# GPS Supplement

[Aff Side 2](#_Toc329590657)

[SQO fail – time and cost 3](#_Toc329590658)

[SQO fail – civilian fail 4](#_Toc329590659)

[Sqo fail – spoofing and jamming 5](#_Toc329590660)

[SQO fail – PPD’s 6](#_Toc329590661)

[A2:No risk of spoofing drones overseas 7](#_Toc329590662)

[A2: Topicality 9](#_Toc329590663)

[AT: DHS 11](#_Toc329590664)

[A2:Privacy 12](#_Toc329590665)

[A2:Ptx 13](#_Toc329590666)

[A2: Spending 16](#_Toc329590667)

[A2: Private CP 17](#_Toc329590668)

[A2: Military Solves 19](#_Toc329590669)

[A2: SQO solves satellites 20](#_Toc329590670)

[A2: DoD Solves 21](#_Toc329590671)

[A2: milt solves jamming 22](#_Toc329590672)

[A2: satellites solve 23](#_Toc329590673)

[A2: Foreign GPS Solves 24](#_Toc329590674)

[AT: XO 25](#_Toc329590675)

[NexGen Scenario 26](#_Toc329590676)

[Hegemony – GPS key – force multiplier 27](#_Toc329590677)

[NoKo – IL - Jamming 28](#_Toc329590678)

[Shipping – IL – Jamming 29](#_Toc329590679)

[Solvency – Time 30](#_Toc329590680)

[Solvency – interoperability/synchronization 31](#_Toc329590681)

[Solvency - Augmentation 32](#_Toc329590682)

[Solvency - Jamming 33](#_Toc329590683)

[Solvency – military 35](#_Toc329590684)

[Solvency – military jamming 36](#_Toc329590685)

[Solvency – Augmentation Solves 37](#_Toc329590686)

[Neg Side 38](#_Toc329590687)

[Spoofing NEG – Solvency t/o 39](#_Toc329590688)

[Privatization CP Solvency 41](#_Toc329590689)

[Privacy Turns 42](#_Toc329590690)

[Solvency – ground forces 46](#_Toc329590691)

[Solvency – unreliable 47](#_Toc329590692)

[solvency – civilian upgrades 48](#_Toc329590693)

[SQO solves - jamming 49](#_Toc329590694)

[Spending Link – 2 billion 51](#_Toc329590695)

[Neg – Spotbeams Turn 52](#_Toc329590696)

[Neg – Private Investment CP 54](#_Toc329590697)

[Neg – Topicality 56](#_Toc329590698)

[CP Solvency - XO 57](#_Toc329590699)

## Aff Side

### SQO fail – time and cost

#### **Current approaches take too long and are too costly**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

As the Department of Defense’s (DoD’s) Global Positioning System (GPS) satellites reach the end of their service lives, the department plans to replace them with ones that can counter deliberate interference by generating stronger signals. Analysis by the Congressional Budget Office (CBO) indicates that an alternative approach—namely, improving military receivers to retain the GPS signal even in the presence of such jamming— would be less expensive than DoD’s plan for upgrading its constellation of GPS satellites. Furthermore, the alternative would yield benefits almost a decade earlier than DoD’s plan. However, the improvements to military receivers could make them larger and heavier (and thereby less useful to personnel operating on foot) until they could incorporate the substantial gains that have been achieved in miniaturization in other applications.

#### Current DoD plans don’t solve until 2030

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

To maintain the constellation as existing and new satellites reach the end of their service lives, DoD plans to launch a total of 50 satellites through 2030 at an average rate of 2 to 3 satellites each year starting in 2012. The department has already purchased—but not yet launched—10 of those GPS satellites capable of transmitting M-code signals. DoD plans to acquire 40 more satellites— known as GPS III—that are capable of transmitting stronger M-code signals than existing satellites over the next 10 to 15 years. DoD plans to develop and purchase the new satellites in three phases. In the first phase, DoD plans to acquire 8 GPS IIIA satellites capable of emitting M-code signals that are three times stronger than those transmitted by current GPS satellites. The first IIIA satellite is scheduled to be launched in 2014. In the second phase, DoD plans to acquire 16 GPS IIIB satellites with M-code signals that are five times stronger than those of current satellites. For the final phase, the department’s plan calls for an initial purchase of 8 GPS IIIC satellites, which will be equipped with a special antenna capable of focusing the M-code signals in a “spotbeam”; however, CBO assumes that the department would need to purchase an additional 8 IIIC satellites in order to have enough IIIC satellites in orbit to take advantage of the IIIC’s advanced capabilities. Those satellites will transmit signals with the same strength as IIIB satellites and will be able to use the spotbeam to illuminate an area with a diameter of 600 miles on the Earth’s surface with signals 100 times stronger than those of current GPS satellites. In addition, IIIC satellites will be equipped with high-speed cross-links, which will allow continuous data updates. As a result, those satellites will be able to provide more accurate data to receivers, enabling a user’s location to be determined within 6 inches, instead of 10 feet (using current satellites) or 3 feet (using IIIA and IIIB models). After the 16th IIIC satellite is launched in 2030, the entire constellation should be composed of GPS III satellites, 16 of which will be IIICs (see Summary Table 1). Over the next 15 years, DoD also plans to develop software to control the M-code signals and the new GPS III satellites and to develop and purchase receivers that are capable of processing the M-code signals. Although 10 satellites capable of transmitting the harder-to-jam M-code signals are currently in orbit (the first one since 2005), no users have been able to benefit from them because DoD does not have the ability to monitor or control the signals, nor has it fielded receivers to process the signals. DoD plans to have a new control system fully in place by the end of 2016. To make the entire planned system functional, however, additional control capabilities, such as being able to update satellite data transmissions continuously when IIIC satellites enter the constellation and to control their spotbeam antenna, will need to be developed. Moreover, to make the planned system useful, M-code-capable receivers will need to be fielded as well. DoD’s current plan envisions fielding the first such receivers in 2017, but because the various armed services now field more than 400,000 GPS receivers, it may be 2030 before all units are fully equipped.

### SQO fail – civilian fail

#### Current upgrade programs only upgrade the satellites and not the receivers, and fails to improve civilian GPS capabilities

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Although the planned upgrades to GPS satellites will not increase the strength of civilian signals and will not improve the performance of civilian receivers in the presence of interference, other planned improvements will benefit both military and civilian users. In particular, GPS IIIA satellites will transmit signals that will enable both types of users to determine their position to within 3 feet, compared with the 10 feet that is possible with signals from current satellites. And once enough IIIC satellites enter the constellation, positioning within 6 inches will be possible for all users, according to DoD. CBO estimates that it will cost DoD roughly $22 billion from 2012 to 2025 to modernize the GPS. That total would include the cost from 2012 onward to develop and purchase the 40 GPS III satellites (including $3.6 billion for the additional 8 IIIC satellites), to develop the software and capability needed to control those satellites and their transmissions, and to develop and purchase hundreds of thousands of military receivers capable of receiving and interpreting the M-code signals. The Government Accountability Office and the Defense Science Board have reviewed DoD’s plan to modernize the GPS and raised several concerns, particularly regarding the plan’s focus on improving the satellites rather than the receivers and the plan’s lack of coordination in terms of the timing for various capabilities. CBO has developed options by which it explores those concerns.

### Sqo fail – spoofing and jamming

#### **GPS interference is on the rise and will only get worse – now is the key time to develop anti-jamming and anti-spoofing capabilities**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

The United States is now critically dependent on GPS. For example, cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System (NEXGEN) cannot function without it. Yet we find increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations. Most alarming, the very recent web availability of small GPS-Jammers suggests the problem will get worse. These so-called personal protection devices (PPDs) as well as other, readily available, more powerful devices can deliberately jam the Global Positioning System (GPS) signal over tens of square miles. They also can be devastating to the other, new foreign satellite navigation systems being deployed worldwide. PPDs are illegal to operate, but many versions are available (for as little as $30) from foreign manufacturers over the Internet. The simplest models plug in to a cigarette lighter and prevent all GPS reception within a line of sight range of 5 to 10 miles. Current penalty for operation is simply that the device is confiscated. We currently lack sufficient capabilities to locate and mitigate GPS jamming. It literally took months to locate such a device that was interfering with a new GPS based landing system being installed at Newark Airport, NJ. This paper provides background on satellite navigation and describes the impact of these dangerous PPDs and other disruptive radio frequency interference (Jamming). It also suggests needed action and discusses technical measures needed to harden GPS receivers against PPDs. The PNT Advisory Board believes that countermeasures and actions must be urgently developed. We strongly believe that the Executive Branch should formally declare GPS a “Critical Infrastructure. But that is clearly only the first action and is by no means sufficient. A multiple agency approach must be urgently developed and executed We must quickly develop and field systems that will rapidly locate, mitigate and shutdown the interference. In addition, laws are needed with the power to arrest and prosecute deliberate offenders. [This would be similar to legal action in response to the recent spate of laser attacks on pilots in flight]. Finally, we discuss the need for alternate navigation systems such as eLoran or a backup system currently being configured by the Federal Aviation Administration (FAA). While the foreign GPSequivalent systems may offer some help against accidental interference, web sites are already offering devices that will effectively shut down all satellite-based radio navigation signals. Note that all of these actions and jamming countermeasures tend to deter those who would deliberately interfere with the signals.

### **SQO fail – PPD’s**

#### **Personal jamming devices are on the rise and affect signals on multiple frequencies over many miles**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

In the past year, so-called personal privacy devices (PPDs) have become widely available on the Internet. A simple example of such products is shown in Figure 1. The most inexpensive PPDs are single antenna devices that jam the one GPS signal frequency (L1) that is used by most users. More expensive units have multiple antennas and attack all three GPS signal frequencies (L1, L2 and L5). As such, these attackers anticipate the next generation of GPS user equipment that would continue to function if only one or two of the three frequencies were jammed. Others PPDs jam cell phone frequencies at the same time, shutting down all calls. They are preferred by car thieves that wish to prevent an on-car warning systems to report the location of a stolen car to the authorities using a GPS receiver connected to a cell phone link. As shown in Figure 2 (Eldredge, 2010), PPDs range in price from $30 to over $300 based on the number of frequencies under attack and the transmitted power. Some radiate only a few milli-watts and other broadcast several watts. The former knock out GPS receivers for hundreds of yards, and the latter can have dangerous effects for many miles. As their name suggests, PPDs are marketed to individuals that fear for their privacy. This sales strategy seems to be effective. An investigation recently initiated by the FAA revealed that trucks traveling on the New Jersey Turnpike were carrying these devices. Perhaps, these drivers worry that the company dispatcher was monitoring their locations. Ironically, the attention of the dispatcher must be drawn to the truck that never provides location reports.

### A2:No risk of spoofing drones overseas

#### GPS vulnerability poses deep threats to national security but no action will be taken until disaster strikes

Franceschi-Bicchierai ‘12

[Lorenzo, *Wired*, July 6; <http://www.wired.com/dangerroom/2012/07/drone-hijacking/all/>]

The rogue takeover exploited a vulnerability in GPS to take control of the drone. It was, by Humphreys’ accounting, the first time somebody proved a civilian drone could be hijacked. Last year, when the CIA lost a drone in Iran, there were reports indicating the Iranians might have launched a spoofing attack and tricked it into landing, but we’ll never know for sure. Also, in September 2011, North Korea reportedly forced a U.S. spy plane to land with a jamming attack. With the planned integration of civilian drones in the American airspace, these problems might be coming to the U.S. The FAA must come up with new rules to allow for a freer use of drones in America by 2015 and, apart from worrying about possible collisions between manned and unmanned aircrafts, now the FAA might have to worry about people hijacking drones with spoofing devices. What’s worse, the experiment at White Sands shows that drone-jacking is “just the tip of the iceberg of a much bigger security issue we have in this country,” according to Logan Scott, a GPS industry consultant who has worked for defense giants like Lockheed Martin. In other words, it’s not only about drones, it’s GPS in general that is not safe. The Global Positioning System, commonly referred to as GPS, is a space-based satellite navigation system. It’s what allows you to get turn-by-turn directions to the mini-mart in your automobile. But most people don’t know that it also has countless other crucial applications. Among others, it’s the backbone of the global air traffic system. It is also used to control the power grid, to power banking operations (for instance, ATMs depend on it) and to keep oil platforms in position. And virtually all communications systems, like the world’s cellular networks, rely on it. “It’s a stealth utility,” says Scott, “meaning that we don’t necessarily know it’s even in the system until something is wrong.” GPS is also free, unauthenticated and unencrypted. Its open nature has been its biggest strength. Now, it could be its biggest flaw. “The core problem is that we’ve got a GPS infrastructure which is based on a security architecture out of the 1970s,” Scott tells Danger Room. “From a security point of view, if you look at GPS’s current status, is more or less equivalent to operating computers without firewalls, with no basic checks.” Since its signals comes from satellites at very high altitude, GPS relies on very weak signals that are extremely vulnerable not only to spoofing attacks but also to jamming – the deliberate or accidental transmission of radio signals that interfere with regular communications. This weakness has already been exposed in a few incidents in the past. In late 2009, GPS receivers at Newark Airport were going down intermittently every day and no one understood why. It took two months to track down the source of the interference: a driver had installed in his truck an illegal GPS jammer – which can easily be bought online for $50– so that his employer couldn’t track his every move. In 2001, a boat’s television antenna preamplifier took out GPS over the entire harbor town of Moss Landing, just south of San Francisco, for weeks. There is no reliable system to spot, let alone prevent, this kind of incidents. If you think of jamming incidents as fires, “what we have today is not quite as archaic, but think of the old forest ranger in the fire tower with his binoculars looking for smoke,” says Milton Clary, an aerospace policy analyst at Overlook Systems, a company that specializes in GPS services. “He sees a smoke column out across the horizon, but he knows nothing regarding the size or source of the fire, and all he can do is feed the information back to the headquarters.” To improve the situation, the Department of Homeland Security and Overlook have been working since 2009 on a program called Patriot Watch, a network of sensors that would be able to detect, characterize and locate interference sources. Unfortunately, according to Clary, the program is underfunded and, at this point, it’s nothing more than a PowerPoint presentation. The problem, says Clary, is that it probably would be too expensive to lay down a network of devices over the entire country. And there hasn’t been a huge-headline-generating incident to push the nation’s bureaucracies to make it a a priority. “We certainly don’t want a GPS Pearl Harbor, but probably it’s gonna take a GPS Mogadishu to get people’s attention,” he says. Meanwhile, other solutions have been proposed. For instance, Navsys is working for the Defense Advanced Research Projects Agency (DARPA) on an app that would make Android cellphones able to detect GPS jamming sources.

