Wireless Pan/Tilt 000615 - $6,995

Unfortunately there wasn't enough time to gather and present data on all this equipment. The important thing to take away from this section is that the FLIR/thermal equipment shown here is expensive, very expensive. Most of the equipment above, despite being expensive, is only capable of detecting humans inside of 800m and recognizing them inside of 200m.

Infrared LED Imaging (IR LED)

IR LED cameras (aka Near-Infrared Illumination cameras) are day time cameras that, when used at night, transition from seeing in color to only black and white.[118] These cameras rely on IR light generated by the camera itself. This light is generated by several LEDs that surround the camera. Typical IR LED cameras can only see between 50 and150ft at night. Moreover, the image generated is low quality and the power required to run them is high (because they generate their own IR light).[119] The advantage to using IR LED cameras is that they are extremely cheap compared to other night vision cameras, ranging in price from $35 to $500.

[118] "How Night Vision Works." Sofradir EC Night Vision Systems, 2013.
[119] "What's The Difference between Thermal Imaging and Night Vision?" FLIR Systems, Inc., 2013.

Image Intensifying

Cameras that employ image intensifying technology are nothing more than extremely sensitive daytime cameras. These cameras are usually referred to as Night Vision Goggles (NVG).[120] An NVG camera works by magnifying the miniscule amount of visible light present at night to such an extent that it produces an image.[121] The image produced by NVG cameras is the classic green and black usually used by military forces on the ground or in the air (e.g. the large binocular goggles used by helicopter pilots to see at night). The short coming of these cameras is that they do not work well in environments almost completely void of ambient light (e.g., in the desert that is hundreds of miles from the nearest city on a moonless night).[122] The picture quality generated and viewable distance NVG cameras can see varies depending the generation of NVG used. High-end NVG cameras are Gen-3 with illuminators, also known unofficially as Gen-4. One of the major benefits of using NVG technology is that it can be combine with traditional devices to generate clear, optically zoomed, images, the type of technology perfect for use as either a spotting or rifle scope. This technology is less expensive than thermal but substantially more than IR LED (several hundred to several thousand dollars). Finally, these cameras/optics are typically only used by military and law enforcement personnel.

There wasn't enough time to catalogue even a few of image-intensifying cameras on the market, but they are a serious technology to consider when creating a new breed of surveillance systems. However, after a careful review of the surveillance equipment on the market it was found that not a single one of them that uses image-intensifying technology are designed for use as a fixed, defensive surveillance system. This fact suggests that there may be some downside to using

[120] Ibid.
[121] "How Night Vision Works." Sofradir EC Night Vision Systems, 2013.
[122] Ibid.

them in this manner, a downside that the research performed in the writing of this thesis has failed to uncover.

Ground Based Radar

There are many varieties of ground based radar, each of which has its limitations. Some of these radars are over 30 m tall and have a range of 80 km, others are man portable and have a range of only a few hundred meters. Similarly, some radars are capable of detecting a man slowly crawling while others can detect objects moving through dense foliage several km away. All of these radars have one thing in common: they are all only capable of detecting and tracking IOIs. The following is a list of radars made by ICx, each of which is named according to the maximum range of that particular system (e.g., a STS-350 has a range of 350m). Unfortunately, the STS-350 is the only system for which procurement and operational cost could be found.

STS-350

Figure 2.14: STS-350 ground based radar[123]

[123] *White Paper: The Secure Border Solution.* ICx Technologies, February 2013. p. 6

The prices below only reflect the cost of the radar itself, not the additional equipment that is required to make it operational. Also, these prices have been taken from the company webpage which was advertising a buyback and upgrade program which means they may or may not be the standard price or the price that ICx has negotiated with some of its larger customers.

Trade in value per STS-350 radar (regardless of condition) - $13,450.

New STS-350 EP model radar with trade - $15,990.

New STS-350 ER (700m) model radar with trade - $18,990.

All new STS-350 & STS-350ER radars include the latest hardware and software and a full 12-month limited warranty

STS-1400

Figure 2.15: STS-1400 ground based radar[124]

[124] *White Paper: The Secure Border Solution.* ICx Technologies, February 2013. p. 6

STS-12000

Figure 2.16: STS-12000 ground based radar[125]

Summary Analysis and Matrix

As was the case with many of the assets and equipment that were slated for review in this chapter, there was not enough time to build a chapter matrix. However, the information logged for the first three assets and the research performed into the IFT program and various types of equipment provide enough information to continue on to the next chapter. Instead of filling out a performance table for every piece of asset and equipment examined in this section, that information will be estimated when it is required for either comparison between chapters 1 and 2 or when input (with respect to the performance of a surveillance system) into a surveillance tool is required.

[125] *White Paper: The Secure Border Solution*. ICx Technologies, February 2013. p. 7

Chapter 3: Analysis

So far the only research performed has been on existing systems and organizations that use those systems. This chapter takes that information and uses it to synthesize a surveillance asset capable of replacing or augmenting existing systems; systems that are capable of filling the gap that exist between an organization's needs (criteria) and the capability of the surveillance asset (s) currently employed by them (condition). The first step in this process is to analyze the data gathered in chapters 1 and 2.

Analysis of Chapters 1 and 2

The reviews conducted in the first two chapters have revealed the requirements of organizations that use surveillance systems, the assets in use by them, and the capabilities of those assets. These reviews contain a large amount of information, most of which is used later in this thesis. For now, the relevant information contained in these chapters is found in the master tables at the end of each. Analysis of these two tables paints a picture of how surveillance systems are currently used, the weaknesses that result from the way in which they are deployed, and what existing surveillance assets are ideal for each scenario (with respect to those that are currently in use).

Tooling up the Analytical Process

An analytical tool has been developed to make this analysis faster and easier than it would otherwise be. This tool is the Scenario Specific Optimization of Surveillance Assets (SOSA, SSOSA just doesn't sound right). SOSA provides the user with ability to perform three functions. First, it generates a topographic map for each of the scenarios in chapter 1, a map that includes the detection ranges and tracking depths of the assets used. This map is useful in determining how effective the current assets are and how resilient that system is. These

scenarios are preprogramed with the actual surveillance assets used in the real world. Simply select the scenario in sheet 2 and view the map in sheet 4. The second function provided by SOSA is the ability to customize the surveillance assets used in each scenario. If the user would like to choose a different set of assets to perform the same scenario -specific surveillance he or she can do so. There is a button above the scenario selection column that, when pressed, clears the current assets but leaves both the scenario itself. The third and final function provided by SOSA is the ability to automatically optimize the placement and type of surveillance assets for a specific scenario – either a preloaded scenario or one that is created by the user. Despite being a useful and robust tool, SOSA is virtually useless if the user in not aware of the operational knowledge specific to each scenario.

So what is operational knowledge and where does it come from? Operational knowledge is defined as the knowledge of the role played by surveillance assets in each scenario with respect to the broader mission. Furthermore, it is important to know the tactics used to accomplish that mission so long as those tactics are influenced by the surveillance provided by the assets used in each scenario. Some of this information is contained in the first chapter, the rest will be provided in the pages to come. Each of the scenarios outlined in chapter 1 are depicted in this chapter using SOSA. Following this depiction is the scenario specific requirements from chapter 1 and the capabilities of the assets, from chapter 2, employed in those scenarios.

Note: Due to the large number of scenarios and the variety of those scenarios (in terms of both the type of assets employed and the type of perimeters they are deployed along), the scenarios depicted in this chapter have been limited to those that employ only ground based, fixed assets. Moreover, the types of perimeters depicted have been limited to geopolitical borders and

exfiltration/infiltration points of SF personnel. Several of the other scenarios will be discussed, just not in the same detail as those that are depicted using SOSA.[126]

Each of the scenarios that modeled by SOSA are done so in one of two 'formats'. The first is the most basic. These are scenarios whose titles include the surveillance assets AND equipment installed on them in their heading (e.g. SkyWatch w/ STS-3000 radar and short-range FLIR). When these scenarios are selected from the interactive sheet, SOSA automatically selects those assets and their placement on the map. The second type of scenario by SOSA is more complex. These are scenarios which have no asset or equipment associated with them. When these scenarios are modeled the surveillance assets and equipment used will either be selected by the author or selected by SOSA (via its built in optimization function). The following page is a screen capture of SOSA's main interactive sheet, **Table 3.1**. (not the final tool, only a beta-design). Immediately following the interactive sheet is **Figure 3.1**, an example of the map generated by SOSA using its sensor-optimization function.

Findings

Ideally, a surveillance network is composed of systems that provide all three capabilities: detection, tracking, and recognition. Unfortunately, most networks are far from ideal. In cases where incomplete surveillance networks (those that are lack one of the three capabilities) are deployed the overall mission of the organization operating those assets is jeopardized / threatened.[127] In some scenarios this is an acceptable and wise decision[128]. Then there are

[126] SOSA is in the process of being modified so that both enclosed perimeters and mobile assets can be modeled. Doing so will allow the user to perform all three functions of SOSA in the same manner those functions are used with the current scenarios.

[127] In the context used, jeopardized / threatened does not refer to absolutes. For example, an organization is conducting a mission that has a 99.9% probability of complete success with all three capabilities. The lack of any

	Asset or System	Mission Type	Portability Rating	Setup and Tear Down Rating	Endurance Rating (days)	Detection Range of Vehicles (meters)	Human Ident. Range (meters)	Intent Specific Identification Range (meters)	Surveillable Area of Detection	Mobility Rating	Terrain Rating	Foliage Rating	Low Observability Rating	Ratio of Active to Inactive Service	Resiliency Rating (Months)	Personnel Cost Per Month	Estimated Maintenance and Resupply Cost Per Month	Total Operating Cost Per Month	Acquisition Cost Per Asset	Number of Assets Required
Detection Asset			5	5	4	3000	1200	400			3	3	3	1		43200	10000	48200	300000	
Class Specific Identification Asset			10	5	4	1100	450	50			3	3	3	1	24	30	394.5833333	394.583	8000	
Intent Specific Human Identification Asset			10	5	4	0	0	80			3	3	3	1	24	30	72.96666667	102.917	1000	
	SkyWatch	Detection/Class Specific Identification				2200	1200	400					1							
	PSN P-Sensor	Intent Specific Identification																		
	PSN C-Sensor	Class Specific Identification																		
	CamV	Defensive	5	5	4	8000	2500				3	3	3	1				7000	79000	
	MQ-9 Reaper																			
	P-3 Orion																			

Asset 1 Total Cost Over 5 Years	Asset 2 Total Cost Over 5 Years	Asset 3 Total Cost Over 5 Years	Total Scenario Cost for 5 Years
0	0	0	0

Scenario	Operator (Organization/ Parent Organization)	Surveillance Mission (Defensive or Offensive)	Objective	Preconditions	Type of Perimeter	Perimeter Length	Required Portability Rating	Required Setup and Teardown Rating	Required Endurance	Terrain Rating	Foliage Rating	Required Low Observability Rating	Required Detection Range of Vehicles	Required Detection Range of Humans	Required Class-Specific Identification Range of Vehicles	Required Class-Specific Identification Range of Humans	Required Intent Specific Identification Range	Required Tracking Depth	Required Class Specific Identification Depth	Required Intent Specific Human Identification Depth
Single SkyWatch tower equipped with STS 12000 radar	CBP	Defensive	Deter	Border	Soft	8000							2500		1500		1350	5000	650	60
Custom Scenario																				

Table 3.1: Interactive page of SOSA. This is the page where the user inputs the variables required to generate either a custom scenario or one that is sensor-optimized

---

one of the three may reduce the probability of complete success by anywhere from 0.1% (or some number impossibly close to 0) to 99.9%.

[128] An example of this would be expanding a manned radar network from 350m to 1400m. At 350m it is borderline possible to recognize an IOI with handheld optics, increasing the recognition capability would make no sense.

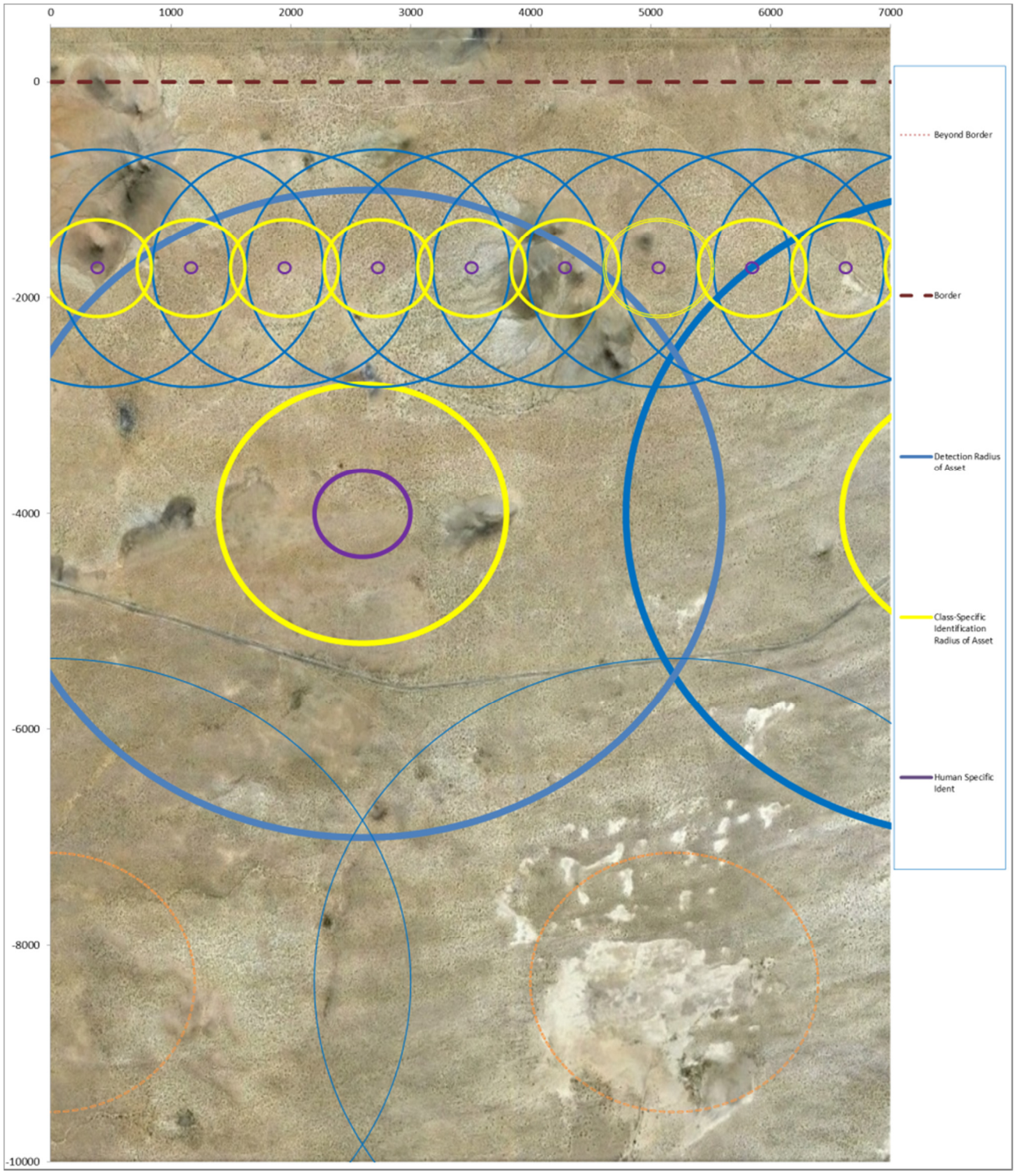

Figure 3.1: Existing sensor network using legacy SkyWatch towers, STS-1400ER FST, and augmented by a choice of STS-1400ER / Cam-V

instances in which one or two of these capabilities are unavailable. There is however one capability that modern surveillance systems lack more than any other.

Analysis of the master tables from chapters 1 and 2 has revealed that the single greatest capability that modern surveillance networks lack is recognition. **Figures 3.1** highlights an example of scenarios in which this capability is not provided. The surveillance network modeled in this figure resembles that which is currently deployed along a 10 mile stretch of the U.S.'s southern border. The overlap in the detection coverage (both human and vehicular) provided by surveillance systems in this scenario is proof that the systems that makeup this network are capable of detection IOIs day or night. However, observation of the recognition range (labeled human specific ident. range in this figure) highlights the fact that there are huge gaps in this networks capability to recognize IOIs, particularly along the border itself (as opposed to further inland from it). This figure is representative of many scenarios in which the surveillance network deployed lacks the ideal capability to recognize IOIs. What this figure fails to illustrate is the degree to which recognition assists in the completion of an organization's primary mission from one scenario to the next. The exact consequences of deploying a surveillance network with insufficient recognition capabilities varies according to the scenario, but the cost can of doing so is always measured in terms of resources (funds, personnel / hardware) and the success of the mission. The loss of resources is easily quantified; the success of a mission is not. Success however is dependent on two other variables: resources and time. The following example illustrates this dynamic.

If recognition is lacking, the enforcement assets responsible for enforcing the region under surveillance will be unaware of the intent or number of IOIs detected. Since the operators of

surveillance networks often send enforcement assets that are capable of overwhelming the IOI encountered, the number and capability of those assets may be inappropriate for the given scenario. Doing so costs the operators time and resources (in this case it is funds, personnel, and hardware). The loss of time and resources leads to (i.e., indicative of) the tying down of enforcement assets that could otherwise be used to intercept additional IOI, IOI which may have been discovered only after detection of the first. The inability to engage fewer IOIs is the most direct impact that the loss of time and resources has on the successful completion of the overall mission. In addition to the – the ability to discern whether or not an IOI is a false positive.

Scenarios in which an IOI is inaccurately classified as a threat is an event commonly referred to as a false positive. It is one thing to send too many enforcement assets in response to the detection of an IOI; it is something else entirely to dispatch those assets when the IOI detected is of no consequence whatsoever. Doing so not only waste time and money, it leaves the operators extremely vulnerable to the use of decoys. With this in mind, the capability to provide range-specific recognition is the only way to determine with absolute certainty whether or not an IOI is a false positive.

Chapter 4: Design and Features of the PSN

Design History of the PSN

Introduction

The final design of the PSN put forward later in this chapter is far from what was originally envisioned. Research into the variety and capability of surveillance assets and equipment (and the organizations that use them) has been the primary motivation behind the dynamic design of the PSN. Nonetheless, the original concept and the requirements that are the foundation of hit have never changes, save one. The original requirements are:

- portable
- modular
- upgradable
- rapidly deployable
- inexpensive
- reusable
- original

History

The requirements above have all been challenging to integrate into the final design. However, one has been far more difficult to integrate than the others – originality. The originality of the PSN was consistently challenged at every turn. The design the PSN changed every time research revealed that it was not original – every time it was revealed that the then current design had already been or was under development. This first part of this section is a record of how the design of the PSN changed from its original incarnation to what it is now. The history described

in this section does not account for minor revisions, only those which led to a redesign of the then current system, versions which, at the time, were thought to have been the final design.

The Original Concept – MSC Version 1.0

Originally the PSN was called the Mobile Sensor Network (MSN). The founding requirements were the same, but the name was different. This system was designed around the idea that a single thermal sensor was capable of detecting and tracking multiple IOI, and that this sensor could be developed and implemented for considerable less than those already on the market. A key component of this concept was that the multitude of relatively cheap thermal sensors used would be capable of talking to one another after deployment, tracking an IOI as it progressed through the area of detection. These sensors had to be capable of being deployed by vehicles, naval vessels, aircraft, and personnel within a short period of time in any terrain (e.g., tropical forest, mountains, deserts, etc.) The air dropped sensors had to be capable of being dropped and guided to specific points on the ground using GPS or triangulation (3G). In an effort to make the design even more original and effective, the design of the sensors had to deployable with as a bundled package. This package was to include a mobile command center and a large number of sensors that were all contained in a 20ft cargo container, the type of container that could be deployed via cargo aircraft or on board a naval frigate (in particular the U.S. Navy's new Littoral Combat Ship, or LCS) similar to the one shown in **Figure 4.1** on the next page.

