Although GPS can support U.S. and allied military activities, it can at the same time create a dependency. Furthermore, enemy uses of GPS can threaten U.S. forces and broader security interests. This dual aspect of GPS—its utility in American and allied hands, along with the risks of dependency and enemy use—highlights a fundamental dilemma for decisionmakers seeking to maximize the benefits of GPS technology while minimizing its risks. To help policymakers deal with this dilemma, this chapter sets forth the benefits and risks associated with military uses of GPS.

The first section considers U.S. military use of GPS. Because U.S. forces rely on GPS, we pay particular attention to potential vulnerabilities and threats that could prevent U.S. forces from taking full advantage of the system. The second section evaluates the threats arising from hostile use of GPS against U.S. assets or those of its allies. Rather than placing equal emphasis on all potential uses of GPS by hostile forces, this study considers those situations that appear to be the most threatening to U.S. forces. For example, the use of GPS by enemy navies appears much less serious than the enemy use of GPS on cruise missiles. It is our assertion that by examining the threats that appear the most significant, we can make a reasonable assessment of the overall risks associated with hostile use of GPS.

The third section of this chapter analyzes how GPS augmentation systems could be exploited by hostile forces. Third-party local- and wide-area differential GPS (DGPS) systems can be used by one nation to attack another. The fourth section examines the effectiveness of two signal modifications implemented by the U.S. government: selective availability (SA) and anti-spoofing (AS). The

---

1 DGPS enhances the accuracy of the basic GPS signal through the use of differential corrections to the basic GPS timing signals. DGPS is based on comparing positioning measurements with known locations at one or more ground reference stations. These differential corrections are then transmitted to the users so that they can make corrections to their GPS receivers. Differential corrections can improve the 100-meter SPS accuracy to about 5–10 meters, or even less, for many GPS applications.
former is designed to decrease the accuracy of signals available to civilian users. The latter was implemented to prevent civilian access to the authorized users’ signals. The final section of this chapter summarizes our findings and discusses how they fit into the overall scope of this report.

**U.S. MILITARY USE OF GPS**

GPS is becoming an integral component of U.S. military forces. It can provide navigation for all types of land vehicles, ships, missiles, munitions, aircraft, and troops. It can be used to supply accurate targeting information and as a common position grid for joint operations. GPS can also improve battle management and command-control-communication-computer-intelligence (C4I) operations. GPS receivers are passive; they provide information to U.S. forces without revealing the location of those forces. GPS can also be easily integrated with other technologies such as inertial navigation systems and telecommunications.

Given the above, it comes as no surprise that GPS equipment is found in almost every type of vehicle fielded by the DoD. In fact, Congress has declared that after the year 2000, any aircraft, ship, armored vehicle or indirect-fire weapon that is not equipped with a GPS receiver will not be funded.\(^2\) The Joint Chiefs of Staff have identified more than 80 missions that can be improved through use of GPS.\(^3\) These missions encompass air, land, sea, and space environments.

It is evident that the U.S. military is moving towards high reliance on GPS, and force structure decisions are being made assuming GPS availability. These developments carry obvious benefits, but there are costs as well. In particular, the more dependent U.S. forces are on GPS, the more vulnerable they are to disruptions of access to GPS. Threats to U.S. military use of GPS can be divided into two classes: internal threats and external threats. The former are generally within the control of the U.S. government while the latter are essentially exogenous.

**Internal Threats**

There are three basic internal threats to successful U.S. and allied military use of GPS: mismanagement of the system, inadequate funding for operation and maintenance, and excessive reliance upon civilian GPS equipment. Although

---


\(^3\) CJCS Master Navigation Plan, CJCSI 6130.01, May 20, 1994. GPS is also useful for peacekeeping and peacemaking operations. For example, GPS was used to accurately air-drop food and supplies to safe havens in Bosnia.
all three problems are potentially troublesome, they can be avoided through foresight and careful planning.

Stewardship of GPS through routine maintenance, technical upgrades, and the training and retention of skilled personnel is the most immediate requirement for continued use of GPS. For example, the GPS master control station at Falcon Air Force Base is using extremely old equipment and outdated software whose maintenance is increasingly difficult. Depending on the length and severity of the problem, a systems failure at this site could seriously affect the quality of GPS information.

Inadequate funding of the GPS space and control segment and inadequate acquisition of military receivers are other obvious threats. For example, budget reductions and competition with other programs could limit the number of replacement satellites that the Air Force will be able to purchase in the next two decades and force longer reliance on aging systems. Reliance upon civilian GPS receivers is another concern. While it is difficult to get an exact estimate on the number of civilian receivers (often termed “standard lightweight GPS receivers” or SLGRs) in use by U.S. forces, there are indications that the figure is in the tens of thousands. There are two drawbacks associated with U.S. military use of civilian GPS receivers. First, the accuracy of the position and velocity information provided by SLGRs will be degraded by SA. This leaves the U.S. government with two choices: it can leave SA on and allow some of its forces to operate with degraded information, or it can turn SA off and allow opposing forces to have the same accuracies as U.S. forces. More important, U.S. forces relying on the C/A-code will be much more vulnerable to jamming than those using the P-code.

External Threats

External threats to GPS originate outside the direct control of the U.S. government. These threats may be directed at either the system segments or the GPS signal itself. There are unintentional and intentional threats. The former include phenomena such as natural disasters and malfunctions. The latter include military attacks and terrorist actions. The GPS master control station at Falcon Air Force Base is well protected, and the high altitude of GPS satellites makes them hard to attack with anti-satellite weapons. Consequently, unin-

---


5SA was turned off in 1990–1991 during Operations Desert Shield and Desert Storm and in 1994 during Operation Uphold Democracy in Haiti.

tentional threats are probably a larger concern for the GPS control and space segments.

If an accident did occur, what might its effect be on the overall GPS performance? The most serious disruptions would occur if the control segment became inoperable. The timing accuracy of the GPS satellites would begin to drift and the positioning accuracy would degrade with time. Current specifications call for the GPS Block IIA satellites to maintain an accuracy of 16 meters spherical error probability (SEP) for 14 days after the last update. The Block IIR satellites will improve on this as a result of autonomous navigation capabilities from multiple satellite cross-ranging. These satellites should provide accuracies of 16 meters (SEP) for 180 days after the last update.

The cessation of service from specific satellite vehicles (SVs) can affect both the area covered by GPS and the accuracy available to users. Although other satellites would continue to broadcast, they might not be positioned well for a particular GPS user, who would experience a geometric dilution of precision (GDOP) (see Appendix A for further discussion). However, because the system was designed to operate with only 21 satellites in orbit (there are currently 24 functioning satellites), up to three satellites could malfunction before serious degradations took place.

The most significant threat to U.S. military GPS use is signal denial. GPS transmissions can be easily jammed by both intentional and unintentional sources. The power of GPS signals when they reach the earth is approximately $10^{-16}$ Watts. Because the GPS signal strength is so low, small jammers can cause a GPS receiver to lose lock at long ranges. For example, tests indicate that a one-Watt jammer can incapacitate a commercial GPS receiver (causing it to lose both code and carrier tracking) at a distance of 22 km.\(^7\)

There are two approaches an adversary can take in an effort to jam U.S. forces using GPS—smart jamming and noise jamming. Smart jamming is often called spoofing. Signals are transmitted that attempt to duplicate the characteristics of the GPS signals being received by users. The goal is for a receiver to track the false GPS signals rather than the real ones. The weapon or user can then be led off-course or crashed into the ground. Spoofing can be accomplished by low-power devices, and may be somewhat effective in preventing C/A-code acquisition, but it will not work well once the GPS codes are being tracked. The P(Y)-code, in particular, will be nearly impossible to spoof because of its one-week code length and encryption.

Noise jammers are a more pervasive threat to GPS signals than spoofing. This approach attempts to overwhelm a GPS receiver (by brute force) with radio noise. Adversaries are likely to pursue one of two options—narrowband or wideband jamming. Narrowband methods include carrier wave (CW) jamming (also known as “tone” jamming), swept CW jamming, and pulsed jamming. These methods have the advantage of concentrating a great deal of power into a narrow spectrum. Narrowband jamming is not, however, an effective strategy for jamming military GPS receivers because they can filter such signals without much degradation in performance.

A better method for jamming U.S. forces is to spread the jammer noise across the entire bandwidth of the P-code (which is 20 MHz, versus 2 MHz for the C/A-code). This strategy is difficult to counter because the jammer signal cannot be filtered before processing. The only effective techniques for countering wideband jammers are those that minimize the amount of jammer energy that enters the antenna. Two such techniques are narrow beam steering and adaptive nulling (which is usually accomplished with a controlled radiation pattern antenna or CRPA). Both of these anti-jam techniques are difficult to implement and expensive, and the latter method only works against a limited number of jammers.8

Jammer power can easily range anywhere from 1 to 10,000 Watts. A small jammer could be battery powered and weigh in the neighborhood of 1–2 lb. A medium-sized jammer in the 100–1000 Watt range could be man-portable. However, large jammers transmitting 1,000 to 10,000 Watts would have to be transported by truck or helicopter. While large jammers appear to provide the largest threats to U.S. forces, they are also the easiest to detect and destroy. On the other hand, large numbers of low-power jammers would be difficult both to locate and counter. For this reason, the proliferation of small wideband jammers is the greatest concern of the U.S. military.

Finally, it is important to note that jammers can be deployed on airborne platforms. Airborne jammers are more effective than ground-based jammers for two reasons. First, their altitude allows them to jam a much larger area than ground-based jammers, especially against low-altitude targets. Second, an airborne jammer’s signal will approach a receiver from the same direction as some GPS satellites; thus, it will be much harder to block out such signals using physical obstacles. However, placing an airborne jammer at the right time and location to jam U.S. forces is not easy to do. In addition, such airborne targets

The Global Positioning System would be extremely vulnerable to both electromagnetic countermeasures and direct attack from U.S. forces.

**Options for Improving Signal Access**

Options for improving GPS signal access include modifications to both the space and user segments. Space segment improvements include increases in the transmission power and/or signal spread spectrum bandwidth. Both of these improvements are technically feasible, but they would be costly and would need to be incorporated in future satellite designs. Thus, they could not be implemented for several years. In addition, the latter option would require modifications in current GPS receivers. The highest-payoff area for improved signal access is likely to be in the user segment—in the GPS receivers themselves and antenna designs.