#### Factually incorrect: Multiple examples prove drones have been hacked

Mick ‘11

[Jason, *Daily Tech*; December 15; <http://www.dailytech.com/Iran+Yes+We+Hacked+the+USs+Drone+and+Heres+How+We+Did+It/article23533.htm>]

Iranian Gen. Moharam Gholizadeh, the deputy for electronic warfare at the air defense headquarters of the Islamic Revolutionary Guard Corps (IRGC), told the Far News, "We have a project on hand that is one [step](http://www.dailytech.com/Iran+Yes+We+Hacked+the+USs+Drone+and+Heres+How+We+Did+It/article23533.htm) ahead of jamming, meaning 'deception' of the aggressive systems... we can define our own desired information for it so the path of the missile would change to our desired destination...all the movements of these [enemy drones are being watched]" and "obstructing" their work was "always on our agenda." At the time the claims by Iran -- under pressure for its suspected nuclear weapons development program -- were largely dismissed as factless national rhetoric. Similarly, when Iranian state-run media revealed last week that it had captured a U.S. intelligence drone, many experts sneered at Iran's claims that it "hacked" the drone. [Remarked](http://www.defensenews.com/story.php?i=8517205&c=AIR&s=TOP) an analyst to the Defense News, "[it'd be] like dropping a Ferrari into an ox-cart technology culture." But while the detailed description of the "electronic ambush" from the interview with the Iranian engineer has not been verified by U.S. military officials, the U.S. gov't and public are now forced to set aside their prejudices and look at those claims far more seriously. According to the source, the first thing the Middle Eastern nation's "cyberwarfare experts" did was to jam the drone's signal. While the report does not specifically mention this, the engineer's claims of using past crashed drones to derive the attack indicate that Iranian experts may have used drones to determine the encrypted control frequencies that the drone was communicating on. Further evidence that adversaries in the region are on to U.S. UAV feed frequencies comes from the fact that in 2009 Iraqi Shiite militants [intercepted live, unencrypted video feeds](http://www.dailytech.com/Insurgents+Intercept+US+Military+UAV+Feeds+with+26+Software/article17168.htm) off a U.S. predator drone, using only off-the-shelf hardware. At the time, Iranian involvement was suspected.

Using its knowledge of the frequency, the engineer claims, Iran intiated its "electronic ambush" by jamming the bird's communications frequencies, forcing it into auto-pilot. States the source, "By putting noise [jamming] on the communications, you force the bird into autopilot. This is where the bird loses its brain." The team then use a technique known as "spoofing" -- sending a false signal for the purposes of obfuscation or other gain. In this case the signal in questions was the GPS feed, which the drone commonly acquires from several satellites. By spoofing the GPS feed, Iranian officials were able to convince it that it was in Afghanistan, close to its home base. At that point the drone's autopilot functionality kicked in and triggered the landing. But rather than landing at a U.S. military base, the drone victim instead found itself captured at an Iranian military landing zone.

#### A2 No risk of drones being compromised

#### The threat is real – downed drone in Iran proves

Christian Science Monitor ’11 [December 15]

[Iran](http://www.csmonitor.com/tags/topic/Iran) guided the [CIA](http://www.csmonitor.com/tags/topic/Central+Intelligence+Agency)'s "lost" stealth drone to an intact landing inside hostile territory by exploiting a navigational weakness long-known to the [US military](http://www.csmonitor.com/tags/topic/U.S.+Armed+Forces), according to an Iranian engineer now working on the captured drone's systems inside Iran. Iranian electronic warfare specialists were able to cut off communications links of the American bat-wing RQ-170 Sentinel, says the engineer, who works for one of many Iranian military and civilian teams currently trying to unravel the drone’s stealth and intelligence secrets, and who could not be named for his safety. Using knowledge gleaned from previous downed American drones and a technique proudly claimed by Iranian commanders in September, the Iranian specialists then reconfigured the drone's GPS coordinates to make it land in Iran at what the drone thought was its actual home base in Afghanistan. "The GPS navigation is the weakest point," the Iranian engineer told the Monitor, giving the most detailed description yet published of Iran's "electronic ambush" of the highly classified US drone. "By putting noise [jamming] on the communications, you force the bird into autopilot. This is where the bird loses its brain." The “spoofing” technique that the Iranians used – which took into account precise landing altitudes, as well as latitudinal and longitudinal data – made the drone “land on its own where we wanted it to, without having to crack the remote-control signals and communications” from the US control center, says the engineer. The revelations about Iran's apparent electronic prowess come as the US, [Israel](http://www.csmonitor.com/tags/topic/Israel), and some European nations appear to be engaged in an ever-widening covert war with Iran, which has seen assassinations of Iranian nuclear scientists, explosions at Iran's missile and industrial facilities, and the [Stuxnet](http://www.csmonitor.com/tags/topic/Stuxnet) computer virus that set back Iran’s nuclear program.

### A2: Topicality

#### **GPS a key element of the transportation infrastructure**

Pace, Director of the Space Policy Institute, 12

Scott, “Space Policy Challenges for the Next Administration,” Remarks to the Washington Space Business Roundtable, May 10, 2012, [www.wsbr.org/pdfs/05-10-12\_Pace.pdf](http://www.wsbr.org/pdfs/05-10-12_Pace.pdf)

Space activities today play critical roles in US national security, the global economy, and scientific achievement. The Global Positioning System (GPS) is an integral part of several critical infrastructures and enables functions ranging from survey and construction, to farming, finance, and air traffic management – not to mention supporting US military forces worldwide. Satellite communications are an integral part of the global information infrastructure and especially vital to developing countries. The International Space Station represents a unique and complex collaborative partnership between the United States, Europe, Canada, Japan, and Russia.

#### **GPS and PNT systems are a part of critical infrastructure**

DHS 8

Department of Homeland Security, UNITED STATES POSITIONING, NAVIGATION, AND TIMING INTERFERENCE DETECTION AND MITIGATION PLAN SUMMARY, April 2008, [www.gps.gov/news/2008/2008-04-idm-public-summary.pdf](http://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf)

On December 8, 2004, the President signed the U.S. Space-Based PNT Policy that superseded previous Global Positioning System (GPS) policy and established guidance and implementation actions for space-based PNT programs, augmentations, and activities for U.S. national and homeland security, civil, scientific, and commercial purposes. This new policy is the foundation of the responsibilities and actions necessary to achieve capability improvements and to effectively manage the GPS into the future. The policy stated that the U.S. must continue to improve and maintain the GPS, its augmentations, and back-up capabilities to meet growing national, homeland, and economic security requirements, and to meet commercial and scientific demands2. The formation of the DHS along with the governing Presidential Directives3 were the result of the U.S. Government’s need to prepare for, protect against, and recover from significant incidents within the U.S. that impact the critical infrastructure underpinning American society. PNT services have been widely recognized as an integral part of the technological foundation of civil and commercial worldwide infrastructure; and they have been recognized specifically as a critical component of numerous parts of the U.S. critical infrastructure. Through this recognition of the importance of PNT services, the question of system vulnerability to interference has been raised, with potential risk issues defined and quantified in completed analyses and studies. This heightened recognition is the impetus behind efforts to plan and prepare for incidents of interference to these systems, and provide guidance for the timely resolution and mitigation of interference events.

#### Authority for the plan is under the DoT – and, the development of ground based backup systems is explicitly transportation infrastructure.

DHS 8

Department of Homeland Security, UNITED STATES POSITIONING, NAVIGATION, AND TIMING INTERFERENCE DETECTION AND MITIGATION PLAN SUMMARY, April 2008, [www.gps.gov/news/2008/2008-04-idm-public-summary.pdf](http://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf)

Under the U.S. Space-Based PNT Policy, the Department of Transportation (DOT) was assigned the following responsibilities that are applicable to this Plan: • Have lead responsibility for the development of requirements for civil applications from all U.S. Government (USG) civil Departments and Agencies. • Ensure, in cooperation with the Secretary of Defense and the Secretary of Homeland Security, the performance monitoring of U.S. civil space-based PNT services. • In cooperation with other Departments and Agencies, promote the use of U.S. civil space-based PNT services and capabilities for transportation safety. • Represent the civil Departments and Agencies in the development, acquisition, management and operations of the GPS. • In coordination with the Secretary of Homeland Security, develop, acquire, operate and maintain backup PNT capabilities that can support critical transportation, homeland security, and other critical civil and commercial infrastructure applications within the U.S., in the event of a disruption of the GPS or other space-based PNT services, consistent with Homeland

#### **GPS is a critical transportation infrastructure – aviation, auto, maritime, and rail all depend on GPS for navigation**

Hoey and Benshoof, 5

Major David Hoey, 746th Test Squadron, USAF, and Paul Benshoof, 746th Test Squadron, USAF, “Civil GPS Systems and Potential Vulnerabilities,” [www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440372](http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA440372)

Our national infrastructure has become dependent on GPS in several ways, many of which typically go unnoticed. Figure 1 shows many of the broad categories of GPS usage. The obvious applications center on navigation, which includes aviation, automobile, maritime, and rail control. GPS provides enhanced position and navigation accuracy that enables efficiency and safety on a large scale, in addition to advanced services such as stolen vehicle recovery. First responders, such as search and rescue teams and paramedics, are among the most visible users of GPS accuracy for critical public services.

### AT: DHS

#### **The counterplan is not sufficient to solve the aff –**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

The United States is now critically dependent on GPS. For example, cell phone towers, power grid synchronization, new aircraft landing systems, and the future FAA Air Traffic Control System (NEXGEN) cannot function without it. Yet we find increasing incidents of deliberate or inadvertent interference that render GPS inoperable for critical infrastructure operations. Most alarming, the very recent web availability of small GPS-Jammers suggests the problem will get worse. These so-called personal protection devices (PPDs) as well as other, readily available, more powerful devices can deliberately jam the Global Positioning System (GPS) signal over tens of square miles. They also can be devastating to the other, new foreign satellite navigation systems being deployed worldwide. PPDs are illegal to operate, but many versions are available (for as little as $30) from foreign manufacturers over the Internet. The simplest models plug in to a cigarette lighter and prevent all GPS reception within a line of sight range of 5 to 10 miles. Current penalty for operation is simply that the device is confiscated. We currently lack sufficient capabilities to locate and mitigate GPS jamming. It literally took months to locate such a device that was interfering with a new GPS based landing system being installed at Newark Airport, NJ. This paper provides background on satellite navigation and describes the impact of these dangerous PPDs and other disruptive radio frequency interference (Jamming). It also suggests needed action and discusses technical measures needed to harden GPS receivers against PPDs. The PNT Advisory Board believes that countermeasures and actions must be urgently developed. We strongly believe that the Executive Branch should formally declare GPS a “Critical Infrastructure. But that is clearly only the first action and is by no means sufficient. A multiple agency approach must be urgently developed and executed We must quickly develop and field systems that will rapidly locate, mitigate and shutdown the interference. In addition, laws are needed with the power to arrest and prosecute deliberate offenders. [This would be similar to legal action in response to the recent spate of laser attacks on pilots in flight]. Finally, we discuss the need for alternate navigation systems such as eLoran or a backup system currently being configured by the Federal Aviation Administration (FAA). While the foreign GPS equivalent systems may offer some help against accidental interference, web sites are already offering devices that will effectively shut down all satellite-based radio navigation signals. Note that all of these actions and jamming countermeasures tend to deter those who would deliberately interfere with the signals.

#### DHS already did the counterplan

DHS 8

Department of Homeland Security, UNITED STATES POSITIONING, NAVIGATION, AND TIMING INTERFERENCE DETECTION AND MITIGATION PLAN SUMMARY, April 2008, [www.gps.gov/news/2008/2008-04-idm-public-summary.pdf](http://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf)

On December 8, 2004, the President signed the U.S. Space-Based PNT Policy that superseded previous Global Positioning System (GPS) policy and established guidance and implementation actions for space-based PNT programs, augmentations, and activities for U.S. national and homeland security, civil, scientific, and commercial purposes. This new policy is the foundation of the responsibilities and actions necessary to achieve capability improvements and to effectively manage the GPS into the future. The policy stated that the U.S. must continue to improve and maintain the GPS, its augmentations, and back-up capabilities to meet growing national, homeland, and economic security requirements, and to meet commercial and scientific demands2. The formation of the DHS along with the governing Presidential Directives3 were the result of the U.S. Government’s need to prepare for, protect against, and recover from significant incidents within the U.S. that impact the critical infrastructure underpinning American society. PNT services have been widely recognized as an integral part of the technological foundation of civil and commercial worldwide infrastructure; and they have been recognized specifically as a critical component of numerous parts of the U.S. critical infrastructure. Through this recognition of the importance of PNT services, the question of system vulnerability to interference has been raised, with potential risk issues defined and quantified in completed analyses and studies. This heightened recognition is the impetus behind efforts to plan and prepare for incidents of interference to these systems, and provide guidance for the timely resolution and mitigation of interference events.

### A2:Privacy

#### Plan only works within existing frameworks: Patriot Act gave the green light for electronic surveillance

Karim ‘04

[Wassim, Attorney, former associate editor of Washington University Journal of Law and Policy; *Washington University Journal of Law and Policy*, Vol. 14; p. 505]

Legislation pertaining to electronic surveillance has been modified repeatedly over the years,133 the most recent development of which has been the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or the USA PATRIOT Act.134 Generally, this legislation broadens federal law enforcement’s authority to use surveillance and eliminates barriers in retrieving intelligence information.135 In particular, by lowering the standard of proof and reducing judicial oversight, the Act broadens the FBI’s ability to obtain the information that a business maintains about an individual when the FBI is conducting an intelligence investigation.136 Furthermore, the Act broadens the government’s ability to conduct searches in secret.137

#### **Plan impacts outweigh privacy considerations**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Newark Airport. In any event, a PPD can cause collateral damage much greater than any privacy protection the user may possible enjoy. The above-mentioned FAA investigation was sparked while the FAA was installing a new GPS-based landing system for aircraft at Newark International Airport. This new system uses GPS receivers on the ground to aid GPS receivers in the approaching aircraft. This technique allows the use of all runways during restricted visibility conditions. The antennas for the FAA’s ground receivers are shown in Figure 3 (Eldredge, 2010), which also shows the proximity to the New Jersey Turnpike. During system test, the FAA noticed that the GPS ground receivers suffered one or two breaks in reception on many days. PDDs were identified as the cause of the continuity breaks after an investigation that lasted several months. If PPDs gain notoriety, they could gain the interest of hackers. These people may not be particularly worried about their location privacy, but may simply enjoy the notion of jamming GPS over wide areas.