MSC Version 2.0

It was discovered during initial research that the function of integrating multiple, low-end thermal cameras had already been developed by companies like FLIR. FLIR developed software that takes their sensors and integrates them into a vast network capable of tracking an IOI from

once sensor to the next. At this point the original design of the MSN, though challenged, was still original – it was still highly portable, air deployable, and included a mobile command center.

Figure 4.1: U.S. Navy LCS-1 Freedom and LCS-2 Independence[129]

Moreover, the requirement that the sensors themselves be inexpensive was given a higher priority than during than originally planned. Research had shown that it would be too expensive to airdrop guided sensors. The only alternative would be to airdrop unguided ones. To make an unguided sensor network effective aircraft would need to deploy a large number of sensors. As the required number of sensors increased the price of them was required to decrease.

Unfortunately, further research revealed that even this design lacked enough originally to proceed. There were already systems that were air deployable that, despite not being thermal,

[129] LCS-1 and LCS-2 are the first ships in their own separate sub-class of LCS (hence two very different ships being referred to as LCS)
Littoral Combat Ships, United States of America. Naval-Technology.com, April 2013. Accessed April 20, 2013 from: http://www.naval-technology.com/projects/littoral/littoral1.html

enabled the tracking of IOI across a region of interest. At this point it was thought that these sensors were different enough that the MSN's ability to identify an IOI as belonging to a particular class (e.g., car vs. person vs. deer). What killed this version of the MSN was research into small, unmanned UAVs equipped with thermal sensors. Some of these UAVs, though more expensive than the MSN, are capable of seeing through fairly thick foliage to the extent that they are capable of identifying IOI as belonging to a particular class. In an unrelated case, it was long after discovering the capability of UAVs that the MSN was renamed PSN. Research revealed that CBP had just finished awarding the MSC contract to ICx. It was decided that the acronyms and requirements of these two systems were too similar to proceed. The decision to rename the MSN was reaffirmed when it became clear that a large portion of this thesis would be presented at a conference attended by a large number of CBP personnel, personnel who may associate the MSN with the MSC.

PSN Version 1.0

The first incarnation of the PSN was a derivation of the MSN. This version of the PSN was the first version with the additional conceptual requirement that the PSN be capable of recognition. The PSN still used thermal cameras, but this time they were used in a different way. First, the thermal cameras used by the PSN did not need to be high-end, they need only be capable of detecting and tracking IOI at a distance of equal to or greater than fifteen hundred feet. These low end thermal sensors, called parent sensors (P-sensors), were to be connected via Wi-Fi to a network of traditional cameras, or child sensors, (C-sensors) capable of optical zoom. The thermal sensors would detect IOIs and then send a signal to the optical camera that tells them the correct pan, tilt, and zoom to take a picture of the IOI. Using this system would allow the cheap acquisition of both tracking (via the thermal sensors) and identification (optical sensors). This

design put life back into the originally envisioned capability of being deployed via aircraft or helicopters. Whereas small UAVs and thermal sensors were both capable of detection and tracking, only this version of the PSN was capable of recognition. Unfortunately, they would only be capable of doing so if the P-sensors dropped by aircraft were a smaller and less capable version of their man portable counterparts.

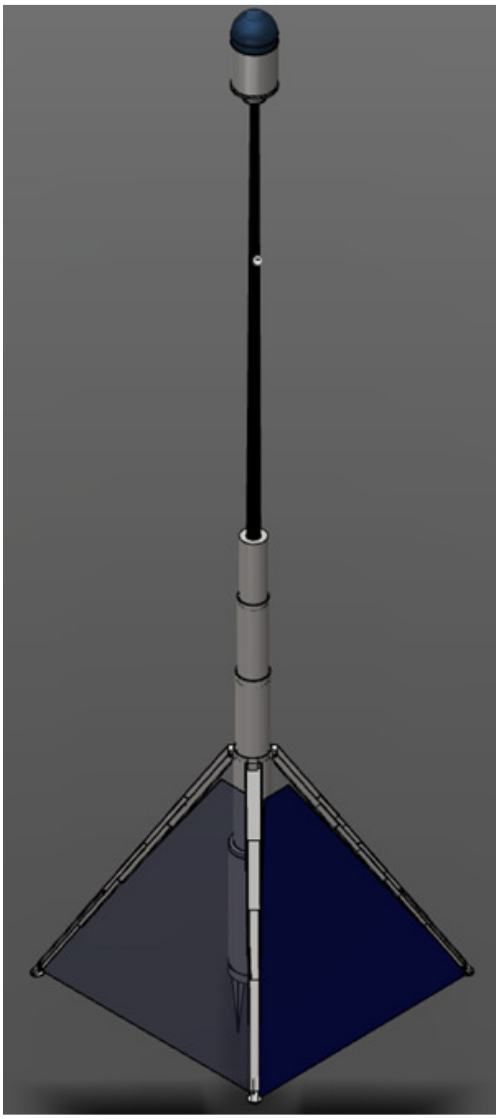

Figure 4.2: P-Sensor deployed (note the size of the arms and panels, which attach to the top of the second tier of cylinders, not the first as in other options) – thermal, solar, and 8ft telescoping mount

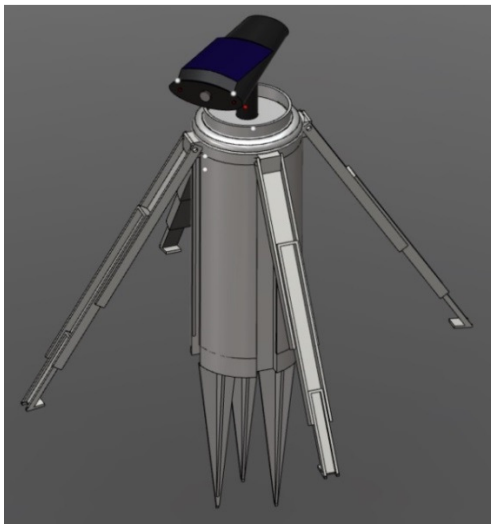

Figure 4.3: C-Sensor option 1 – IR and solar

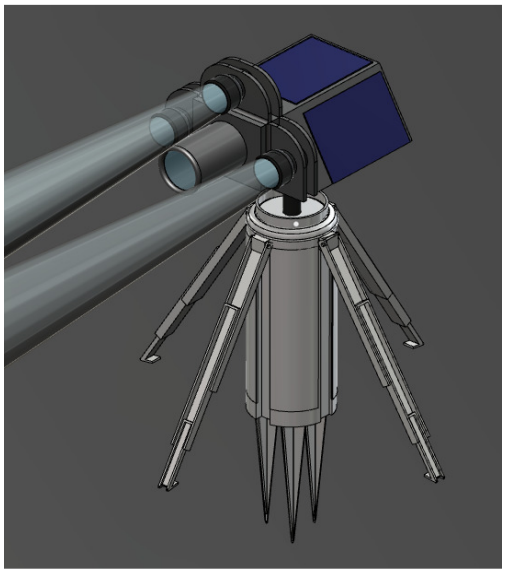

Figure 4.4: C-Sensor option 2 – camera, flash, and solar

The demise of this version of the PSN began with the discovery of networks in which thermal and radar were used to detect IOIs and long-range cameras, equipped with large spot lights built in to them, were used to identify them day or night. Radar proved to be far better at detecting IOIs than thermal, at least on flat, devoid of foliage. Still, hope for this version (the 3rd, possibly 4th version depending on how you count it) remained despite the unavoidable use of radar and thermal for detection. One of two actions could be taken: embrace radar and integrate it into the design of the PSN or exploit the advantages thermal sensors have over radar.

Figure 4.5: FLIR EnforcIR[130]

PSN Version 2.0: Radar or Thermal

Radar and thermal each have their advantages. Radar can cover a larger area than low end thermal sensors but it cannot see through thick foliage nor can it work in rough terrain as well as thermal sensors. The decision was made to embrace the advantages of thermal sensors. A plan was developed that highlighted the use of thermal sensors on mountainous, uneven terrain as

[130] *Ranger MS-UC EnforcIR Brochure*, FLIR Systems, 2013. p. 1

Figure 4.6: FLIR Ranger III[131]

well as terrain that was covered by thick foliage. The cost and tracking ability of IOI through this terrain was mapped and proven to have its advantage over radar – at least until more research was performed into the capabilities of ground radar.

Ground radar capable of detecting humans through thick foliage has been around since the late 1960's. It was deployed by the U.S. in Vietnam as a way of detecting Vietcong attacking FOBs. This technology has evolved over the decades to such an extent that nearly all mid and long range ground radars are capable of doing so. To make the design PSN 2.0 even less original was discovery of sensor networks that use radar to detect IOIs and high end cameras equipped with spotlight s for identification. This deployment of radar and sensors was the second blow to what is a design that's foundation was three fold: the ability to see through foliage; the use of long rage sensors to detect and track IOIs complimented by flash cameras for identification; and the use of thermal sensors and flash sensors on mountainous terrain. Version 2.0 was not dead yet, only limping along.

[131] *Ranger MS Illuminator*, FLIR Systems, 2013. p. 1

Version 2.0 was officially killed when research uncovered software developed by FLIR that coordinates the use of radar, thermal cameras, and flash cameras to provide full coverage in any terrain.[132] At this point it seemed like the time to throw in the towel. All the good ideas had already been thought of, nothing else remained. That is when research was performed into the price, resilience, and long term deployment of the surveillance assets examined thus far.

During this stage of development it was projected that the PSN P-sensors would cost $8,000 to $12,000 while the C-sensors would cost $700 to $1,000. It was thought that the cost of the proposed system would be similar to that of current equipment (e.g., radar, long-range thermal), the advantage of the PSN being that it is capable of both identification and detection whereas existing systems could only detect IOIs. The estimated cost of these systems was based on the advertised price of similar, commercially available, systems. It turned out that these systems were incredibly more expensive than originally thought. This meant that once again the entire design of the PSN was a viable option. Despite the fact that it shares similar capabilities with existing systems it can do so for a fraction of the price.

PSN Version 3.0: Cost

The debate was finally settled, the final version of the PSN would be: thermal sensors for detection, flash for illumination, traditional daytime optics for recognition, and communication between the P-sensors and C-sensors accomplished via the use of narrowband Wi-Fi.

The only thing left to do was conduct assessments to determine the exact cost of each component and to conduct mock deployments. During the course of conducting these assessments two

things became obvious: each component, particularly the C-sensors, would cost much more than expected and the PSN itself would take too long to deploy. Each of the C-sensors required a laser range finder and an auto focus camera. Furthermore, the telemetry and focus required by each C-sensor to take a viable picture of an IOI meant that C-sensors and P-sensors need to work in unison (an expensive proposition). Although not impossible, the cost to implement these changes negates any advantage the PSN once had over existing systems.

Despite having already been proven impractical, further analysis of the PSN 3.0 was conducted in an effort to determine if the current version had any other flaws. This analysis revealed that the PSN took too long to deploy. The most laborious aspect of deployment was aligning the narrowband Wi-Fi installed on each of the sensors, a design flaw that plagued this and nearly every other previous version of the PSN – rendering them all defunct.

PSN 4.0

The only way to make the PSN viable was to address the flaws inherent to the prior version and all those that preceded it. The only problem was that there seemed to be no one way to address even one of the problems at hand (the need for cheap auto focusing camera, a faster way to align the narrowband Wi-Fi and coordinate the operation of the C-sensors with the P-sensors). There seemed to be only one solution: get rid of the C-sensors entirely. The decision to do so was the last major step that culminated in the PSN's final design.

The Design of PSN 4.0

The PSN 4.0 is designed to function as an all-inclusive system, as opposed to the PSN 3.0 which had both C-sensors and P-sensors. The same equipment installed on the two sensors that makeup PSN 3.0 has been combined in the design of the PSN 4.0 to form a single system. Doing so

removed the extremely expensive hardware and software required to integrate the operation of multiple sensors. When fully assembled, the specifications of the PSN are (all dimensions are visible in **Figures 4.7**, **4.8**, and **4.9**):

- 50.0cm (19.7”) tall (dimension 1)
- 12.7cm (5”) diameter (dimension 2)
- 13.5cm (5.3”) tall (dimension 3)
- 19cm (7.5”) wide (dimension 4)
- 27.9cm (11”) long/depth (dimension 5) (length does not include stakes which are removable)

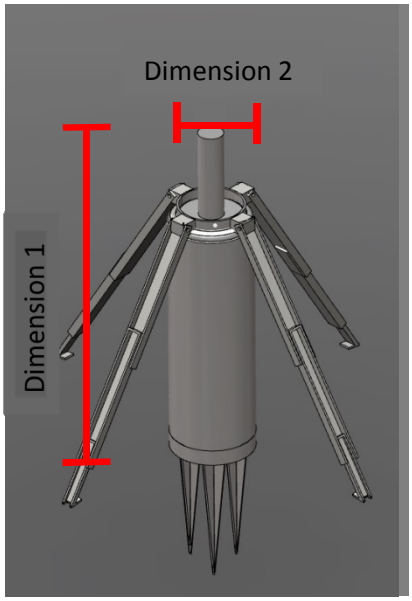

Figure 4.7: Mount

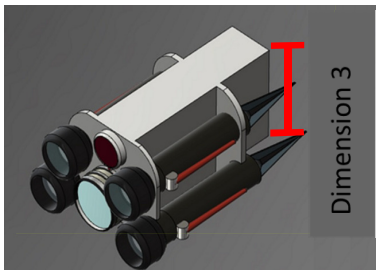

Figure 4.8

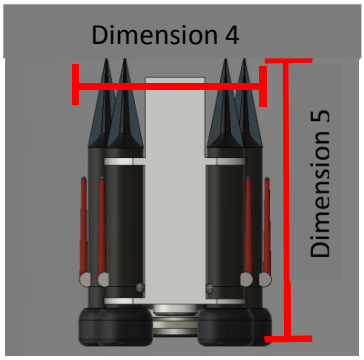

Figure 4.9

Figure 4.10: Complete system

The drawback of creating a combining all of the sensory equipment into a single system is that the cost of acquiring the number of systems needed to construct a viable network has risen dramatically. The single greatest reason costs have risen is that each PSN 4.0 system must have a thermal camera installed on it, whereas the PSN 3.0 only required one thermal camera for

every three or four systems (one P-sensor for every three or four C-sensors). More information on this topic, the deployment and operation of the PSN, is discussed in chapter 5.

Chapter 5: Deployment of the PSN

Variations and Outfitting

The PSN has been designed in such a way that it enables those who deploy it to gain maximum flexibility with minimal effort, a necessity in a world where surveillance requirements can vary greatly from mission to mission. This flexibility (i.e., feature) is all the more important when looking back at one of the original goals outlined in the introduction: the development of a system that can be used by multiple organizations (in an effort to reduce costs). In the case of the PSN, the flexibility it provides its operators comes from its modular design. Though modular, the current design is limited to a few configurations, or variations, which are defined according to how each is outfit with an array of different components.

All variations of the PSN share a similar set of core components: lower mount and associated hardware (e.g., battery), digital camera, rangefinder, and infrared camera. The only thing that changes from one variation to the next is the number of flashlights installed on the sensor and the decision of whether or not to equip it with certain, key options. It is also important to note that every PSN sensor is intended to run using the same software. This enables every PSN built to be capable of being modified so as to take full advantage of all options, deployment scenarios, and flashlight variations. **Figures 5.1** through **5.7** illustrate the four different ways a PSN can be outfit with flashlights. **Figure 5.1** shows the variation of the PSN that has been presented thus far. Since the lower mount used in this figure is identical to that used by every PSN manufactured (independent of the variation), the rest of the variations presented in this section (and the figures of them) only illustrate the upper assembly.

Figure 5.1: 4 flashlights

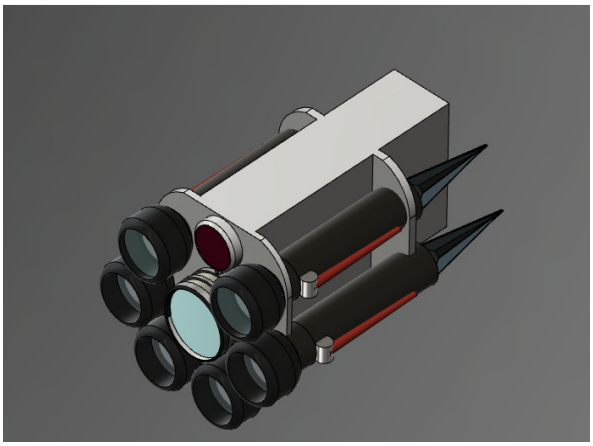

Figure 5.2: 6 flashlights

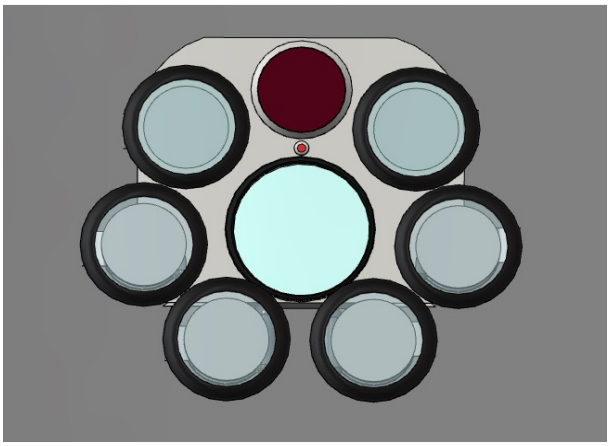

Figure 5.3: 6 flashlights

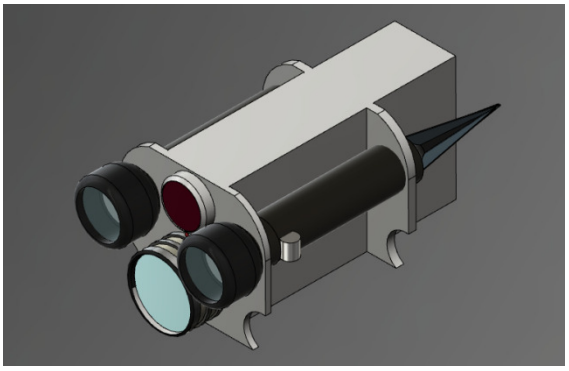

Figure 5.4: 2 flashlights

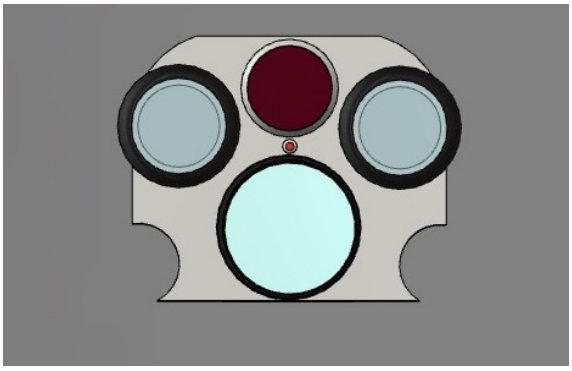

Figure 5.5: 2 flashlights

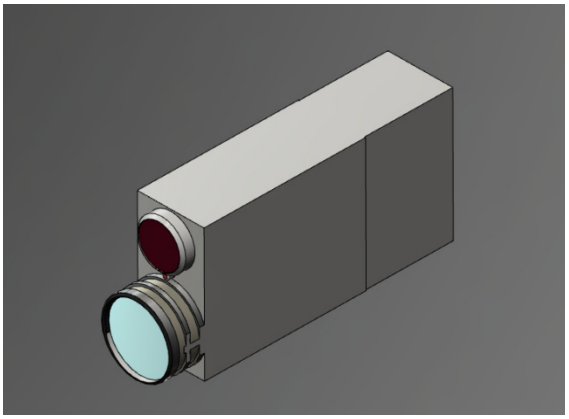

Figure 5.6: no flashlights

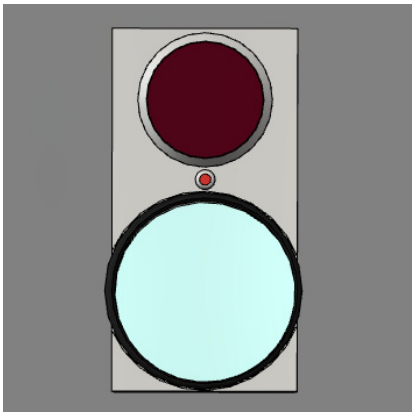

Figure 5.7: no flashlights

Each of the four variations above can be equipped with one of four options: one or more narrowband Wi-Fi transmitters, solar panels, compact telescoping upper mount, and extra-long telescoping upper mount (e.g., the pole on which the upper assembly rests). The narrowband Wi-Fi transmitters enable the PSN to communicate with deployed flashlights over a longer distance (without the need for Wi-Fi in the flashlights); solar panels dramatically increase the time a PSN sensor can remain in the field without needing to be recharged / have its battery(s) replaced; and the use of a telescoping upper mount allows the PSN to operate from a higher vantage point. Other than cost, the use of the compact or extra-long telescoping upper mounts is the only options that have potentially negative side effects.