GPS receivers use spread-spectrum processing to detect, track, and demodulate extremely weak signals transmitted from the satellites. Proper operation requires a minimum threshold ratio between the GPS signals and the combined sum of receiver thermal and jamming noise. Typical values for current GPS receivers are shown in Table 3.1 as a function of tracking state. The jamming-to-signal (J/S) limits are shown for a moving GPS user with an inertial navigation system (INS) or for an unaided stationary receiver. The incremental J/S contribution from INS-aiding is about 10–15 dB. The J/S ratios shown assume an antenna gain of 1 (0 dB). As shown, loss of both carrier and code tracking, defined as State 3, occurs for current receivers at a J/S ratio of about 54 dB. GPS anti-jam enhancements possible for advanced military receivers are shown Table 3.2.

In Table 3.2 note that a GPS receiver is most vulnerable to jamming when it is trying to acquire the C/A-code. A potential solution to this problem is for U.S. forces to be equipped with receivers that can acquire the P-code directly.

**Table 3.1**

<table>
<thead>
<tr>
<th>Tracking State</th>
<th>Description</th>
<th>J/S Threshold (dB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Normal start, C/A-code acquisition</td>
<td>25</td>
</tr>
<tr>
<td>2</td>
<td>Hot start, direct P-code acquisition</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>Maintain code and carrier track</td>
<td>44</td>
</tr>
<tr>
<td>3</td>
<td>Maintain code track</td>
<td>33</td>
</tr>
</tbody>
</table>

NOTE: Assumes IMU aiding (ΔJ/S = 10–15 dB).
Unfortunately, direct P-code acquisition is difficult because of the length of the code ($6 \times 10^{12}$ bits versus 1023 bits for the C/A-code). This is an important and challenging technical problem and work is in progress to address this source of U.S. vulnerability.

Other goals of advanced GPS receivers are to decrease their size, weight, and power, to provide higher anti-jam margins against jammers, and to minimize the time-to-first-fix. With INS aiding, the J/S performance for advanced military receivers operating in State 3 (maintain code tracking) has been increased from about 54 to about 64 dB against wideband noise jammers by using multiple correlators and increasing the signal dwell time. The multiple correlators are used so that the signal does not drift outside the observation window. The longer dwell time allows for narrowing the loop bandwidths, which results in a J/S improvement of about 6 dB. An additional 3 dB of processing gain is obtained for wideband jamming as compared with narrowband jamming.9 The typical GPS receiver performance of 54 dB J/S is normally referenced to a narrowband jamming signal.10

An additional anti-jam margin of about 6 dB J/S can be obtained by data stripping, also referred to as data aiding or data wiping. Data stripping requires knowledge of the current navigation message so that the message can be removed from the GPS signal. This results in narrowing the tracking bandwidth, which in turn provides higher J/S margins. Prior to the mission, the navigation message would need to be loaded into the receiver. Collecting the navigation message data and accounting for unexpected changes in the data for many weapons is not expected to be operationally simple.

Additional anti-jam enhancements can be obtained by changing the differential gain pattern of the GPS antenna (spatial filtering). The use of a narrow beam antenna that focuses on the GPS satellites would provide 10 to 20 dB of addi-

---

9Based on conversation with Jack Murphy, Rockwell International, Collins Avionics and Communications Division, Cedar Rapids, IA, November 8, 1994.

10Interview with Tyler Trickey, Rockwell International, Collins Avionics and Communications Division, Cedar Rapids, IA, November 9, 1994.
tional jamming resistance. Adaptive null steering places a null in the direction of a jammer. These antennas are extremely effective—they can provide 30 to 40 dB of jamming resistance—but they only work against a limited number of jammers. The current CRPAs under development by the DoD can null either six or three jammers, depending on the model.

The jamming ranges for various GPS receiver states with INS-aiding are shown in Figure 3.1. Without additional anti-jam enhancements, a 1-Watt jammer can cause loss of code track for a P-code receiver at about 4.3 km. The jammer can also prevent direct P-code acquisition out to a range of 45 km. An advanced GPS receiver with –10 to –20 dB antenna gain can maintain code track to about 4 km from a 1-kW jammer source.

It is clear that the use of GPS for military applications is extremely vulnerable to jamming without a design that includes additional anti-jam enhancements and an adequate INS to ensure graceful degradation after loss of GPS. Anti-jam GPS enhancements would include an advanced receiver and an antenna with a shaped pattern.

As stated earlier, military GPS receivers expected to operate in a “challenged” environment need to provide enough anti-jam enhancements such that the adversary is forced to employ a jammer that can be effectively attacked if necessary.

---

**Figure 3.1—Jamming Range Versus Jamming Power**
The growth of the vehicle navigation error after loss of the GPS signal is shown in Figure 3.2 for various levels of INS quality. The quality of the inertial navigation system is expressed in terms of an equivalent gyro drift rate that results in position errors arising from uncertainties in the gyroscopes, accelerometers, and platform/sensor misalignments.

After loss of the GPS signal, the short-term navigation error growth during the first 1 to 2 minutes results primarily from random gyro drift terms, assuming a conventional transfer alignment of the INS. The parameter used to specify INS quality is equivalent gyro drift rate, which accounts for gyro, accelerometer, and alignment errors. The navigation CEP from both targeting and guidance errors is arbitrarily assumed to be 10 meters prior to loss of GPS carrier and code tracking. The quality and representative costs of these hypothetical inertial platforms, assuming large-quantity purchases in the year 2000, are shown in Table 3.3. For comparison purposes, a 0.01 degree/hr quality INS in a high-performance aircraft costs in the range of $100,000 to $200,000.

---

**Table 3.3**

<table>
<thead>
<tr>
<th>Inertial guidance only after GPS jammed (min)</th>
<th>Navigation CEP (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>0</td>
</tr>
<tr>
<td>1.0</td>
<td>10</td>
</tr>
<tr>
<td>10.0</td>
<td>90</td>
</tr>
<tr>
<td>20.0</td>
<td>100</td>
</tr>
</tbody>
</table>

**Figure 3.2—CEP Degradation After GPS Loss-of-Lock**

11 This curve is based on work by Sean Gilmore and William Delaney of Lincoln Laboratory, Lexington, Massachusetts.

12 Ibid.
Table 3.3
Missile INS Quality

<table>
<thead>
<tr>
<th>Equivalent gyro drift rate (deg/hr)</th>
<th>Type of INS</th>
<th>Estimated cost ($K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Interferometric fiber optic gyro</td>
<td>20–50</td>
</tr>
<tr>
<td>1</td>
<td>Advanced micromechanical</td>
<td>2–5</td>
</tr>
<tr>
<td>10</td>
<td>Near-term micromechanical</td>
<td>1</td>
</tr>
</tbody>
</table>

The findings of this analysis can be summarized as follows:

- A major jammer threat arises from the proliferation of low-power, wide-band jammers. It is therefore important for U.S. forces to acquire P-code before entering a jamming environment. In addition, an aided military receiver can be designed to achieve a jamming resistance of about 70 dB. Antennas can provide an additional anti-jam margin of from 10 to 30 dB. In all cases, GPS-guided weapons will require low-cost INSs if they are to maintain high accuracies through jamming near a target.

- If the adversary employs a large jammer, it will be an attractive target for attack by precision-guided munitions such as anti-radiation missiles.

HOSTILE EMPLOYMENT OF GPS

There are a variety of ways that hostile forces can take advantage of GPS. This report looks at the four areas that pose the highest risks to U.S. forces: use by land forces (including targeting), by naval forces, by aircraft, and by cruise and ballistic missiles.

Ground Operations

The recent war in the Persian Gulf highlighted one of the benefits of positioning services such as GPS. The large-scale coordinated movement of VII Corps through the desert showed one way such services could be used by an attacking force operating in relatively unfamiliar terrain with few landmarks. However, that movement, while facilitated by GPS receivers, would not have been possible had U.S. forces not been well trained for complex maneuver warfare, with apparatus available to support forces movement. Warfare, especially ground warfare, is facilitated by technology such as GPS, but is dependent on the underlying people and equipment. In assessing GPS in the hands of an
adversary, it is important to determine if they have all that is necessary to allow them to capitalize on the system.

There are a few areas where GPS/DGPS might be helpful, at least on a small-unit level:

- Improved capability to conduct shoot-and-scoot operations when operating away from presurveyed regions if the units are trained and equipped for that class of operation.
- Improved helicopter operations, provided accurate digital charts and flight software are available.
- Improved technical intelligence by exploiting timing signals and avoiding the need for more expensive distributed timing devices.
- Improved capability to establish mine fields, or safe corridors through mine fields.

In sum, GPS provides three major benefits for land-based military operations—self-location accuracy, navigation, and target location. Self-location accuracy is crucial because simple projectile-type weapons must be programmed to fly a given distance. The accurate positioning information provided by GPS can increase the lethality of artillery, rocket-launchers, and mobile missiles by reducing their location uncertainties at launch.

In addition to its high accuracy, GPS allows users to determine their location passively; that is, users can find out where they are without transmitting signals that could be detected and targeted by enemy forces. Improved self-location information can also reduce fratricide (i.e., unintentional attacks on one’s own forces) if the information is processed effectively, which depends on the command, control, communications and intelligence (C3I) capabilities of a given military.

Accurate navigation information provided by GPS can be crucial in environments where other navigation methods falter. For example, GPS was an invaluable asset to U.S. forces during the Gulf War in part because they were operating in a featureless terrain. Good-quality navigation information can also increase the movement rate of ground troops and improve movement coordination and attacks. However, many developing nations may not have the

---


necessary prerequisites—including equipment and training—to take full advantage of the information provided by GPS.\textsuperscript{15}

The third benefit that land forces can gain through the use of GPS is accurate target location. The drawback of this application is that a GPS receiver must be located at or near a target to determine its coordinates.\textsuperscript{16} Forward observers could use GPS to more accurately locate U.S. units on the move. Furthermore, GPS position information could be combined with high-resolution remote sensing data to accurately locate fixed targets. In addition, fixed facilities such as docks, airfields, and warehouses could be pretargeted with GPS receivers before a conflict began.