### A2:Ptx

#### Plan is popular – Bipartisan support for securing GPS signals

Nelson ‘12

[Ben, U.S. Senator (NE),*Congressional Documents and Publications*, February 21]

Keeping GPS Free of Interference

Any interference to GPS could have a far-reaching and detrimental impact across our state and nation. As high-powered communication networks continue expanding, the government must make sure GPS isn't disrupted or degraded because it's an essential utility to millions of Americans.

It's technical and it's complicated but it's extremely important that we protect the nation's GPS network that the vast majority of Nebraskans and people nationwide have come to rely on.

Bipartisan Effort to Protect GPS

Last summer Senator Pat Roberts and I sent a letter, co-signed by 31 other senators from both parties, to the chairman of the FCC, asking that all assurances be made that a waiver granted to LightSquared, a satellite broadband company that was looking to enhance its mobile network, would not cause harmful interference to GPS receivers and users.

Because of concerns raised by the National Telecommunications and Information Administration after multiple tests were conducted that showed significant interference caused by LightSquared's signals on GPS equipment operability, the FCC gave us a gift on Valentine's Day when it revoked the company's application for a conditional waiver to begin operations.

Chalk One Up for Us

Providing additional broadband capabilities is a commendable goal; it just shouldn't be done by interfering with other established systems like GPS that so many people now rely on in their daily lives. My hat is off to the FCC for listening to our concerns and protecting GPS users.

#### Plan is popular - Long history of strong bipartisan support for GPS programs

Russo ‘11

[Anthony, NOAA National Coordination Office, Space-Based Positioning, Navigation & Training; Congressional Testimony before the House Committee on Armed Services; September 15]

The global positioning system has grown into a worldwide utility whose multi-use services are integral to our national and homeland security. Services dependent on GPS information are now an engine for economic growth and improve both the safety and the quality of life. The system is essential to first responders and a key component to multiple critical infrastructure sectors.

Since 1983, the United States has had a multi-use policy in place for GPS. This policy has had strong bipartisan support and each successive administration has strengthened the interagency participation in the program. In 2004, President Bush issued a policy establishing a deputy secretary-level Executive Committee or EXCOM to advise and coordinate on GPS issues.

#### GPS monitoring of terrorist suspects would be extremely popular

Gershman ‘10

[Bennett L., Professor of Law @ Pace University, *Pace Law Review*, Vol. 30, No. 3; p.939-940]

In discussing whether Knotts should be the controlling doctrine on whether the use of a GPS device involves a constitutional search, the majority observed that the use of GPS “forces the issue.”88 Notwithstanding that round-the-clock GPS surveillance may be extremely popular and have many useful applications,89 as the majority acknowledged, this widespread use should not be taken as a “massive, undifferentiated concession of personal privacy to agents of the state.”90 Where there has been no voluntary utilization of this tracking technology, and when the GPS is surreptitiously installed by the police, there “exists no basis to find an expectation of privacy so diminished as to render constitutional concerns de minimis.”91 Moreover, the majority observed, the Supreme Court in Knotts acknowledged that the Fourth Amendment issue would be more directly presented if “twentyfour hour surveillance of any citizen of this country [were] possible, without judicial knowledge or supervision.”92

#### Plan would have bipartisan support & strong lobbying efforts

Congressional Documents & Publications, 5/20/11

[Sen. Roberts](http://www.lexisnexis.com.www2.lib.ku.edu:2048/lnacui2api/search/XMLCrossLinkSearch.do?bct=A&risb=21_T15078235447&returnToId=20_T15078281956&csi=247474&A=0.868264131738696&sourceCSI=9369&indexTerm=%23PE0009XOR%23&searchTerm=Sen.%20Roberts%20&indexType=P) and [Sen. Nelson](http://www.lexisnexis.com.www2.lib.ku.edu:2048/lnacui2api/search/XMLCrossLinkSearch.do?bct=A&risb=21_T15078235447&returnToId=20_T15078281956&csi=247474&A=0.868264131738696&sourceCSI=9369&indexTerm=%23PE0009XOR%23&searchTerm=Sen.%20Nelson%20&indexType=P) led the bipartisan letter, co-signed by Sen. Chuck Grassley (R-Iowa), Sen. Tom Harkin (D-Iowa), Sen. Jerry Moran (R-Kan.), Sen. Debbie Stabenow (D-Mich.), Sen. Jim Inhofe (R-Okla.), Sen. Tim Johnson (D-S.D.), Sen. Saxby Chambliss (R-Ga.), Sen. Jeanne Shaheen (D-N.H.), Sen. John Hoeven (R-N.D.), Sen. Kent Conrad (D-N.D.), Sen. Richard Lugar (R-Ind.), Sen. Patrick Leahy (D-Vt.), Sen. Rob Portman (R-Ohio), Sen. Claire McCaskill (D-Mo.), Sen. Orrin Hatch (R-Utah), Sen. Mike Enzi (R-Wyo.), Sen. Johnny Isakson R-Ga.), Sen. Scott Brown (R-Mass.), Sen. John Barrasso (R-Wyo.), Sen. Roy Blunt (R-Mo.), Sen. Ron Johnson (R-Wis.),Sen. John Boozman (R-Ark.), Sen. Kelly Ayotte (R-N.H.), Sen. Mike Crapo (R-Idaho), Sen. Jim Risch (R-Idaho), Sen. Lindsey Graham (R-S.C.), Sen. David Vitter (R-La.), Sen. Tom Coburn (R-Okla.), Sen. Richard Burr (R-N.C.), Sen. Mike Lee (R-Utah), and Sen. John Thune (R-S.D.). The letter asks that the full Commission be involved in the process of making sure GPS is not compromised in any way, that the FCC require an objective demonstration of non-interference with GPS, and that the waiver for LightSquared be withdrawn until this demonstration is met. Full text of the letter is below: We write to express concern regarding a recent order by the International Bureau granting LightSquared Subsidiary LLC ("LightSquared") a waiver of the "integrated service" rule with regard to its Mobile Satellite Service license in the L-Band. We urge the full Commission to give appropriate attention to this matter. Numerous parties have raised significant concerns about interference from the LightSquared system into the Global Positioning System (GPS) frequencies. These parties included the GPS industry, aviation, agriculture, construction, cellular telecommunications companies and government entities such as the National Telecommunications and Information Administration (NTIA), the Department of Defense, the Department of Transportation, and the Department of Homeland Security. We have substantial concerns that LightSquared's proposal places an unacceptable risk to public safety through interference with GPS receivers necessary for aviation, first responders, agriculture, construction, maritime navigation, E-911, and national defense systems. GPS is integral to the functioning of our economy, and is essential for public safety. To ensure full protection that GPS service is not compromised in any way, we request the full Commission require LightSquared to demonstrate non-interference of GPS as a condition prior to any operation of its proposed service, and we request the Commission rescind LightSquared's waiver until this demonstration can be made. We recognize the Commission's unique obligation to the public, and its commitment to ensure appropriate use of the nation's airwaves. We urge the Commission, therefore, to ensure the uninterrupted operation of our nation's critical GPS system.

#### GPS highly vulnerable to jamming and spoofing – threatens military primacy

Thomas ‘11

[Dr., Lt. Col Michael; Systems Engineer at the Naval Space and Warfare Center; *Geospatial Intelligence Forum*, Vol. 9, No. 5; July/August]

While natural phenomena such as solar flares can interfere with a GPS signal, we need to understand that GPS signals are very weak and are therefore subject to interference. As one expert has noted, “The strength of a GPS signal is about as strong as viewing a 25 watt light bulb from a satellite 10,000 miles away. It’s no surprise then that GPS signals are vulnerable to natural and, increasingly, criminal interruptions.” GPS jammers are available for sale on the Internet for as little as $49. The capabilities of these devices seem limited to a 10-15 meter range, however, and would not seem to be much of a threat to a force whose aircraft can drop GPS-guided ordnance that will leave a crater twice this size. However, tests conducted in the United Kingdom have demonstrated the ability to jam a GPS signal for a radius as large as 30 km and detected a way of spoofing the signal to provide erroneous position and velocity information. This technology jams the L1/L2 and L5 frequency bands, on which GPS currently broadcasts or is projected to do so in the future. The 30 km potential jamming radius combined with the ability to jam multiband frequencies shows that the threat of losing required combat capability is very real. Accidental jamming also takes place, as was demonstrated by an incident in December 2001. While preparing for an upcoming systems test, engineers accidentally left on a frequency jammer in Mesa, Ariz., hampering GPS usage as far as 180 nautical miles away. The L1 frequency band jammer was radiating at a power of only 0.8 milliwatts and operated continuously for four and a half days. The impact on air traffic control operations was immediate. The jammer disrupted GPS signals as far as 45 nautical miles away. Air traffic control issued an advisory to pilots on the second day after numerous pilots reported loss of GPS navigation and other people reported inoperable handheld GPS receivers. Worse yet, experts indicate the possibility of spoofing the system by manipulating a weapon’s GPS guidance while it is in flight to a target. “The average person doesn’t realize how much infrastructure is based on GPS and how vulnerable it is,” noted Brent Ledvina, who helped build a GPS spoofer to reveal system weaknesses. The spoofing signal “looks exactly like a real GPS signal. Everything looks completely normal, but the spoofer is controlling your position in time and space.” Because many of our current adversaries are not very capable of using GPS for military operations, U.S. forces possess unprecedented opportunities to shape and control the battlespace to achieve national objectives. However, as our adversaries become more capable, these unique abilities may erode and enemies may target them. Most U.S. kinetic weapons are fully integrated into networks designed to conduct network-centric operations (NCO), and the rest are scheduled for replacement or upgrades to enable such employment. Recent efforts by the North Korean government to jam the GPS signal on the Korean peninsula, as well as the potential interference posed by proposed commercial 4G broadband networks, only reiterate the vulnerability of the current signal.

### A2: Spending

#### **Plan saves 2 billion dollars from DoD plans over the next six years**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Option 1 would improve the ability of military GPS receivers to provide accurate location data in a jamming environment by employing two techniques that, when combined, could reduce the effective range of noise jammers by 97 percent.6 Because the techniques have already been researched and developed, it should be possible to field large numbers of improved receivers by 2018, significantly sooner than any improved systems acquired under DoD’s plan could be fielded. Furthermore, the overall cost to carry out this option would be slightly more than $2 billion less than the total cost through 2025 to implement DoD’s plan.

### A2: Private CP

#### The private investment counterplan has already been tried with GPS technologies, only federal funding kept private gps satellites from failing – federal involvement key to solve

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

An additional drawback of Option 2 is that operation of iGPS requires the use of two separate satellite systems, GPS and Iridium, the latter of which is not owned by the U.S. government. Even though the Iridium satellite network has been operating for more than a decade and the next generation of satellites is scheduled to begin operating in 2017, the company’s continued operation is not guaranteed. The company that launched the original Iridium constellation, Iridium LLC, went public in 1997 but declared bankruptcy two years later. As a result of the bankruptcy, there was discussion of destroying the Iridium satellite constellation by de-orbiting it. In 2001, the company was acquired from bankruptcy, and that entity formed the foundation of the present Iridium Communications Inc. Shortly after Iridium emerged from bankruptcy, DoD announced a two-year $72 million contract for satellite phone service from Iridium (worth roughly $90 million in 2012 dollars), which at the time amounted to 40 percent of the cost to operate the Iridium network. At present, Iridium Communications Inc., with its core business of satellite phone communication, is profitable, and it has announced secured funding for its Iridium NEXT satellite constellation. If, however, Iridium runs into financial difficulty and stops operating its satellite network or is bought by a hostile party that could deny service to the U.S. government, iGPS would no longer function. Although DoD could avoid that situation by providing more financial support or buying out Iridium, doing so would increase the costs associated with this option.

#### Perm solves

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The third option would combine the improvements included in the two previous options. The resulting increase in the ability of GPS receivers to operate in a jamming environment would be significant, exceeding that recommended by the Defense Science Board in 2005 and reducing the effective range of enemy jammers by more than 99.9 percent.24 CBO estimates that this option would cost about $1.3 billion less than DoD’s plan. It would have the same disadvantages as Option 1 and Option 2, however, including additional weight and greater power requirements for receivers, the loss of the stronger and more accurate military signals transmitted by the canceled IIIB and IIIC satellites, and reliance on the commercial Iridium satellite system. Description, Schedule, and Cost Option 3 would make the improvements to the GPS included in both Option 1 and Option 2. Specifically, it would acquire and integrate improved antennas and inertial navigation systems into military GPS receivers, and it would augment the current GPS receivers with information provided through the Iridium satellite network. This option would acquire sufficient hardware to ensure that all military GPS receivers from all services were integrated with improved antennas that could filter out jamming signals and with INSs to compensate for errors introduced by jammers. In addition, this option would fully integrate the Iridium satellite system with the GPS so that it could, when called upon, provide GPS users with additional data that would improve the performance of appropriately modified receivers in difficult environments. To take advantage of the information transmitted by the Iridium satellites, this option would upgrade slightly more than 200,000 Army DAGRs so that they could receive and process the iGPS data; the remaining DAGRs would still benefit from improved antennas and inertial navigation systems. The schedule for acquiring and fielding the hardware needed to carry out this option is the same as that outlined in each of the previous options. If purchases of improved antennas and inertial navigation systems began in 2013, then half of the services’ receivers would be upgraded by 2018. Similarly, if upgrades to Army DAGRs to enable them to receive data from the Iridium satellites began in 2014, then roughly 100,000 units could be using iGPS data by 2018. The total cost for those improvements would be $3.0 billion from 2012 through 2025, CBO estimates, with almost all of the cost realized between 2012 and 2021 (see Table 3-2).25

#### Perm solves Jamming best

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The combined effects of the various improvements and augmentations made to the Global Positioning System under Option 3 would greatly enhance the system’s ability to perform in the presence of jammers. Excluding the contributions from M-code-capable receivers and stronger signals from IIIA satellites, the enhancements in this option—improved antennas, integrated INSs, and augmentation with iGPS—would reduce the effective range of enemy jammers by 99.8 percent.26 The effective range of a 10-watt jammer would decrease from 55 miles with current DAGRs to slightly less than 0.1 mile. And because the hardware needed to make the improvements has already been developed, many receivers with enhanced performance could be in the field by 2018 (see Figure 3-1). Additional improvements in capability would be realized as IIIA satellites and M-code-capable receivers were fielded. All told, the effective range of enemy jammers could be reduced by 99.96 percent, exceeding the DSB’s recommendations for improvement. 27 Ultimately, by 2026, when 28 IIIA satellites could be in orbit and large numbers of M-code-capable receivers fielded, the effective range of a jammer that today could cause a DAGR to lose track of a signal at 55 miles would be reduced to roughly 130 feet.