When the compact telescoping upper mount is equipped it reduces the size of battery that can be carried in the lower mount (the center of the lower mount is hollowed out to provide room for the pole to retract into). The extra-long telescoping upper mount is both easier to detect and is more cumbersome to transport and deploy - the actual pole is several feet long and must be carried separately from the sensor itself. **Figures 5.8** and **5.9** illustrate how PSN sensors look when equipped with solar panels and an extra-long upper mount.[133]

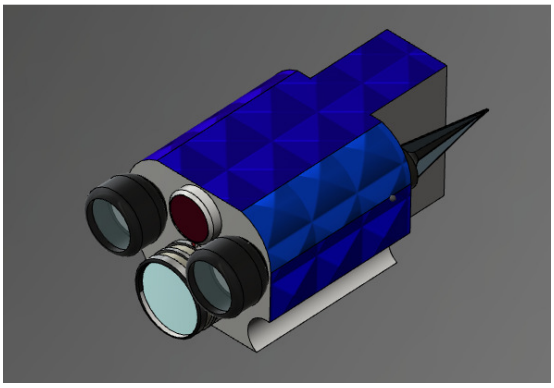

Figure 5.8: 2 flashlights and solar

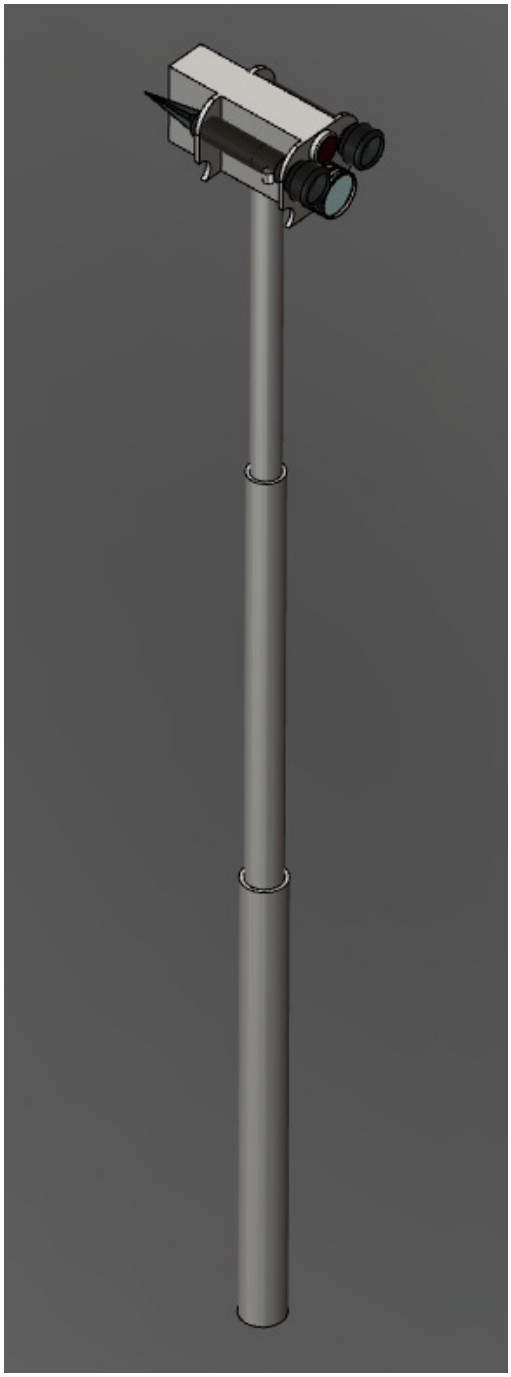

Figure 5.9: 2 flashlights and extra-long upper mount[134]

[133] No figure was generated to show the use of a compact telescoping pole since the use of that pole would look similar to that of a regular PSN (taller by approximately 6" but with the added ability to collapse completely into the lower assembly). There would be a figure illustrating the use of directional Wi-Fi but difficulties arose when attempting to generate the model.

[134] Total elevation between the ground and the sensor when using the extra-long upper mount is 2.5m vs. the standard 0.5m

The final component that determines a specific systems unique variation is the type of flashlight used. All PSN are equipped with a flash light that is capable of being staked into the ground or used on the sensor itself. All of these flashlights have rotating heads, identical battery supplies, and bulbs (LEDs). Options that can be installed on these flashlights include solar panels, Wi-Fi transmitters (as opposed to just a Wi-Fi receiver), and sirens (audible alarm). **Figures 5.10**, **5.11**, and **5.12** illustrate what these options look like when installed on a standard PSN flashlight.

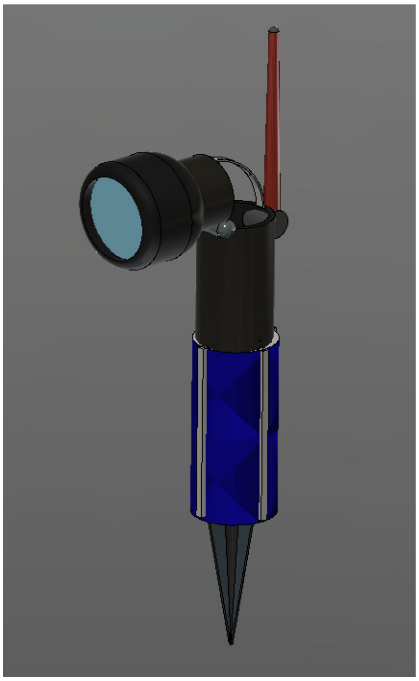

Figure 5.10: Solar stored

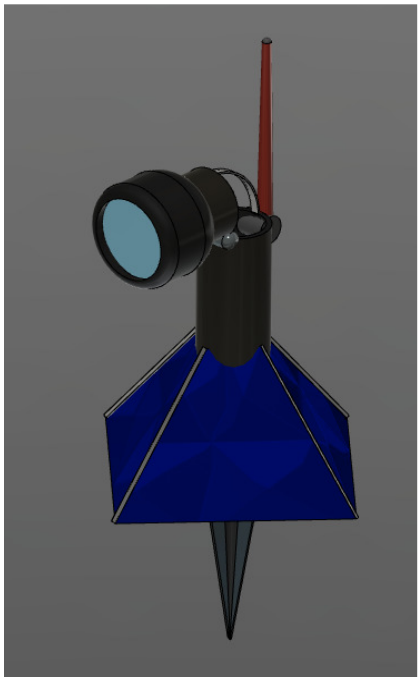

Figure 5.11: Solar deployed

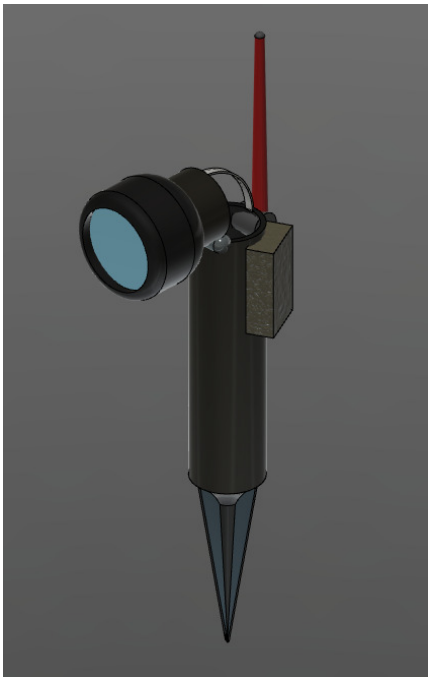

Figure 5.12: Wi-Fi transmitter

Deployment and Operation

Each variant of the PSN can be deployed and operated in a multitude of different ways. The way in which a specific system or network of systems is deployed and operated depends on the mission, the type of systems being deployed, and the number of systems on hand. Off the two, deployment is least complex.

Deployment

Deployment of the PSN can be done in two different configurations, both of which depend on the location of the flashlights used to illuminate IOIs at night. The first way is deploy each PSN system as a single unit. This configuration places all of the flashlights on the system itself. A single PSN system deployed in this manner is capable of detecting, tracking, and recognizing IOIs during the day according to the maximum effective range (usually between 200m and 400m) of each piece of equipment installed (i.e., digital camera, rangefinder, and thermal camera). At night, the maximum detection and tracking range depends solely on the thermal camera. Night time recognition depends on the type of digital camera and number of flashlights

mounted on the upper assembly. A standard digital camera, effective when used with a moderate amount of ambient light (early dawn, late dusk), is estimated to be capable of taking high-quality night time images of IOIs at the following, flashlight dependent, ranges:

- 0 flashlights: 0m
- 2 flashlights: 115m
- 4 flashlights: 145m
- 6 flashlights: 160m

Although these distances are only rough estimates, they are estimates derived from the testing of a flashlight similar in capability to ones intended for use on PSN systems (1200 lumens).[135] The testing of this flashlight was done in near total darkness at ranges up to 150m. A single flashlight was more than capable of completely illuminating IOI at over 100m, in some cases 130m. The estimates for the effective ranges of night time recognition of IOIs presented in this section are highly conservative; estimates that take into account the effect various atmospheric phenomena have on a flashlight's ability to effectively illuminate an IOI at night. These ranges (yellow = 115m, blue = 145m, red = 160m) are illustrated in Figure **5.13** below, a mock deployment of the PSN around a military installation with a hard perimeter.

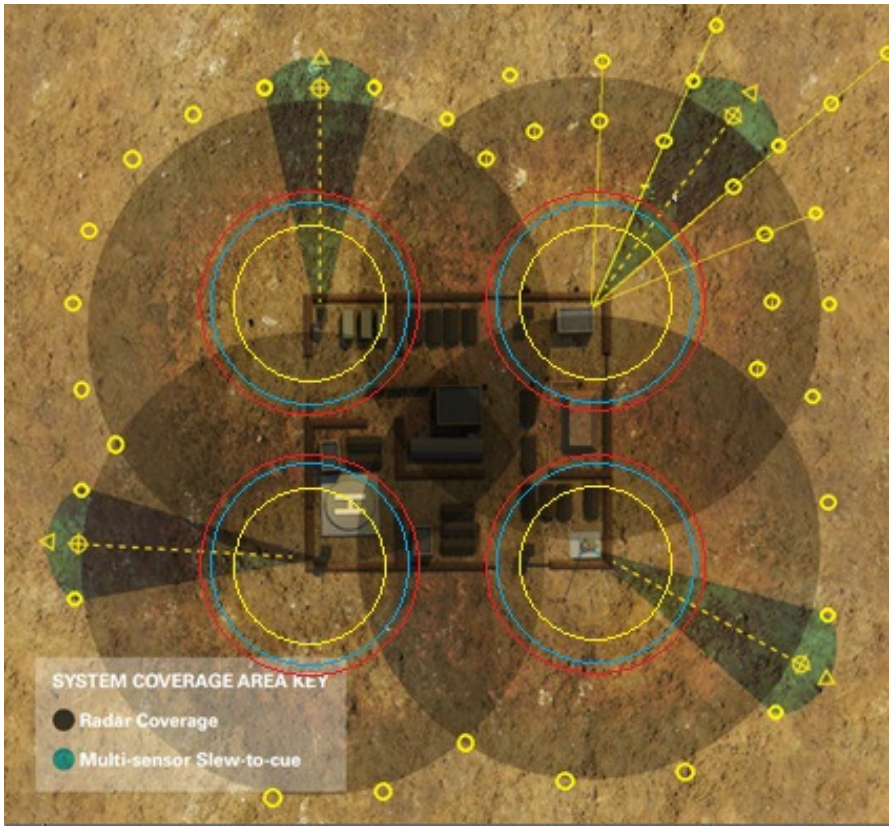

Figure 5.13: Mock deployment of the PSN around a military base with a hard perimeter

[135] See the appendix for a detailed description of this flashlight.

The second type of deployment may or may not have flashlights installed on the upper assemblies. What makes this deployment unique is that there are two or more flashlights deployed on the ground at a distance from the primary system. These flashlights can be deployed in a variety of configurations at ranges between 35m to 250m from the nearest (PSN) system. The primary disadvantage of doing so is that, regardless of the distance between the flashlights and the primary system, it requires far more flashlights than a standalone system. The exact number of flashlights required depends on the orientation of them and how far the operators want to extend the range at which a PSN can recognize IOIs. A rough approximation of the number of flashlights needed to extend this range is illustrated in **Figure 5.14**. Even when deployed at extremely short ranges (<20m), this configuration has its advantages - it removes the flash from the primary system, making it harder to detect. **Figure 5.13** illustrates the mock deployment of flashlights, depicted by the small yellow circles, around a network of PSN systems.

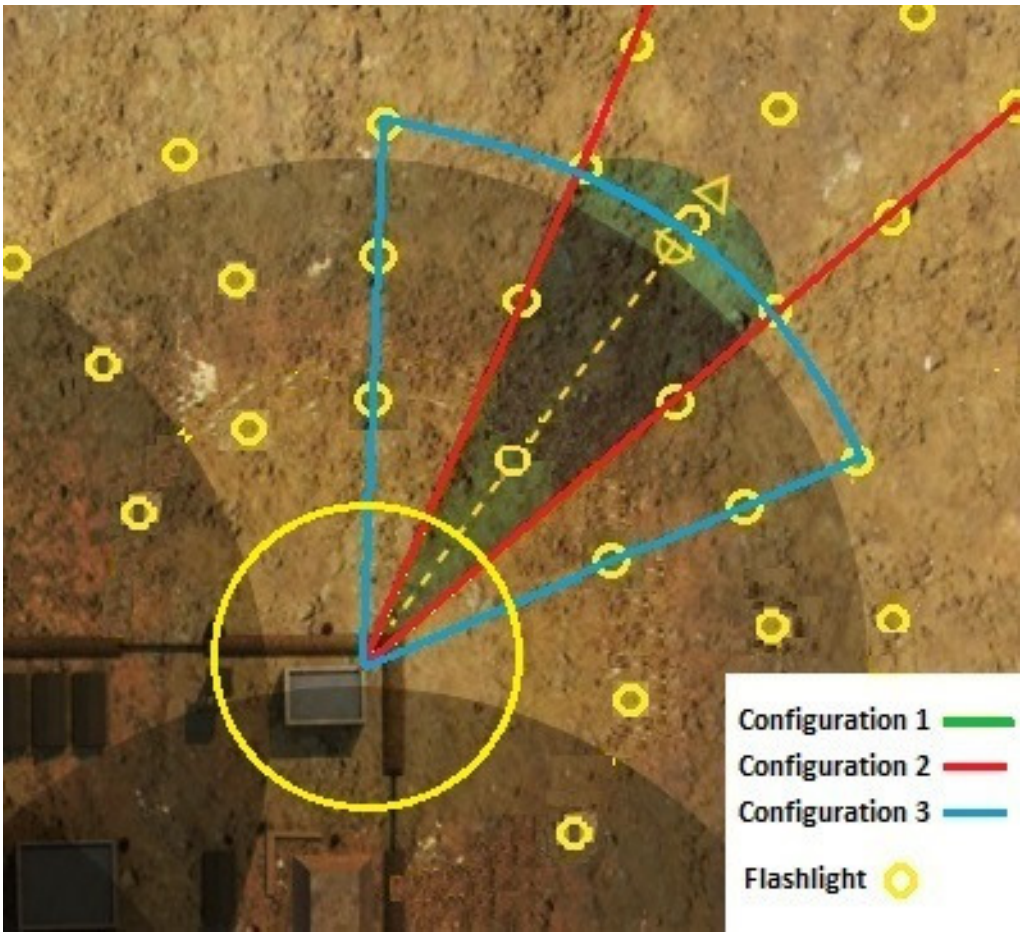

Figure 5.14: Flashlights required for extended range recognition vs. the detection range of a STS-350 radar

Figure 5.13 goes even further; it compares the deployment of four STS-350 radars against that of a PSN network with four systems. The shaded region represents the detection range and

tracking area of a single STS-350 radar. In this scenario the PSN is capable of detecting and tracking IOIs at 300-400m, approximately the same range as the STS-350. The final aspect of deployment is the orientation those flashlights deployed in the field, which, after study, suggest that many more flashlights are required than the number indicated in **Figure 5.13** (to illuminate IOIs at the ranges in that figure in such a way that any IOI that falls inside that range is recognizable).

Flashlights must be oriented so that they illuminate the front side of all IOIs that close within the rangefinders specified range. If the front side is not illuminated the camera onboard each primary system will be unable to see the IOI at night. There are several ways of accomplishing this, none of which is the 'perfect solution'. The number and orientation of flashlights depends on the area needing illumination. However, the fact of the matter is this: the numerous unique paths from which IOIs can approach a camera's activation range (as set by the rangefinder) make it difficult to illuminate the front of them (IOIs) unless many flashlights are used (see **Figure 5.14**). With that in mind, the most effective way of using deployed flashlights is when the region being monitored is less than 30° wide. The use of flashlights in this type of scenario makes it much easier to properly illuminate approaching IOIs. **Figure 5.15** illustrates an example of the PSN deployed under these conditions.

