FUTURE WAR PAPER

TITLE:
GPS and Military Warfare in the 21st Century: An Integrated Approach to Mitigate Interference

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF OPERATIONAL STUDIES

AUTHOR:
Major Nicholas C. Nuzzo, USMC

AY 2013-14

Mentor: Dr. Bradley J. Meyer
Approved: Bradley J. Meyer
Date: 22 April 2014
In order to succeed in future military warfare, the United States military must fully integrate technical and non-technical countermeasures to ensure GPS remains a powerful warfighting capability. The U.S. military continues to increase its reliance on the GPS for PNT applications. In the meantime, capabilities for intentional GPS interference, such as jamming or spoofing, have continued to emerge. A broad and integrated approach that combines technical and non-technical measures is required to have an effective and efficient system that also takes into consideration the fiscally constrained environment the U.S. military faces for the foreseeable future. The technical measures include technological improvements to the subsystems of GPS and the development of non-GPS alternatives and active measures based on tactical and operational measures that include taking an offensive approach towards the GPS interference threat.
EXECUTIVE SUMMARY

Title: GPS and Military Warfare in the 21st Century: An Integrated Approach to Mitigate Interference

Author: Major Nicholas C. Nuzzo, United States Marine Corps

Thesis: In order to succeed in future military warfare, the United States military must fully integrate technical and non-technical countermeasures to ensure GPS remains a powerful warfighting capability.

Discussion: The U.S. military continues to increase its reliance on the Global Positioning System (GPS) for positioning, navigation, and timing (PNT) applications. In the meantime, capabilities for intentional GPS interference, such as jamming or spoofing, have continued to emerge. A broad and integrated approach that combines technical and non-technical measures is required to have an effective and efficient system that also takes into consideration the fiscally constrained environment the U.S. military faces for the foreseeable future. The technical measures include technological improvements to the subsystems of GPS and the development of non-GPS alternatives as redundant or back-up systems. Non-technical measures include passive measures based on PNT alternatives and active measures based on tactical and operational measures that include taking an offensive approach towards the GPS interference threats.

Conclusion: No approach alone stands out as a full solution. However, integrating both technical and non-technical approaches ensures a robust countermeasure system the U.S. military can use against adversaries who attempt to interfere or deny use of GPS. That is, an integrated approach will enable the U.S. military to maintain “GPS superiority.”
DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report Documentation Page</td>
<td>ii</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>iii</td>
</tr>
<tr>
<td>Disclaimer</td>
<td>iv</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>v</td>
</tr>
<tr>
<td>List of Figures</td>
<td>vii</td>
</tr>
<tr>
<td>List of Acronyms</td>
<td>viii</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>GPS Vulnerabilities and Threats</td>
<td>2</td>
</tr>
<tr>
<td>GPS Basics and Vulnerabilities</td>
<td>2</td>
</tr>
<tr>
<td>Jamming</td>
<td>3</td>
</tr>
<tr>
<td>Spoofing</td>
<td>5</td>
</tr>
<tr>
<td>Technical Approaches</td>
<td>5</td>
</tr>
<tr>
<td>Space Segment Improvements</td>
<td>6</td>
</tr>
<tr>
<td>User Segment Improvements</td>
<td>8</td>
</tr>
<tr>
<td>Alternative Means</td>
<td>10</td>
</tr>
<tr>
<td>Non-Technical Approaches</td>
<td>12</td>
</tr>
<tr>
<td>Passive Approach</td>
<td>12</td>
</tr>
<tr>
<td>Active Approach</td>
<td>13</td>
</tr>
<tr>
<td>Criteria and Assessment</td>
<td>15</td>
</tr>
<tr>
<td>Conclusions and Recommendations</td>
<td>16</td>
</tr>
<tr>
<td>Notes</td>
<td>18</td>
</tr>
</tbody>
</table>
Bibliography