#### Perm is most net beneficial of all the options to upgrade

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Of the three options that CBO considered, this one would yield the greatest improvement in GPS performance and do so at a lower cost than DoD’s plan. Compared with DoD’s plan, savings under Option 3 would total $1.3 billion (or slightly less than 6 percent) from 2012 through 2025. The improvement in performance in a jamming environment would be substantial relative to today’s capabilities, reducing the effective range of jammers to roughly 130 feet. As a result, jammers would be only 1 percent as effective under this option as they would be under DoD’s plan (see Table 3-3 and Figure 31).28 (Improvements in accuracy would be roughly equivalent under both plans.) Another advantage of this option is that it would rely on several different methods to defeat an enemy’s jamming efforts. If one method should become unavailable—such as the signal from the Iridium satellites—then the antijamming capability provided by the upgraded GPS receivers would still yield improvements over today’s Global Positioning System and even that planned by DoD.

#### The DA’s to the perm link to the plan and counterplan just as much

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The disadvantages of adopting this option include those common to all of the options. Improvements to the receivers’ capabilities would require greater weight and power given current technology, which would make usage more difficult for personnel operating on foot. Although military suppliers are rapidly developing improved receivers that are much smaller and require less power than the DAGR, it may be several years before such miniaturized models are widely available. In addition, canceling the IIIB and IIIC satellites forfeits planned improvements in signal strength that would be particularly beneficial in situations where it was not feasible to increase the weight of and power available to the receivers. This option also shares with Option 2 the disadvantage of relying on the commercially owned Iridium satellite system. That reliance carries the risk that the service will not be there when needed or, alternatively, that DoD will have to bear most or all of the cost to support it.

### A2: Military Solves

#### The military has not developed receivers to decode M-signals – they cannot stop jamming in the SQO

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

One of the major upgrades that DoD made to the satellites was enabling them to transmit new signals— designated M-code—for military use only. Those signals cover a wider frequency range and are separated from the civilian signals in order to make jamming more difficult. (See Appendix A for a discussion of M-code signal structure.) Currently, 10 satellites in orbit have that capability (8 IIR-M and 2 IIF), slightly more than half of the 18 satellites that are needed to provide continuous worldwide coverage. DoD has purchased but not yet launched 10 additional IIF satellites with M-code capability; they are scheduled to be launched as existing satellites fail and need to be replaced. However, DoD has neither developed nor fielded any receivers capable of receiving and deciphering the M-code signals.

### A2: SQO solves satellites

#### New satellites wont be ready until 2030

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The Department of Defense plans to continue upgrading all three segments of the Global Positioning System, investing $7.3 billion from 2012 through 2016 and $15 billion over the subsequent nine years (see Table 2-1). When fielded, all of DoD’s fully modernized GPS components should improve the system’s ability to perform, even in a jamming environment. But fully implementing all of DoD’s plans could take until 2030. Description and Cost of DoD’s Plan During the next decade, DoD plans to purchase enough of the next-generation GPS III satellites to eventually replace the entire constellation and to upgrade the ground control system so that it can fully control existing and future satellites. DoD also plans to develop military receivers that can decode the new M-code signals and to purchase and field those receivers to all military users. Plans for Satellites The 2011 President’s Budget (submitted in February 2010) included a plan for modernizing the GPS. However, the Air Force later outlined a less ambitious modernization program in a September 2010 Cost Analysis Requirements Document (CARD). Moreover, at the same time that the CARD was being prepared and published, the Air Force was also investigating alternative programs for GPS III satellites. The results of that analysis, which was expected to be completed in September 2011, were not available prior to the publication of this study. DoD’s plans currently include launching the remaining 10 (out of 12 total) IIF satellites—the latest model of GPS II satellite—and deploying an entirely new generation of GPS III satellites. As of February 2011, the Air Force expected to launch the last IIF satellite (which was purchased in 2006) in 2014. The GPS III satellites, which are designed to have stronger military signals, are already under development, although the full rollout of that program will not be completed until 2030. According to Air Force plans, the GPS III satellite program will be carried out in three stages, with each stage yielding satellites of increasing capability.

### A2: DoD Solves

#### DoD upgrades would be insufficient

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

DoD’s planned improvements in the ability of GPS to operate in a jamming environment rely heavily on new military signals from space. Those include the M-code signals, the more powerful M-code signals that will be transmitted by IIIA and IIIB satellites, and the focused M-code signals from IIIC satellites. The increased resistance to jamming provided by those improvements, although significant, will not be available for 10 to 20 years. The antijamming improvements expected from the Mcode signals will not be realized until sufficient numbers of M-code-capable receivers are in the field—probably no earlier than 2026.18 At that time, the effectiveness of enemy jammers could be lessened significantly (see Figure 2-1). Similarly, although the first IIIA satellite is scheduled to be launched in 2014, 1 satellite alone will not provide sufficient coverage to make a difference to GPS users. A minimum of 18 satellites need to be in the constellation to guarantee that at least 3 will be visible at all times. Thus, it could be 2022 before enough satellites— 8 IIIA and 10 IIIB—are in the constellation to make it likely that strong signals from 3 satellites will be available at any given time (see Figure 2-1). And even then, only small numbers of M-code-capable receivers will have been fielded. Thus, the benefits of stronger signals from the GPS III satellites will be available only to a small number of users in 2022. Finally, GPS IIIC satellites promise a 100-fold improvement in the strength of M-code signals compared with signals from today’s satellites. However, the stronger signals will not be available worldwide until 16 IIIC satellites are in the constellation, which is not likely to occur before 2030. Even when all of the improvements included in DoD’s plan are in place, they might not be sufficient to counter the hostile environment that users might face. The Defense Science Board (DSB), in a 2005 report, recommended that antijamming improvements be made to achieve a GPS system that could withstand jamming levels that were 10,000 to 1 million times greater than current levels.19 DoD’s planned enhancements, combined, will improve performance in a jamming environment by at most a factor of 500, far short of the level of improvement recommended by the DSB.

### A2: milt solves jamming

#### **Military signals used to prevent jamming are not being utilized because receivers have not been upgraded yet**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

By the end of 2006, DoD had purchased several satellites with the improved capabilities that had been identified as critical, including 20 satellites capable of transmitting the new M-code signals. Only a limited amount of that capability had actually made it into the field by the end of 2011, however. The first IIR-M satellite was launched in September 2005, and the last of 8 was launched in August 2009. The first 2 IIF satellites were launched in May 2010 and July 2011, but only 1 was fully operational on October 1, 2011. Therefore, by the end of 2011, only 10 GPS satellites capable of transmitting the harder-to-jam M-code signal were in orbit, and only 8 were fully operational, far short of the 18 needed to provide continuous worldwide coverage.12 In addition, the upgrades to the ground control system needed to monitor and control the M-code signal were not complete by the end of 2011, and, according to DoD, will not be available for several more years. Finally, the other satellite enhancements needed to meet the new military goals— primarily the ability to transmit M-code signals at higher power—were deferred to be installed on a future model GPS satellite as part of the GPS III program. Some of the improvements to GPS receivers that DoD had viewed as necessary in its report to the Congress in 1999 have been made. In particular, more than 250,000 Defense Advanced GPS Receivers were purchased from 2000 through 2010, and funds for an additional 13,000 receivers have been requested. However, no receivers capable of receiving and deciphering the M-code signals have been fielded, even though several satellites are in orbit transmitting that signal.

#### DoD plans to upgrade receivers in the SQO - but they wont be ready until 2030

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

At the end of July 2011, the GPS constellation included 10 satellites capable of transmitting the new harder-tojam M-code signals. However, the services do not have any receivers capable of interpreting those signals. To fix that situation, DoD plans to invest $500 million from 2012 through 2016 to begin full-scale development of M-code-capable receivers in 2013 and to begin testing modules in various platforms in 2016. DoD has directed the GPS program office to develop a common module that would receive and process the M-code signals and that could be embedded in different models of receivers designed to meet the specific needs of each service.9 According to DoD, the Army could begin fielding the lead platform equipped with the modules—the Raven unmanned aerial vehicle—in 2017, and the first receivers specifically designed to be mounted in aircraft and ships sometime after 2019. Handheld receivers would be the last to be fielded, with production scheduled to begin in 2020. Because the various services now field more than 400,000 GPS receivers—three-quarters of which are the handheld variety—it could be 2030 before all U.S. military forces are fully equipped with receivers capable of interpreting the M-code signals.10 Total funding required from 2012 to 2025 to develop and purchase M-code-capable receivers would be $2 billion, CBO estimates (see Table 2-1). DoD has not publicly released estimates of the cost to develop the receivers after 2016 or the cost to purchase the receivers in sufficient numbers to replace those in the field. Because the Army fields more than 90 percent of the military’s receivers and because the Army’s requirements for replacement receivers are publicly available, CBO estimated the cost to replace the Army’s currently fielded receivers on the assumption that this would capture most of the cost.11 Assuming that half of those receivers would be replaced between 2017 and 2025 (with the remainder replaced thereafter), CBO estimates that the cost to the Army would be about $1.5 billion during that period.12

#### **Military signals can get jammed easily**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Jamming is accomplished by generating a signal with enough power to overwhelm a weaker signal, in much the same way that the headlights from an oncoming car make it difficult to see the light reflecting from the dividing line in the middle of the road at night. Although the military GPS signals are encrypted and are not easy to replicate, they can be masked by stronger signals of the appropriate frequency rather easily. As an example, a jammer broadcasting 1 watt of power at the appropriate frequencies could theoretically prevent a military receiver 40 miles away from locating and acquiring a GPS signal. Once the receiver has acquired and locked on to the military signal, the same 1-watt jammer would need to be within 18 miles to cause the receiver to lose track of the signal.9 Such a jammer could be as small as a 12-ounce soda can and easily be carried by an individual. (See Appendix B for pictures and diagrams of some typical jammers.) A larger, but still portable, 10-watt jammer could prevent the same receiver from acquiring a GPS signal at a distance of 125 miles and could cause the receiver to lose track of the signal at 55 miles. (For additional discussion of jamming, see Box 1-1.)

### A2: satellites solve

#### **Current plans for augmentation require multiple satellite launches and are not ready for deployment for at least 5 years**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Developing the new satellites, control systems, and receivers carries some risks.20 The risks are relatively small for the IIIA satellites, because their planned capabilities are not that much greater than those of the IIF satellites. And the IIIB satellites in DoD’s plan represent only a small increase in capability over the IIIA model. Providing the IIIC satellites with high-speed cross-links to communicate with other GPS satellites, in contrast, requires new antennas and other hardware whose development could carry greater risk. In addition, GPS IIIC satellites, which will be capable of focusing the signal on to specific regions on Earth, will need to be equipped with a dedicated large and steerable antenna and the hardware needed to direct the antenna and signal to the desired spot on Earth as a satellite passes overhead. Those significant increases in capability require the development of new technologies needed to produce satellites to the desired specifications, ensure that they operate correctly, and control them from the Earth. In the past, when the GPS program tried to increase the capability of its satellites significantly (as was the case with the upgrade from the IIR to the IIF model) or its ground control system (such as by adding the ability to manage the M-code signals), the program experienced increases in costs and delays in the planned delivery of improved capabilities. As currently structured, the GPS program could realize the same problems, especially for those portions that would develop and procure the IIIC satellites. CBO estimates that the investment needed to complete DoD’s planned modernization of the GPS satellites, control system, and user equipment will be slightly greater than $22 billion. (DoD has not published those costs.) Most of the costs would be attributed to the satellite portion of the program, with investment requirements equal to or exceeding $1 billion per year through 2025.

### A2: Foreign GPS Solves

#### **New foreign systems don’t solve intentional jamming – only receiver hardening solves**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

As described above, GPS receivers should certainly be made more robust against jamming. In addition, we feel that the nation should vigorously support efforts to provide Alternate Position, Navigation and Time (APNT). In this final section, we first describe the role of planned foreign satellite systems (GNSS) that are similar to GPS. Unfortunately they have the same susceptibility to interference as GPS. Next we describe two alternate techniques to determine PNT (APNT) that are more jam-resistant and could be readily made operational. GNSS. GPS is now recognized worldwide, and other nations are responding with satellite navigation systems of their own. The Russians are reinvigorating their satellite navigation system called GLONASS, and new systems are being developed in China, Europe, Japan and India. Taken together, GPS and these other systems are called Global Navigation Satellite Systems (GNSS). These other systems are valuable for improved accuracy and integrity. In addition they will offer frequency diversity. Therefore they will be helpful in countering unintentional interference at a single frequency. The new PFD (Jammers) being sold on the web will also prevent use of these foreign GPS-like systems as well as cell phones. Thus these new foreign systems will not be helpful in operating during deliberate jamming radiated by the better devices currently available.

### AT: XO

#### Highlighting the critical nature of GPS infrastructure solves the plan

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

There is not any practical way to completely eliminate GPS interference. But steps can be taken to greatly reduce the frequency and impacts of such interference. Further, actions can be taken to insure that GPS receivers do not give false indications of position or time. Our recommendations are:. 1. National Focus. GPS is absolutely critical US National Infrastructure. This has not been formally recognized. GPS should be formally declared critical infrastructure by Executive Branch and managed as such by DHS. This is necessary to elevate the importance of GPS to our critical infrastructure and bring the needed attention to the interference problem. The various existing national interference programs must be coordinated and gaps must be filled with additional funded efforts (see later recommendations). Senior leadership must recognize the vulnerabilities of the current critical infrastructure and give high priority to budgets and solutions.