Deployment and Operation

The operation of a PSN system begins with the engagement process. The generic process by which the PSN engages (detect, track, and recognize) IOIs, regardless how that network is deployed, is as follows:

1) The thermal camera detects the heat signature indicative of an IOI
2) The thermal camera tracks the IOI, using the pan and tilt mechanist to keep the IOI in the very center of the thermal cameras display
3) As soon as the thermal camera begins to track the IOI, the laser rangefinder starts measuring the distance between the IOI and the PSS (the rangefinder is fixed to the upper assembly, directly below the thermal camera)
4) The focus of the camera, which is located directly below the rangefinder, is adjusted so that it is constantly in focus. This is accomplished by linking the focus of the camera to the distance measured by the range finder

Steps 5 and 6 when the PSS is operating during the day:

5) At a predetermined, user defined distance the camera takes a series of digital photographs (still frames, not video)
6) These photographs are relayed to a local or regional command and control center (the type of communication equipment used depends on the needs of the operator)

Steps 5 through 7 when the PSS is operating at night:

5) At a predetermined, user defined distance the upper assembly broadcast a signal via narrowband Wi-Fi (or via different methods discuss later in this section) to all flashlights (both those on the PSS itself and those in the field) connected to that specific system telling them to turn on for a short period of time (usually between 1/5th and 1 second).
6) The camera takes a series of digital photos a fraction of a second after the upper assembly tells the flashlights to turn on
7) These photographs are relayed to a local or regional command and control center

The operation of a PSN system and the overall network to which it belongs depends on the deployment of those systems and the options installed. The actual operation of each system is identical to that which is described in steps 1 through 4 on the previous page. Following step 4, the operation of each system is unique. The following are descriptions are examples of how various PSN networks operate according the deployment of the systems that make up each network and the options installed on them (the individual systems).

Example 1: Operation of a standalone PSN system or standard, Wi-Fi equipped, PSN with flashlights installed in the field

The operation of this example is identical to the steps outlined above. The only exception to this operation is when the flashlights used are equipped with sirens. If they are, the sirens will sound as soon as the flashlights are triggered. These sirens will continue to emit sound until the preset time has elapsed (time varies based on user input, but would most likely vary from a few seconds to several minutes).

The only limitation of this system is that the W-Fi installed on it has a very short range (max of 35-40m, but usually less). This means that if flashlights are deployed in the field they are only capable of extending the night time recognition range of a PSN system by exactly that distance, a distance which is trivial given the recognition range of a standalone system (max of 160m). However, there is an operational advantage to deploying flashlights in the field using Wi-Fi - it is by far the easiest and least expensive method of doing so.

Example 2: Operation of a narrowband Wi-Fi equipped PSN with flashlights in the field

Example 3: Operation of a standard, Wi-Fi equipped PSN with Wi-Fi transmitter equipped flashlights in the field

Estimating the Cost of a Single PSN System

Chapter 6: Conclusion

The type of equipment intended for deployment on PSN assets was and has always been off the shelf and commercially available. Knowing this information made it possible to predict, within reason[136], what the price of each variant of the PSN would be. Research into the cost of various models of ground based radar, thermal sensors, and even high end flash optics opened another door for the PSN. Regardless of whether it is competing against high-end radar suites that cost $150,000 and up or against thermal cameras costing between $50,000 and $100,000, the PSN is capable of providing superior recognition for a fraction of the cost. The PSN is also more capable at detecting, tracking, and recognizing IOIs than low-radars that cost $75,000 and up (radars may cost only $20,000, but the supporting equipment needed to make them operational increases the price a minimum of two times over).[137] Even more surprising was the cost of high-end cameras equipped with spotlights. Many of these systems (in use with CBP and the military) cost $50,000 or despite the fact that they're use is augmented with other assets, usually radar. When standing on their own these cameras can see 2-3 km during the day, their ability to recognize IOIs at night via the use of their spotlights is limited to 1.5 kilometers (usually less, ½ to 1 kilometer). The financial advantage of using the PSN is clear; when compared against existing systems, the PSN can perform equally as well on flat terrain, better on thickly foliated terrain, and far better on mountainous terrain while doing so for a fraction of the cost.

The resilience of the PSN also gives it an advantage over existing systems. When a single, more capable asset fails, all of the surveillance capability provided by that asset is lost with it. If one or two PSN fail the PSN is still capable of performing its mission. This alone is a reason to

[136] See chapter 5 for more information and details regarding the PSN's estimated cost.
[137] A GSA contract between the federal government and ICx listed the acquisition cost of entire STS-350 systems, which use $15,000-$20,000 radars, at between $45,000 and $80,000.

seriously consider the PSN over traditional, high end optics. Intermingled with the benefit of resilience is that of endurance. Expensive, high-end optics require a significant amount of power. If they are deployed in remote terrain they will require some type of local support. If they are battery powered they will eventually need their batteries replaced. Even if they are equipped with solar panels to provide additional endurance, it is unlikely that the operation of the spotlight will be able to last long without some type of external charging. The PSN on the other hand is a network that deployed over a large area. Each individual camera and the lights associated with it is unlikely to be used more than once a night, perhaps even once every few days. One small solar panel would be capable of sustaining power for years (panel generates equal to or greater than the average power consumed). To make things even more plausible, each unit would be equipped with batteries that, on a full charge, can power each asset for over a month. This type of reserve ensures that the solar panels used by the PSN will never run out of power, despite the degradation of the panel itself. Finally, the number of PSN systems that are deployed within a given interval is higher than that of conventional spotlight/camera. This means that, despite the fact that companies like FLIR can setup a network to optimize coverage, on mountainous terrain the capability of that network to completely cover every bit of that terrain is less than the PSN.

Considering the information above and the fact that the PSN has met or exceeded all of its requirements, it can be declared that the objectives declared in chapter 1 have been fulfilled. The PSN 4.0 is a marketable surveillance system that, in addition to fulfilling its stated requirements, provides niche surveillance capabilities that not provided by existing systems: nearly 100% cover in mountainous terrain and the use of thermal cameras purely for the detection (and never identification) of IOI.

Glossary

a – Acceleration

a_d – Deceleration

A – Area

A_d – Area of sensor perpendicular to its velocity

A_{dp} – Area of a parachute perpendicular to its velocity

A_{dpf} – Total area of a parachute when lying flat

A_{ds} – Area of a deployed sensor perpendicular to its velocity

A_p – Area of a parachute perpendicular to its velocity

APSS – Agent Portable Security System

ASP – Advanced Security Products

BSAT – Balance Survivability Assessment Team

BZSS – Border Zone Surveillance System

CAS – Close Air Support

C_d – Coefficient of Drag

C_{dp} – Coefficient of drag for a parachute

C_{ds} – Coefficient of drag for a sensor

CBP – Customs and Border Protection

C-Sensor – Child Sensor

CAP – Combat Air Patrol

CAS – Close Air Support

d – Diameter

d_{dp} – Diameter of deployed parachute

DHS – Department of Homeland Security

DoD – Department of Defence

DTRA – Defense Threat Reduction Agency

E_k – Kinetic energy

E_p – Potential energy

EM – Electromagnetic

EO – Electro-optical

F – Force

F_g – Force of gravity

FEMA – Federal Emergency Management Agency

FLIR – Forward Looking Infrared

FOB – Forward Operating Base

GAO – Government Accountability Office

HC – Heavy camera

HSPD – Homeland Security Presidential Directive

IFT – Integrated Fixed Tower

IFTBSS – Integrated Fixed Tower Border Surveillance System

IOI – Item of Interest

k – Spring constant

LAPES – Low altitude parachute extraction system

l_p – Length of a single section/beam/rectangle of a cross parachute

LC – Light camera

LE – Law Enforcement

M - Mass

MSC – Mobile Surveillance Capabilities

ODP – Office of Domestic Preparedness

OAM – Office of Air and Marine

P – Momentum

POE – Point of Entry

P-Sensor – Parent Sensor

PSN – Portable Sensor Network

RRAP – Regional Resiliency Assistance Program

RF – Radio Frequency

RVSS – Remote Video Surveillance System

S_d – Stopping distance

SBI – Secure Border Initiative

SBI*net* – Secure Border Initiative Network

SDT – Sensor Development Tool

SRPP – State and Regional Preparedness Program

t – Time

TALCE – Tanker Airlift Control Element

t_b – Time to go from impact to zero velocity for the batteries, spikes, part 1, and part 3

t_c – Time to go from impact to zero velocity for the camera, part 2, and associated electronics

TSS – Threat Stalker Surveillance System

UAS – Unmanned Aerial Surveillance System

UAV – Unmanned Aerial Vehicle

UGS – Unattended Ground Sensor

UGV – Unmanned Ground Vehicle

USI – Urban Security Initiative

V_{di} – Velocity of a descending sensor at impact

V_{dt} – Terminal velocity of a descending sensor

VAT – Vulnerability Assessment Team

VSTOL – Vertical Short Takeoff and Landing

W – Work

w_p – Width of a single section/beam/rectangle of a cross parachute

Appendix i – Matrix Definitions and Ratings

Chapter 1 – Scenario Specific Surveillance

Portability Requirements Rating: The portability requirements associated with a specific scenario. These requirements represent the maximum size and weight of surveillance assets that can be used in a particular scenario. These requirements are rated on a scale from 1 to 10 with 10 being the most portable. The approximate translation of this scale into real world requirements is as follows:[138]

1) No portability requirements at all. Major components can be assembled on site with no respect given to their size and weight.
2) Every component of the surveillance asset(s) used must be transportable via cargo ship
3) Every component of the surveillance asset(s) used must be transportable via heavy transport aircraft
4) Fully assembled surveillance asset(s) must be transportable via cargo ship
5) Fully assembled surveillance asset(s) must be transportable via heavy transport aircraft
6) Every component of the surveillance asset(s) used must be transportable via large, wheeled combat truck (e.g., deuce and a half)
7) Fully assembled surveillance asset(s) must be deliverable to the battlefield via transport aircraft (e.g., airdrop or low-altitude parachute extraction system (LAPES)[139]. This level of portability also applies to manned surveillance aircraft and UAVs which are required to take off and land from a permanent airfield
8) Fully assembled surveillance asset(s) must be transportable via large, wheeled combat truck
9) Fully assembled surveillance assets must be transportable via light truck or in a small trailer capable of being towed by a light truck (e.g., HMMWV (aka 129umvee or hummer) or commercial pickup).
10) Most stringent portability requirements. Every component of a surveillance asset must be man-portable.

Setup and Teardown Requirements Rating: The time and manpower requirements associated with a specific scenario. These requirements represent the maximum time and manpower allotted to initially setup and then later repackage a particular scenario's surveillance assets. These requirements are rated on a scale from 1 to 10 with 10 requiring the least time and manpower. The approximate translation of this scale into real world requirements is as follows:

---

[138] Every asset with a rating of 2 or higher must also be capable of ground transport via 20 ft or 40 ft shipping containers. If this requirement were not imposed the surveillance assets used may be too large or heavy to be deployed where they are needed.

[139] LAPES is a system used by transport aircraft for the delivery of equipment that is too heavy for conventional airdrop. An aircraft delivering cargo to the battlefield via LAPES will fly very low to the ground, perhaps even touching it with its main (rear) landing gear. The cargo and a parachute attached to the rear of it are then pushed out the rear of the aircraft (cargo is mounted on a pallet designed specifically for LAPES). The aircraft then gains altitude and flies away while the cargo it deployed skids across the ground, eventually coming to a stop (the parachute attached to it aids in slowing the cargo as it skids across the terrain).
"Lockheed C-130 Hercules." The Aviation Zone, March 2013.

1) The least stringent rating. Scenarios that receive a rating of 1 are in no rush to setup their surveillance assets. These assets may require hundreds of workers years to construct/setup and once having done so can never be redeployed (i.e., surveillance assets that are themselves permanent installations)

2) Scenarios that require any surveillance asset(s) deployed be capable of redeployment, but ones that were not necessarily designed or initially deployed with the intention of doing so (redeployment). This type of asset may require dozens of personnel months to either setup or redeploy. Redeployment may require the fabrication of new parts and/or the laying of a new foundation. Finally, the initial setup and redployment of these assets may require the installation of supporting infrastructure, such as power and communications lines

3) Scenarios that require the use of surveillance assets designed to be redeployable, but ones that often serve as permanent installations. The setup and redeployment of these assets may take a dozen individual between one week and a month to accomplish

4) Scenarios that require the deployment and redeployment of surveillance assets in less than a week. These types of assets have command and control centers that require more time to deploy and redeploy than the sensors themselves (approximately a week for the command and control center compared to a few hours for the sensors). Deployment, redeployment, and the addition of sensors is more common than the redeployment of the entire asset

5) Scenarios that require the deployment and redeployment of surveillance assets in less than 24 hours

6) Scenarios that require the deployment and redeployment of surveillance assets in less than 6 hours. This rating also applies to satellites with circular and polar orbits that, depending on their altitude and type of orbit, can provide surveillance at intervals of between 90 minutes and 6 hours[140]

7) Scenarios that require the deployment and redeployment of surveillance assets in less than an hour. This rating also applies to the use of in theatre (forward deployed) or on the scene maritime assets, UAVs and manned aircraft, the rational being that the time required for these assets to arrive is approximately 1 hour (Depending on the scenario, the time required to arrive on scene could take anywhere from a few minutes to several hours. An approximation of 1 hour was chosen to simplify the rating system)

8) Scenarios that require any surveillance asset(s) used consist of sensors that are networked to a mobile command and control center. The time required to deploy and redeploy these assets is dependent on by number of individuals deploying the network, the number of sensors deployed, and the distance those sensors are from the command and control center. The sensors used by these assets must be capable of linking to the mobile command and control center within minutes of their deployment

9) Scenarios that require any surveillance asset(s) utilized be capable of deployment and redeployment in less than 15 minutes by a maximum of one or two individuals

10) The most stringent rating. Scenarios that receive a rating of 10 require the use of surveillance asset(s) capable of being deployed and redeployed by a single person in less than one minute. The sensors used by these assets must be linked immediately following their deployment to an interface possessed by the operators (individuals who deployed the sensors)

Terrain Rating: Terrain rating is used to quantify the type of terrain in which a particular scenario takes place. Another way of thinking about this rating is to interpret it as the mobility requirements for assets operating in this scenario. The terrain quantified is only that terrain which falls within the scope of that scenario (e.g., terrain beyond

[140] "What is the Orbit of a Satellite?" Space Today Online, March 2013.

a given scenario's required distance of detection or identification is irrelevant). This rating varies on a scale from 1 to 5 with 5 being the most uneven. An approximate translation of this scale into real world topographic features/landscapes is as follows

Scenarios with a terrain rating of:

1) take place on completely level ground
2) take place on slightly uneven terrain with infrequent, small, rolling hills and/or depressions
3) take place on uneven terrain with a high frequency of small rolling hills, a high frequency of small, rolling hills, and/or a high frequency of shall but steep changes in elevation
4) take place on highly uneven terrain with a high frequency of large hills
5) take place on mountainous terrain with large, frequent changes in elevation

Foliage Rating: Foliage rating is used to describe the type and density of vegetation in which a scenario takes place. Both the type and density of foliage are represented by a single variable. In addition to describing type and density, this rating defines how much the foliage present inhibits the operation of surveillance assets. Foliage is rated on a scale from 1 to 5, with 5 being the most surveillance inhibiting

Scenarios with a foliage rating of:

1) take place on a landscape with short grass or none at all, on which only the occasionally patch of thick vegetation is present. This type of foliage does not inhibit surveillance equipment whatsoever
2) take place on a landscape with tall grass and the occasional tall trees. This type of foliage may inhibit surveillance assets that are operating at ground level but should not inhibit those that are operating several meters or more above the grass (the higher the asset is the further it can detect and identify IOIs)
3) take place on a landscape with short or tall grass that is surrounded by large, dense patches of trees. This type of foliage inhibits surveillance assets in a manner identical to that of rating 2. However, in addition to the inhibiting effects of rating 2, the foliage present on this landscape can greatly inhibit an asset's ability to detect and identify IOIs at long range
4) takes place on a thickly forested landscape composed of boreal or temperate vegetation. This type of foliage can vary from location to location. It can greatly inhibit the abilities of a surveillance asset to detect and identify IOIs at both short and long ranges. However, the right assets used in the right locations can make the detection and identification of IOI at all ranges possible (e.g., the use of ground cameras to see through forests with thick canopies but little to no foliage close to the ground)
5) take place on a thickly forested landscape composed of subtropical or tropical vegetation. This type of vegetation makes it nearly impossible to detect and identify IOIs unless they either leave the forested region or approach uncomfortably close to the surveillance asset

Note: The foliage ratings above are just a guide. In most cases the foliage present in a particular scenario will not perfectly match one of the descriptions above. If this is the case, choose the rating from the list above that best matches the surveillance restrictions present in the new scenario

Chapter 2 – Rating of Individual Surveillance Assets

Portability Rating: Indicates how portable an asset is. This rating is based on the size and weight of an asset. If an asset changes size and/or weight when it is being deployed, the size and weight of that asset in its stowed configuration is the data that should be entered. Finally, this rating takes into account the terrain type of terrain an asset can traverse (e.g., self-propelled vs. towed, wheel vs. tracked). The portability of each system is rated on a scale from 1 to 10 with 10 being the most portable

1) No portability requirements at all. Major components can be assembled on site with no respect given to their size and weight.

2) Every component of the surveillance asset(s) used must be transportable via cargo ship or larger

3) Every component of the surveillance asset(s) used must be transportable via heavy transport aircraft or larger

4) Fully assembled surveillance asset is capable of being transported via cargo ship or larger

5) Fully assembled surveillance asset is capable of being transported via heavy transport aircraft or larger

6) Every component of the surveillance asset is capable of being transported via large, wheeled combat truck (e.g., deuce and a half) or larger

7) Fully assembled surveillance asset capable of being delivered to the battlefield via aircraft (e.g., airdrop or low-altitude parachute extraction system (LAPES) or larger. This level of portability also applies to manned surveillance aircraft and UAVs which are required to take off and land from a permanent airfield

8) Fully assembled surveillance asset is capable of being transported via large, wheeled combat trucks or larger

9) The fully assembled surveillance asset is capable of being transported via light truck or a small trailer towed by a light truck (e.g., HMMWV (aka a humvee or hummer) or commercial pickup) or larger

10) Every component the surveillance asset is man-portable

Setup and Teardown Rating: This variable represents the maximum time and manpower required to initially setup and then later repackage an asset. Both the time and manpower to do so are rated on a single scale from 1 to 10 with 10 requiring the least time and manpower. The following is a description of that scale:

1) Impossible to redeploy this asset. The only way to relocate an asset with a rating of 1 is to scrap the existing asset for components that can be used in the new one.