### LIST OF FIGURES

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1.</td>
<td>A 20-Watt GPS Jammer</td>
<td>4</td>
</tr>
<tr>
<td>Figure 2.</td>
<td>Examples of Personal Privacy Devices</td>
<td>4</td>
</tr>
<tr>
<td>Figure 3.</td>
<td>The GPS anti-jam technology (GAJT&lt;sup&gt;TM&lt;/sup&gt;) antenna</td>
<td>9</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>C/A code</td>
<td>coarse/acquisition code</td>
<td></td>
</tr>
<tr>
<td>EGBU</td>
<td>Enhanced Guided Bomb Unit</td>
<td></td>
</tr>
<tr>
<td>eLORAN</td>
<td>enhanced Long Range Navigation</td>
<td></td>
</tr>
<tr>
<td>GMLRS</td>
<td>Guided Multiple Launch Rocket System</td>
<td></td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
<td></td>
</tr>
<tr>
<td>HARM</td>
<td>High-speed Anti-Radiation Missile</td>
<td></td>
</tr>
<tr>
<td>INS</td>
<td>inertial navigation system</td>
<td></td>
</tr>
<tr>
<td>JDAM</td>
<td>Joint Direct Attack Munition</td>
<td></td>
</tr>
<tr>
<td>LPS</td>
<td>local positioning system</td>
<td></td>
</tr>
<tr>
<td>MEMS</td>
<td>microelectromechanical systems</td>
<td></td>
</tr>
<tr>
<td>M-code</td>
<td>Military Code</td>
<td></td>
</tr>
<tr>
<td>P-code</td>
<td>military precision code</td>
<td></td>
</tr>
<tr>
<td>PNT</td>
<td>positioning, navigation, and timing</td>
<td></td>
</tr>
<tr>
<td>PPDs</td>
<td>personal privacy devices</td>
<td></td>
</tr>
<tr>
<td>TTPs</td>
<td>techniques, tactics, and procedures</td>
<td></td>
</tr>
<tr>
<td>UAV</td>
<td>Unmanned Aerial Vehicle</td>
<td></td>
</tr>
</tbody>
</table>
Introduction

The U.S. military continues to increase its reliance on the Global Positioning System (GPS) for positioning, navigation, and timing (PNT) applications. Ground troops, military aircraft, and naval vessels use GPS to navigate. Mounted troops use GPS-based systems, such as the Blue Force Tracker, to determine their own locations and the locations of their adjacent units, as well as to provide a common operational picture to higher headquarters. Military communication systems require the accurate timing GPS provides for the synchronization needed to encrypt communication and transmit data.¹ U.S. military precision guided munitions use GPS to achieve the "smart" effect desired. Examples include the Joint Direct Attack Munition (JDAM), Tomahawk, Harpoon, Enhanced Guided Bomb Unit (EGBU) - 15, Excalibur, and the Guided Multiple Launch Rocket System (GMLRS).² In the meantime, capabilities for intentional GPS interference, such as jamming or spoofing, have continued to emerge. In our adversaries' hands, these capabilities pose a significant risk to our ability to fight and win future wars. In order to succeed in future military warfare, the United States military must fully integrate technical and non-technical countermeasures to ensure GPS remains a powerful warfighting capability.

A broad and integrated approach that combines technical and non-technical measures is required to have an effective and efficient system that also takes into consideration the fiscally constrained environment the U.S. military faces for the foreseeable future. The technical measures include technological improvements to the subsystems of GPS and the development of non-GPS alternatives as redundant or back-up systems. Non-technical measures include passive measures based on PNT alternatives and active measures based on tactical and operational measures that include taking an offensive approach towards GPS interference threats. No
approach alone stands out as a full solution. However, integrating both technical and non-technical approaches ensures a robust countermeasure system the U.S. military can use against adversaries who attempt to interfere or deny use of GPS.

This paper takes the following path to support this argument. First, it will provide a brief overview of what makes GPS vulnerable. Second, it will present technical approaches for mitigating GPS interference. Next, it will present non-technical approaches. Fourth, it will provide criteria for assessing the solutions and an overall assessment. Finally, in the conclusions section, this paper includes recommendations for further studies and actions.

**GPS Vulnerabilities and Threats: Jamming and Spoofing**

**GPS Basics and Vulnerabilities**

A basic understanding of GPS provides the context required to understand its vulnerabilities. GPS consists of three segments: the space segment, the control segment, and the user segment. The space segment includes the constellation of GPS satellites. Each satellite is approximately 12,600 miles above the earth. The control segment consists of the ground-based facilities responsible for updating and keeping track of the satellites. Finally, the user segment includes the individuals and systems using receivers and antennas to convert the satellite signals to PNT data. Due to satellite power limitations and distance, by the time the GPS signal reaches the user it is extremely weak - equivalent to a "25-watt light bulb shining" from over 12,000 miles away. Additionally, the military signals are transmitted on only two published and well-known frequencies. In other words, the GPS signal is extremely susceptible to interference.