**Naval Operations**

For naval forces, the story is a little different. Naval forces are usually moving to patrol an area or seek/avoid an enemy force. However, GPS/DGPS can help specific classes of operations:

- Mine warfare, since GPS/DGPS provides a fixed reference point for mines being laid, mine sweeping, and corridors through mine fields.
- Locating ships by providing better location information from surveillance platforms and assisting in signal intelligence that can locate emitters at sea.
- Providing location information for anti-ship missiles in flight to decrease guidance drift after launch.

As with the earlier discussion of ground forces, one of the prerequisites for an improved capability is having a force capable of exploiting it. The effective use of GPS usually assumes other related capabilities and the ability to bear additional costs. For example, anti-ship missiles might employ GPS-aided guidance schemes to decrease the cost of the onboard IMU, and the initial fix may be better, but this could increase the cost of onboard radar or other sensors employed to search the area where the target ship might be located.

Operating navies is an expensive and difficult proposition, and few nations operate significant blue-water (deep ocean) forces. However, the major concern then is that GPS/DGPS might be useful to forces operating near their homeland, and could enhance the threat from green water (coastal) forces. Position information can certainly help such forces, but it would not appear to alter the


\textsuperscript{16}A technique called relative targeting allows one to determine the position of a target relative to a landmark with a known location.
primary threats to the U.S. Navy, which will likely remain anti-ship missiles, submarines armed with torpedoes, and naval mines.

The problem for the United States is not just GPS/DGPS, but the proliferation of advanced conventional weapons. The contribution of GPS/DGPS to potential threats is to somewhat decrease the entry cost for parties wishing to begin a process of denying easy access to nearby waters. The additional cost for a GPS/DGPS-aided capability might be a few tens of thousands of dollars, which—unless the price of the total system is driven down dramatically—will make only a small difference in terms of the quantitative and qualitative threat faced.

Air Operations

Foreign air forces can benefit from the use of GPS in three areas: aircraft navigation, air-to-air missions, and air-to-surface missions. One of the fundamental factors hindering the capability of many foreign air forces is the limited skills of their air crews. Reliable and inexpensive navigation systems like GPS can assist air crews in navigating to and from target areas. The ability to find their airbases at night or in bad weather will greatly increase the range of conditions under which these air forces might operate.

In air-to-air operations, the ability to accurately locate friendly, enemy, and unknown aircraft is extremely important. A radar site might be able to detect and track aircraft, but there are significant errors associated with such measurements. By using GPS in conjunction with data links and radar data, ground controllers can more effectively control an air battle. Furthermore, when air-to-air operations occur within close proximity of friendly surface-to-air (SAM) missiles, a nation’s aircraft must avoid flying into keep-out areas. The precision-location information provided by GPS allows aircraft to operate with smaller safety margins, thus potentially increasing the number of SAM engagements against opposing aircraft. On the whole, however, the contribution of GPS will likely be minor except for the most-capable air forces. The training and command-control-communications capabilities needed for effective counter-air operations, with or without GPS, are considerable.

In air-to-ground operations, GPS can help aircraft navigate to and from a target, coordinate air operations, and increase the accuracy of air-delivered ordnance. Of these applications, the most important is probably the latter. By minimizing

---


18A more serious threat is probably the proliferation of stealth technology that can decrease the utility of anti-ship defense systems.
their self-location errors, aircraft can determine their bomb drop points more accurately, which increases the likelihood that their bombs will hit designated targets.\textsuperscript{19} If GPS information is combined with sophisticated radars and targeting algorithms on a weapon that can compensate for ballistic errors and wind effects, bomb accuracy can begin to approach that of precision-guided weapons (10 meters or less). While such technologies are currently out of reach for most Third World nations, their basic building blocks will be in the hands of several countries fairly soon. It is also possible that such systems will become available on the international arms market along with other advanced conventional weapons.

**GPS-Guided Ballistic Missiles**

The proliferation of Third World ballistic missiles is a major U.S. concern.\textsuperscript{20} These missiles can carry weapons of mass destruction, reach targets quickly, and are difficult to intercept. The ballistic missile activity of selected developing nations is shown in Table 3.4.

Most of the guided ballistic missiles possessed by developing nations today are based on the Scud B, a missile developed by the former Soviet Union more than 40 years ago and, in turn, based on the German V-2 rocket design of World War II. This missile has a nominal range of about 300 km and can deliver a 1000-kg payload with an accuracy of approximately 500 to 1000 meters. The Scud B has a single-stage, liquid-fueled rocket and a single warhead that does not separate from the booster. The Scud B is a low-tech, inaccurate missile with limited military utility. However, it has been suggested that the accuracy of Scud missiles could be improved by an order of magnitude through the use of GPS guidance.\textsuperscript{21}

We examined two of the most common guided ballistic missiles in the world—the Scud B and the No Dong 1. The No Dong 1 is a medium-range North Korean missile. It is based on a Scud design, but the No Dong 1 has four strap-on engines and the warhead separates from the booster after thrust cutoff. This design change allows the missile to have a longer range than the Scud B

\textsuperscript{19}Miniature GPS receivers can also be placed aboard bombs to create “smart munitions” that can guide themselves to a target. This is a technically demanding task that is unlikely to be successfully accomplished by developing nations. See Gerald Frost and Bernard Schweitzer, “Operational Issues for GPS-Aided Precision Missiles,” paper presented at the 1993 National Technical Meeting of the Institute of Navigation, Washington, D.C., January 1993.


Table 3.4
Ballistic Missile Capability of Selected Developing Countries

<table>
<thead>
<tr>
<th>Nation</th>
<th>Range Category (km)</th>
<th>Supplier</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>300–500</td>
<td>500–1000</td>
</tr>
<tr>
<td>China</td>
<td>M-11</td>
<td>M-9</td>
</tr>
<tr>
<td>Egypt</td>
<td>Scud B</td>
<td>Scud C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>Agni</td>
<td></td>
</tr>
<tr>
<td>Iran</td>
<td>Scud B</td>
<td>Scud C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iraq</td>
<td>Scud B</td>
<td>Scud C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Israel</td>
<td>Jericho 1</td>
<td>Jericho 2</td>
</tr>
<tr>
<td>Libya</td>
<td>Scud B</td>
<td>Scud C</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>North Korea</td>
<td>Scud B</td>
<td>Scud C</td>
</tr>
<tr>
<td>Pakistan</td>
<td>M-11</td>
<td>Hatf 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Saudi Arabia</td>
<td>CSS-2</td>
<td></td>
</tr>
</tbody>
</table>

without sacrificing payload. However, the No Dong 1 has poor accuracy at the longer range. The estimated characteristics of the two missiles are given in Table 3.5.

The boost guidance concept assumed for Scud-type short-range ballistic missiles (SRBMs) is a simplified velocity-to-be-gained guidance law. Prior to launch, a ground-based computer calculates the sensed burnout velocity state that must be attained for a missile to hit a given target. An accelerometer mounted in the direction of the missile’s longitudinal axis measures the vehicle’s sensed velocity. When the difference between the calculated velocity and the actual velocity approaches zero, booster thrust is terminated. For liquid propellant engines, thrust is terminated by closing the valves to the fuel and oxidizer tanks. An open-loop, body-mounted inertial system as described above is assumed to be representative of that used by Scud-type missiles. A more complex boost guidance system can improve accuracy. Such a system
could include a full axis gimbaled or strapdown inertial reference system, digital computer, and a separating warhead with a vernier control system for providing fine velocity adjustments during payload deployment. An advanced missile would also be designed to minimize the other major factors contributing to the weapon system CEP, such as reentry errors.

Tables 3.6 and Table 3.7 show the estimated accuracy for the Scud and No Dong 1 based on use of a velocity-to-be-gained guidance law. As one can see, in both cases velocity cutoff errors make significant contributions to missile CEP. These errors arise from two primary sources—the longitudinal accelerometer and the thrust termination control system. The former depends on the quality of a missile’s accelerometers. The latter results primarily from errors in the booster cutoff control system, which include contributions from thrust impulse after cutoff and timing errors in the cutoff signal to the engine valves. Thrust impulse variations differ for each specific booster and with environmental conditions such as pressure and temperature.

Ballistic missiles use inertial sensors to navigate to the desired burnout state. When a missile reaches the desired position and velocity state, thrust is terminated and the weapon hits the designated target. GPS receivers can provide accurate position and velocity measurements, which may improve the CEP of

---

**Table 3.5**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Scud B</th>
<th>No Dong 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Length (m)</td>
<td>11.3</td>
<td>15.5</td>
</tr>
<tr>
<td>Diameter (m)</td>
<td>0.9</td>
<td>1.3</td>
</tr>
<tr>
<td>Range (km)</td>
<td>300</td>
<td>1000</td>
</tr>
<tr>
<td>Payload (kg)</td>
<td>1000</td>
<td>1000</td>
</tr>
<tr>
<td>System CEP (m)</td>
<td>500–1000</td>
<td>1500–3000</td>
</tr>
<tr>
<td>Total mass (kg)</td>
<td>5400</td>
<td>19000</td>
</tr>
<tr>
<td>Propellant mass (kg)</td>
<td>4000</td>
<td>16000</td>
</tr>
<tr>
<td>Burn time (sec)</td>
<td>70</td>
<td>70</td>
</tr>
<tr>
<td>Thrust (kN)</td>
<td>130</td>
<td>540</td>
</tr>
<tr>
<td>Reentry ballistic coefficient (N/m²)</td>
<td>190,000</td>
<td>36,000–48,000</td>
</tr>
</tbody>
</table>

Table 3.6  
**Baseline Scud Accuracy**

<table>
<thead>
<tr>
<th>Error Sources</th>
<th>1-σ Downrange (m)</th>
<th>1-σ Crossrange (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position, alignment</td>
<td>100</td>
<td>300</td>
</tr>
<tr>
<td>Boost phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accelerometers</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Gyros</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Alignment</td>
<td>100</td>
<td>200</td>
</tr>
<tr>
<td>Cutoff control</td>
<td>400</td>
<td>100</td>
</tr>
<tr>
<td>Reentry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winds, density, aerodynamics</td>
<td>440</td>
<td>360</td>
</tr>
<tr>
<td>Target location</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Root-sum-square</td>
<td>640</td>
<td>600</td>
</tr>
<tr>
<td>Weapon system CEP</td>
<td></td>
<td>730</td>
</tr>
</tbody>
</table>

NOTE: Error estimates are for a Scud B missile fired to a range of 300 km. Error components for the baseline Scud are based on reasonable technical assumptions for a system that has an overall weapon system CEP of about 0.5 to 1.0 km.