### NexGen Scenario

#### **GPS key to NextGen Air Traffic Control systems**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Much of our infrastructure is critically dependent on Positioning and Time from GPS. Two such dependencies illustrate this. First, most telephone cell towers require GPS time to insure they are synchronized and cooperate. Recent instances of jamming in New York have rendered whole neighborhoods without cell service including Emergency Service Providers. A Second example is the use of GPS for Aircraft Approach to Landing Fields. These GPS based systems are being deployed and are particularly useful at airports where good alternatives are not available such as at Aspen, CO and Juneau, AK. There are now more FAA-sanctioned GPS approaches than the older beam-steering type. (Over 2000 GPS approaches). The value of these systems is enormous but the vulnerability is not universally appreciated: it took over a month to locate the deliberate small Jammer that was periodically driven by Newark airport. This example is particularly pertinent because the FAA’s NextGen Air Traffic Control System is critically dependent on GPS. Proliferated Jammers would cripple the new system which is expected to greatly reduce aircraft delays. Other Applications: GPS as a “Stealth” Utility. GPS has been aptly called the Stealth Utility. There are literally 100s of additional application examples. Some are safety-of-life (e.g. air and marine), some are startling productivity improvements (e.g. agriculture) and some are simply convenience or recreation (e.g. car navigation). It is now estimated that there are close to 1 Billion GPS receivers worldwide.

#### **SQO doesn’t solve NextGen for the FAA**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Today, the FAA uses an extensive network of terrestrial navigation aides to mitigate GPS outages. This backup navigation capability is based on ground-based navigation aids that precede GPS. All of these extant systems support point-to-point navigation. Even though these transmissions are reasonably robust against RFI, this point-to-point capability may not be suitable for the Next Generation Air Transportation System (NextGen). NextGen anticipates an increase in air operations by a factor of two or more by 2025, and will enable a host of operational improvements needed to smoothly support this traffic increase. NextGen is based on GPS, satellite-based augmentation systems (SBAS), and ground-based augmentation systems (GBAS). All of these systems provide so-called area navigation (RNAV). In other words, they provide guidance over a volume, and the alternate navigation system of 2025 also needs to provide a volumetric aid to navigation. Thus, the FAA is actively exploring alternate position, navigation time (APNT) as part of their NextGen effort, because the airspace should not revert to inefficient point-to-point navigation should RFI interrupt GPS-based operations in the 2025 timeframe. This APNT capability would be based on a reconfiguration of existing or planned FAA ground facilities (Eldredge, 2010), and Figure 8 shows part of the ground infrastructure that can be utilized to provide this APNT area navigation capability. Time Synchronization: As part of their APNT effort, the FAA has identified three architectures that may be suitable for alternate area navigation in 2025. These straw men are based on the sites shown in Figure 8, but two of these APNT architectures require time synchronization of neighboring ground sites. To this end, the FAA has investigated time transfer based on hardened GPS receivers and low earth orbiting satellites (LEOs). In the former case, jammers are attenuated by so-called controlled radiation pattern antennas. In the latter case, the needed processing gain derives from the proximity of the LEOs. Indeed, the altitude of the LEOs is approximately twenty times less than the GNSS altitude. Thus LEOs have small earth footprints and cannot provide the navigation performance associated with GNSS. However, the signal received from this nearby source is approximately 400 times greater than the power received from GNSS. Thus, LEOs could provide the robust time transfer capability needed to support APNT, because time transfer only requires one satellite to be in the common view of the ground stations to be synchronized. We encourage the FAA to continue efforts and to provide an APNT that is a robust backup to GPS and deterrent to malicious interference.

### Hegemony – GPS key – force multiplier

#### **GPS is a key force multiplier and preserves both situational awareness and command and control superiority on the battlefield**

Filler, et al 4

Dr. Raymond Filler Mr. Steven Ganop Mr. Paul Olson Dr. Stanley Sokolowski US Army Command and Control Directorate (C2D), “Positioning, Navigation and Timing: The Foundation of Command and Control” http://www.dodccrp.org/events/2004\_CCRTS/CD/papers/229.pdf

As stated previously, C2 systems rely on frequent and automatically updated digitized position reports. Reports that are based on inaccurate or unavailable information can have devastating effects. One incident that was described in the Washington Post (1) indicated that a forward air controller during Operation Enduring Freedom called for a Joint Direct Attack Munition (JDAM) on what they mistakenly reported to be a target but was actually their own location. Ultimately a dead battery and training was cited as the reason for this tragedy. The US Army Training and Doctrine Command (TRADOC) recognizes the importance of high quality positioning/navigation information as evidenced in the operational requirement documents (ORD) for the Future Combat System and the Land Warrior, and also in the TRADOC Pamphlet 525-66 on Force Operating Capabilities (FOC) (2). These requirements essentially describe a requirement for a very precise positioning system that operates in all environments and under all conditions. They further state these systems need to be fully interoperable with all Army Battle Command Systems (ABCS) that include Air Defense, Combat Service Support, Fire Support, Intelligence and Electronic Warfare, and Maneuver. These same documents acknowledge electronic threats to positioning systems and state a requirement to counter them. Recent lessons learned from Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF) have stated the need for affordable positioning equipment and have gone as far as to state that every soldier should be provided a system. A quote in an Inside the Army (3) article earlier this year stated that “…a majority of soldiers brought their own commercial GPS receivers”, and the article expressed the concern of the DOD due to the vulnerability of commercial GPS receivers. While less obvious in requirements documentation but arguably even more important is the accuracy and availability of synchronized time on the battlefield. Time is used in communications, sensor, and intelligence system is ubiquitous; it is used by virtually every unit on the battlefield, e.g. frequency hopping or cryptology. FM 100-14 defines Situational Awareness as “The ability to have accurate and real-time information on friendly, enemy, neutral, and noncombatant locations; a common, relevant picture of the battlefield scaled to specific level of interest and special need.” (4). When individuals report their positions, a collective picture is “drawn”. This is called the Common Operational Picture (COP). Friendly units and sensors further report enemy, neutral, and noncombatant locations by estimating them based on the known friendly locations (or by the use of laser ranging technology). These are converted into digital coordinates and “drawn” on the COP. Accurate and timely position information of these units is the key enabler to achieve these capabilities. Joint Pub 1-02 defines command and control as “The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission.” (5) The commanders that have better situational awareness will make the better decisions. Having accurate position locations of friendly forces through frequently updated position reports lifts much of the “fog of war”, and commanders are better able to issue directions to their units. All this draws the conclusion that Positioning, Navigation and Timing information is, without a doubt, the foundation of Command and Control (C2) or a force multiplier. The US has identified that GPS is a critical element of the nation’s transportation infrastructure. For the exact same reasons, GPS and the other positioning systems described in this paper need to be considered a critical element of battlefield’s infrastructure (6) and require a very high level of protection.

### **NoKo – IL - Jamming**

#### **North korea possesses Jamming technology and has shown the commitment to use it against south Korean targets**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Military – North Korean Incident. Malevolent RFI is known as jamming. Enemy Jammers were deployed in Iraq to interfere with US weapons systems during Operation Dessert Storm. Most recently, military analysts have expressed concern about recent GPS jammers tested by the North Koreans. (Telematics, 2010). On August 23 and 25 of this year, jamming signals emanating from the North Korean city of Kaesong. These attacks interfered with South Korean GPS military and civilian receivers on land and at sea. Officials say the jammers were repeatedly switched on for 10-minute periods over a number of hours during the three days. South Korea's defense minister, Kim Tae-young, voiced concern to members of the National Assembly. He correctly observed that the North Koreans can mount transmitters on vehicles that can jam GPS signals within a 50 to 100 kilometer radius. Professor Park Young-wook, with Kwangwoon University's Defense Industry Research Institute, states that such jamming must be considered a serious threat if it reoccurs because GPS is an integral part of the infrastructure, not only for the military but for many other industries. We certainly share the concerns voiced by Minister Tae-young and Professor Young-wook. However, we feel that the greater danger is posed by the propagation of GPS jamming technology to the wider public through devices sold on the Internet. These threats were described earlier

### **Shipping – IL – Jamming**

#### Jamming has devastating effects on maritime transportation and location awareness

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Maritime Controlled-Jamming Experiments. Until recently, GPS receivers for non-aviation purposes have not enjoyed the scrutiny or extensive testing used by the aviation community. Because of their 6/10 designs and clear line-of sight exposure, Maritime receivers can certainly be more vulnerable then aviation receivers. The following figures (Last, 2010) depict some disquieting results from recent trials conducted by the General Lighthouse Authorities (GLA) of the United Kingdom and Ireland. During these trials, a jammer was deployed in Flamborough, and the zone of impact is the wedge shown in Figure 4. As shown in Figure 5, this jammer had a devastating effect on the shipborne GPS receiver carried through the jamming zone. The receiver reports a faithful position track (in light blue) when the ship is far to the Northwest or far to the Southeast of the jamming wedge. Within the wedge, the receiver is overwhelmed and reports no position fix – the jammer breaks GPS continuity. GPS shows no solution. As the receiver approaches or has just departed the wedge, an extremely hazardous result occurs. The receiver suffers large position errors without an accompanying warning – integrity is broken. This is shown as the string of dots to the south and to the southeast of the actual blue track. These last results are most troubling, because the bridge personnel would not be warned that the navigation system was degraded. In another set of trials, the GLA placed a low power jammer on board the Trinity House Vessel Galatea. As shown in Figure 6, this jammer induced position reports that skipped across Scandinavia and Ireland while the ship sat steadfastly in the English Channel (the yellow track). Among the systems affected by the interference were the ship's radar and gyrocompass, key reversionary systems when GPS fails. The worrisome results shown in Figures 5 and 6 would not affect an aviation receiver, because aviation standards insist on an internal set of tests (algorithms) for RFI. We later recommend that these algorithms or equivalents become part of the standards for receivers used in any safety-of-life applications.

### Solvency – Time

#### **Plan solves faster than the SQO -**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Compared with DoD’s plan, the options would yield greater improvements in reception and would yield improvements sooner. Under DoD’s plan, the full benefit of the increased M-code signal power of the IIIC satellites would not be fully realized until 2030, when the 16th IIIC satellite could be in orbit. The earliest benefits would probably come once the constellation of 18 GPS III satellites—comprised of 8 IIIA and 10 IIIB satellites— is in orbit, scheduled for 2022, but only small numbers of military receivers capable of processing the stronger M-code signals would be in the field then. While the IIIC satellites were being placed in orbit, the benefit of their stronger signals would be unavailable to users until sufficient numbers of M-code-capable receivers were fielded, possibly no earlier than 2026. In contrast, the technologies included in CBO’s options—those for improved antennas for GPS receivers, small inertial navigation devices, and iGPS—have already been developed. The fielding of ancillary devices to augment existing military GPS receivers could begin in a few years, with appreciable numbers of improved receivers in the field by 2018. Consequently, the options could increase the military’s antijamming capability eight years before large numbers of M-code receivers could be in the hands of military users under DoD’s plan. Additional advantages of Options 2 and 3 come from augmenting the GPS constellation with the Iridium satellites in low-Earth orbit. That fuller coverage would virtually ensure that receivers had a line of sight to at least one satellite, even in mountainous terrain and urban settings where tall buildings block the view of the sky. In addition, because data can be received and updated frequently, receivers using iGPS can determine their position with almost the same accuracy as would be possible using data from IIIC satellites—but the receivers would have that ability several years earlier.

### Solvency – interoperability/synchronization

#### **Plan solves lack of synchronization between different segments of the GPS system**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Another concern that has been highlighted by the

Defense Science Board and the Government Accountability Office is the lack of synchronization among the three segments of the GPS program.21 For example, although 10 GPS satellites transmitting M-code signals were in orbit at the end of July 2011, DoD has not developed or fielded any receivers capable of processing those signals—and the initial fielding of the first common ground modules to demonstrate the capability to decode the signals is not scheduled until 2017. Because full production of the handheld receivers is not scheduled to begin until 2021, after one year of low-rate production, large numbers of M-code-capable receivers to replace the current DAGRs are not likely to be fielded before 2026. And even if some military receivers capable of processing the M-code signals could be fielded earlier, the ground control system would be incapable before the end of 2016 of ensuring that the satellites were transmitting the correct data on the M-code signal.22 Thus, although satellites with enhanced capabilities are being developed, purchased, and launched, no one will be able to take advantage of those improvements for at least five more years.

### Solvency - Augmentation

#### **Plan solves augmentation through the re-establishment of the eLoran navigation system that was advocated but never implemented**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

e-Loran: Loran is a ground-based radio-navigation system that preceded satellite navigation. It finds its origins in World War II, and enjoyed wide spread adoption after the grounding of the Argo Merchant on Georges Bank. At that time, the U.S. Coast Guard began to require Loran carriage by ships over a certain tonnage in the Coastal Confluence Zone of the United States. Importantly, Loran is based on the broadcast of extremely high power signals in the low frequency portion of the radio spectrum. The frequency of transmission is 10,000 lower than the GPS frequencies in the microwave band, and the power of the transmission is 1000 times greater than the GPS transmission power. An updated version of called eLoran has now been developed and tested. It is very robust, resistant to interference and has two dimensional accuracies of about 20 meters in critical areas. It is not nearly as accurate as the best GPS, and the lack of the vertical dimension reduces eLoran’s effectiveness, yet it is a very robust APNT system. In December 2006, an Independent Assessment Team was appointed, reporting to DOT and DHS. It was under the administration of the Institute for Defense Analysis (IDA). After careful review over many weeks, they unanimously recommended that the eLoran deployment be completed as a backup for GPS. Yearly cost to maintain this in the US was about 20 $M. This is about 1/10th the cost of a single GPS satellite. The DHS then made an announcement that eLoran was the official APNT system for the US. The Schlesinger-chaired PNT Advisory Board has also unanimously recommended that eLoran be deployed and maintained as a GPS backup. For these reasons, the international navigation community has also strongly supported the upgrade and sustainment of the Loran system in any number of forums. This recommendation has been heeded in Europe. Indeed, Figure 7 shows the faithful position track provided by enhanced Loran (e-Loran) as the ship traverses the jamming wedge generated by the General Lighthouse Authorities from Flamborough. Figure 7 provides a stark contrast to the GPS-based results in Figure 5. Unfortunately, DHS has not followed through with their announcement: the Loran system in the United States has been turned off. We strongly recommend that the previously announced decision (to deploy eLoran as the primary APNT) should be reconfirmed and quickly implemented. The reasons for this are clearly stated in the IDA white paper. It is the most viable and robust backup to GPS and can be implemented in a way that is virtually seamless to the user.