2) This type of asset requires dozens of personnel months to either setup or redeploy. Redeployment of this asset will require the fabrication of new parts and/or the laying of a new foundation. Finally, the initial setup and redeployment of this asset may require the installation of supporting infrastructure, such as power and communications lines

3) This type of asset has been designed to be redeployable, but to do so requires so much effort that it is often used as a permanent installation. The setup and redeployment of this asset may take a dozen individuals between one week and a month to accomplish

4) The deployment and redeployment of this asset takes less than a week. This type of surveillance asset has a command and control center that requires more time to deploy and redeploy than the sensor network it is linked to (approximately a week for the command and control center compared to a few hours for the sensors). Deployment, redeployment, and the addition of sensors is more common than the redeployment of the entire asset

5) This asset is capable of deployment and redeployment in less than 24 hours

6) This asset is capable of deployment and redeployment in less than 6 hours. Satellites with circular or polar orbits that, depending on their altitude and type of orbit, can provide surveillance at intervals of between 90 minutes and 6 hours are also receive a rating of 6[141]

7) This asset is capable of deployment and redeployment in less than an hour. Forward deployed or on the scene maritime assets, UAVs and manned aircraft are rated at 7; the rational being that the time required for these assets to arrive is approximately 1 hour (Depending on the scenario, the time required to arrive on scene could take anywhere from a few minutes to several hours. An approximation of 1 hour was chosen to simplify the rating system)

8) This type of asset consists of sensors that are networked to a mobile command and control center. The time required to deploy and redeploy this asset is dependent on by number of individuals deploying the network, the number of sensors deployed, and the distance those sensors are from the command and control center. The sensors used by this asset must be capable of linking to the mobile command and control center within minutes of their deployment

9) This asset is capable of deployment and redeployment in less than 15 minutes by a maximum of one or two individuals

10) This type of asset is capable of being deployed and redeployed by a single person in less than one minute. The sensors used by these assets must be linked immediately following their deployment to an interface possessed by the operator(s) (individuals who deployed the sensors)

Mobility Rating: The ability of an asset to traverse rough terrain based on the published capabilities of the asset in question and its design features (e.g., self-propelled vs. towed, wheel vs. tracked). This rating is takes into account the terrain rating of a particular scenario, rough terrains demand assets with higher mobility ratings. Mobility is rated on a scale from 1 to 5 with 5 being the most mobile

Assets with a mobility rating of:

1) are capable of traversing slightly uneven terrain with infrequent, small, rolling hills and/or depressions
2) are capable of traversing uneven terrain with a high frequency of small rolling hills, a high frequency of small, rolling hills, and/or a high frequency of shall but steep changes in elevation
3) are capable of traversing highly uneven terrain with a high frequency of large hills
4) are capable of traversing mountainous terrain with large, frequent changes in elevation
5) are airborne and not at all limited by terrain. These assets include manned aircraft, UAVs, and satellites

Foliage Rating: Foliage rating is used to quantify the effect foliage has on the surveillance capabilities of a surveillance asset. As with terrain, the specific type and density of vegetation is not taken into account. Instead, this rating represents the extent to which any foliage inhibits the surveillance capability of an asset relative to other assets. Foliage is rated on a scale from 1 to 5, with 5 representing an asset whose surveillance capabilities are least affected by foliage

Assets with a foliage rating of:

1) can operate effectively in a landscape with short grass or none at all, on which only the occasionally patch of thick vegetation is present
2) can operate effectively in a landscape with tall grass and the occasional tall trees

[141] "What is the Orbit of a Satellite?" Space Today Online, March 2013.

3) can operate effectively in a landscape with short or tall grass that is surrounded by large, dense patches of trees
4) can operate effectively in a thickly forested landscape composed of boreal or temperate vegetation
5) can operate in a thickly forested landscape composed of subtropical or tropical vegetation. This asset may have its surveillance capabilities inhibited but not the extent that it is incapable of providing effective surveillance

Note: The foliage ratings above are just a guide. In most cases the foliage present in a particular scenario will not perfectly match one of the descriptions above. If this is the case, choose the rating from the list above that best matches the surveillance restrictions present in the new scenario

Appendix ii – Off the Shelf Components Compatible for Use Onboard the PSN

Thermal Cameras

FLIR First Mate II and First Mate II MS - $1,900 - $3,000

These are thermal cameras manufactured by FLIR that are designed for use by mariners. The resolution of the thermal images the First Mate II and First Mate II MS are 240 x 180 and 320x240 respectively. Depending on which is purchased, these cameras are capable of detecting (and distinguishing between other IOIs detect) humans at between 1100 and 1500ft and small vehicles at between three and four thousand feet. Both units of them are capable of running for over 5 hours on 4 AA batteries and can be operated continuously for years without malfunction or harming the camera in any way.[142]

Figure ii.1: Handheld FLIR thermal cameras[143]

[142] Information pertaining to the continuous operation of these units was acquired via email with FLIR customer service, a fact which online research reaffirmed.
The rest of the information on these two units was acquired from:
"First Mate II & First Mate II MS Handheld Thermal Night Vision Cameras." FLIR, April 2013.
[143] Ibid.

PTZ M1-D Micro Thermal Camera - $4,000 - $15,000

Despite the fact that it isn't a standard, inexpensive, and commercially available thermal camera, the M1-D is a product worth considering. It is a self-contained system that, in a dome only 4.5" wide, has a thermal camera, standard daytime digital camera, and rangefinder. The hardware cost between four and six thousand dollars, but does not include a controller. The cost of purchasing the camera and all of the ancillary equipment needed to make it work is between approximately twelve and fifteen thousand dollars. Despite having performed a large amount of online research and successfully contacting the manufacturer via email, it is difficult to

Figure ii.2: PTZ M1-D thermal camera[144]

determine what, if any, additional equipment (that equipment which drives the price beyond the cost of the camera itself) would be required to use the M1-D in the construction of a sample PSN system. It is probable that the cost of using the M1-D will be prohibitive even if none of this equipment is required; it may be more expensive and difficult to program around an already

[144] "M1-D Micro Thermal FLIR PTZ Camera." SPI Infrared, April 2013.

developed system than it is to construct and program one from scratch. Moreover, these cameras are manufactured by a single company which is based in China. Using a single, foreign supplier may drive the price up and put US operators at unacceptable risk (e.g., the threat of a virus embedded in the hardware, yes hardware, of the circuitry inside the camera).

Rangefinders

Unfortunately there wasn't enough time to catalogue any commercially available laser rangefinders. However, research has confirmed that there are many different makes and models of them available on the commercial market. The majority of these rangefinders, which cost between $150 and $500, are used for either hunting or golfing. All of them are capable of ranging IOI the size of a person out to 300m, while some (over half) do so at distances of over 750m – far beyond the detection distance of all the thermal cameras being considered for use in the construction of the PSN.

Flashlights

Barska

1200 Lumen High Power LED Tactical - $130-$150

Only a few flashlights were tested for use with the PSN, the most capable being the Barska High Power LED Tactical Flashlight, or BTF (not an official acronym). The BTF was purchased at a retail price of $130, is made from aircraft quality aluminum, has a maximum diameter of 2" and a handle diameter of approximately 1". The small size of both the lens and handle make this an ideal component for inclusion in the construction of a PSN system. Perhaps the most impressive aspect of this flashlight is that it can, on just two AA batteries, operate continuously on its brightest setting (1200 lumens) for 45 minutes.

Testing revealed that a single flashlight is capable of illuminating an area 10m wide at distances approaching 150m. However, at 150m the light may not be enough to capture a good, high-quality image of an IOI. At shorter distances, 90-100m, the flashlight was able to successfully illuminate objects to such an extent that (at night when using this flashlight) an individual (using only their mk 8 sights) is capable of seeing all the detail they would be able to see during the day. These tests suggest that two flashlights would be able to provide this level of illumination at distances between 115-130m, all the while illuminating a much larger area. The only problem with estimating the performance and/or cost of using this flashlight in the construction of a PSN system is the unknown cost of modifying it to the specifications required for use on a PSN system.

Figure ii.3: Barska 1200 lumen flashlight[145]

[145] "1200 Lumen High Power LED Tactical Flashlight." Barska, April 2013.

Appendix iii - Dimension and Mass of Each Sensor and Component

(using 6061 T6 aluminum for all "plates and tubes")

Part 1A: 4.25" x 0.25" plate (0.164 kg), two 4.25" x 0.125" plates (0.082 kg each), twelve 3.8" x 1.5" x 0.125" sheets (0.018 kg each) = 0.462 kg

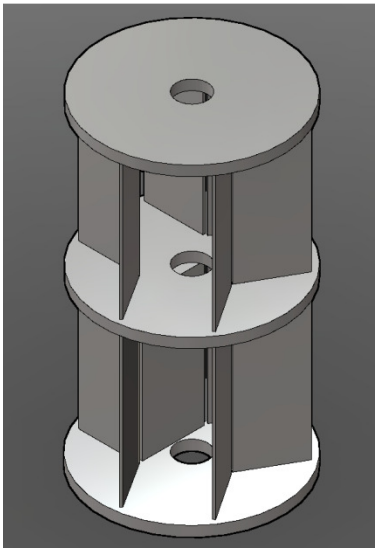

Figure iii.1: Part 1A – Top

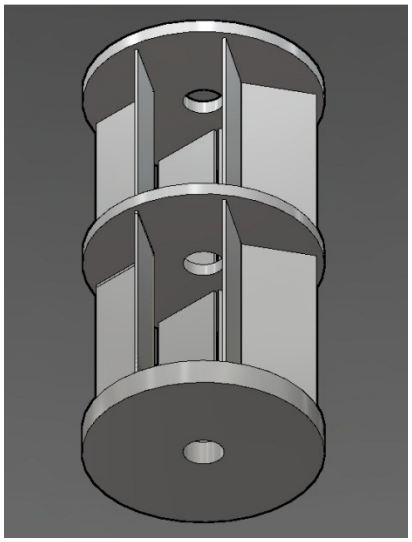

Figure iii.2: Part 1A - Bottom

Part 1B: 4.25" x 0.25" plate (0.164 kg), three 4.25" x 0.125" plates (0.082 kg each), eighteen 3.8" x 1.5" x 0.125" sheets (0.018 kg each) = 0.652 kg

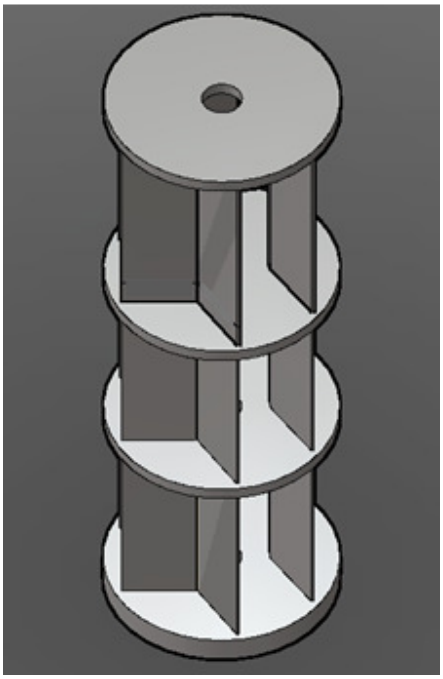

Figure iii.3: Part 1B – Top

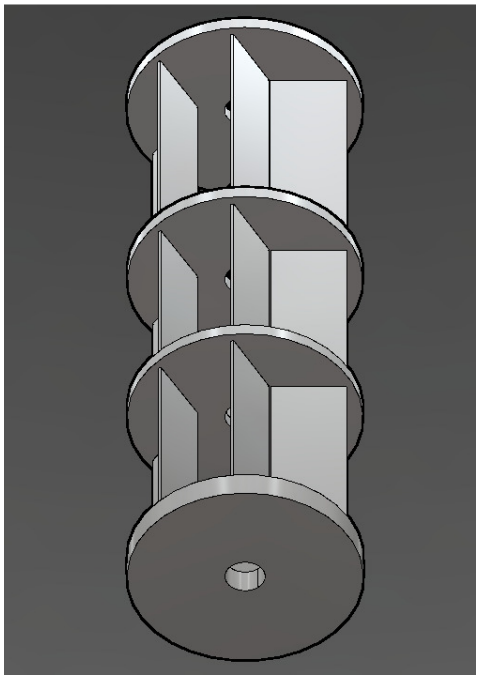

Figure iii.4: Part 1B – Bottom

Part 2A: 4.5” x 1” plate (0.704 kg)

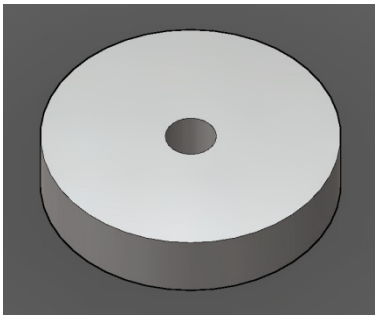

Figure iii.5: Part 2A Top

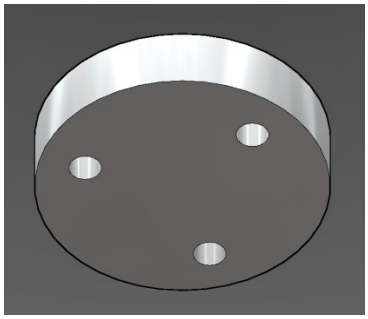

Figure iii.6: Part 2A Bottom

Part 2B: 4.5” x 1” plate (0.352 kg)

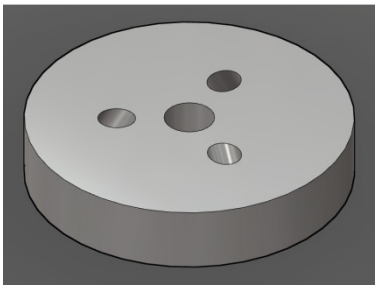

Figure iii.7: Part 2B Top

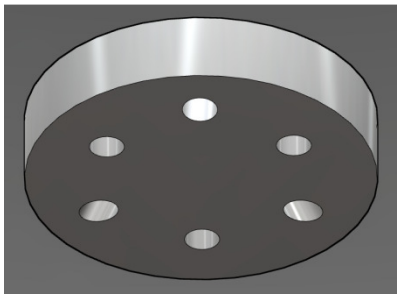

Figure iii.8: Part 2B Bottom

Part 3A: 3” x 8” x 0.25” tube (1.692 kg), 4.5” x 13.5” x 0.125” tube (1.031 kg), 4.5” x ½” plate (0.352 kg), 0.75” x 14” rod (0.606 kg) = 3.682 kg

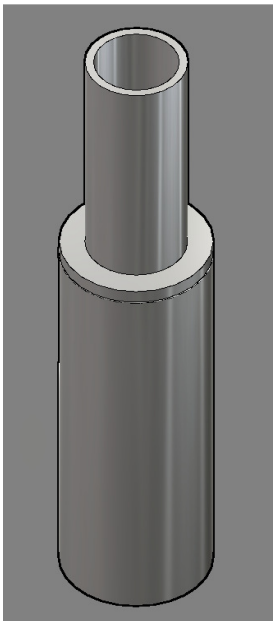

Figure iii.9: Part 3A – Top

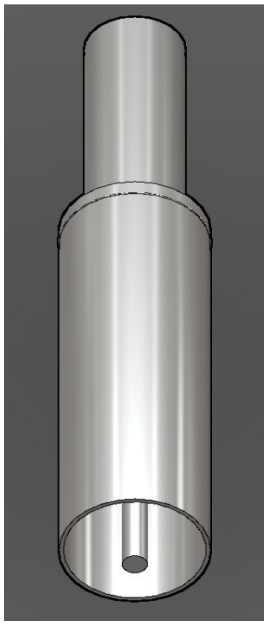

Figure iii.10: Part 3A - Bottom

Part 3B: 3.5” x 8” x 0.125” tube (xxx kg), 4.5” x 13.5” x 0.125” tube (1.031 kg), 4.5” x ½” plate (0.352 kg), 0.75” x 14” rod (0.606 kg), four 1.25” x 0.5” x 8” x 0.125” U-shaped (xxx kg), four 1” x 0.5” x 8” x 0.125” (xxx kg), four 0.75” x 0.25” x 0.125” (xxx kg) = xxx kg

Part 4A: 2.5” x 8” x 0.25 tube (0.332 kg), 4.5” x ½” plate (0.352 kg), 4.5” x 7.5”, x 0.125” tube (0.573) = 1.553 kg

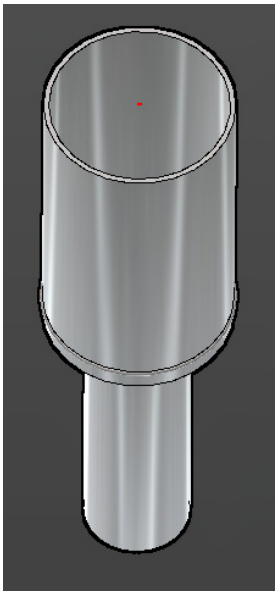

Figure iii.11: Part 4A Top

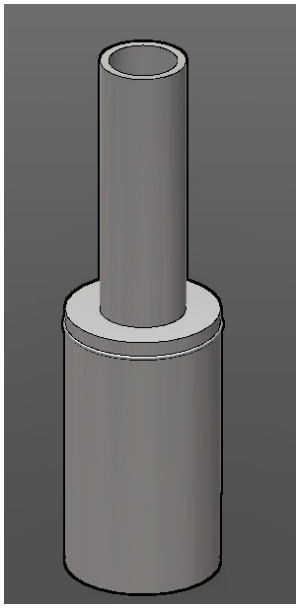

Figure iii.12: Part 4A Bottom

Part 5: two 4” x 0.125” plates (0.070 kg), ¾” x 2” rod (.039 kg) = 0.179 kg

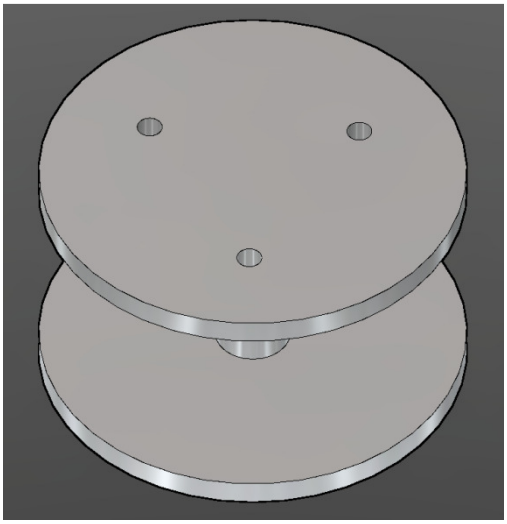

Figure iii.13: Part 5 – Top

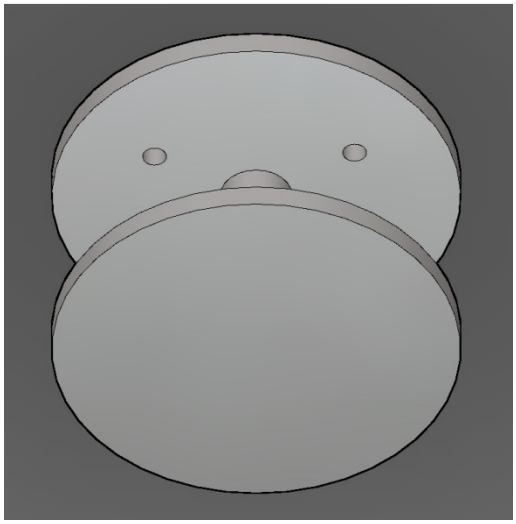

Figure iii.14: Part 5 - Bottom

Part 6A: batteries (0.284 kg each for 11,000 mah batteries), three spikes (0.068 kg each), camera and lens (0.284 kg), three springs (0.243 kg average each) = 1.59 kg with 3 batteries, 2.442 kg with 6 batteries, and 3.294 kg with 9 batteries

Part 6B: batteries (0.284 kg each for 11,000 mah batteries), three spikes (0.068 kg each), camera and lens (1.0 kg), three springs (0.243 kg average each) = 2.306 kg with 3 batteries, 3.154 kg with 6 batteries, and 4.196 kg with 9 batteries