Table 3.7  
**Baseline No Dong 1 Accuracy**

<table>
<thead>
<tr>
<th>Error Sources</th>
<th>1-σ Downrange (m)</th>
<th>1-σ Crossrange (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial conditions</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Position, alignment</td>
<td>100</td>
<td>900</td>
</tr>
<tr>
<td>Boost phase</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accelerometers</td>
<td>300</td>
<td>300</td>
</tr>
<tr>
<td>Gyros</td>
<td>200</td>
<td>700</td>
</tr>
<tr>
<td>Alignment</td>
<td>200</td>
<td>700</td>
</tr>
<tr>
<td>Cutoff control</td>
<td>800</td>
<td>200</td>
</tr>
<tr>
<td>Reentry</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Winds, density, aerodynamics</td>
<td>900</td>
<td>1100</td>
</tr>
<tr>
<td>Target location</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Root-sum-square</td>
<td>1300</td>
<td>1800</td>
</tr>
<tr>
<td>Weapon system CEP</td>
<td></td>
<td>1850</td>
</tr>
</tbody>
</table>

NOTE: Error estimates are for a No Dong 1 missile fired to a range of 1000 km. The assumptions used for the Scud calculations also apply to the No Dong 1 case.

ballistic missiles. In addition, the use of GPS can allow for simplified initialization and alignment methods. Table 3.8 describes the position and velocity accuracies for GPS in various operating modes.

Table 3.9 describes the three scenarios examined in this chapter. We note that the improvements described in Cases B and C are technically challenging and may be beyond the reach of many developing nations for some time.
### Table 3.8

**GPS Position and Velocity Accuracy**

<table>
<thead>
<tr>
<th>GPS Signal</th>
<th>Position (m)</th>
<th>Velocity (m/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>2 drms</td>
<td>1 σ</td>
</tr>
<tr>
<td>SPS</td>
<td>100</td>
<td>36</td>
</tr>
<tr>
<td>C/A without SA</td>
<td>20–30</td>
<td>7–11</td>
</tr>
<tr>
<td>PPS</td>
<td>21</td>
<td>8</td>
</tr>
<tr>
<td>DGPS</td>
<td>5</td>
<td>2</td>
</tr>
</tbody>
</table>

NOTE: Velocity estimates are approximate. The quality of a user’s velocity measurements will depend on a variety of factors such as the type of receiver, the kinematics of the user vehicle, the geometry and distance between the user and a differential station, and so forth.

### Table 3.9

**GPS-Aided Ballistic Missile Cases**

<table>
<thead>
<tr>
<th>Case</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Baseline missile with a simplified guidance and control system, and GPS aiding.</td>
</tr>
<tr>
<td>B</td>
<td>The same as Case A except vernier controls are added in the boost thrust direction.</td>
</tr>
<tr>
<td>C</td>
<td>The same as Case B except that reentry and targeting errors are reduced by 50 percent.</td>
</tr>
</tbody>
</table>

NOTE: All cases assume that GPS is used to correct all of the errors that accumulate during the boost phase. This is a generous assumption, but it allows us to consider worst-case scenarios.

Figure 3.3 shows the overall weapon system accuracy for a Scud-type missile as a function of GPS velocity measurement errors for the cases described in Table 3.9.

**Case A:** GPS velocity measurements improve the overall CEP of a Scud by about 20 percent through reductions in the initial-condition and boost-phase errors. However, a missile using DGPS shows little improvement over one using the Standard Positioning Service (SPS) because contributions from other error sources such as cutoff control and reentry effects dominate the weapon system CEP.

**Case B:** As expected, the CEP in Case B is smaller than that in Case A because of a reduction in the cutoff control errors by the vernier engines. The overall weapon system accuracy is still relatively insensitive to changes in the quality of the GPS velocity measurement errors because the largest remaining errors arise from reentry dispersions.

**Case C:** The Scud’s overall CEP for this case is about 40 percent less than Case A. Again, however, one can see that the missile’s accuracy is fairly insensitive to
GPS velocity measurement errors. For example, the difference in CEP between missiles using SPS and DGPS is almost insignificant—because reentry errors remain sufficiently large to dominate the weapon system CEP.

In sum, GPS-aiding can improve the accuracy of Scud-type missiles by about 20 percent. Greater gains in accuracy can then be achieved by reducing thrust termination errors and reentry dispersions. Scuds gain little benefit by using DGPS instead of the SPS because GPS velocity measurement errors are insignificant compared with other error sources.

Figure 3.4 illustrates the effect of GPS-aiding for the No Dong 1 missile. The findings here are similar to those for the Scud case. Use of GPS velocity aiding improves the accuracy of a No Dong missile by about 25 percent. However, there is little difference in CEP between No Dongs using the SPS and those using DGPS. This result holds for all three cases. Thus, the velocity degradations resulting from selective availability have almost no effect on the accuracy of GPS-guided short- and medium-range ballistic missiles.

This study has examined the application of GPS for short- and medium-range ballistic missiles, finding that these missiles experience modest gains in accuracy from GPS-aiding. It appears, however, that long-range ballistic missiles can experience significant accuracy improvements with GPS-aided inertial
guidance. This is true because velocity errors in the range-sensitive direction at burnout can lead to large downrange impact errors for missiles traveling long distances. For example, a missile with a 10,000-km range using accelerometers meeting the Missile Technology Control Regime (MTCR) control guidelines (130 ppm scale factor), will have a velocity measurement error of about 1 m/s at burnout. This will result in a downrange error of about 1900 meters. A missile using the SPS will have a downrange error due to velocity measurement uncertainties that is a factor of three smaller than the one calculated above, but still not one that could be described as precise.

The other major error that can be significantly reduced through the use of GPS is initial azimuth alignment uncertainty at the launch site. Accurate ICBMs require azimuth alignments to a few arc-seconds because the crossrange error sensitivity for a 10,000-km-range missile is about 30 m/arc-sec. The use of GPS-aiding in the boost phase would allow for low-cost gyrocompassing and rough azimuth alignment because these errors would be reduced to the position and velocity uncertainties associated with GPS. The remaining errors would result
from reentry vehicle dispersions that are not corrected by GPS (unless the reentry vehicle can be maneuvered) and target location uncertainties.²³

**Advanced Short-Range Ballistic Missiles**

Might the effects of GPS-aiding be significantly greater for a more advanced short-range ballistic missile? Selective availability may have only a minor benefit for the most common ballistic missiles, but would there be significant benefits for more-advanced missiles and thus a proliferation incentive for advanced missiles if SA were turned off or DGPS were widely available? To examine this possibility, the effects of differing levels of GPS service were examined for the case of a notional single-stage ballistic vehicle that can be quickly launched from a mobile transporter-erector-launcher (TEL).

The major performance improvements of this advanced short-range missile compared with Scud- and No Dong-type missiles are the ability to accurately deploy the payload and an attitude control system that aligns a separating payload vehicle to achieve zero angle of attack at reentry. These improvements reduce major contributions to the weapon system’s CEP. A missile of this type could deliver a 500-kg payload to a range of 600 km with a CEP of approximately 600 m (0.1 percent of range). This section investigates the possible further reduction in weapon system CEP through application of GPS-aiding of the missile’s inertial navigation system.

Accurate thrust termination control will reduce some of the major impact errors that were significant for Scud- and No Dong-type missiles. The transformation of burnout velocity uncertainties into impact miss errors for short-range ballistic missiles is approximated by

\[ \frac{\Delta R_o}{\Delta V_o} = 2V_o/g \sin 2\gamma_o \]

where

- \(V_o\) = missile burnout velocity (m/s)
- \(\gamma_o\) = burnout flight path angle (deg)
- \(g\) = acceleration due to gravity (m/s/s).

²³A standard civilian GPS receiver could determine a target’s location to about 10 meters by time-averaging the SPS signals. The limiting factor is the ability of a single frequency receiver to model the ionospheric delays experienced by L-band radio waves.
For a minimum energy trajectory (neglecting aerodynamic drag and assuming instantaneous boost velocity), the miss sensitivity is about

$$\Delta R_O / \Delta V_O = 500 \text{ m/m/s}$$

assuming

$$R_O = 600 \text{ km}, V_O = 2400 \text{ m/s}, \text{ and } \gamma_O = 45 \text{ deg.}$$

The actual miss sensitivity will be less than this partial at the point of payload separation. The downrange impact miss due to an inertial accelerometer with a measurement uncertainty of 130 ppm (which falls within the MTCR export control limits) would then be about 150 meters. This particular error source, plus other position and velocity errors at burnout, could be greatly reduced by GPS-aiding of the missile’s inertial navigation system. The GPS receiver provides accurate corrections for missile position and velocity errors that accumulate up to the point of payload deployment. These errors result from uncertainties in missile initialization and booster navigation and control. The magnitude of CEP reduction will depend on the quality of the position and velocity measurements and type of GPS receiver.

The advanced-missile CEP is also improved compared with the Scud and No Dong missiles because of reductions in reentry errors associated with the ballistic coefficient, atmospheric density and winds, and vehicle angle-of-attack effects. Targeting and payload separation uncertainties also contribute to weapon system CEP.

The quality of the velocity measurements obtained by a GPS receiver depends on the type of receiver and the GPS operating mode.