Despite its vulnerabilities to interference, GPS has permeated throughout the U.S. military. The examples delineated in the opening paragraph of this paper are just a sample of the
U.S. military's reliance on GPS for PNT required to execute military operations. GPS has become a critical part of the U.S. military infrastructure since its degradation would significantly impact a wide spectrum of capabilities. Technology capable of degrading GPS by exploiting these vulnerabilities already exists and continues to advance.

**Jamming**

Jamming, as the word implies, prevents a signal from arriving at the intended receivers by replacing it with a more intense, meaningless signal. A brief overview of GPS jamming examples is prudent to appreciate both current jamming capabilities and future possibilities as jamming technology advances. Additionally, this overview provides context for the proposed countermeasures that follow. Prior to the U.S. invasion of Iraq in 2003, Saddam Hussein acquired GPS jammers in recognition of the U.S. military reliance on GPS. The Iraqi military did not succeed in employing the jammers effectively due to its lack of experience and training. In 2010, North Korean GPS jammers in Kaesong successfully interfered with seaborne and land-based GPS receivers, both military and civilian, in South Korea. At the time North Korea had vehicle mounted GPS jammers capable of jamming out to 100 kilometers. A year later, Iranian engineers alleged that they were able to capture a U.S. drone flying over Iran by interfering with the GPS signals the drone was using to navigate. Though the U.S. military did not officially accept GPS interference as a reason for the loss of the drone, jamming is a plausible explanation. The author's last unit lost a high value Unmanned Aerial Vehicle (UAV) during a training exercise due to loss of the GPS signal. Though significantly less sophisticated than the aforementioned drone, an aerial vehicle solely relying on GPS for navigation will eventually return to earth when it loses the GPS signals, no matter the cause. Since the late 1990s, companies around the world have been selling relatively compact and low-powered GPS
jammers with ranges of 70 to 200 kilometers for $500 to $40,000. Figure 1 illustrates an example of a new family of GPS jammers introduced in 2009.

![Figure 1. A 20-Watt GPS Jammer.](image)

Examples of jamming on the civilian side further illustrate the severity of the threat. Though illegal, personal privacy devices (PPDs) are available from as low as $30 to over $300, with some models using cigarette lighters as a power source. These devices are capable of jamming GPS receivers from hundreds of yards for the inexpensive models to ten miles for the high-end ones. Examples of PPDs are depicted in Figure 2.

![Figure 2. Examples of Personal Privacy Devices.](image)
In 2009, a truck driver using an inexpensive PPD unintentionally jammed the GPS receiver of a navigation aid at the Newark airport. In 2011, the commanding general of Air Force Space Command voiced concern that LightSquared, a U.S. wireless broadband company, jammed GPS signals up to 12 miles from their towers. Several months later, at a congressional hearing on sustaining GPS for national security, the subcommittee Chairman expressed fear that if the Federal Communications Commission allowed LightSquared to proceed "the DoD's training activities in the United States may come to an end." 

**Spoofing**

Spoofing is another form of interference. Instead of sending meaningless noise to the receiver to jam it, spoofing sends a stronger signal of simulated information to spoof, or trick, the receiver. Though there have been many examples of spoofing on civilian GPS systems, spoofing is less of a concern for full, up-to-date military GPS systems because of the ability to encrypt the signal.

Now that we have a basic understanding of GPS vulnerabilities and the threats against it, we will transition to examining potential solutions to the problem of GPS interference. Countermeasures to GPS interference fall into two broad categories: technical and non-technical approaches. We will initially focus on the technical approaches.

**Technical Approaches**

The technical approaches focus on the scientific aspects of GPS. The obvious starting point is examining the system itself. Technical improvements to the space segment and the user segment of GPS can mitigate interference. In other words, modifications to the GPS satellites and the receivers and antennas of GPS devices can counter GPS jamming and spoofing.
additional technical approach is to establish alternative means for receiving PNT information. These alternative means serve as a redundant or back-up system that can work in conjunction with GPS or in its place. This section will sequentially address the three categories of these technical approaches: improvements to the space segment, improvements to the user segment, and establishment of alternative means.