#### Only the aff solves – gps systems are vulnerable for at least the next 5 years in the SQO

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Although significant improvement would come from introducing receivers capable of processing M-code signals earlier than DoD’s plan allows, the Government Accountability Office has reported that accelerating the fielding of such receivers through the infusion of additional funds is not possible because of technical difficulties. 2 Several different approaches that could yield improved receivers in the next 5 to 10 years are possible, however. Approaches recommended by the DSB include equipping receivers with antennas that block jamming signals and integrating miniature inertial navigation systems into receivers to enhance their ability to process the GPS signal and to limit interference from jamming signals. Another path to improving the capabilities of GPS receivers that DoD has been pursuing for several years would use the Iridium commercial low-Earth orbiting satellite constellation to provide data to military receivers that would enhance their ability to process the GPS signal in the presence of jamming.

### Solvency - Jamming

#### **Plan solves jamming**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The ability of military receivers to process GPS signals could be improved in the next few years through antenna enhancements that limit the interference from jamming signals and through techniques that eliminate errors that are introduced during signal processing. This option would enhance receivers’ capabilities through a combination of those two techniques, each of which could reduce a jammer’s effective range by 82 percent.7 Improved antennas for GPS receivers use various types of filtering to limit the interference from a jamming signal. If the jamming signal is limited to a very narrow frequency range, spectral filters can prevent reception of the signal at those frequencies.8 If the jamming signal covers the military signal’s full range of frequencies, however, as is the case with commonly used wide-band noise jammers, that technique will not work. To counter wideband jamming signals, advanced antennas that limit input on the basis of the signal’s angle of arrival can filter out most of the jamming noise. Directional antennas block signals from ground-based jammers by receiving only those signals that come from satellites that are visible at least 10 degrees above the horizon. The Army has developed that type of antenna for installation on some of its weapon systems.9 More sophisticated directional antennas that are composed of a number of separate elements use a technique called nulling to prevent the receiver from being overwhelmed by jamming noise. If one of the elements detects a jamming signal, that element is turned off, leaving the rest of the antenna to function normally and receive the GPS signal without interference. Those types of antennas can block signals from jammers located at several different positions around the receiver. DoD has developed several versions of those antennas and installed them on some military aircraft and ships; newer and smaller versions could also be mounted on vehicles or carried in a backpack. (See Appendix B for some examples of such antennas.) The use of improved antennas such as those described here could prevent 97 percent of jamming noise from reaching the receiver and reduce a jammer’s effective range by 82 percent.10 Even though improved antennas can filter out most of the noise and associated errors introduced by jamming signals, they would not be able to prevent the introduction of all errors. Augmentations to receivers’ processing abilities and components could further improve their performance in hostile jamming environments. One improvement studied by DoD would couple a GPS receiver with an inertial navigation system, which can measure changes in location by accurately monitoring a user’s movements. Integrating information from the INS enhances a receiver’s ability to process the GPS signal and to filter out noise. Tightly integrating an INS with a GPS receiver could, by itself, also reduce the effective range of enemy jammers by 82 percent.11

#### **Plan solves jamming**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The ability of military receivers to operate in a jamming environment would be significantly improved within just few years by fielding the enhancements to receivers envisioned under Option 1. The combined increase in capability afforded by the two enhancements—compared with the capability available using the Army’s Defense Advanced GPS Receiver and the signal from a IIF satellite— would reduce the range at which an enemy jammer broadcasting a 10-watt signal could cause a DAGR to lose track of a GPS signal from 55 miles to about 2 miles (see Figure 3-1).13 And because the hardware associated with the proposed enhancements could be purchased and fielded quickly, CBO estimates that roughly half of the military’s receivers could be upgraded by 2018. Additional improvements in capability would follow when 18 IIIA satellites were put into orbit and when large numbers of M-code-capable receivers were fielded. Although 18 IIIA satellites transmitting a stronger M-code signal will be in the constellation by 2022, most of the GPS receivers in the field at that point, particularly handheld versions, would not be capable of processing the M-code signal. Only by 2026, CBO estimates, would roughly half of military users have M-code-capable receivers. At that point, the combined enhancements would reduce the effective range of a 10-watt jammer against updated receivers even further—to 0.4 miles (see Figure 3-1 and Table 3-3). Thus, when all the improvements introduced by this option have been fielded in sufficient number, the effective range of enemy jammers should be reduced by 99.3 percent, from 55 miles to 0.4 miles in the case of a 10-watt jammer.14

#### **Only the plan can solve identification and reduction of interference**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

National Alerting and Pinpointing Interference Locations. The NATIONAL EXECUTIVE COMMITTEE should establish and sponsor a National GPS Interference Locating , Reporting, and Elimination System ; coordinating and expanding on the resources of several Departments. It took several months to locate the PPD that shut down the Newark landing system. Technology exists to locate such sources much more quickly. To rapidly alert and pinpoint interference, two elements are required: 1. sensing of the interference and 2. a communications channel to report the problem in real-time. For example, every cell phone tower could be configured to expand the functionality of their GPS timing receiver by promptly recognizing and reporting interference, including pertinent characteristics. The incremental cost would be extremely small. Another example: many toll booths routinely videotape vehicles including license plates. A properly configured GPS receiver at the booth could identify vehicles that are broadcasting interference. There are many more national reference receivers that could be so configured. Cell phones that include GPS receivers can be configured to sense and automatically report suspected interference. This would constitute a near instantaneous reporting channel, worldwide. Of course a central data-gathering location is needed; it could be collocated with preexisting civil/military resources such as WAAS, NGPS or the Air Force’s 2SOPS. In turn, the located sources must be reported for appropriate action. No such National (or International) Real-Time System exists today or is even currently planned.

#### **Shielding and anti-jamming technologies must be integrated to strengthen GPS receivers**

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

Hardening GPS Receivers and Antennas. In addition to legal action, we wish to galvanize a technical effort to strengthen all GPS receivers. GPS receivers should never give the Hazardous and Misleading Information (HMI) that is shown in figure 6. The techniques to avoid this are well known and specified for all FAA certified equipment. All GPS safety-of life receivers should include the integrity algorithms specified by the FAA. There are also well-known design techniques to greatly reduce outages of GPS receivers due to interference. Examples include: special antennas that null interference, coasting thorough interference by using inertial components and/or small atomic clocks, as well as physical shielding in the direction of presumed jamming. Some would add significant cost but may be warranted for safety-of life and other critical applications. New supplementary devices can make GPS receivers more robust and are becoming more affordable. (e.g. miniature accelerometers, chip scale atomic clocks etc.) Some actions are being taken. For example, the FAA is already hardening the GPS receivers and antennas placed on the ground at Newark International Airport. Changes include: GPS antennas that are less vulnerable to radio frequency interference; improved practices for placement of GPS antennas on the airport (farther from public roadways); and receiver algorithms that more quickly recover when the PPD moves away from the GPS antenna. Manufacturers should speed up the offering of interference resistant GPS receivers, especially for safety-of-life applications such as commercial maritime. These receivers should use FAA techniques to insure they do not display Hazardous and Misleading Information during periods of interference.

### Solvency – military

#### Aff solves for military jamming problems through antenna upgrades – and for more complex military difficulties through augmentations to the processors

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The ability of military receivers to process GPS signals could be improved in the next few years through antenna enhancements that limit the interference from jamming signals and through techniques that eliminate errors that are introduced during signal processing. This option would enhance receivers’ capabilities through a combination of those two techniques, each of which could reduce a jammer’s effective range by 82 percent.7 Improved antennas for GPS receivers use various types of filtering to limit the interference from a jamming signal. If the jamming signal is limited to a very narrow frequency range, spectral filters can prevent reception of the signal at those frequencies.8 If the jamming signal covers the military signal’s full range of frequencies, however, as is the case with commonly used wide-band noise jammers, that technique will not work. To counter wideband jamming signals, advanced antennas that limit input on the basis of the signal’s angle of arrival can filter out most of the jamming noise. Directional antennas block signals from ground-based jammers by receiving only those signals that come from satellites that are visible at least 10 degrees above the horizon. The Army has developed that type of antenna for installation on some of its weapon systems.9 More sophisticated directional antennas that are composed of a number of separate elements use a technique called nulling to prevent the receiver from being overwhelmed by jamming noise. If one of the elements detects a jamming signal, that element is turned off, leaving the rest of the antenna to function normally and receive the GPS signal without interference. Those types of antennas can block signals from jammers located at several different positions around the receiver. DoD has developed several versions of those antennas and installed them on some military aircraft and ships; newer and smaller versions could also be mounted on vehicles or carried in a backpack. (See Appendix B for some examples of such antennas.) The use of improved antennas such as those described here could prevent 97 percent of jamming noise from reaching the receiver and reduce a jammer’s effective range by 82 percent.10 Even though improved antennas can filter out most of the noise and associated errors introduced by jamming signals, they would not be able to prevent the introduction of all errors. Augmentations to receivers’ processing abilities and components could further improve their performance in hostile jamming environments. One improvement studied by DoD would couple a GPS receiver with an inertial navigation system, which can measure changes in location by accurately monitoring a user’s movements. Integrating information from the INS enhances a receiver’s ability to process the GPS signal and to filter out noise. Tightly integrating an INS with a GPS receiver could, by itself, also reduce the effective range of enemy jammers by 82 percent.11

### Solvency – military jamming

#### **Augmentation solves jamming issues with current military receivers in the short term while tech upgrades will close the gap in the long term**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Option 1 would augment military receivers to provide users with a better ability to keep track of their location in jamming environments. The improvement would come from new antennas—capable of rejecting signals from jammers—and from the integration of very small inertial navigation systems, which would reduce location errors introduced by interference and enable users on the move to determine their position accurately even after losing the GPS signal entirely. By increasing the level of noise that receivers could tolerate and still be able to detect and process the GPS signal, those augmentations to receivers could reduce the effective range of a wideband noise jammer by 97 percent. (The effective range of a 10-watt jammer would be decreased from 55 miles to about 2 miles, which means that the jammer would need to be within 2 miles of the receiver to have an effect.) Because the hardware for the improvements in this option has already been developed, modifications to existing receivers could begin almost immediately, and a significant number of improved receivers could be in the field by 2018. The additional signal power from the IIIA satellites and the antijamming capabilities of M-code receivers would further enhance the overall capability of military receivers to operate in the presence of jamming. By 2026 (the point at which about half the force could be equipped with M-codecapable receivers), the combined improvements under this option would reduce the range of a 10-watt jammer by 99.3 percent, to 0.4 miles (see Summary Figure 1).

### Solvency – Augmentation Solves

#### Only a continuous investment in upgrades and augmentations can maintain the role of GPS as a critical force multiplier

Filler, et al 4

Dr. Raymond Filler Mr. Steven Ganop Mr. Paul Olson Dr. Stanley Sokolowski US Army Command and Control Directorate (C2D), “Positioning, Navigation and Timing: The Foundation of Command and Control” http://www.dodccrp.org/events/2004\_CCRTS/CD/papers/229.pdf

This paper has discussed the evolving role for systems that provide position and time information from a role of navigation aid for individual consumption to a much greater role of enhancing Situation Awareness for remote commanders. This enhanced Situational Awareness capability has been shown to directly improve Command and Control capability to the point that it is identified as a force multiplier. The success of this position and time information evolution into greater utility has spawned many new concepts for its use. The new concepts generally place greater demands on the reliability, accuracy and timeliness of the position location and time information than current systems can provide. The NAVSTAR GPS was identified as a national dual use asset, ubiquitous in both the civilian and military environments. It is interesting to note that the number of civilian GPS users far outnumber the military users with applications that span from the casual recreational user needs to paramilitary uses that impact real life or death situations. The Army, as the military’s largest user of GPS receivers, has integrated GPS as the central component in deriving position and time information on individual platforms that report this information to Command and Control Systems on the battlefield. Due to the utility, practicality and performance of the GPS it is recognized today as an essential component of any navigation subsystem and will remain the central component in the foreseeable future. As remarkable as GPS is to be applied in so many applications, limitations in complex military environments dictate continued work in developing technology that enhance and augment GPS capability in these environments. Additionally, size, weight, power (SWAP) and cost enhancements to expand the utility of military GPS use must be addressed in future work. This paper further discussed several technology efforts being managed at CERDEC in the Navigation, Position, and Timing Branch to address not only the limitations of the GPS (and augmented navigation systems in general) but also address the affordability and utility to a wider number of platforms such as the dismounted soldier. Currently today’s various combinations of Army missions, platforms and need for position location and timing accuracy requirements stress the limits of the available technology applied to various Army positioning applications. Clearly, at present there is no single navigation suite of systems that could possibly be the optimal fit for the various Army applications. The technologies identified for investigation were carefully selected to enhance the Army’s navigation capability operating in complex military environments as well as address the SWAP and cost of the technology. Solutions in these military complex environments certainly have application and capability to improve the overall navigation system when operated in less stressful environments as well. It is ironic that as the closer we get to satisfying today’s Army requirements in position location and timing, tomorrows evolution of new concepts for future operational capabilities continually drives the need for enhanced capability from the Army’s navigation systems while increasing the SWAP and cost constraints.

## Neg Side

### Spoofing NEG – Solvency t/o

#### Multiple causes of accuracy errors – plan can’t ensure solvency

Zubinaite & Preiss ‘11

[Vilma, Vilnius Gediminas Technical University (Lithuania); George, Gjovik University College (Norway); *Aviation*; Vol. 15, No. 2; p. 45]

Since the beginning of global satellite positioning, it has been a challenge to eliminate and correct the error sources that affect positioning accuracy. Scientists have found mathematical solutions to reduce these errors as much as possible. Some of the errors can be totally eliminated, while others can be corrected to a certain degree. Some of the errors, like ionospheric errors, are still being examined and modelled. The goal of this paper is to examine whether the errors in a satellite’s orbital location, due to high solar activity, can affect the accuracy of ground receivers and, if so, how these errors can be controlled. When a ground receiver determines its position, there are many possible sources of errors: ––Ionospheric and tropospheric delays – signal delays due to the signal passing through various layers of the atmosphere; ––Orbital errors (ephemeris errors) – errors caused due to satellites transmitting inaccurate orbit parameters; ––Signal multipath – these errors can occur when the signal is reflected off objects before reaching the receiver; ––Receiver clock errors – the receiver clock is not as accurate as the atomic clocks on the satellites, which can lead to timing errors; ––The number of visible satellite – accuracy is better if the receiver observes more satellites; ––Geometry of the satellites – relative position of the satellites in the sky affects the accuracy, best if the satellites are spread widely. Researchers have been trying to find out ways to eliminate these errors. Some of the methods used are: ––Differencing; ––Using more signal frequencies; ––Modelling ionospheric errors. The first sources of errors, ionospheric and tropospheric delays and orbit errors, are affected by levels of solar radiation activity. It is generally assumed that satellites’ orbit errors are eliminated by differencing, in other words by using two or more receivers simultaneously (Būga 1999).