**SPS Mode.** GPS provides civilian users a 100-m horizontal accuracy (2 drms) with SPS. This level is set by policy and achieved by intentional degradation of the basic signal by selective availability (SA). There is no equivalent standard for velocity accuracy; however, observations show that the rms velocity accuracy of the SPS signal is about 0.3 m/s.\(^24\)

**PPS Mode.** The rms velocity accuracy for a P-code receiver is specified to be 0.1 m/s for any axis; however, typical receiver performance is better than specifica-

tions.\textsuperscript{25} We assumed a horizontal rms velocity accuracy range of 0.05 to 0.1 m/s per axis, where the vertical component is larger than the horizontal component by a factor of about 2. Similar performance is also expected for a C/A-code receiver operating without SA. The accuracy of GPS velocity measurements also depends on the severity of the vehicle kinematics. Receiver kinematics introduces noise into the phase tracking loop and can cause the oscillator frequency to drift. Therefore, it is best to perform GPS-aiding during free flight after booster burnout. A small velocity-correction package on the payload would be needed.

**DGPS.** A DGPS operation assumes that a GPS reference station is located near (100–200 km) the missile at payload deployment. The objective of DGPS is to improve missile position and velocity in the presence or absence of SA. Errors in the known location and velocity of a GPS reference station are measured and pseudo-range and pseudo-range rate corrections are sent to the missile, using conventional broadcast standards such as RTCM SC-104.\textsuperscript{26}

The major factors that influence the velocity accuracy of DGPS corrections are the quality of the base station and missile receivers, separation distance, effects of geometry (which is given by the Position Dilution of Precision [PDOP] factor), and user kinematics. For the case of a stationary remote GPS user, where the DGPS ground station receiver takes several seconds to form a correction and transmits every few seconds, the rms horizontal velocity error for a PDOP of 1.5 to 2.0 is found from test results to be about 2.5 cm/sec.\textsuperscript{27} The velocity estimates are determined by measuring the Doppler shift in the carrier frequency. This quality-of-accuracy measurement results from the short wavelength (19 cm) of the carrier frequency. Estimated carrier phase measurement errors of a few percent taken every second with a PDOP of 2 results in a vehicle velocity accuracy estimate of 1–2 cm/sec, which compares favorably with test results.

However, experiments have shown that the accuracy of the velocity corrections will degrade depending on the level of receiver kinematics. For example, the uncertainty in the missile’s velocity could be greater than 0.1 m/s during boost. Therefore, it is important to perform the GPS measurements after completion of the boost phase. For this analysis, DGPS is assumed to provide an rms velocity accuracy in the range of 0.02 to 0.05 m/s if the corrections are made during the free flight phase after booster burnout.

GPS-aiding for an advanced short-range ballistic missile provides significant improvement in weapon system CEP. With SPS, the CEP is reduced from an as-


\textsuperscript{26}Radio Technical Commission for Maritime Services, Special Committee 104, Washington, D.C.

\textsuperscript{27}J. Clynech et al., op. cit.
sumed baseline of 600 m to about 215 m. For this case, the uncorrected errors arising from payload separation, reentry vehicle dynamics, and targeting are assumed to be 150 meters (see Figure 3.5).

For C/A-code without SA, the comparable accuracy is about 160 meters. As shown, SA has more of an effect for this system than for a Scud missile; however, SA has only a moderate effect on system performance. Weapon system CEP improvements for GPS velocity measurement accuracy below 0.1 m/s is minor; therefore, the addition of a ground-based DGPS system with associated uplink to the missile is not warranted. Besides the obvious improvements in weapon system CEP, GPS-aiding relaxes the initial positioning and alignment requirements. This allows the use of low-cost inertial instruments for initial azimuth alignment, which provides for a fast missile launch.

The findings of this section can be summarized as follows:

- GPS-aiding of Third World missiles such as the Scud and No Dong 1 can improve overall missile accuracy by 20–25 percent. Further improvement in missile accuracy cannot be achieved simply by reducing the burnout velocity measurement errors. Vernier engines are needed to minimize cutoff control uncertainties. More important, thrust termination control and reentry dispersion errors need to be minimized. The latter can be

![Figure 3.5—Advanced Missile Accuracy Versus GPS Velocity Measurement Error](image-url)

Figure 3.5—Advanced Missile Accuracy Versus GPS Velocity Measurement Error
accomplished by spin-stabilizing the reentry vehicle or designing it to have a high ballistic coefficient. This is a significant technical challenge.

- Selective availability has little effect on the accuracy of short- and medium-range GPS-guided ballistic missiles.
- GPS-aiding of ICBMs can significantly improve their CEP. It allows the use of low-cost inertial instruments for initial azimuth alignment and can minimize the effects of boost-phase inertial instrument errors. These benefits may be achieved with the SPS; DGPS is probably not required. These missile systems require sophisticated post-boost vehicles (PBVs) if they are to accurately deliver their warheads.

GPS-Guided Cruise Missiles

In the last few years, interest in the problem of cruise missile proliferation has grown substantially. One of the main reasons for this interest in cruise missiles, especially land-attack cruise missiles, is the fact that less-developed nations can use GPS to obtain high navigation accuracies. Whereas there is general agreement among analysts that GPS-guided cruise missiles (GCMs) pose a potential threat to U.S. security, there is wide disagreement on the magnitude of that threat. This section summarizes the results of research to assess the risk posed to U.S. forces by GCMs using GPS.

The analyses focus on attacks against U.S. forces in a theater of operations; attacks against the Continental United States (CONUS) are not considered for two reasons. First, the likelihood that the United States will become involved in a military conflict with an adversary both capable of and willing to conduct military attacks against CONUS is small. Second, terrorist attacks against CONUS are an ever-present danger. GCMs may provide terrorists with another weapon, but their overall contribution to the risks already facing U.S. citizens from terrorism is marginal.

To understand how GPS can significantly affect cruise missile guidance, one must understand the inherent limits of inertial navigation systems. Although INS packages are commercially available and are jam-proof, they have one major drawback—the physical forces that affect the gyroscopes and accelerometers used in inertial navigation systems create errors that accumulate over

---

28 GPS can be of particular benefit to sea-launched ballistic missiles (SLBMs) and mobile ICBMs because it reduces their position uncertainty at launch.

29 In this report, a cruise missile is defined as an unmanned, self-propelled vehicle that sustains flight through the use of aerodynamic lift over most of its flight path.

30 An inertial navigation system consists of gyroscopes, accelerometers, and some type of processor.
time. The navigation errors resulting from inertial drift are large enough to undermine the military utility of INSs for all but short-range missions. To illustrate this point, Figure 3.6 shows CEP as a function of inertial drift for three inertial navigation systems and compares these accuracies with the accuracy provided by GPS.\(^{31}\)

The drift error of the 10 deg/hr INS surpasses the position error of GPS almost immediately. The drift error for the 1 deg/hr INS surpasses the GPS error in approximately two minutes. For a 0.1 deg/hr INS, the two errors are equal after 10 minutes. In assessing the availability of these systems, note that the 10 deg/hr INS is an extremely low-quality system; a less-developed country (LDC) will al-

---

\(^{31}\)Figure 3.6 shows the accuracy available to civilian users when SA is turned on. The graph is based on an inertial navigation model found in Edward R. Harshberger, *Long-Range Conventional Missiles: Issues for Near-Term Development*, RAND, N-3328-RGSD, 1991, p. 121. Although the model expresses its navigation errors in deg/hr rather than nmi/hr, the model does include the errors from both gyroscopes and accelerometers. An excellent discussion of all the errors that have to be included in such a model is given in Morris M. Kuritsky and Murray S. Goldstein (eds.), "Inertial Navigation," *Proceedings of the IEEE*, Vol. 71, No. 10, October 1983, pp. 1156–1176.
most certainly be able to do better. The 1 deg/hr INS is very close to the limit of what an LDC could purchase legally. The 0.1 deg/hr INS is a high-quality system that falls under export restrictions.32

Before discussing the lethality of GCMs, we review cruise missile survivability. This is a vital topic for one simple reason—if a cruise missile cannot reach a target, its lethality is irrelevant. A missile attempting to attack U.S. forces will probably have to penetrate several layers of air defenses. An analysis of a missile’s ability to do this must consider the physical characteristics of the missiles, the number of missiles employed in an attack, and the deployment strategy.

The survivability of individual cruise missiles depends on two factors: how easy they are to detect and how easy they are to intercept once they are detected. The ability of U.S. forces to detect GCMs depends on the radar cross section, altitude of flight, and velocity of the missiles, as well as the capabilities of U.S. radars. These characteristics are as important in assessing the threat of GCMs as the guidance accuracy and payload. Many GCMs are likely to have small radar cross sections and fly at low altitudes, making them hard to detect because their radar returns will be buried in ground clutter. In addition, slow-flying low-technology cruise missiles could be hard for airborne radars to detect.

If they are detected, individual GCMs will probably be easy to shoot down because they do not react to fighters or SAMs employed against them.33 However, large numbers of missiles employed in a coordinated attack can stress both defensive fighters and terminal surface-to-air defenses.34 For example, while penetrating an area defended by fighters, a spreadout group of GCMs could force fighters to expend their fuel pursuing individual missiles, thus decreasing the total number of possible engagements or exhausting the available missile loadout of the fighter force. Similarly, GCMs might overwhelm terminal defenses by saturating a single SAM site—by exploiting the limited line-of-sight that ground-based radars have against low-flying missiles and by attacking in large numbers.

---

32High-accuracy gyroscopes, accelerometers, and INSs are export-controlled. For example, U.S. law prohibits the sale without licenses of gyroscopes with drift rates of 0.1 deg/hr (at linear accelerations of less than 10 g) and INSs with navigation errors of 0.8 nmi/hr (CEP). See Code of Federal Regulations (C.F.R) Vol. 15, Chapter VII, Part 799, Section 799.1, Item 7A03A, Office of the Federal Register, National Archives and Records Administration, Washington, D.C., 1993.

33Some GCMs may pose a challenge for air defenses. For example, slow-flying missiles may be hard for aircraft to intercept, particularly if they are flying at low altitudes. High-flying, supersonic cruise missiles could also be difficult to intercept because they compress time lines to the point where few shot opportunities are available for the defense.