**Space Segment Improvements**

We have established that the main vulnerability associated with GPS is its weak signal strength. Additionally, there are only two frequencies through which the GPS signal is transmitted. This combination allows an adversary to send a stronger signal of meaningless noise across these two frequencies to jam the receiver or send a stronger signal of simulated information to spoof, or trick, the receiver. Therefore, one obvious technical approach is to address the source of the signal -- the GPS satellites. There are three options within the technical approaches to counter GPS interference associated with the space segment: increase the signal strength, increase the frequencies, and modify the signals.

Increasing the GPS satellite signal strength will challenge devices meant to interfere with those signals. There is an opportunity to make improvements in signal strength each time the U.S. adds GPS satellites to the constellations or simply replaces older ones. As a matter of fact, this is something the U.S. Department of Defense is planning. The next version of GPS satellites, the IIA, will have a three-fold signal increase compared to its predecessors, the IIF.\textsuperscript{15} Plans for follow-on satellite models, the IIIC, add an even more impressive capability referred to as the "spotbeam." The IIIC satellites will be able to focus their signals over a desired region, approximately 600 miles in diameter, with a planned signal strength increase 100 times greater than that of the IIF satellites.\textsuperscript{16} Adversaries will have to bring their jamming devices closer to
their targets, increase their signal strength, or both. In the case of the "spotbeam," a 10-watt GPS jammer's effective range will decrease from 55 miles to approximately 2 miles, a 96 percent reduction in effectiveness.\textsuperscript{17}

Increasing the number of frequencies at which GPS satellites emit their signals will also challenge an adversary attempting to jam them. Transmitting the signal across additional frequencies will require jamming across a wider spectrum. This will require a more sophisticated jamming system and one that is easier to detect as it transmits its jamming signal across a wider spectrum. The main challenge with this approach is that it requires a parallel adjustment within the user segment. That is, it will require the user segment to modify or replace its GPS receivers. Additionally, there are potential challenges associated with frequency allocation in an already tight market as exemplified in the aforementioned LightSquared case. Nonetheless, despite the challenges, adding frequencies to GPS is a viable approach.

The final technical approach to mitigate GPS interference within the space segment is to modify the signal. Creating a more sophisticated signal intended for military users and subsequently encrypting it will mitigate intentional interference. Current GPS satellites provide these options and future satellites will make improvements. GPS satellite signals include two codes: the coarse/acquisition code (C/A-code) and the military precision code (P-code).\textsuperscript{18} C/A-code is the simplest code and is meant for commercial GPS receivers. P-code modulates at a frequency ten times greater than C/A code resulting in a signal that is ten times more dense and difficult for a jammer to "swamp."\textsuperscript{19} GPS satellites have the ability to counter spoofing by encrypting the P-code. Without this encryption, an adversary is unable to transmit a legitimate encrypted P-code signal and therefore unable to spoof a receiver capable of decrypting it.\textsuperscript{20} One challenge that remains is that the military still uses many receivers that have to find the C/A-code.
first before they transition to the P-code. The latest GPS satellites, Block IIR-M, include a new code -- the Military Code (M-code). Technology exists for receivers to acquire the M-code directly without having to first acquire the C/A code. In the aforementioned GPS IIIC satellites, the capability exists to use M-code in conjunction with the "spotbeam." In other words, a more sophisticated, encrypted code will be carried on a significantly stronger signal focused on a specific region on earth. Similar to increasing the frequencies, this final approach within the space segment requires correlating changes to the receivers within the user segment.

Having reviewed the technical approaches of countering GPS interference at the source of the signal, the space segment, the logical next step is to examine what can be done on the receiving end, the user segment of GPS.

**User Segment Improvements**

One commonality among the existing threats reviewed earlier was that they were based on earth and intentionally or unintentionally interfered with the GPS receivers and antennas. A technical approach would, therefore, need to find a way to ignore the interference and focus on the signal, or at the very least, detect the interference and notify the user. Within the user segment there are two techniques for mitigating interference: antenna-based and receiver-based.

Antennas serve as the entry point of the GPS signal or unwanted interference into a GPS receiver. There are four anti-jamming techniques with respect to antennas: antenna switching, adaptive array processing, polarization nulling, and beamforming. Antenna switching uses multiple antennas, and in the presence of jamming the receiver relies more heavily on antennas with higher signal-to-jammer power ratios. This technique is not as effective as others and has to have enough space on the platform for the multiple antennas. Adaptive array processing is similar to antenna switching except that it uses elements of antennas instead of full antennas,
thus decreasing the required space. The adaptive arrays allow for improved nulling, or canceling out, of the jamming signal. The effectiveness of this technique and the cost of the antenna correspond directly with the number of antenna elements. An example of this type of antenna is the GAJT™ (for GPS anti-jam technology; pronounced "gadget"). It became available in 2011 and is designed to replace older GPS antennas on military vehicles. Figure 3 depicts a GAJT™.