#### Can’t solve spoofing – models predicting success are unrealistic & robustness is a liability, not an advantage

Wesson ‘12

[Kyle, PhD candidate in Electrical & Computer Engineering @ University of Texas; Daniel Shepard, PhD candidate at the University of Texas & Todd Humphreys, Professor of Aerospace Engineering & Engineering Mechanics @ University of Texas; *GPS World*, January, p. 33-34]

Although our spoofer fooled all of the receivers tested in our laboratory, there are significant differences between receivers’ dynamic responses to spoofing attacks. It is important to understand the types of dynamics that a spoofer can induce in a target receiver to gain insight into the actual dangers that a spoofing attack poses rather than rely on unrealistic assumptions or models of a spoofing attack. For example, a recent paper on time-stamp manipulation of the U.S. power grid assumed that there was no limit to the rate of change that a spoofer could impose on a victim receiver’s position and timing solution, which led to unrealistic conclusions.

Experiments performed in our laboratory sought to answer three specific questions regarding spooferinduced dynamics: ◾ How quickly can a timing or position bias be introduced? ◾ What kinds of oscillations can a spoofer cause in a receiver’s position and timing? ◾ How different are receiver responses to spoofing? These questions were answered by determining the maximum spooferinduced pseudorange acceleration that can be used to reach a certain final velocity when starting from a velocity of zero, without raising any alarms or causing the target receiver to lose satellite lock. The curve in the velocity-acceleration plane created by connecting these points defines the upper bound of a region within which the spoofer can safely manipulate the target receiver. These data points can be obtained empirically and fit to an exponential curve. Alarms on the receiver may cause some deviations from this curve depending on the particular receiver. **FIGURE 1** shows an example of the velocity-acceleration curve for a high-quality handheld receiver, whose position and timing solution can be manipulated quite aggressively during a spoofing attack. These results suggest that the receiver’s robustness — its ability to provide navigation and timing solutions despite extreme signal dynamics — is actually a liability in regard to spoofing. The receiver’s ability to track high accelerations and velocities allows a spoofer to aggressively manipulate its navigation solution.

#### Can’t solve spoofing – No anti-spoofing technologies solve 100%

Wesson ‘12

[Kyle, PhD candidate in Electrical & Computer Engineering @ University of Texas; Daniel Shepard, PhD candidate at the University of Texas & Todd Humphreys, Professor of Aerospace Engineering & Engineering Mechanics @ University of Texas; *GPS World*, January, p. 33-34]

To avoid unrealistic expectations, it should be noted that no anti-spoofing technique is completely impervious to spoofing. GPS signal authentication is inherently probabilistic, even when rooted in cryptography. Many separate detectors and cross-checks, each with its own probability of false alarm, are involved in cryptographic spoofing detection. FIGURE 2 illustrates how the jammer-to-noise ratio detector, timing consistency check, security-code estimation and replay attack (SCER) detector, and cryptographic verification block all work together. This hybrid combination of statistical hypothesis tests and Boolean logic demonstrates the complexities and subtleties behind a comprehensive, probabilistic GPS signal authentication strategy for security-enhanced signals.

#### A2 NMA Mechanism

#### NMA (Navigation Message Authentication) insufficient to solve spoofing

Wesson ‘12

[Kyle, PhD candidate in Electrical & Computer Engineering @ University of Texas; Daniel Shepard, PhD candidate at the University of Texas & Todd Humphreys, Professor of Aerospace Engineering & Engineering Mechanics @ University of Texas; *GPS World*, January, p. 60]

NMA is inherently less secure than SSSC. NMA security code chip interval (that is, 20 milliseconds) is longer than a SSSC chip interval, thereby allowing the spoofer more time to estimate the digital signature on-the-fly. That is not to say, however, that NMA is ineffective. In fact, tests with our laboratory’s spoofing testbed demonstrated the NMA-based signal authentication structure described earlier offered a receiver a better-than 95 percent probability of detecting a spoofing attack for a 0.01 percent probability of false alarm under a challenging spoofing-attack scenario. NMA is best viewed as a hedge. If the SSSC approach does not gain traction, then NMA might, since it only requires defining two new CNAV messages in the GPS IS — a relatively minor modification. CNAV-based NMA could defend receivers tracking L2C and L5. A new CNAV2 message will eventually be broadcast on L1 via L1C, so a repackaged CNAV2-based NMA technique could offer even single-frequency L1 receivers a signalside anti-spoofing defense.

#### A2 Non-Cryptographic Mechanism

#### Non-cryptographic anti-spoofing requires additional hardware – too expensive & too large

Wesson ‘12

[Kyle, PhD candidate in Electrical & Computer Engineering @ University of Texas; Daniel Shepard, PhD candidate at the University of Texas & Todd Humphreys, Professor of Aerospace Engineering & Engineering Mechanics @ University of Texas; *GPS World*, January, p. 62]

Non-cryptographic techniques are enticing because they can be made receiver-autonomous, requiring neither security-enhanced civil GPS signals nor a side-channel communication link. The literature contains a number of proposed non-cryptographic anti-spoofing techniques. Frequently, however, these techniques rely on additional hardware, such as accelerometers or inertial measurements units, which may exceed the cost, size, or weight requirements in many applications. This motivates research to develop software-based, receiver-autonomous anti-spoofing methods.

### Privatization CP Solvency

#### Private companies would manage GPS better than the federal government & solve the risk of attacks

Thomas ‘11

[Dr., Lt. Col Michael; Systems Engineer at the Naval Space and Warfare Center; *Geospatial Intelligence Forum*, Vol. 9, No. 5; July/August]

With its questionable reliability during conflict, GPS might be more properly managed by a nonmilitary government agency or even a private company. Shrinking defense budgets might require the military to outsource GPS management. If GPS is no longer a reliable technological contributor to the military’s war fighting capability, the time will soon come to let someone else take responsibility for its day-to-day operation, maintenance and upgrades. One possibility would be to transfer the GPS mission and system architecture to the National Geospatial-Intelligence Agency. Transferring GPS to a private company might make the system less of a target than if a government agency operated the system. Corporate business models for using satellite technology already abound, and one solution could be as simple as charging an annual usage fee determined by the accuracy required. The U.S. civilian population and the rest of the world have become accustomed to free GPS service, but now may be the time to move beyond that paradigm if GPS is to survive. Based on the comments of the Air Force chief of staff, current trends in research and development, and the well documented GPS system vulnerabilities, the U.S. military seems to be preparing to progress to the next set of technologies that will preserve or enhance the capabilities currently provided by GPS. The civilian sector needs to start looking at ways to move in that direction as well.

Security Presidential Directive-7.

### Privacy Turns

#### GPS technology ensures gov’t overreach & privacy violations p. 501-2

Karim ‘04

[Wassim, Attorney, former associate editor of Washington University Journal of Law and Policy; *Washington University Journal of Law and Policy*, Vol. 14; p. 501-2]

Up to this point, this Note has considered privacy concerns relating to the consumer data generated by personal tracking devices. However, another potential privacy problem involves the government’s possible use of the devices for surveillance and data collection. Given the enormous potential that these devices can have for law enforcement, it is certainly conceivable that law enforcement officials will attempt to use them. Recently, for example, police departments have used GPS systems in automobiles to track carjacking suspects.102 As history has shown, the government has tried to use surveillance—legally or illegally—when opportunities to do so are available, and a greater opportunity than the personal locator for the surveillance of people is scarcely imaginable.103 As such, we must consider the degree to which people who use GPS tracking devices are making themselves vulnerable to surveillance and profiling. Where corporations have the potential to collect data about individuals for their use, the government has the capability to consolidate the information and to create all-inclusive profiles on individuals.104 While the Privacy Act of 1974105 prohibits the government from maintaining profiles on individuals who are not the targets of investigation,106 the Act does not prohibit the government from purchasing information from private organizations.107 In fact, reports indicate that the Justice Department has an eight million dollar contract with Choicepoint, a data collection company, for access to their database of personal information.108

#### New technologies enable surveillance creep by the government

Karim ‘04

[Wassim, Attorney, former associate editor of Washington University Journal of Law and Policy; *Washington University Journal of Law and Policy*, Vol. 14; p. p. 509-510

Personal tracking devices will potentially present a significant threat to privacy with regard to government abuse in data collection and surveillance. With new technology such as the personal locator developing at a more rapid rate than that with which the law can keep pace, the potential for abuse intensifies.155 More importantly, the bigger threat, as identified by Jay Stanley and Barry Steinhardt of the ACLU, is the “Synergies of Surveillance”: the capability of the government to unify different technologies and data resulting in comprehensive surveillance and collection of data systems.156 The result of this comprehensive network could have an unprecedented chilling effect on society.157

#### GPS allows for unprecedented invasions of privacy

Gershman ‘10

[Bennett L., Professor of Law @ Pace University, *Pace Law Review*, Vol. 30, No. 3; p. 937-9]

The majority in Weaver conceded that Knotts appeared to be a formidable precedent that would seem to allow police investigators to use virtually any type of surveillance technology to track the progress of a vehicle on public roads.75 However, as the majority pointed out, there are significant differences between the “very primitive tracking device” in Knotts, and the “vastly different and exponentially more sophisticated and powerful technology” of a GPS device.76 The beeper in Knotts, the majority noted, was used for a limited and discrete purpose—to learn the destination of a particular item.77 The beeper merely served to enhance the sensory faculties of the police to enable them to follow the vehicle closely and maintain actual visual contact, which the Supreme Court compared to the agent‟s use of a searchlight, marine glass, or field glass.78 According to the Weaver majority, the GPS device is quantitatively and qualitatively different. GPS has a “remarkably precise tracking capability,”79 and can be cheaply and easily deployed to track a car “with uncanny accuracy to virtually any interior or exterior location, at any time and regardless of atmospheric conditions.”80 Such “constant” and “relentless” surveillance, according to the majority, is much more intrusive than “a mere enhancement of human sensory capacity.”81 Indeed, such tracking, the majority observed, “facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period.”82 For law enforcement to “see” and “capture” such information, the majority added, “would require, at a minimum, millions of additional police officers and cameras on every street lamp.”83 The implications to personal privacy of using a GPS device, the majority further argued, are staggering. They offered this stark portrayal: “[t]he whole of a person‟s progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods.”84 According to the majority, the police would be able to retrieve data that could instantaneously describe with “breathtaking quality and quantity . . . a highly detailed profile” of where we go, and in effect, who we are.85 Illustrative of the kinds of information that this technology potentially could reveal and record, the majority noted, are “trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.”86 The majority suggested that by using this technology, and by drawing easy inferences, the government would be able to assemble patterns of a person‟s professional and personal activities and could learn, with remarkable precision, his or her political, religious, amicable, and amorous associations.87

#### Warrants are essential to ensure ethical surveillance practices

Michael ‘06

[Katina; Andrew McNamee & MG Michael, Information Technology and Computer Science at the University of Wollongong (Australia), Presented at International Conference on Mobile Business (Denmark), July 25-27]

7.1.4. Do police need a warrant to track a suspected criminal or terrorist? Several cases have ruled that tracking a person with a GPS device is the same as following them on the street. However, GPS tracking is much more pervasive. First, a person is usually more aware of a person following them, than if a small tracking device were attached to their vehicle. Additionally, a GPS tracker can find a person’s location anywhere at anytime even when trailing is not possible. Furthermore, since a tracked person’s location is digitized it can be instantly analyzed to make inferences, in ways that simple observations cannot [57]. If the issuing of warrants is not compulsory there will be no barriers for police or security personnel to place tracking devices on any individual. Warrants are essential to ensure GPS tracking devices are used justly and ethically.

#### GPS monitoring sacrifices freedom at the altar of national security

Michael ‘06

[Katina; Andrew McNamee & MG Michael, Information Technology and Computer Science at the University of Wollongong (Australia), Presented at International Conference on Mobile Business (Denmark), July 25-27]

Molnar and Wagner [65] ask the definitive question “[i]s the cost of privacy and security ‘worth it’?” Stajano [10] answers by reminding us that, “[t]he benefits for consumers remain largely hypothetical, while the privacy-invading threats are real.” Indeed, when we add to privacy concerns the unknown longterm health impacts, the potential changes to cultural, social and political interactions, the circumvention of religious and philosophical ideals, and a potential mandatory deployment, then the disadvantages of the technology might seem almost burdensome. For the present, proponents of emerging LBS applications rebuke any negatives “under the aegis of personal and national security, enhanced working standards, reduced medical risks, protection of personal assets, and overall ease-of-living”[9]. Unless there are stringent ethical safeguards however, there is a potential for enhanced national security to come at the cost of freedom, or for enhanced working standards to devalue the importance of employee satisfaction. The innovative nature of the technology should not be cause to excuse it from the same “judicial or procedural constraints which limit the extent to which traditional surveillance technologies are permitted to infringe privacy” [56]. The aim of this present research is to understand the ethical implications of current LBS applications, with a view to emphasising the need for future innovators to ethically integrate these technologies into society.