34GPS timing and navigation information could be useful in coordinating such attacks. It could also provide increased flexibility for mission planning.
Once cruise missiles penetrate enemy defenses, the central issue becomes how much damage the missile can inflict on a target. To understand this problem, we will examine two cases: cruise missiles carrying high explosives, and cruise missiles carrying weapons of mass destruction (WMD). Through this analysis we will assess the effect that GPS can have on the lethality of cruise missiles. This will give us a better understanding of the implications of enemy use of GPS for cruise missile guidance.

The lethality of conventionally armed GCMs depends on several variables— their horizontal and vertical navigation accuracy, the angle of their terminal dives, their range and payload characteristics, their targeting accuracy, and the size and hardness of a given target. The following graphs show the single-shot probability of kill (SSPK) for GCMs carrying high explosives (HE) as a function of GPS accuracy for several scenarios. Figure 3.7 illustrates the effects of conventionally armed GCMs against soft point targets such as a wooden building. Figure 3.8 illustrates the effects against a hard target such as a sturdy industrial installation.

It is evident that the lethality of GCMs attacking point targets is highly dependent on the magnitude of targeting errors. Neither soft nor hard point targets face high risks from GCMs with large targeting uncertainties. If targeting errors are small, then the lethality of GCMs depends on their navigation accuracy. Cruise missiles attacking soft point targets will have low SSPKs if they use SPS, and high SSPKs if SA is off and/or if they use DGPS. GCMs attacking hard point targets will require the accuracies associated with DGPS to achieve high SSPKs.

Figures 3.9 and 3.10 show that the lethality of GCMs is higher against area targets than against point targets. The larger the target, the higher the lethality. It is also apparent that the utility of SA diminishes as a target’s area increases.

In summary, the lethality of conventionally armed GCMs depends on several factors. A key variable is targeting accuracy. If targeting errors are large, the ability of GCMs to successfully attack point targets drops significantly. In addition, many important point targets are mobile. Third World nations will have an extremely hard time trying to locate such targets. Thus, it is highly

---


36 These curves assume the attacking cruise missile performs near-vertical terminal dives. Thus, they represent a worst case from the point of view of U.S. military planners.
Figure 3.7—GCM Attacks Against Soft Point Targets

Figure 3.8—GCM Attacks Against Hard Point Targets
The Global Positioning System

Figure 3.9—GCM Attacks Against Small Area Targets

Figure 3.10—GCM Attacks Against Large Area Targets
unlikely that GCMs will pose a significant threat to point targets in the near future.

On the other hand, fixed area targets such as ports, warehouses, and airfields are much more vulnerable to cruise missile attacks. Locating such targets should be relatively easy and many of them could be pretargeted before a conflict began. In addition, GCMs do not require DGPS accuracies to achieve high SSPKs against these structures; SPS is sufficient.

The story is somewhat different for cruise missiles employing weapons of mass destruction than for GCMs carrying ordinary conventional warheads. In the former case, the attacker’s problem is to ensure that small numbers of valuable warheads arrive on target. Similarly, a defender facing missiles carrying WMD must ensure that no weapons leak through the defenses.

Many of the cruise missiles that Third World nations are likely to acquire for land-attack missions will either have long ranges and small payloads (e.g., unmanned aerial vehicles) or short ranges and large payloads (e.g., converted anti-ship cruise missiles). This may limit their ability to effectively deliver chemical and nuclear weapons. On the other hand, biological weapons are so lethal that even small payloads can completely cover a city, though the effects are far less predictable than for nuclear weapons.

In contrast to conventionally armed cruise missiles, GCMs carrying nuclear weapons could land within hundreds of meters of most targets and still accomplish their mission. The same is generally true of missiles carrying chemical and biological weapons. In most cases, SPS provides more than enough accuracy for cruise missiles carrying weapons of mass destruction. Thus, SA does little to limit the threat posed by such missiles—other defenses will have to be used against them.

In sum, the threat posed by GPS-guided cruise missiles is highly dependent on the physical characteristics of the missiles, the type of payload they are carrying, the intelligence and reconnaissance capabilities of the adversary, and the performance of air defenses. Specific conclusions are scenario dependent, but the analyses conducted herein point to some general observations.

---

37 For an analysis of the coverage areas of GCMs carrying chemical and biological weapons, see Irving Lachow, “GPS-Guided Cruise Missiles and Weapons of Mass Destruction,” in Kathleen C. Bailey (ed.), *The Director’s Series on Proliferation #8*, Lawrence Livermore National Laboratory, Livermore, CA, June 1, 1995, pp. 1–22. Note that nuclear weapons produced in the Third World will probably weigh at least 500 kg, which is more than many cruise missiles can carry. However, warheads obtained from other sources may be more compatible with cruise missile delivery. See Eric H. Arnett, “The Most Serious Challenge in the 1990s? Cruise Missiles in the Developing World,” in Eric H. Arnett and Thomas W. Wander (eds.), *The Proliferation of Advanced Weaponry: Technology, Motivations, and Responses*, American Academy for the Advancement of Science, Washington, D.C., 1992, p. 111.
• Conventionally armed GCMs may pose a significant threat to large fixed targets but do not threaten most mobile targets.

• GPS-guided cruise missiles appear to be good platforms for delivering chemical and biological weapons (CBW), especially the latter. However, the efficacy of CBW attacks may be greatly reduced if slow-flying cruise missiles are detected early enough to warn U.S. forces and be destroyed.

• At present, it is highly unlikely that nuclear weapons will be delivered by GPS-guided cruise missiles. That situation may change if advanced cruise missiles or small nuclear warheads become available to less-developed countries.

• SA can be quite effective when hard point targets are attacked. If soft or large targets are attacked, SA has minimal effect on the lethality of GCMs. In any case, GCMs using DGPS can achieve high SSPKs.

There is no question that GPS provides LDCs with access to signals that can be used to guide cruise missiles. However, it is the availability of the basic GPS signal itself that provides the greatest benefit to Third World nations. Selective availability may reduce the lethality of GCMs in some situations, but it does not eliminate the threat to U.S. forces. In addition, the proliferation of both local- and wide-area DGPS services will give Third World nations access to high accuracies in the near future. In sum, GPS-guided cruise missiles are a new feature on the landscape. The threat posed by cruise missiles using satellite navigation will exist whether SA is on or off, and may exist even if GPS should be turned off in the future.

PROVISION OF DGPS SERVICES

The Wide-Area Augmentation System (WAAS) is a space-borne system for providing differential GPS corrections over large areas of North American airspace. It may also serve as the prototype of a worldwide system of space-borne DGPS systems. However, the basic attributes of the system as currently articulated—to provide high accuracy to all users over wide areas—pose some concerns for national security planners. Since the DGPS accuracy provided will be better than the PPS available to the U.S. military and allied forces, hostile forces and groups might make use of the system. There is also concern that in conflicts between third parties, DGPS signals might be used to support military operations, and hence make the United States politically, if not legally, culpable.

---

38In discussions with foreign officials, security matters concerning GPS were conspicuously treated as an American matter, provided these matters did not interfere with other aspects of the system such as maintaining system availability at its current levels or altering the cost structure to end-users.
Differential correction signals can be distributed through several possible technologies. Figure 3.11 lists several approaches. The corrections themselves are obtained by combining information from a known reference location, or set of locations, and comparing that to the location obtained by observing a set of satellites. A receiver is placed at a surveyed location (i.e., a location whose position is known precisely). The GPS signals that arrive at that location contain errors that offset the position of the surveyed point by some amount. The errors in the GPS signal are determined by comparing the site’s known position with its position according to GPS. Correction terms for each satellite can then be calculated and transmitted to users. Those correction terms allow a user’s receiver to eliminate many of the errors in the GPS signal.\(^\text{39}\)

The DGPS correction signals can be transmitted many different ways, ranging from maritime telephones to satellite transmissions. The extent of the coverage is determined by the distribution of reference stations and the physical range of the transmitters. Long-range transmission of signals is practical if a sufficient number of reference stations are available to ensure that the appropriate correction can be applied in a region of interest and if the stations can be networked with the transmitters.

The operation of space-based DGPS transmitters with no intrinsic selective denial capability creates a dilemma for U.S. security officials, because interfering with the transmissions or the satellite might adversely affect other nations in the satellite’s antenna footprint. Figure 3.12 illustrates the coverage available from three notional satellites located at geosynchronous orbits. The contours denote elevation angles (0, 15, 30, and 45 degrees) at the ground terminal.

\begin{table}[h]
\centering
\begin{tabular}{|l|l|}
\hline
Space-based & Terrestrial \\
\hline
WAAS (L1 band) & FM-subcarrier \\
Low earth orbit communication satellite (LEO COMSAT) & Medium-frequency radio beacons \\
MTSAT & Maritime phones \\
INMARSAT & L1 band transmitters \\
& Cellular networks \\
\hline
\end{tabular}
\caption{Selected DGPS Distribution Methods}
\end{table}

\(^{39}\)All bias errors are eliminated. The remaining errors vary randomly and therefore cannot be corrected in this manner. However, the random errors contribute little to a user’s position uncertainty.
While options—such as encryption and steerable antennas—can improve a system’s ability to deny use of its signal to hostile groups, these options add cost and operational complexity to the use of the satellite. Thus, they run counter to the civil/commercial aspects of the system that call for its widespread availability at low cost. Also, the idea that a civil navigation system might be so configured has concerned allied governments, receiver manufacturers facing adverse impacts on sales, and those not wishing to foster support for alternatives to GPS.

In addition, uplinks (transmissions to the satellite) and downlinks (transmissions from the satellite to users) may be vulnerable to spoofing (where another transmitter inserts false information into the data-steam to mislead the receiver). National security planners are concerned about any system being constructed without prudent security precautions. However, any options to address system security would add at least marginally to the cost of the system,
An alternative to basing a DGPS system in space is to place an array of differential transmitters on the earth’s surface. Such transmitters might use FM-subcarriers, cellular phone networks, or maritime radios (all of which cover relatively short ranges), or might use medium-frequency (MF) transmitters such as the U.S. Coast Guard and Army Corps of Engineers’ system being established in the United States. Ground-based systems have some vulnerabilities from the national security perspective in that many transmission sites in a conflict would be located in a belligerent nation and would be subject to either physical destruction or electronic warfare.