The third antenna-based technique is that of polarization nulling. This antenna has the ability to sense and attenuate a jamming signal analogous to attenuating ultraviolet rays with sunglasses. The final antenna-based technique is based on beamforming, or beam-steering, technology. These antennas turn toward a legitimate signal and away from a jamming signal. These four types of antennas provide approaches for mitigating GPS interference before the receiver calculates the PNT data.
After the GPS signals transition through the antenna of a GPS device and enter the receiver a final opportunity remains to mitigate interference. Three receiver-based approaches include the use of anti-jam filters, all-in-view receivers, and Chip Scale Atomic Clocks. A receiver with an anti-jam filter first detects and then eliminates the noise associated with the jamming signal. The receiver detects the jamming signal by measuring the base-line noise of the signals it is receiving. A signal with a relatively significant noise increase corresponds to jamming. The receiver can then entirely eliminate signals from that direction or use software to filter out the jamming signal. An "all-in-view" receiver can also mitigate jamming. Standard receivers track one or two satellites in addition to the four satellites required to calculate the four variables of time and a three-dimensional position. An "all-in-view" receiver tracks all satellites in view resulting in a more accurate PNT calculation. Finally, as technology associated with a Chip Scale Atomic Clock progresses, adding such a device to a receiver eliminates the need to calculate one of the four PNT variables. A receiver with accurate time from an atomic clock can determine accurate positions of the GPS satellites. By comparing that information with the calculations based on the GPS signals, the receiver becomes highly resistant to interference - both jamming and spoofing. In a jamming environment, maintaining accurate time allows for the synchronization needed to encrypt communication and transmit data. Accurate time from an atomic clock means that a GPS receiver can still provide an accurate two-dimensional position if even two signals are being successfully jammed. A GPS system with accurate time can also identify an unsophisticated spoofing signal.

**Alternative Means**

Having presented the two technical approaches of mitigating interference associated with GPS itself, we now turn to alternative means for receiving PNT information. One approach is to
identify an alternative that can work in coordination with GPS, such as an inertial navigation system (INS). Considering the other two technical approaches already presented and the speed of a platform using GPS, it is conceivable that GPS jamming or spoofing will not be a continuous phenomenon for that platform. If GPS jamming is successful at times and a platform can detect it, PNT requirements can be handed off to a redundant system, such as INS, allowing the platform to "coast" through the jammed area. INS is only accurate for a short duration; therefore, GPS-based PNT data will need to keep it updated until successful jamming occurs.\textsuperscript{30} As the advancement of microelectromechanical systems (MEMS) continues to progress, the potential to integrate GPS with INS into smaller platforms increases.\textsuperscript{31} The Iridium Satellite System could also enhance GPS as these satellites are closer to earth and have stronger signals. This would require modifications to Iridium satellites and GPS receivers.\textsuperscript{32}

Finally, there are technical alternatives that can completely replace the scope of GPS satellites. One approach is to use a local positioning system (LPS) where the signal producing devices are relatively near the location a military unit requires PNT data.\textsuperscript{33} This mitigates the signal attenuation associated with the distance of GPS satellites from the receivers. Though signal sources do not have to be airborne, one example of an LPS is the use of UAVs as pseudo-satellites over a military area of operation.\textsuperscript{34} On a larger scale, the use of a system such as enhanced Long Range Navigation (eLORAN) ground-based radio towers could be an alternative approach.\textsuperscript{35} Finally, another option in a jamming environment is the use of digital scene matching with some type of imaging sensor.\textsuperscript{36} Though not meant to be an exhaustive list, the aforementioned approaches serve as technical alternatives to GPS.
Non-technical Approaches

Now that we have reviewed the technical approaches to mitigating GPS interference, we turn to the non-technical approaches. For the purpose of this paper, non-technical approaches refer to the ones that are not related to the scientific aspect of GPS or aforementioned technical alternatives of obtaining PNT information. A passive approach accepts an environment of GPS interference and uses alternative, non-technical means of obtaining PNT information. An active approach uses non-technical means to counter the interference. This section of the paper explores both approaches.