Part 7: parachute and cord = 0.680 kg

Mass Calculations for the Entire Assembly Less Batteries, Camera, Springs

Mass of the assembly with 9 batteries and 6A = 10.885 kg

Mass of the assembly with 6 batteries and 6A = 9.843 kg

Mass of the assembly with 9 batteries and 6B = 11.021 kg

Mass of the assembly with 6 batteries and 6B = 10.559 kg

Assembled Sub-Components

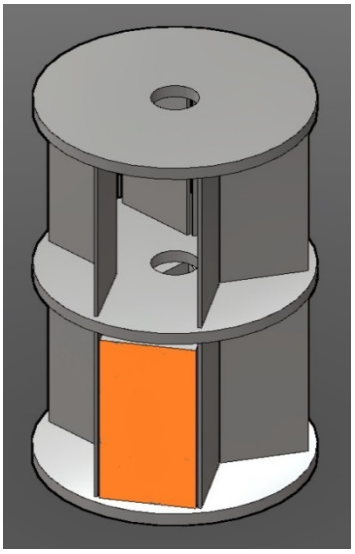

Figure iii.15: Part 1A with 3 batteries installed

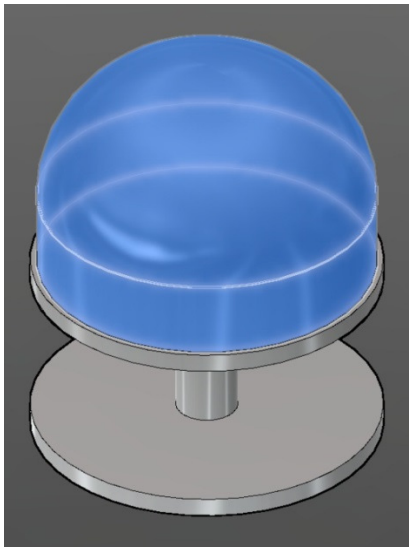

Figure iii.16: Part 5 with camera dome installed

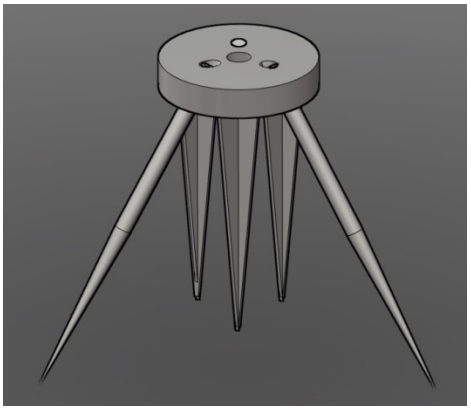

Figure iii.17: Part 2B w/ Spikes

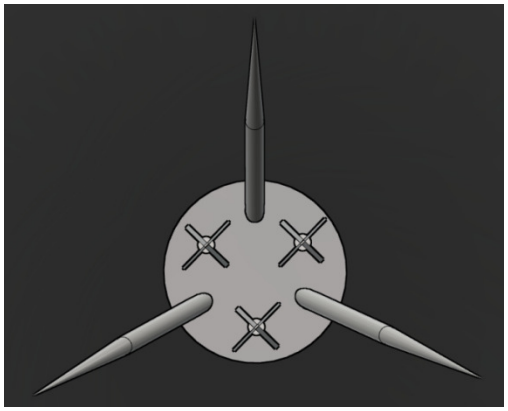

Figure iii.18: Part 2B w/ Spikes Profile

Fully Assembled Air Drop/Tactical P-Sensors

Option 1: 100% waterproof w/ FLIR, 3G, and Wi-Fi

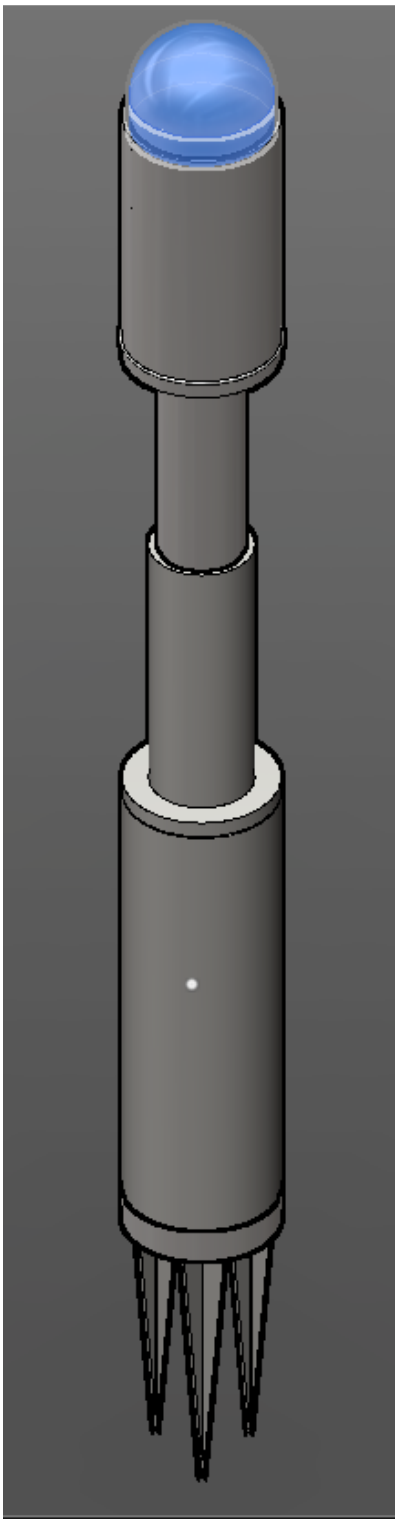

Figure iii.19: Deployed Air Drop Sensor

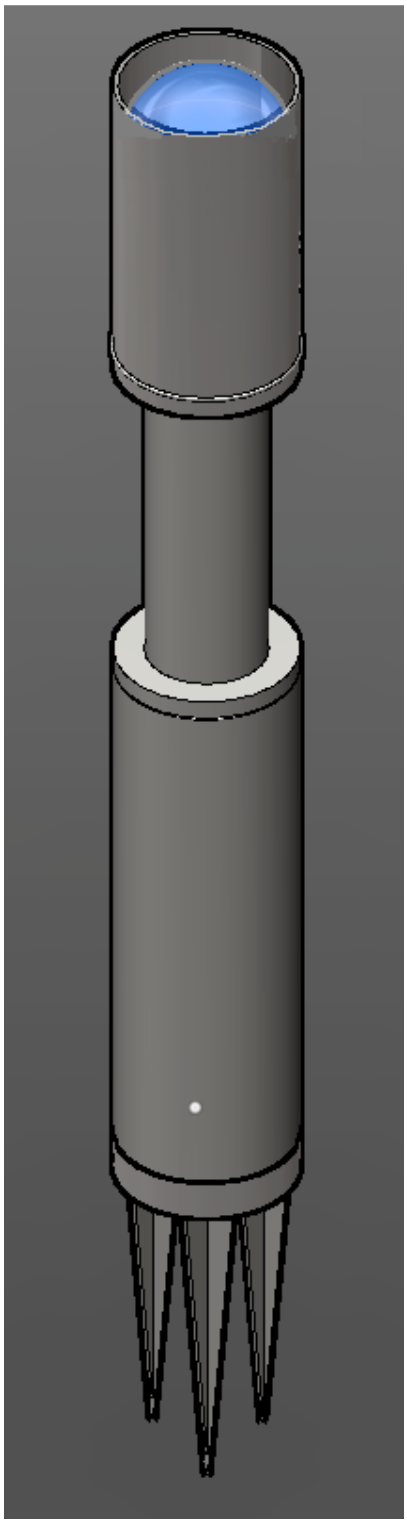

Figure iii.120: Stowed Air Drop Sensor

Fully Assembled Ground Sensors

Option 1: 100% waterproof w/ FLIR, 3G, and Wi-Fi

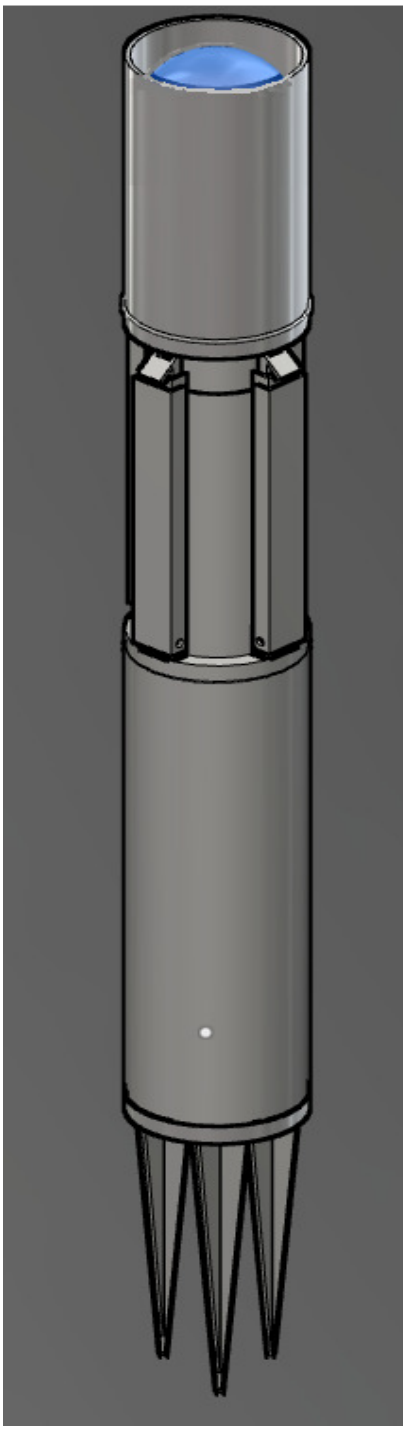

Figure iii.21: Option 1 Stowed

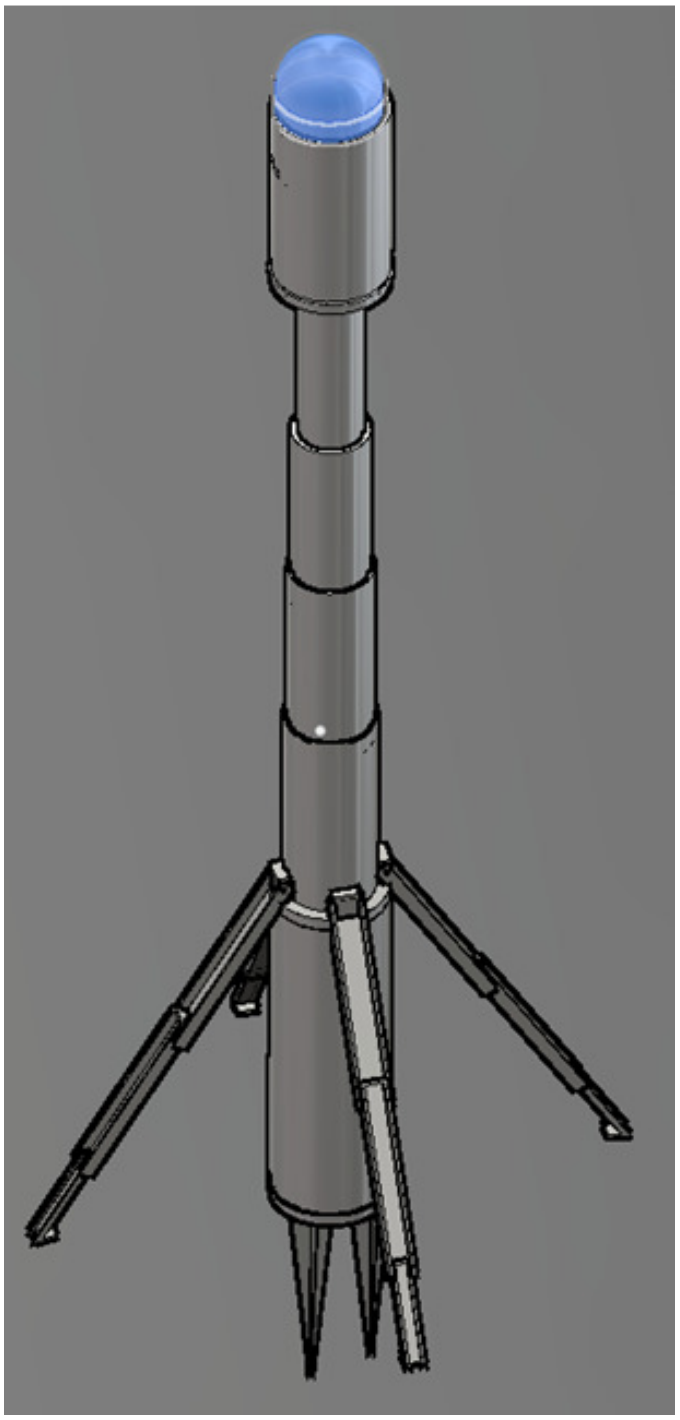

Figure iii.22: Option 1 Deployed

Option 2: FLIR, 3G, Wi-Fi, solar and telescoping sensor array (9.5ft sensor and communications)

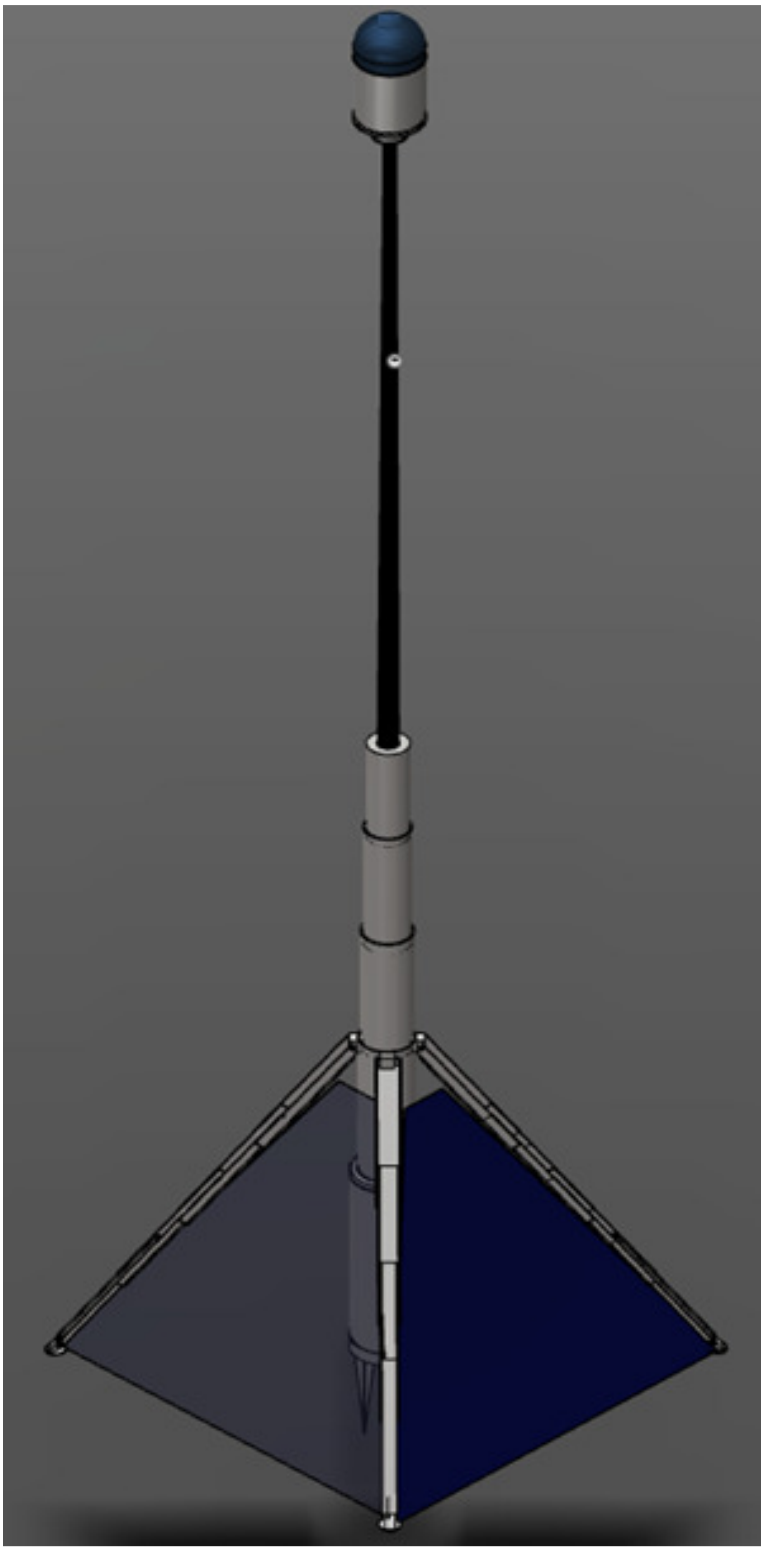

Figure iii.23: Option 2 deployed (note the size of the arms and panels, which attach to the top of the second tier of cylinders, not the first as in other options)

Fully Assembled C-Sensors (camera sits approx. 15" above the ground, 12" for center tube, 2" support shaft, from camera bottom to lens)

Option 1: IR, Wi-Fi, all-terrain mount, solar

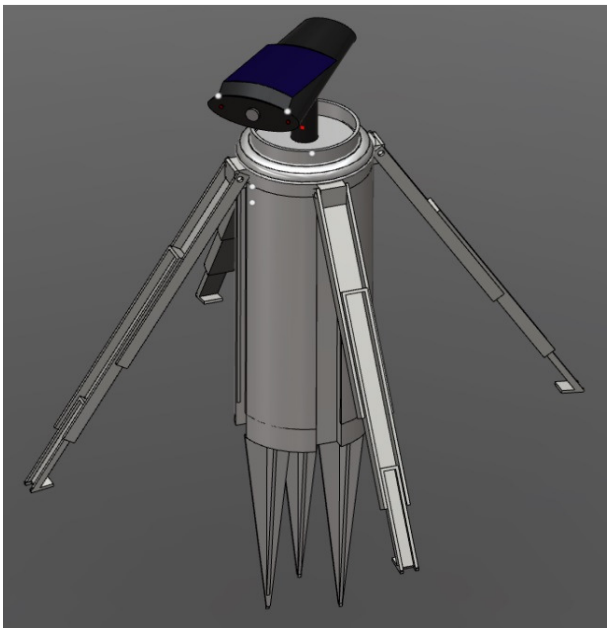

Figure iii.24: Option 1 Deployed

Option 2: Optical zoom with flash, all-terrain mount, solar

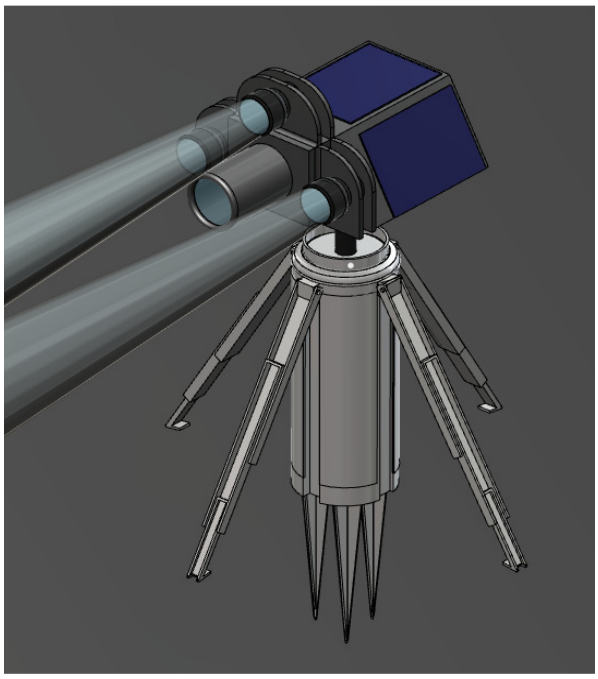

Figure iii.25: Option 2 deployed – front

Appendix iv – Equipping Air Dropped Sensors and the Sensor Development Tool

At the end of this appendix there is a printout from an Excel spreadsheet that was created to enable the quick testing of various sensor configurations. This spreadsheet, sometimes referred to as the Sensor Development Tool (SDT), can determine the G forces at impact and terminal velocity of sensors based on their configuration (what components are installed) and the selected parachutes specifications. The resulting info is compared against the known tolerances of the equipment carried by each sensor. Based on this comparison, adjustments to the design of the parachute are made to attain a velocity that is less than or equal to V_{dt}.[146] In addition to assisting in the design and selection of a parachute, this spreadsheet was designed to be a highly dynamic, time saving tool.