There is, however, a wrinkle to this matter, at least if MF systems are used. Because of the propagation characteristics of the MF signal, it is possible to use the signal at significantly long ranges from a transmitter site—particularly at night. Also, if networked into arrays of ground stations that provide the correction signals, modest numbers of transmitters can cover extended areas. One could intentionally place DGPS sites to support one’s own military activity or a neighboring nation’s activity as part of an overtly civilian system that is available to all end-users. Furthermore, DGPS sites are readily immunized by placement on or near sensitive installations such as hospitals, and by their overt use in the civilian sector. Even military transmitters could be survivable given their relatively low power requirements of 1–120 Watts and their small size. Hunting down and destroying a proliferated network would be difficult, although electronic warfare against the sites appears relatively simple.

An MF DGPS signal may propagate in several ways (see Figure 3.13). The signal may propagate via a direct wave when the receiver has an unobstructed line-of-sight to the transmitter. The signal can propagate via a ground wave (the primary mode for a DGPS system) that is diffracted (and to some extent refracted by the atmosphere) around the earth’s surface, and is attenuated by varying amounts depending on the conductivity and dielectric constant of the earth’s surface along the signal’s path. At night, when the absorptive D-layer of the lower ionosphere is depleted, the MF signal may traverse it and be reflected off the higher E-layer, and thereby be received at longer ranges than a ground wave.

Interestingly enough, if the system were purely commercial, many of the security precautions suggested by the national security community might be needed to avoid liability for the space-based DGPS system (protecting the signal uplinks and downlinks), and to allow for revenue production (controlling end-user access). However, there is no guarantee that a commercial company would in fact be U.S. or that it could be forced to follow the direction of the United States government.
A system designer might design the system to exploit only the ground wave, since it is the most robust of the modes (allowing 24-hour propagation) and would constitute conservative design practice. A military planner might attempt to exploit the signal at longer ranges by opting for nighttime operations when the sky wave is strong, although utility at longer ranges is lessened because of the difficulty in maintaining view of the same satellites and the lesser accuracy available at significant distances from a reference location. There is also the possibility of networking remote reference stations together (possibly even covert reference stations passing information over other communications media), and propagating the signal via MF transmitter.

The difference between the extent of coverage that the system designer might anticipate and the range a military planner might achieve is exploitable under well-understood circumstances. (See Figure 3.14.) As one can see, concerns over DGPS signals being available to belligerent nations is not removed by promoting terrestrial DGPS systems over space-based systems. Consider the problems arising in the example shown if the sites illustrated were located in neutral territory. Extending the conflict to neutralize these sites could be of uncertain value while escalating the conflict dramatically.

To quantify the problem, signal transmission and reception were analyzed using a simulation that evaluates signal propagation over paths radiating away
Figure 3.14—Designers’ and Military Planners’ Views of Medium-Frequency DGPS Signals Differ Significantly

from the broadcast stations. Figure 3.15 shows the basic approach toward assessing the impact of multiple transmitters on coverage throughout a region. Each transmitter had a set of spokes assigned to it, along which pseudo-receivers were located. The strength of the received signal was calculated for each pseudo-receiver along the spokes and repeated for all transmitter sites considered. Calculations were made for Southwest Asia and the Far East to demonstrate the effects of differing terrain on ground conductivity with line-of-sight calculations. Simulation runs examined the impact of seasonal variations (winter/summer), and time of day (noon, dawn, dusk, and midnight). Receiver altitude was also examined to better understand the effect of equipping missiles and aircraft with DGPS receivers and the expected strength of the signal at the time of reception. The added signal strength at altitude could be important in properly assessing the possibility of jamming the DGPS signal.

Figure 3.16 shows the output for a single spoke with signal strength plotted against range from the transmitter. Signal components from the direct wave, ground wave, sky wave, and the resultant total signal wave are plotted, along with representative thresholds for the receiver. A sky-wave/ground-wave interference calculation was explicitly modeled for the region where sky wave and ground wave interact. The case shown is for a single spoke radiating away from a transmitter site located on the Korean peninsula.
Candidate transmitter locations identified
Signal propagation assessed at 10 km increments along sets of spokes
1-Watt and 120-Watt ERP
Multiple altitudes for receivers assessed

Model Included:
Direct wave
Ground wave
Sky wave (night)
Ground-wave/sky-wave interference

Seasonal variations:
Time of day
Geographic
Man-made and natural noise sources

Figure 3.15—Medium-Frequency DGPS Signal Propagation Assessment Methodology

Figure 3.16—Nations Can Take Advantage of Enhanced Ranges by Exploiting the Sky Wave
There is an appreciable difference between the strength and range of the signal during daylight hours and at night. In both cases, night and day, the dominant portion of the signal is the direct wave until line-of-sight is broken, when it falls to the signal from the ground wave. For the noon case (Figure 3.16, left), the signal decreases with range, following the ground-wave’s attenuation contour. For the midnight case (Figure 3.16, right), the signal follows the ground-wave portion of the curve until it intercepts the sky wave, and then falls off with range as does the sky wave. The region where the sky wave and ground wave have approximately the same strength can involve either positive or destructive interference. However, an airborne vehicle would probably traverse that region in a short time.

If the system accuracy is acceptable at longer ranges, and the technical limitations associated with maintaining view of the same satellites and remote reference stations are overcome, the longer range should be exploitable by friendly and hostile forces. In the case of a signal provided by a neutral party, a logical option would be to reduce its transmitter power. In civil and commercial applications, transmitted power is reduced to avoid interference with remote AM radio stations operating at frequencies close to DGPS stations.

Figure 3.17 shows the propagation of DGPS signals in Northeast Asia from sites at which 120-Watt ERP DGPS transmitters could be located. The four cases shown are for winter, with variations in the necessary signal-to-noise threshold for the GPS receiver (10 dB/0 dB) and for the time of day (noon/midnight). The 10-dB receiver thresholds are based on the performance of commonly available equipment, whereas the 0-dB values represent a more sophisticated receiver. Noon was chosen as the representative time that system designers might use, and midnight was chosen to highlight the maximum range to which the signal might propagate.

In the cases shown, receiver stations falling within \( \pm 3 \text{ dB} \) of the target sensitivity are highlighted. Rings with large open regions indicate that receivers were still outside the receiver threshold when calculations were terminated. The striking aspect of this is that a relatively small number of transmitter stations, as distinct from monitoring stations, can cover large areas.

The other point to keep in mind is that all regions of the world are not of equal interest to the United States either in geopolitical or economic terms. When one examines the regions where the United States has significant interests (such as Northeast Asia, Southwest Asia, and Europe), two facts become apparent: (1) terrestrial DGPS services will quite possibly be used within those regions, and (2) DGPS distribution services that cross borders might pose a problem. Wide-scale deployment of DGPS services could likewise cover many regions of interest.
The Global Positioning System

• 13 sites
• 10-dB SNR threshold
• 120-W ERP

Maximum coverage at midnight in Northeast Asia

• 13 sites
• 0-dB SNR threshold
• 120-W ERP

Maximum coverage at noon in Northeast Asia

Figure 3.17—DGPS Reference Station Propagation in Northeast Asia
The key attributes of DGPS services are shown in Figure 3.18. In all likelihood, it will be difficult to interfere with DGPS stations in near-war situations. The inability to interfere with this class of target arises from the nonmilitary use of the system, including possible safety-of-life functions within the target country. Even if those attributes could be set aside, DGPS signals will not necessarily respect borders, and it is possible that critical regions like the Middle East will have neutral-nation systems overlapping regions of interest. This is especially true for many space-based systems with intrinsically wide-area coverage, some of which may not be under the control of the United States.

Assuming that DGPS services are a possible problem—whether or not space-based distribution of corrections occur, how can the United States mitigate the fact that hostile groups have access to GPS/DGPS signals? It would be helpful to have a range of options, such as agreements with countries hosting DGPS networks to limit their operations upon request, as well as to ensure the ability to jam or attack such networks if necessary. To the maximum extent possible, it is in the security interest of the United States to have DGPS systems that cross international boundaries under the direct control of allied nations, as opposed to potential adversaries or international civil organizations. Direct control may or may not include encrypting the DGPS communications link or limiting transmissions to ground-based sites. The important point is that such systems be subject to control for international security purposes.

A higher-order question is whether DGPS and other improvements over the SPS signal would substantively alter any current U.S. defense plans, or substantively alter the ability of U.S. forces to operate around the world. The ability to deter or negate the hostile use of DGPS signals may be part of layered missile and air defense strategies, but it is not likely to be the most important factor. Other capabilities, such as target detection and interdiction as well as the direct suppression of attacks will justifiably consume more resources and attention.
SELECTIVE AVAILABILITY

Selective availability is a technique that intentionally degrades the accuracy of GPS signals available to civilian users. A random process dithers the satellite clocks and falsifies the satellite ephemerides so as to produce position and time errors for SPS users of the service. When SA is active (“on”), the horizontal position accuracy of the civilian signals drops from 20–30 meters to 100 meters (95 percent probability) and the timing accuracy is reduced from 200 nanoseconds to 340 nanoseconds (95 percent probability) relative to Coordinated Universal Time (UTC).41 This accuracy is available worldwide and without restriction to any user. The actual accuracy of SPS with SA off can approach about 5 meters, which is much better than the system specification.

The main justification for SA is that it prevents the use of high-accuracy signals by adversaries. However, it is not evident that SA is successfully accomplishing this mission; high-accuracy signals can be obtained through the use of differential GPS methods. In fact, it is possible that the SA control policy has actually encouraged some users to turn to differential services because the SPS accuracies were not adequate for their needs. Whether or not this is true, both local and wide-area DGPS services are spreading rapidly around the world. It has also been stated that the current SA policy benefits U.S. companies that currently have an edge over foreign competitors. This benefit, however, is limited to a few firms and may only be a short-term artifact that could quickly change.

Another problem with the argument that SA alone prevents the hostile use of GPS is that many factors affect the lethality of a weapons system. For example, the lethality of a GPS-guided cruise missile depends on its navigation accuracy, its targeting accuracy, the angle of its terminal dive, its payload, and the size and hardness of a given target. Although GPS provides positioning information that can be extremely useful to military forces, that information can only be exploited to the extent that the forces are properly equipped and trained to use it. It has also been stated that SA is important because it degrades the velocity information inherent in GPS signals. Such information could be used to update the inertial systems on board hostile ballistic missiles. This concern was addressed in previous sections that showed that much of the benefit of GPS is already realized with access to SPS accuracy levels.