Passive Approach

The passive approach requires the U.S. military to rely on other means besides GPS for PNT applications. This is obviously something it has been able to do since before the advent of GPS. However, the military's focus and reliance on GPS over the past few decades will require the rebalancing of techniques, tactics, and procedures (TTPs) related to PNT. This approach requires military units to be fully trained and equipped to perform their tasks through the use of traditional means that do not rely on GPS or other technical alternatives. This may mean a loss in the precision that GPS offers. However, there may be no other alternatives in an environment of GPS jamming.

In an environment with no GPS or other technical alternatives, ground troops will need to be capable of using maps, compasses, and terrain association to determine their position and to navigate. Pilots and sailors will need to be capable of dead reckoning and celestial navigation when other means are not available. Higher and adjacent headquarters will need to be prepared to develop a common operational picture through reporting, information sharing, and manually updating positions on maps. Pilots will also need to be able to drop bombs on targets using slant
range calculations. Laser guided munitions will serve as "smart bombs." These are just examples of the many TTPs one can use within this passive approach.

**Active Approach**

An active approach requires new tactical and potentially operational measures to counter GPS interference. The challenge is to find a method to counter GPS interference outside the technical approaches that focus on the system itself or related alternatives. One approach is to establish a framework that outlines the sequence of steps the U.S. military must take to address an adversary that is intentionally interfering with GPS. One such framework is (1) detect GPS interference, (2) locate the source of GPS interference, and (3) mitigate the threat.

Detecting GPS interference should be a relatively straightforward endeavor with the appropriate TTPs. An individual could determine GPS interference is occurring by emplacing a GPS device at a stationary, known location and monitor it. When the GPS device reports an incorrect location or fails to report a location this would be an indication of interference. At the tactical level, battalions, even companies, could assign small "GPS interference detection teams" with this "GPS monitor" task. Extrapolating this approach across the battlefield has operational implications. An operational-level headquarters that requires all subordinate units to use this approach and report their findings can obtain an operational view of the adversary GPS interference actions leading to appropriate counter-actions. Battle damage assessment data resulting from GPS guided bombs will supplement this data. A pattern of GPS guided bombs striking outside the acceptable GPS error region also serves as an indication of adversarial interference. Detection of GPS interference using TTPs like these will, at the very least, inform the military units that they will need to use alternate means in the affected areas until the "GPS interference detection teams" report otherwise.
The logical step after detecting GPS interference is to locate the source. This is obviously more challenging than just detection of GPS interference. One approach would be to use the operational view a headquarters has generated and study the patterns. A legitimate starting point would be the center of an area that is experiencing jamming. A higher density of interference reports will result in a narrower potential location of the source. Additionally, a crude, but more robust approach, than the basic set up of a "GPS interference detection team" could provide additional clues. Instead of monitoring one GPS device, a detection team could monitor a series of collocated GPS devices. One device serving as the baseline unit is placed in an appropriately sized hole shielding it from GPS interference. The remaining GPS devices are placed in a circle around the baseline unit shielded in a fashion that allows them to be jammed from only one general direction. If multiple "GPS interference detection teams" use this approach, then a higher headquarters could use their reports to determine the interference source location through triangulation.

The final step in this framework is mitigation. The commander will have to decide whether to isolate or destroy the source of GPS interference. One can use two approaches to isolate. One isolation approach would be to use means other than GPS for obtaining PNT data. The other isolation approach would be to tactically fix the jammer at its location and have units operate outside the affected area. Both isolation approaches come at a cost -- the former requires units to transition PNT techniques in the middle of an operation, while the latter requires time to displace and resources to fix the adversary (that is, "pin down" the adversary's jamming device). A commander's decision will obviously rely on his mission and available resources. The mitigation alternative to the isolation approach is to destroy the source of GPS interference. Since interfering with GPS requires emitting radiation, the use of an anti-radiation missile, such
as the High-speed Anti-Radiation Missile (HARM) is certainly an option for this scenario. Ultimately, whether the source of GPS interference is isolated or destroyed, a commander will have completed the "detect, locate, and mitigate" process against GPS interference.

Criteria and Assessment

With a foundation in GPS vulnerabilities, threats, and technical and non-technical approaches towards GPS interference, we can establish a framework of criteria to use in assessing potential solutions. Though there are many considerations, the three main criteria should include cost, effectiveness, and ease in implementation. The cost of implementing countermeasures should be the dominant criterion considering the fiscal constraints that have been imposed on the defense budget for the foreseeable future. Assessing the relative effectiveness of proposed countermeasures to GPS interference is an obvious consideration. Finally, the ease in implementation is a significant criterion as it combines important considerations such as simplicity and time to implement. With this framework of criteria as a backdrop, we will briefly review the potential solutions to GPS interference.