The spread sheet associated with this appendix uses a variety of constants including: the mass of various components, C_d estimates for each type of parachute, and the suspension travel allotted by various components. The ability to alter these values without having to modify the rest of the spreadsheet makes it much easier know how a sensor will perform if modification are made. Without this spreadsheet any change in the design of the sensor would require recalculating many of these values from scratch. The detail put into the development of this spreadsheet has enabled it to serve functions beyond its intended use. For example, the process of actively updating the specification of various components (e.g., cameras, shocks, etc.) was originally very tedious, now all of that can be done by changing values in this one spreadsheet. Nonetheless, the primary purpose of this spreadsheet is to assist in the design of parachutes. The following pages

[146] V_{dt} is used because there are several different velocities being calculated when deploying an air dropped sensor. Further confusing the matter is the fact that some variables, such as terminal velocity and impact velocity, are actually representing the exact same value. However, they need to be given distinct variables since, despite representing the same value, they are a function of different variables. This will become clear later in the appendix. In this case V_{dt} is used as the variable to represent the terminal velocity of the descending sensor.

provide brief introductions to the various physics at work in this spreadsheet, organized by the sub-chapter based on the value that sub-chapter sought to derive.

Calculating Average Deceleration Through Impact
(assuming constant deceleration through impact)

The deceleration through impact is quite possibly the most important value to consider when constructing an air dropped sensor. This value is usually given in terms of 'G's', nomenclature which stands for G-forces or gravitational forces. One gravitational force is equal to 9.81 m/s^2, the acceleration of imparted on objects by the Earth when those objects are at sea-level. With this in mind, G-forces calculated in this section will be done so using the SI unit of m/s^s. After this task has been accomplished, these values will be converted into G-forces in an effort provide a more tangible value, one that is more easily comprehended by the average person than m/s^2.

What makes the calculation of the average deceleration so important is that it provides a reference point for the design of the sensor itself. Each component in a sensor is rated to withstand a maximum sustained deceleration. These components are shielded against near instantaneous deceleration by devices designed to dampen the impact of going from terminal velocity to a complete stop in only a fraction of a second. These 'dampeners' work by extending the time it takes for various components of the sensor to come to a complete stop. Unfortunately, there is little room to increase the existing dampening of the sensor. These limitations imposed by the compact design of the sensor and the desire use as many components from the standard sensor as possible. As a result, the average deceleration through impact must be controlled by altering the sensor's impact velocity, which in this case is also the sensor's terminal velocity.

Terminal velocity is the speed at which the force imparted on an object by gravity is equal to the force of drag. When an object reaches this velocity it will cease to accelerate. This section uses both known and derived values to determine what the terminal velocity must be to ensure that the sensor's various sub-components are not subjected to deceleration that exceeds the specified tolerance of each sub- component. Meanwhile, the design of the sensor itself leaves little room for modifications that reduce the

The first step in calculating the terminal velocity of a sensor based on its average deceleration through impact is determining what the stopping distance, S_d, is for each sub-component of the sensor itself. The following is taken directly from the spreadsheet:

Component & Unsprung Length (m)	***Component Travel (m)***	***LC Low G***	***LC High G***	***HC Low G***
LC Synthetic Cushion / 0.0064	0.0032	Yes	Yes	No
HC Synthetic Cushion / 0.0128	0.0064	No	No	Yes
Main Shock Absorber / 0.381	0.1778	Yes	Yes	Yes
Stakes / 0.2032	0.1524	Yes	Yes	Yes
High G Battery Shocks / 0.0889	0.0445	No	Yes	No
LC Shocks / (0.0381)	0.0191	Yes	Yes	No
Battery Cushion (0.0128)	0.0064	Yes	Yes	Yes
	Total Sensor Travel S_d (m)	0.3525	0.3525	0.3366
	Total Battery Travel S_d (m)	0.1588	0.2033	0.1588

Table iv.1: Average deceleration per component

The table above is broken down by component and sensor variant. In this case, sensors vary based on their payload and the magnitude of deceleration (or G's) that sensor is designed to endure. The three variants are: Light Camera Low G, Light Camera High G, and Heavy Camera Low G. The total S_d of each sensor is located at the bottom of the table. Using these values, a hypothetical value for the velocity of the sensor at impact (V_{di})[147] and the time (t) required to

[147] Velocity of the descending sensor at impact. The formula used is the same formula used to calculate V_{dt}. This is based on the assumption that the sensor will reach V_{dt} before impacting the ground. If it does not this value will be different, hence the use of a different variable.

decelerate from $V_{di} \rightarrow V_0$ can be calculated. Based on this calculation the acceleration (a_d) through impact can be derived using the following formula:

$$S_d = ½\ a_d * t^2 – V_{di} * t$$

Unfortunately, the objective is to determine what V_{di} is required for a specific deceleration, not the other way around. Therefore, the equation must be rewritten so that V_{di} is a function of t, S_d, and a_d. This new equation is:

$$V_{di} = (½\ a_d * t^2 - S_d) / t$$

At this point the equation above is still a function of t. This equation must be rewritten as a function of a_d and S_d since t itself is not a known value. Fortunately, this is a simple equation to derive:

$$V_{di} = ½\ a_d * t^2 \rightarrow t = ((2 * S_d) / a_d)^{0.5}$$

By combining the functions for A_d and t we arrive at the final equation for V_{di} which is:

$$V_{di} = (½\ a_d * (((2 * S_d) / a_d)^{0.5})^2 - S_d) / (((2 * S_d) / a_d)^{0.5})$$

Determining the Proper Parachute Design for Air Dropped Sensors

The proper parachute is an essential component of the air dropped sensor. Too small a parachute and the sensor will be damaged on impact. If too large a parachute is used there are a myriad of problems that become obvious. The first of these deals with the flight of the sensor itself. A parachute that is too large may cause the sensor to strike the earth with insufficient velocity to plant (or stake) itself in the ground. Another problem dealing with the flight of the sensor is drift. The larger the parachute the more likely the parachute is to either sail or oscillate while descending. If the parachute does either then its descent has a lateral component, increasing the chance that the sensor will not properly plant itself in the ground. Finally, a large parachute may inhibit the sensors ability to penetrate dense foliage.

The second set of concerns that must be addressed when deciding on a parachute deal with the technical and operational needs of the system itself. If too large a parachute is used each sensor will be both heavier and more expensive. Using a heavy sensor means that aircraft will be able to carry less of them than they otherwise could. Moreover, if the sensor descends slowly, on the back of a large parachute, it is more likely to be spotted by those whom the sensor is intended to monitor.

A final detail to consider is what type of chute. Various chutes have their benefits and shortcomings. Beyond that, one can choose certain 'options' for a parachute such as how long the risers are or how large, if any, of a hole is in the center of the canopy. Regardless of what issues are considered when choosing a parachute, the objective should be to use one that provides the most stable and highest velocity flight path that is technically possible (without damaging the sensor).

The spreadsheet at the end of this appendix uses a plethora of variables to determine a sensor's terminal velocity, most of which have to do with the massive variety of parachute options that are available. Deriving the terminal velocity of a sensor based upon its aerodynamic and Newtonian qualities may seem at first a little counter-intuitive given what the objective of this chapter: to determine a correct parachute for a specific sensor. However, this is exactly what is being calculated and for good reason. Unlike the previous calculations performed to derive V_{di} as a function of a_d, there are many combinations of variables that can produce the same terminal velocity (V_{dt}) when choosing a parachute (in the case of deceleration, there was only one value of V_{di} for a given value a_d since S_d was known from the start). With parachutes it is more important to select the type of parachute first, usually a decision that is based on the type of sensor being deployed, the environment of deployment, and the operational needs of the mission.

However, even after deciding on a specific type of parachute there is still more than one independent variable left. Nonetheless, a specific parachute can be calculated based on additional criteria such as the desired stability of a falling sensor. Unfortunately it is difficult to determine how changes to the parachute affect these criteria without conducting real life trials using full size sensors. Because of this limitation, those attributes which are difficult to predict/calculate will be left out of the discussion, with the exception being that when parachute designs are introduced any inherent qualities of those parachutes will also mentioned.

The next few paragraphs will introduce the various types of parachutes available, design variables, and any qualities inherent to them. In addition, the equations used to derive the terminal velocity for each parachute will be summarized, beginning with the only equation which is inherent to every type of parachute.

Note: All of the parachutes in this section are going to serve the role of a drogue parachute. This type of parachute typically functions at very high speeds and can typically be found on aircraft, spacecraft, and airdropped munitions.

Equations Inherent to All Parachute Types

The following equation is used to determine the terminal velocity of an object given certain perimeters:

$$V_{dt} = \left(\frac{2*m*Fg}{\rho*A*Cd}\right)^{0.5}$$

This equation depends on the coefficient of drag (C_d), mass (m) in kg, force of gravity (F_g) in m/s^2, air density (ρ) in kg/m^3, and surface area (A) in m^3 of the object that is perpendicular to the velocity of that object. Some of these variables have been already been introduced, some have not.

C_d is a dimensionless variable that expresses the ability of a shape to resist the force of drag imparted on it by the fluid, in this case air, through which that shape is moving. This value is independent of the both the shape's size, mass, and density (i.e., two objects can have the same size, shape, and different masses but still possess the same C_d). All things constant, as C_d increases so too does the force of drag acting on the object. There is however more to estimating the C_d of a falling object. As V_{dt} can increase or decrease (depending on the parachute) as C_d decreases, if only marginally. This variation is difficult to gauge since the flow of air around the object itself can change radically with a change in V_{dt}. Because of this, the C_d for each component will be estimated using a more simple method for all calculations performed using the SDT.

Every component of a sensor must be accounted for when calculating the V_{dt} of a falling object. In this case that usually means the drag due to the sensor and the parachute. When deciding on the surface area to account for it had to be determined whether to account for the surface area of the sensor (A_{ds}) and that of the entire parachute (A_p) or the surface area of the sensor and parachute less the area of the parachute directly above the sensor. The two facts that decided whether to account for the drag of the sensor and the parachute above it were the shape of the sensor and the distance between the top of the sensor and the bottom of the parachute. Since nearly every air dropped sensor has a rounded top and is suspended a distance of between two to three meters below the parachute it is highly probable that the vacuum created behind the path of the falling sensor will have dissipated by the time that air contacts the parachute. Next, the equation above must be rewritten so that it can account for drag imparted by both the sensor and the parachute, each of which has its own C_d and A_d.

From this point on the C_d and A_d for parachutes and sensors will be represented by the following variables:

C_{dp} = C_d of a parachute C_{ds} = C_d of a sensor A_{dpd} = A_d of a deployed parachute A_{ds} = A_d of a sensor

Using these variables the equation for V_{dt} is rewritten to account for the drag imparted on the falling sensor by both the sensor itself and the parachute dangling above it. This new equation is:

$V_{dt} = \left(\frac{2*m*Fg}{(\rho*Ads*Cds)*(\rho*Adp*Cds)}\right)^{0.5}$ where m is the mass of the entire assembly

The final equation shared by nearly all the parachutes examined in the thesis is that which governs the base C_{dp} for each parachute. This simple equation is only an estimate, but is as follows:[148]

$C_{dp} = A_{dpd} / A_{dpf}$

In this equation A_{dpf} is the total surface area of the parachute (i.e., if the parachute were laid out flat) while A_{dpd} is the previously stated variable representing the area of the parachute that is perpendicular to the motion of the descending sensor. Bear in mind that this relationship does not account for velocity. If it did, flat parachutes would be superior to all others, which they are not. This is simply a reference point for how parachutes of a similar design behave when their geometry is altered.

In addition to the formula above there are some constants worth mentioning that are used in the coming sections and in the SDT. First, the C_{ds} used for each all calculations of V_{dt} is C_{ds} = 0.75. This is a rough calculation based on the known C_d for long cylinders (0.82), short cylinders

[148] Sher, S. and Young, I. *Drag Coefficients for Partially Inflated Flat Circular Parachutes.* NASA, Washington DC, September 1971. p. 2

(1.15)[149] and spheres (0.47). This estimation takes into account the general shape of the sensor (long cylindrical), the narrow center section with partially exposed cylindrical faces on the top and bottom (short cylinder), and the dome shaped camera lens (spherical). The last and final constant is actually one which is programmed into the spreadsheet itself. In order to attain realistic values of terminal velocity for each parachute, the C_{dp} was first determined using the equation above, after which V_{dt} was calculated as normal. Next, this V_{dt} was used to calculate a second C_{dp} that takes into account the original velocity. This new C_{dp} is then used to calculate a final V_{dt}. The trick was to modify the second C_{dp} equation so that the second C_{dp} mirrors those of real parachutes. Though exhaustive, this process provides an excellent estimation of how C_d varies with velocity.

Flat Parachutes

Flat parachutes are the least efficient and capable of all commonly used parachutes. Their C_{dp} is fairly high at low velocities (below 10 m/s).[150] Because of this, the previous equation for calculating a parachute's C_{dp} works well so long the velocity is low. However, the C_{dp} of flat parachutes decreases considerably. Because of this, these parachutes tend to collapse the faster they travel. Making matters worse, when this parachute collapses its diameter decreases and its height increases, resulting in lower values for both C_{dp} and A_{dpd}.

Unfortunately it is difficult to determine the how much a flat parachute's A_{dpd} decreases as velocity increases. To simplify the problem, this characteristic was accounted for (in SDT) when programing the calculation of this parachutes velocity-corrected C_{dp}. As if the flat parachute was not lacking in enough qualities already, it is also inherently unstable at high velocity. The only

---

[149] Ludtke, W. *Effects of Canopy Geometry on Drag Coefficients of a Cross Parachute in the Fully Open and Reefed Conditions for a W/L ratio of 0.26.* Naval Ordinance Laboratory, Silver Spring, MD, August 1971.

[150] Sher, S. and Young, I. *Drag Coefficients for Partially Inflated Flat Circular Parachutes.* NASA, Washington DC, September 1971. p. 8

real advantage to using a flat parachute is that it is inexpensive and performs well at low velocity. Considering the fact that the V_{di} of PSN sensors is two to three times velocity at which flat parachutes are designed to function, these parachutes are not a viable option for use on PSN sensors.

Figure iv.1: A 36" flat parachute used the U.S. Army to deploy flares

Domed Parachutes

Domed parachutes are some of the most common parachutes in existence. These parachutes perform considerably better at higher velocities than flat ones. Depending on the specific design of the parachute and velocity, C_d can vary between 0.4 and 1.4. For the sake of this thesis, SDT was calibrated according to NATO tests performed at high velocities on a several different

domed parachutes[151]. These parachutes tested varied considerably based on seeming innocuous details such as the type of stitching and fabric used to construct them. With that in mind, the variables used to determine the V_{di} for these parachutes has been reduced to C_{dp}, hole diameter, and canopy inflation.

The only new variable to consider is hole diameter, or d_h. This variable refers to a hole that can be cut into the very top of the parachute. This hole allows some of the air trapped in the canopy to escape through it, increasing stability and reducing lateral drift. This value is usually between $1/6^{th}$ and $1/7^{th}$ the diameter of a deployed parachute (d_p).

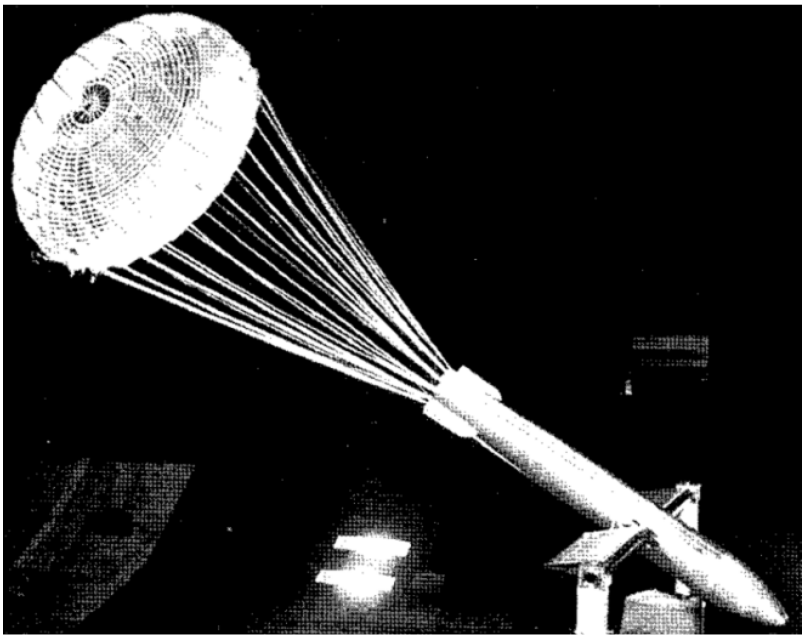

Figure iv.2: Dome type drogue parachute with hole in the top[152]

Cross Parachutes

The modern cross parachute is a relatively recent design compared to those which have been discussed so far. While it is more complicated to construct than a flat parachute it is easier to

[151] Maydew, R.C. and Peterson, C.W. *Design and Testing of High-Performance Parachutes*. Advisory Group for Aerospace Research and Development, Neuilly Sur Seine, France, 1991. p. 15
[152] Ibid. p. 162

construct than a regular dome parachute and both less expensive and considerably less complex than high speed dome parachutes. It should come as no surprise that cross parachutes are also an excellent design for high speed applications, in most cases serving a drogue parachute. Drogue chutes are parachutes that are designed to slow but not necessarily stop a craft. This means that the average cross parachute is designed to function at a higher velocity than most flat and domed type parachutes. Just as important is the fact that these cross parachutes are fairly stable at high speeds – they have to be when serving as a drogue parachute that is attached to an aircraft or bomb!

Because cross parachutes are designed to function at high velocity they are the only parachute studied in this appendix that has a C_{dp} that increases, however slightly, as velocity increases. There is a slight drop between 0 and 15 m/s but it immediately climbs as velocity increases, well beyond 90 m/s. The average C_{dp} for this type of parachute is 0.68 at 30 m/s, 0.70 at 60 m/s, and 0.72 at 90 m/s.[153] The SDT has been calibrated using these values as a baseline. When it comes to high velocity parachutes the cross is hard to beat. This is an important fact when considering what parachute to equip the PSN airdropped sensors with since these sensors would be released from aircraft traveling at velocities that are often in excess of 100 m/s. The cross parachute's ability to sustain a relatively high C_{dp} at this velocity means that the initial deceleration will be faster than that of dome parachutes, something which is crucial if PSN sensors are deployed at a high velocity and low altitude.

The A_{dp} and A_{df} of the cross parachute are as follows:

$A_{dp} = (2 * ((l_p * w_p))/(0.5 * \pi) - (1/3 * w_p)$ $\quad$ $A_{df} = 2*(l_p * w_p) - (1/3 * w_p)$

[153] Ludtke, W. *Effects of Canopy Geometry on Drag Coefficients of a Cross Parachute in the Fully Open and Reefed Conditions for a W/L ratio of 0.26.* Naval Ordinance Laboratory, Silver Spring, MD, August 1971.

In this equation l_p is the variable representing the length of a single rectangular section and w_p the width of that same section.