On the other side of the debate, it has been argued that turning SA off in peacetime would help to promote international acceptance and reliance on the U.S. GPS system. A comparison of the advantages and disadvantages of selective

---

41 The spatial and temporal accuracies for GPS with SA on are defined in the U.S. Federal Radionavigation Plan and also in the GPS SPS signal specification document. These accuracies are given and have not been estimated or calculated by the authors.
availability is shown in Table 3.10. The SA issue is more fully discussed in Chapters Four and Six.

ANTI-SPOOFING

GPS anti-spoofing (AS) encrypts the P-code so that only authorized users can have access to it. The resulting signal is known as the Precise Positioning Service (PPS). Access to PPS can be obtained only with receivers equipped with a cryptographic key. PPS provides users with a horizontal accuracy of 22 meters (95 percent probability) and 200 nanoseconds (95 percent probability). In addition to protecting access to the P-code, AS makes the PPS signal extremely difficult to spoof (hence its name). Despite its benefits, the AS policy does have some drawbacks such as expensive receiver equipment and the need for a cryptographic key management infrastructure.

<table>
<thead>
<tr>
<th>SA on in Peacetime</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denies high accuracy (10–15 CEP) to adversaries, required for some military missions</td>
<td>SPS satisfies many military needs and DGPS methods circumvent SA</td>
<td></td>
</tr>
<tr>
<td>Shows political resolve, which may discourage foreign military dependence on GPS</td>
<td>Encourages reliance on DGPS, wide-area DGPS or other satnav systems (e.g., GLONASS)</td>
<td></td>
</tr>
<tr>
<td>Would be difficult to reactivate SA if turned off</td>
<td>Clear policy stating conditions for reactivation of SA reduces concern</td>
<td></td>
</tr>
<tr>
<td>Prevents accurate GPS velocity updates for ballistic missile applications</td>
<td>Significant CEP errors such as reentry dispersions not corrected by GPS; also DGPS can provide velocity updates</td>
<td></td>
</tr>
<tr>
<td>Benefits DGPS companies; maintains edge over foreign competitors</td>
<td>Benefits limited to certain companies—a short-term view that could quickly change</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SA off in Peacetime</th>
<th>Pro</th>
<th>Con</th>
</tr>
</thead>
<tbody>
<tr>
<td>Promotes international acceptance of, and reliance on, GPS-based technologies.</td>
<td>Foreign users primarily concerned with DoD control of GPS rather than status of SA</td>
<td></td>
</tr>
<tr>
<td>Provides improved accuracy to all GPS users, less reliance on DGPS</td>
<td>Less revenue for companies that provide DGPS services</td>
<td></td>
</tr>
<tr>
<td>Reduces DGPS correction update rate, conserving spectrum bandwidth</td>
<td>Amount of conservation not significant</td>
<td></td>
</tr>
</tbody>
</table>
OVERALL THREAT ASSESSMENT

There are many possible uses of GPS and augmented GPS in the military arena. GPS information can influence many aspects of warfare, including the operation of space, air, ground, naval, and special forces. In most cases, the benefits provided by GPS are not revolutionary; rather, they increase the efficiency of forces in the field. The military benefits of GPS to U.S. forces in large part draw from the way the United States has chosen to organize, train, and equip those forces. As with other information technologies, the effective use of GPS requires an extensive infrastructure, training, and—perhaps most important—a doctrine that combines GPS information with other systems for operational employment. Indeed, a relatively small number of nations are capable of truly exploiting the full potential of GPS technology over the near to mid term, and virtually all of them are U.S. allies.

Aside from the performance of individual weapons, the number and type of weapons threatening the United States need to be considered. Typically, potential adversaries have access to tens to low hundreds of the kind of precision weapons that we have discussed. By comparison, the United States employed 288 TLAMs (Tomahawk Land Attack Missiles) during Operation Desert Storm against Iraq, and these were only a small portion of the total number of precision weapons used during the conflict. Given a nominal assignment of two to six missiles per militarily significant aim point, the coverage expected from a small cruise-missile-equipped force would not be very extensive.

Precision weapons could be used against small numbers of politically sensitive targets. In this role, the actual damage is not as important as the effort itself. In the Persian Gulf War, attacks by Iraq against Saudi Arabia and Israel were political attacks, and they served that role well. Presumably, a more accurate system with a better chance of striking a particular target, such as a parliament building, would have greater effect. However, GPS-aided weapons are not the only means of delivering such attacks (enemy special operations forces might be effective here). Whereas improved accuracy helps in the attack of politically sensitive targets, the nature of the targets themselves and their disposition within a country usually lend themselves to other lines of attack as well.

The examination of GPS-aided ballistic and cruise missiles shows that improvements in performance are possible; however, those improvements need to be seen within a broader set of considerations such as the nature of the threat (e.g., numbers and types of warheads on the weapons), planned U.S. re-

sponses to the threat already being deployed (e.g., upgrades to the Patriot air defense system), as well as additional countermeasures necessitated by the availability of GPS (e.g., better jammers and receivers able to acquire P-code directly), and the costs associated with both sets of responses.

National security threats to the United States will continue to exist independent of the possible exploitation of GPS/DGPS, but we must understand whether the potential for hostile GPS exploitation and denial will drive current U.S. force structure and R&D investment plans in different directions, or change how the United States conducts military operations or its strategy for particular regions. For example, will the existence of GPS-aided cruise missiles change plans to conduct defensive operations against modest-sized forces exploiting weapons of mass destruction? For the most part, the answer appears to be no. U.S. planning will still need to avoid single-point failure modes vulnerable to small numbers of weapons. In addition, air defenses will have to be sized to handle raids consistent with a larger-scale conventional attack or a WMD attack masked by decoys and conventional weapons.

### Placing the Threat in Context

Hostile forces using GPS for guidance can pose some risk to U.S. forces, but that risk must be placed in context. Figure 3.19 summarizes the magnitude of the GPS-based threat to U.S. national security.

<table>
<thead>
<tr>
<th>Does an adversary’s use of GPS:</th>
<th>Threat</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Threaten survival of U.S.?</td>
<td>*</td>
</tr>
<tr>
<td>B. Prevent the U.S. from winning a major regional contingency?</td>
<td>**</td>
</tr>
<tr>
<td>C. Enable destruction of critical national assets?</td>
<td>***</td>
</tr>
<tr>
<td>– Key military facilities</td>
<td></td>
</tr>
<tr>
<td>– Civilian infrastructure</td>
<td></td>
</tr>
<tr>
<td>D. Improve adversary’s ability to attack military targets?</td>
<td>****</td>
</tr>
<tr>
<td>– Fixed targets, ships</td>
<td></td>
</tr>
<tr>
<td>E. Threaten U.S. lives and property?</td>
<td>*****</td>
</tr>
<tr>
<td>– Terrorists, special operations</td>
<td></td>
</tr>
</tbody>
</table>

Figure 3.19—Assessing the Threat of Hostile Forces Using GPS
Thus, enemy forces using GPS can threaten U.S. lives and property and can probably improve an adversary’s ability to attack U.S. military targets. However, these forces’ ability to destroy critical national assets is marginal, and the likelihood that they will either prevent the United States from winning a medium regional contingency (MRC) or threaten the survival of the United States itself is quite low.

National Security Findings

During the course of the analysis, a number of national security findings were reached. While the detailed analyses highlighted the impact of GPS on specific types of operations as well as methods of exploiting augmented signals, these findings must be placed in the context of high-level decisions. GPS/DGPS services can improve the ability of properly trained and equipped forces to operate against the United States. However, the overall magnitude of that threat appears manageable provided the United States proceeds prudently in preparing an array of defensive measures designed to operate in a world where precision time and location services are available. These measures might include fielding theater air defenses designed to operate against raids that might intermix conventional weapons and weapons of mass destruction, electronic warfare assets to degrade the guidance of conventionally armed weapons, passive defenses to protect personnel and installations, and mobility to avoid creating an attractive target for the enemy.

Changes in GPS practices, such as keeping SA on or off, will not materially alter U.S. plans for theater air defenses and theater missile defenses, because the intrinsic accuracy of most delivery systems is adequate for the WMD payloads that represent the greatest concern. The U.S. military will still require both active and passive defense programs against cruise and ballistic missiles to deal with WMD threats. Furthermore, because the consequences of leaks is so serious, active defenses designed to deal with large-scale attacks of WMD-equipped missiles should be more then adequate to deal with conventional attacks of comparable size.

Current approaches to GPS control such as SA have limited utility over the long run and may accelerate the development of competitors to GPS that are difficult to deal with both technically and politically. As the detailed analyses demonstrated, SA can degrade the accuracy of threats in the short term, even though access to the C/A-code already provides most of the added utility. Also, the costs of approaches like SA create conditions conducive to the creation of competing systems that might undermine the benefits of maintaining ultimate control of the GPS constellation.
The United States needs to think about how it can and should shape the international environment for space-based navigation services at the same time it considers appropriate responses to changing threats from long-range weapons delivery systems such as cruise missiles. For example, a stable and predictable GPS policy in the United States can help promote GPS as a global standard. In the case of DGPS services that cross international boundaries, it is in the security interests of the United States to have such systems under the direct control of allies, as opposed to potential adversaries or international civil organizations. Direct control can encompass a spectrum of techniques, from using encryption of the DGPS communications link to ensure access only by authorized receivers through diplomatic agreements to limit areas and times of operation when international conditions warrant.

Examination of the technology underlying GPS indicates that the United States cannot count on maintaining a monopoly on precision time and location services forever. Indeed, because of the relative simplicity of GPS-like technologies, it is vital that the United States begin preparing to operate in a world where access to GPS-type and augmented GPS services are the norm. The economic and technical barriers to entry for a competing satellite navigation system are shrinking with the creation of LEO communication satellite networks (which may lower the costs of building and launching satellites). Thus it will become increasingly risky to assume that no other party will be able to introduce a competing system should GPS become unavailable or unreliable.