The costs associated with the technical approach are understandably higher than the costs of the non-technical approach. Costs associated with the improvements in the space section illustrate this. The costs of the original GPS Block II satellites, the updated Block IIR-M and IIF satellites, and the projected costs of Block III satellites are $30+ million, $60-80 million, and $100-150 million, respectively.\(^{37}\) Recall that most of the satellite improvements correspond to modifying or replacing receivers. Even if the focus was in improving the user segment, the costs associated with replacing or modifying the hundreds of thousands of receivers would be significant. Though the cost of upgrading the satellites and receivers would be a fraction of the
cost of the most recent Iraq or Afghanistan wars, the fiscally constrained environment the U.S. military is in makes the non-technical approaches more enticing.

It is a challenge to measure effectiveness without empirical data from tests of the technical and non-technical approaches. However, this paper illustrates how neither side is fully effective. The technical approaches illustrate the potential for a signal strength race between legitimate signals and jamming signals. Though more powerful jammers are easier to locate, one must use an integrated approach to locate and destroy them. Passive non-technical measures cannot offer the same precision as GPS offers on the battlefield. The active non-technical measures rely on crude techniques that require fallible humans to execute. A single approach does not appear to be overwhelmingly more effective than the others.

Finally, implementing the technical fixes to the GPS system would be easier than developing new TTPs or a doctrine associated with the non-technical approaches. If cost was not a factor, the U.S. military could improve satellites and provide users with new and improved GPS antennas and receivers that operate in the same way as previous versions. This would result in a seamless transition. On the other hand, assigning new tasks, such as "GPS interference detection teams," and requiring training of old or new TTPs for a military force that is downsizing poses significant implementation challenges.

**Conclusions and Recommendations**

The assessment of the criteria illustrates that no technical or non-technical approach alone offers a complete and ideal solution. However, as each approach is applied to a particular military capability preferences become apparent. For instance, in the case of precision guided munitions, combining GPS satellite signal improvement and the enhancement associated with
inertial navigation systems proves to be an effective approach that is worth the cost when
precision is required. Ground-based operations could effectively combine the technical approach
associated with LPS and the spectrum of non-technical approaches to operate successfully in an
environment with GPS interference. It is apparent that no approach alone is the panacea. The
United States military must integrate technical and non-technical approaches in order to ensure it
maintains GPS as a powerful warfighting capability.

Though GPS interference mitigation is the focus of this paper, this study additionally
establishes the bases for gaining "GPS superiority." The more the U.S. military learns about how
to defend against GPS interference, the better it will become in using it against an adversary. By
developing a U.S. military with a robust capability of GPS interference mitigation that fully
integrates technical and non-technical approaches, the U.S. military will possess an asymmetric
advantage over most adversaries. For an enemy that is overly reliant on GPS or a GPS-like
infrastructure, we jam the entire environment and rely on traditional means to fight and win. For
an enemy that is more reliant on traditional PNT means but may possess some jamming
capability, we exercise full offensive and defensive GPS measures and gain "GPS superiority" to
overwhelm and defeat him.

Further studies on military capabilities that rely on GPS, including experiments and
analysis on costs, effectiveness, and ease of implementation, are warranted. In particular,
examining the appropriate combination of approaches that should be integrated for each type of
military mission and capability is paramount. Though mitigating GPS interference may not
warrant a stand-alone doctrine, a serious development of the topic covering the issues in this
paper should be included in space and electronic warfare doctrine.
NOTES


8 Consolidated information from the following sources:

9 Ibid., 2-3.


11 Ibid.


15 Congressional Budget Office, 9.

16 Ibid., 11.

17 Ibid., 24.

18 Foxwell, 32.

21 Schechter, 2.
22 Defense Science Board Task Force, 55.
23 Scott, Part III, 6.
24 Consolidated information from the following sources:
25 Pengelley, 2.
26 Scott, Part III, 6.
27 Ibid.
28 Defense Science Board Task Force, 60.
29 Ibid., 37.
32 Congressional Budget Office, 25.
36 Schechter, 2.
37 Defense Science Board Task Force, 46.
BIBLIOGRAPHY