Figure iv.3: F-16 using a cross type drogue parachute - Photo courtesy of Aerazur

Inverted Rigid Parachutes

a_d = Deceleration, which is measured in m/s^2, ft/s^2, or G's. One G = 9.81 m/s^2 or 32.2 ft/s^2

S_d = Stopping Distance, which is measured in m/s or ft/s Time from impact to zero velocity = t

t_b = time to go from impact to zero velocity for the batteries, spikes, and parts 1 and 3

t_c = time to go from impact to zero velocity for the camera, part 2, and associated electronics

$S_d = ½ A_d*t^2 – V_d * t$ = total distance internal components have to decelerate from V_d to 0

S_d will vary based on the component and how far the sensor sticks into the ground (max of 0.667 ft)

For the purpose of this derivation S_d for the batteries and impact spikes (and all of parts 1 and 3) will be estimated at S_b = 8" (0.203 m) and S_{c1} = 16" (0.406 m) with 8" (0.406 m) of spring

compression, S_{C2} = 24” (0.610 m) for a device with 16” (0.406 m) of spring compression, and S_{c3} = 18” = 0.457 m and 10” (0.254 m) of spring compression.

Determining What Spring to Use for Each Section

Stopping distance = x = 3” for under camera, 7” for center tube, and 8” for spikes = 1.416 ft = 0.508 m

Stopping distance for the batteries is 8” for the spikes and 2” for the battery springs = 0.833 ft = 0.254 m

Total mass of the assembly with 3 batteries = 9.453kg

Total mass of the assembly with 6 batteries = 10.301 kg

So, the first spring constant is that for the entire bottom assembly which will be stopping in 0.203 m (spikes). However, after this section has stopped the rest of the sensor will still be in motion. The batteries will have a travel of 0.051” additional travel. The spring used in the batteries should prolong the impact as much as possible but also ensure that the batteries are stopped when the spring is fully compressed. If they are not, the batteries will experience rapid deceleration and extremely high G forces as the remaining velocity is absorbed near instantaneously.

The second step is to ensure that shock absorber and spring in the mid-section have the proper spring constant. If they do, they will extend the time through impact as long as possible but also ensure that the upper section (minus camera assembly) to a complete stop when the spring is nearing full compression. In this section, the force imparted by the camera and its assembly are ignored to simply the problem. The mass of the camera, though not negligible, can be accounted for by using a slightly stiffer center spring.

The final component is to determine what the proper spring constant is for the spring below the camera. Once again, the objective is to extend the stopping time as long as possible. However, in this case, the time that the spring should extend time beyond is the time it takes the center

spring to fully compress. As in the previous cases, the camera should come to a complete stop when the spring in the upper section has reached its maximum compression.

m = meters for the equations below

F = Force = N p = momentum = kg * (m/s) = N*s x = spring compression/stopping distance = m
E_k = Kinetic Energy = (kg * m^2)/s^2 = J E_p = Potential Energy = J k = spring constant = N/m
w = work = J

m = mass for the equations below = 9.453 kg v_{di} = velocity at impact = 14.691 m/s x = 16" = 0.406 m

$E_k = ½ m * (v_{di})^2$ and $E_p = E_k = ½ k * x^2 \rightarrow k = (2*E_k) / x^2$

$E_k = ½*9.453 * 14.691^2 = 1020.099$ J $E_p = 1020.099 \rightarrow w = F * x = 1020.099$
F = w / x = 1020.099 / .403 = 2512.559 N through impact $F = k*x \rightarrow k = F / x = 6188.569$ N/m

m = mass for the equations below = 9.453 v_{di} = velocity at impact = 22.007 m/s x = 16" = 0.406 m

$E_k = ½ m * (v_{di})^2$ and $E_p = E_k = ½ k * x^2 \rightarrow k = (2*E_k) / x^2$

$E_k = ½*9.453 * 22.007^2 = 2289.082$ J $E_p = 2289.082 \rightarrow w = F * x = 2289.082$
F = w / x = 2289.082 / .403 = 5680.104 N through impact $F = k*x \rightarrow k = F / x = 13990.404$ N/m

Note: Additional calculations required to determine the correct springs and dampeners for use in the final design. The work provided in this section is more than enough of a starting point from which that work can be performed.

References

Criteria: Based on legislation, policy, and audits/reviews

"2011 Air and Marine Milestones." U.S. Department of Homeland Security: Customs and Border Protection: Office of Air and Maritime, December 2011. Accessed February 26, 2013 from: http://www.cbp.gov/xp/cgov/border_security/am/operations/2011_achiev.xml

A Line In The Sand: Countering Crime, Violence And Terror At The Southwest Border. U.S. Congress: House Committee on Homeland Security, November 2012.

Arizona Border Surveillance Technology: More Information on Plans and Costs Is Needed before Proceeding. U.S. Government Accountability Office, November 2011.

Border Patrol: Key Elements of New Strategic Plan Not Yet in Place to Inform Border Security Status and Resource Needs. US Government Accountability Office, December 2012.

"Border Patrol Overview." U.S. Department of Homeland Security: Customs and Border Protection: Border Patrol, January 2011. Accessed February 22, 2013 from: http://www.cbp.gov/xp/cgov/border_security/border_patrol/border_patrol_ohs/overview.xml

Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders. U.S. Government Accountability Office, March 2011.

Border Security: Opportunities Exist to Ensure More Effective Use of DHS's Air and Marine Assets. U.S. Government Accountability Office, March 2012.

"CBP Intercepts Cocaine Smugglers in Open Water" U.S. Department of Homeland Security: Customs and Border Protection, January 2013. Accessed March 12, 2013 from: http://www.cbp.gov/xp/cgov/newsroom/news_releases/local/2013_nr/jan13/01302013_3.xml

"Critical Infrastructure Protection." U.S. Department of Homeland Security, February 2013. Accessed February 26, 2013 from: http://www.dhs.gov/topic/critical-infrastructure-protection

"December 17th 2003, Homeland Security Presidential Directive/HSPD-7." White House, December 2003. Accessed February 26, 2013 from: http://georgewbush-whitehouse.archives.gov/news/releases/2003/12/20031217-5.html

"DHS Napolitano' Touts Border Security." CBS News, February 2013. Accessed February 23, 2013 from: http://www.cbsnews.com/8301-250_162-57567822/dhs-napolitano-touts-border-safety/

Fact Sheet: CBP Northern Border Division. U.S. Department of Homeland Security: Customs and Border Protection, May 2012.

Fact Sheet: Office of Air and Marine. U.S. Department of Homeland Security: Customs and Border Protection: Office of Air and Marine, January 2011.

"FLIR Ranger III MS." ThermalVideo.com

Homeland Security: DHS is Addressing at Chemical Facilities, but Additional Authority is Needed. U.S. Government Accountability Office, June 2006.

"Iran Shows Film of Captured US Drone." BBC World News, December 8, 2011. Accessed April 23, 2013 from: http://www.bbc.co.uk/news/world-middle-east-16098562

Lewis, Ted G. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley and Sons Inc., Hoboken, New Jersey, 2006.

"MANPADS: Combating the Threat to Global Aviation from Man-Portable Air Defense Systems" U.S. Bureau of Political-Military Affairs, July 27, 2011. Accessed March 12, 2013 from: http://www.state.gov/t/pm/rls/fs/169139.htm

Mobile Surveillance Capability. Telephonics Corporation, 2012.

National Drug Threat Assessment for 2011. U.S. Department of Justice: Drug Enforcement Agency, August 2011.

"Our Mission." U.S. Department of Homeland Security, February 2013. Accessed February 22, 2013 from: http://www.dhs.gov/our-mission

Performance and Accountability Report: Fiscal Year 2011. U.S. Department of Homeland Security: Customs and Border Protection, March 2012.

Progress Made and Work Remaining after Nearly 10 Years in Operation. U.S. Government Accountability Office, February 2013.

"Protecting Our Borders: This is CBP." U.S. Department of Homeland Security: Customs and Border Protection, September 2012. Accessed February 22, 2013 from: http://www.cbp.gov/xp/cgov/about/mission/cbp.xml

Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure. U.S. Government Accountability Office, December 2005.

Secure Border Initiative Fence Construction Cost. U.S. Government Accountability Office, March 9, 2009

Snapshot: A Summary of CBP Facts and Figures for 2012. U.S. Department of Homeland Security: Customs and Border Protection, January 2013.

"Tactical airfield landing" Wyoming Air National Guard: 153rd Airlift Wing, Cheyenne, WY, March 2013. Accessed March 31, 2013 from: http://www.153aw.ang.af.mil/photos/mediagallery.asp?page=6

"Who We Are and What We Do." U.S. Department of Homeland Security: Customs and Border Protection: Border Patrol, September 2008. Accessed February 18, 2013 from: http://www.cbp.gov/xp/cgov/border_security/border_patrol/recruiting_hiring/who_we_are.xml

Zuckerman, Jessica. "The 2013 Homeland Security Budget: Misplaced Priorities." The Heritage Foundation, March 23, 2012. Accessed January 3, 2013 from: http://www.heritage.org/research/reports/2012/03/the-2013-homeland-security-budget-misplaced-priorities

Existing and Proposed Systems: Used for comparison to the PSN, as a source of criteria, and as a source of the features expected to be included in the design of the PSN

"1200 Lumen High Power LED Tactical Flashlight." Barska, April 2013. Accessed April 24, 2013 from: http://www.barska.com/Flashlights-1200_LUM_Flashlight_with_Rechargeable_Batteries.html

Cam-V Mobile Security System Spec-Sheet. Cameras Onsite, 2013.

"Customs Blackhawk from Tucson Air Branch at Dover A.F.B. to provide air security." Customs and Border Protection, April 2013. Accessed April 23, 2013 from: http://www.cbp.gov/ImageCache/cgov/content/newsroom/photogallery/9_5f11_5fwtc/highresimage/wtc_5f14_2ejpg/v1/wtc_5f14.jpg

Davis, Katrina. "Police to buy mobile observation tower." U-T San Diego, March 2, 2009. Accessed February 28, 2013 online from: http://www.utsandiego.com/news/2009/jan/08/1cz8tower205326-police-buy-mobile-observation-towe/

Fact Sheet: CBP Northern Border Division. U.S. Department of Homeland Security: Customs and Border Protection, May 2012.

"Factsheet: MQ-1 Predator Unmanned Aerial Vehicle." U.S. Air Force, November 5, 2008. Accessed April 23, 2013 from: http://www.acc.af.mil/library/factsheets/factsheet.asp?fsID=2352

"Factsheet: MQ-9 Reaper." U.S. Air Force, January 5, 2012. Accessed April 23, 2013 from: http://www.af.mil/information/factsheets/factsheet.asp?id=6405

Fact Sheet: SBInet Block 1. U.S. Department of Homeland Security: Customs and Border Protection, March 2009.

Fact Sheet: SBInet Field Test Lab. U.S. Department of Homeland Security: Customs and Border Protection, March 2009.

Fact Sheet: SBInet Project 28. U.S. Department of Homeland Security: Customs and Border Protection, March 2009.

"FEMA: Port Security Grant Program." U.S. Department of Homeland Security: Federal Emergency Management Agency, June 2012. Accessed February 28, 2013 from: http://www.fema.gov/port-security-grant-program

"First Mate II & First Mate II MS Handheld Thermal Night Vision Cameras." FLIR, April 2013. Accessed April 24, 2013 from: http://www.flir.com/cvs/americas/en/maritime/view/?id=51292&collectionid=785&col=51293

"FLIR Systems Announces Agreement to Acquire ICx Technologies." FLIR Investor Relations, August 16, 2010. Accessed April 2, 2013 from: http://investors.flir.com/releasedetail.cfm?ReleaseID=499403

"Gatekeeper – Automatic and Under Vehicle Inspection Systems." Army-Technology.com, 2012. Accessed March 5, 2013 from: http://www.army-technology.com/contractors/surveillance/gatekeeper

GENERAL SERVICES ADMINISTRATION FEDERAL SUPPLY SERVICE AUTHORIZED FEDERAL SUPPLY SCHEDULE PRICE LIST, CONTRACT NUMBER:GS-07F-0117U, U.S. General Services Administration, 2005.

Gunter, Ford. "Local Firms Mobile Surveillance System Could be Border Solution. Houston Business Journal, 2012. Accessed March 3, 2013 from: http://www.camerasonsite.com/news/ASAPSecurity_border_news.pdf

"Greenville Operations." Lockheed Martin, April 2013. Accessed April 21, 2013 from: http://www.lockheedmartin.com/us/aeronautics/mmro/greenville-operations.html

"Ground Surveillance Systems IFT." Telephonics, March 2013. Accessed March 23, 2013 from: http://www.telephonics.com/cis_groundsurvsys.asp

Hock, Jessica. "FLIR Purchases ICx Technologies for $274 million." Oregon Business, August 16, 2010. Accessed February 28, 2013 from: http://www.oregonbusiness.com/the-latest/3964-flir-systems-icx-technologies-goverment-division

"ICx Technologies Inc." Security Technology News, April 2013. Accessed April 20, 2013 from: http://www.security-technologynews.com/suppliers/icx-technologies-inc.html

"Integrated Fixed Towers." Federal Business Opportunities Office, January 2011. Accessed March 24, 2013 from:

https://www.fbo.gov/index?s=opportunity&mode=form&id=ddaa2027c96f3944a325426c6877b35a&tab=core&_cview=1

IT Program Assessment: CBP Video Surveillance System Program. U.S. Department of Homeland Security: Office of the Chief Information Officer, March 2012.

IT Program Assessment: Customs and Border Protection Mobile Surveillance System. U.S. Department of Homeland Security: Office of the Chief Information Officer, March 2012.

Miller, Greg. "CIA flew stealth drones into Pakistan to monitor bin Laden house." The Washington Post, May 17, 2011. Accessed March 12, 2013 from: http://articles.washingtonpost.com/2011-05-17/world/35233221_1_stealth-drone-bin-laden-house-new-stealth

"Napolitano Cancels Virtual Border Fence Project, Proposes Alternative." Fox News, January 14, 2011. Accessed January 3, 2013 from: http://www.foxnews.com/politics/2011/01/14/napolitano-cancels-virtual-border-fence-project-proposes-alternative/

Performance and Accountability Report: Fiscal Year 2011. U.S. Department of Homeland Security: Customs and Border Protection, March 2012.

Ranger MS Illuminator, FLIR Systems, 2013.

Ranger MS-UC EnforcIR Brochure, FLIR Systems, 2013.

SBInet Program: Program-Specific Recovery Act Plan. U.S. Department of Homeland Security: Customs and Border Protection, May 15, 2009

SkyWatch data sheet and brochure. FLIR, February 2013.

"M1-D Micro Thermal FLIR PTZ Camera." SPI Infrared, April 2013. Accessed April 24, 2013 from: http://www.x20.org/m1-d-micro-thermal-ptz-camera

"Telephonics: Ground Surveillance Radar and Long Range Systems." Armed Forces International, 2012. Accessed March 3, 2012 from: http://www.armedforces-int.com/suppliers/air-traffic-control-systems.html

White Paper: The Secure Border Solution. ICx Technologies, February 2013.

Z. Sun, P. Wang, M. Vuran, M. Al-Rodhaan, and A. Dhelaan. *BorderSense: Border Patrol through advanced wireless sensor networks*. Ad-Hoc Networks, 2011, Vol. 9 pp. 468-477

Academic Research and/or Unapplied Technology: For use as a source of the features expected to be included in the design of the PSN

M. Argany, M. Mostafavi, F. Karimipour, and C. Gagne. *A GIS Based Wireless Sensor Network Coverage Estimation and Optimization: A Voronoi Approach*. Center for Research in Geomatics, Laval University, 2011.

R. Kumar, J. Shin, L. Iftode, and U. Ramachandran. *Mobile Virtual Sensors: A Scalable Programming and Execution Framework for Smart Surveillance (Position Paper)*. Georgia Institute of Technology and Rutgers University, 2008

"Research at ARRI: Mobile Sensor Networks." University of Texas at Arlington: Automation and Robotics Research Institute, 2006. Accessed January 4, 2013 from: http://arri.uta.edu/smart_micromachines/distributed_devices/mobile_sensor_networks.html

Tertiary References: References used in this report that are not surveillance specific

"Department of Defense Federal Budget: Fiscal Year 2012." Office of Management and Budget, 2012. Accessed March 12, 2013 from: http://www.whitehouse.gov/omb/factsheet_department_defense

"Department of Homeland Security Federal Budget: Fiscal Year 2012." Office of Management and Budget, 2012. Accessed March 12, 2013 from: http://www.whitehouse.gov/omb/factsheet_department_homeland

Farley, R. (2011). Obama Says Border Patrol Has Doubled the Number of Agents Since 2004. Politifactcheck.com, May 2011. Accessed on November 26, 2011 from: http://www.politifact.com/truth-o-meter/statements/2011/may/10/barack-obama/obama-says-border-patrol-has-doubled-number-agents/

Glossary I: Military Abbreviations and Acronyms. Global Security.org, March, 2013. Accessed March 31, 2013 from: http://www.globalsecurity.org/military/library/policy/army/fm/55-9/gloss.htm

"How Night Vision Works." Sofradir EC Night Vision Systems, 2013. Accessed April 1, 2013 from: http://www.hownightvisionworks.com/#IRI

"Littoral Combat Ships – Mission Modules." U.S. Department of the Navy, 2012. Accessed January 5, 2013 from: http://www.navy.mil/navydata/fact_display.asp?cid=2100&tid=406&ct=2

"Littoral Combat Ships, United States of America." Naval-Technology.com, April 2013. Accessed April 20, 2013 from: http://www.naval-technology.com/projects/littoral/littoral1.html

"Lockheed C-130 Hercules." The Aviation Zone, March 2013. Accessed March 15, 2013 from: http://www.theaviationzone.com/factsheets/c130.asp

Ludtke, W. *Effects of Canopy Geometry on Drag Coefficients of a Cross Parachute in the Fully Open and Reefed Conditions for a W/L ratio of 0.26.* Naval Ordinance Laboratory, Silver Spring, MD, August 1971.

Maydew, R.C. and Peterson, C.W. *Design and Testing of High-Performance Parachutes*. Advisory Group for Aerospace Research and Development, Neuilly Sur Seine, France, 1991.

Molzahn, Rios, and David A. Shirk. *Drug Violence in Mexico: Data and Analysis Through 2011*. University of San Diego, Trans-Border Institute: Joan B. Kroc School of Peace Studies.

National Drug Threat Assessment for 2011. U.S. Department of Justice: National Drug Intelligence Center, August 2011.

Njock-Libbi, Josue. "USING HYPERGEOMETRIC FUNCTIONS TO DETERMINE THE TERMINAL SPEEDS OF PARACHUTES". *American Society for Engineering Education*, 2006-58.

"Planned stealth destroyer could underpin Navys China strategy." Fox News, June 4, 2012. Accessed March 4, 2013 from: http://www.foxnews.com/politics/2012/06/04/planned-stealth-destroyer-could-underpin-us-navy-china-strategy/

"Special Operations." Military.com, March 2013. Accessed March 10, 2013 from: http://www.military.com/special-operations

Sher, S. and Young, I. *Drag Coefficients for Partially Inflated Flat Circular Parachutes.* NASA, Washington DC, September 1971.

Washington, Douglas Waller. "The CIA's Secret Army." Time Magazine, February, 2003. Accessed March 10, 2013 from: http://www.time.com/time/magazine/article/0,9171,1004145,00.html

"What is the Orbit of a Satellite?" Space Today Online, March 2013. Accessed March 15, 2013 from: http://www.spacetoday.org/Satellites/SatBytes/SatOrbits.html

"What's The Difference between Thermal Imaging and Night Vision?" FLIR Systems, Inc., 2013. Accessed April 1, 2013 from: http://www.flir.com/cvs/americas/en/view/?id=30052