#### Unfettered use of GPS surveillance ensures Orwellian overreach

Jallad ‘10

[Tarik, JD Candidate @ University of North Carolina; *North Carolina Journal of Law & Technology*, Vol. 11, Issue 2; Spring; p. ]

Have we, members of a free society, turned a blind eye to the government’s squandering of our constitutional liberties? Have our courts, the true guards protecting us from those veiled under the dark color of law, injudiciously watched as our intrinsic Fourth Amendment1 protections dissolved in plain sight? Consider the following assertions, reflecting on the unfettered use of Global Positioning System (“GPS”) surveillance: The sky is not falling—yet. But, if we continue to allow the Court’s Fourth Amendment law to be interpreted in a limited fashion that reads the amendment’s protections into oblivion, George Orwell’s 1984 will become a much more likely version of our future.2 The privacy violations arising from governmental abuse of GPS data from cellular phones and vehicle tracking systems are vast, thus legislative intervention is imperative.3 [T]he question becomes whether technology has eroded the protections provided by the Fourth Amendment, as interpreted by the U.S. Supreme Court. So far, the answer seems to be yes. . . .4 To some, this Orwellian future is no longer a sci-fi fantasy, but a prophetic reality knocking on our door—or more accurately, ringing the doorbell. This Recent Development, however, does not share this view.5 Rather, glancing only at the past few decades, this Recent Development seeks to explain how the precedent governing previous vehicle-tracking technologies still applies to the devices currently used by law enforcement officers.

#### GPS surveillance is the modern iteration of the Panopticon

Armstrong & Ruggles ‘05

[Marc P., Department of Geography @ University of Iowa; Amy J., Rand McNally & Co., *Cartographica*, Vol. 40, No. 4; Winter; p. 63-4]

Recent developments in geospatial information technologies have begun to generate rising levels of concern about privacy in the popular media. While researchers have initiated discussion about emerging interactions between geospatial technologies and in dividual-level privacy (Armstrong, Rushton, and Zimmerman 1999; Armstrong 2002; Curry 1997, 1998; Dobson 1998, 2000; Dobson and Fisher 2003; Goss 1995; Monmonier 2002; Onsrud, Johnson, and Lopez 1994; Waters 2000), the rapid pace of co evolutionary change requires further elucidation of emerging issues. The general purpose of this article, therefore, is to sketch out the role, both actual and potential, that geospatial technologies play in the negotiation of personal privacy. Particular emphasis is given to the surveillance capabilities of remote sensing systems (sateUite and terrestrial) and to how administrative records and other information, sometimes obtained as an adjunct of newly emerging location based services, can be mapped and cross-referenced to reveal the identities and characteristics of individuals from information that is often available on-line. Though writers such as Jeremy Bentham (1843) and Michel Foucault (1977), in their discussions of the panopticon, did not explicitly anticipate panoptic surveillance and the routine use of geospatial technologies to monitor the space-time activities of individuals, many scholars (see Elden 2003; Koskela 2003; Wood 2003) are increasingly concerned about such issues. In the case of remote sensing technologies, this role has already been explicitly acknowledged in the title of one of the first edited books on this topic: The Surveillant Science: Remote Sensing of the Environment (Holz 1973). While other geospatial technologies lack such a specific label, they clearly are being used, both individually and in combination, in surveillance. Moreover, as existing technologies develop, becoming smaller, lighter, and faster, and as their prices plummet, they will penetrate into most facets of our daily lives. Many individuals will complacently welcome these new technologies because of their real (or imagined) benefits. In other cases, however, awareness of the power of such technologies will encourage some to attempt to geospatially cloak themselves, living in the shadows of the panopticon.

#### GPS surveillance creep ensures the complete erosion of personal privacy

Armstrong & Ruggles ‘05

[Marc P., Department of Geography @ University of Iowa; Amy J., Rand McNally & Co., *Cartographica*, Vol. 40, No. 4; Winter; p. 71-2]

The pace of technological change in advanced societies is increasing, and we are now truly on the cusp of living under the continuous gaze of government and business interests; digitally encoded information about many routine activities is being collected and used, with and without consent. Our goal has been to elucidate some of the increasingly significant impacts of geospatial technologies on what were once thought to be private day-to-day activities. Remote sensing technologies are increasing in resolution to permit the identification of everyday objects and individuals fi-om space. Closer to home, effectively invisible technologies such as stealthy remotely piloted aircraft and closed-circuit television systems can now be used to conduct surveillance of individuals without their consent. Other geospatial operations can be applied to widely available digital maps to uncover the identities of the mapped and to monitor their proclivities. As the capabilities of geospatial technologies are not generally known and understood by the public, many individuals will find it difficult to guard against unwanted intrusions into their personal lives. Many will remain permanently unaware of the surveillant power of geospatial technologies, while others will remain complacent about their use, perhaps until they are confronted with a personal fact gleaned about them from the bitstream. Individuals can try to opt out of the panoptic surveillance of geospatial technologies, but this will be difficult to accomplish. As was widely reported through a variety of news outlets in 1999, Scott McNealy, CEO of Sun Microsystems, responded to a question about on line privacy in the following way: "You have zero privacy anyway. Get over it." It appears that we are headed to a similar place with respect to location privacy.

#### Warrants are key to checking privacy invasions of innocent parties – even the DOJ agrees

Shah ‘09

[Ramya, JD, University of Illinois; *Journal of Law, Technology & Policy*; Spring; p. 291]

Interestingly, even the Department of Justice‘s Electronic Surveillance Manual agrees and recommends securing a warrant because ―it often cannot be determined in advance whether a package containing a beeper will be taken inside a place where a person has a valid expectation of privacy, a search warrant should be obtained to cover that eventuality.‖115 Requiring a warrant before tracking a suspect would better serve the Fourth Amendment‘s purpose. True exigencies might arise ―[f]or example, during a bank robbery, [when] a bank teller acting as an agent for the police might slip a beeper into a money bag, thereby enabling the police to track the culprits.‖116 Even in such instances, ―the beeper would have to be attached at the scene of the crime or immediately thereafter, at a time when it would be impossible for police to obtain a warrant.‖117 Even in those cases, the safest policy would be for police ―to apply for a warrant as soon as possible after the tracking begins‖ in order to comply with the Fourth Amendment.118 State v. Campbell applied the concept of exigency announced in United States v. Karo.119 While Campbell reemphasized that in some cases, securing a warrant ―would be impracticable because of the ‗exigencies‘ surrounding their use and because of the need to satisfy the particularity requirements of the Fourth Amendment,‖120 the court nonetheless reasoned that because no exigency was present in this case, a warrant was required.121 Because a GPS device is attached to the vehicle, it has the potential to intrude upon the privacy of anyone who drives the vehicle or is a passenger in the vehicle. For instance, police could not only track the suspect but could also monitor a suspect‘s innocent friend or relative who uses the suspect‘s vehicle with the GPS attached to it. Unless the police are able to turn off the device or retrieve it when the vehicle is driven by someone else, the privacy rights of third parties may well be implicated.

### Solvency – ground forces

#### **Plan cripples ground force GPS system**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The options would have several disadvantages when compared with DoD’s plan, however. All of the options would require hardware additions to existing receivers: an improved antenna and integrated inertial navigation system for Option 1; a module to interpret data relayed from Iridium satellites and an inertial navigation system for Option 2; and all of the above for Option 3. Each of those hardware devices might not be much larger or heavier than a typical military handheld receiver, which is about six inches long and weighs about a pound, but when combined, they would add bulk and requirements for additional power. Although that added weight might not prove too onerous for military personnel in a vehicle, plane, or ship, it could prove troublesome for those on foot. The current trend in miniaturization has made it possible to integrate such devices into military receivers designed specifically for use in munitions (such as cruise missiles or small guided bombs) or in the confined space of very small unmanned aerial vehicles. But, designing and integrating such miniaturized devices for and into existing receivers would take time and could entail costs not included in CBO’s estimates.

### Solvency – unreliable

#### Aff relies on iridium satellites that are not guaranteed to be operable into the future

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

A final disadvantage shared by Options 2 and 3 is the dependence on the commercial Iridium satellite constellation and support network, which is not controlled by DoD. The future of the Iridium constellation cannot be guaranteed by the government, at least not without a cost that CBO has not included in its estimates. Although apparently financially healthy at the end of 2011, the Iridium communications system has had financial setbacks in the past. The risk that DoD might need to infuse funds into the system in the future is a disadvantage of relying on iGPS to enhance the ability of GPS receivers to operate in a jamming environment

### solvency – civilian upgrades

#### **Plan fails at civilian upgrades – doesn’t permit for the decoding of more sophisticated military systems**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

For each of the three options considered in this Congressional Budget Office (CBO) analysis, the effect on civilian users would be the same and would result primarily from the cancellation of the capabilities introduced by the IIIC satellites included in the Department of Defense’s (DoD’s) plans. All of the options would purchase enough IIIA satellites to maintain the Global Positioning System (GPS) constellation as long as DoD’s plan would— probably until at least 2030. The improvements to civilian signals associated with the introduction of the IIIA satellites would be retained in all of CBO’s options. Those improvements would result from the addition of the L1C signal, which, according to DoD’s statements, would improve tracking of GPS signals by civilian receivers and also enable those receivers to determine their position with greater accuracy than using signals from current satellites. The size of the improvement in accuracy is uncertain at this time; if it was similar to that afforded to military users, it would mean an increase in location accuracy from 10 feet to 3 feet. However, without the constantly updated data that would be transmitted by DoD’s planned IIIC satellites, civilian users would not be able to determine their position as accurately as they would if DoD’s plans were carried out. For military users with access to iGPS (High Integrity GPS) in Options 2 and 3, that disadvantage would be essentially negated. But civilian users would not have access to the iGPS network, so they would not benefit from its enhanced accuracy. Consequently, civilian users under CBO’s options would have the improved accuracy—to within roughly 3 feet—resulting from the more modern civilian signal transmitted by IIIA satellites, but they would not be able to attain the location accuracy of 6 inches promised by the constantly refreshed data transmitted by the IIIC satellites. Moreover, the improvements to performance in the presence of interference that would accrue to military users in CBO’s options would not pertain to civilian users, for several reasons. First, civilian users would not have access to the harder-to-jam M-code signal that would be available to military users. Second, GPS III satellites, including the IIIA model, would not broadcast civilian signals at higher strength than current GPS satellites. And finally, CBO’s options would not include any enhancements to civilian receivers similar to those proposed for military receivers. Although the performance of civilian receivers could be improved by using enhancements that are similar to those proposed for military receivers—that is, adding improved antennas and integrating inertial navigation systems—such improvements might cost as much as, or more than, the receiver itself. (The Defense Science Board estimated the cost to upgrade a handheld receiver in its 2005 report to be $2,000.)1

### SQO solves - jamming

#### Currently planned upgrades would reduce jamming effects by 96%

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The increased capabilities of GPS satellites and receivers under DoD’s plan would better enable military users to operate in the presence of radio frequency interference— the main goal of the plan. Likewise, improvements to the satellite and ground control capabilities that are included in that plan would allow military and civilian users to determine their position more accurately than they can today. The planned improvements would enable military GPS receivers to pick up signals from satellites and to retain those signals in the presence of higher levels of electromagnetic interference. One way to characterize the magnitude of the improvement is to estimate the reduction in one type of jammer’s effectiveness. For example, if a 10watt jammer can cause a Defense Advanced GPS Receiver (DAGR) to lose a GPS signal that it was tracking from a IIR-M or IIF satellite at a range of 55 miles, how much would that range be diminished after DoD has fielded the improvements that it plans for GPS? The combined effects of all of DoD’s planned improvements would be to reduce the effective range of noise jammers by an estimated 96 percent.13 Each component of the system would contribute to that overall improvement. A new receiver, for example, that was capable of processing the M-code signals from the older-model satellites already in orbit would be able to maintain track of the GPS signals as close as 25 miles to the same 10-watt jammer (see Table 2-3).14 In other words, fielding receivers capable of decoding the M-code signals would reduce the effective range of a noise jammer by an estimated 55 percent.

#### Dod Plans would reduce location errors to 6 inches

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The effective range of a 10-watt jammer would be diminished even further—to 14 miles—once GPS IIIA satellites are added to the constellation. That is because those satellites will transmit M-code signals that are roughly three times stronger than those transmitted by IIR-M and IIF satellites (see Table 2-2).15 When GPS IIIC satellites are added, they will be capable of focusing the M-code signals on to a specific region on Earth, raising the strength of the signal within that region to 100 times that of the most modern GPS satellites now in orbit.16 By doing so, the range at which a 10-watt jammer could defeat an M-code-capable receiver would be reduced to an estimated 2.5 miles, less than 5 percent of its range against current receivers trying to track signals from current satellites (see Table 2-3). Another improvement in the capability of GPS overall would result from the ability to continuously update data transmitted by the satellites with the fielding of GPS IIIC satellites. Once a sufficient number of satellites with high-speed cross-link antennas are in the constellation, the ground control system will be able to update hourly the time data broadcast by the satellites. That improvement would reduce time and position errors to such an extent that military and civilian GPS users would probably be able to determine their location to within less than 6 inches.

#### Current antennas solve jamming on aircraft and for general military receivers

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The Army has developed antennas to mount on weapons platforms (such as rocket launchers) that are designed to filter out interference from ground-based jammers. Those ground-masking antennas limit the jamming effects of all ground-based jammers regardless of the signal’s angle of arrival. One example of such an antenna developed by the Army is roughly 4 inches high, weighs 1 pound, requires 2 watts of power, and can be easily mounted on a vehicle’s roof. Controlled Reception Pattern Antennas. Controlled reception pattern antennas (CRPAs) have been developed to provide antijamming protection, primarily for aircraft. The antenna has the capability to form “nulls” in the reception pattern in the direction from which the jammer’s energy is arriving, thereby reducing the effectiveness of jamming signals. (The number of separate elements that make up the CRPA determines the number of different jammers—equal to the number of elements minus one—that can be nullified at one time.) The 7-element CRPAs currently used on aircraft weigh 4.5 pounds, and one model is roughly 14 inches in diameter (see Figure B5). The conformal version of the antenna—the CCRPA— reduces radar reflections, is 14 inches on each side, and can be mounted on the outside of an aircraft. The smaller 4-element CRPA is about half the size of the 7-element model—it has a 7-inch diameter and weighs 1.5 pounds—but can negate only half as many jammers as the larger antennas.

#### Current policies solve interference

DHS 8

Department of Homeland Security, UNITED STATES POSITIONING, NAVIGATION, AND TIMING INTERFERENCE DETECTION AND MITIGATION PLAN SUMMARY, April 2008, [www.gps.gov/news/2008/2008-04-idm-public-summary.pdf](http://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf)

The provisions made in the U.S. Space-Based PNT Policy recognize the importance of GPS and encourages its use for applications in the critical infrastructure as well as for safety-of-life applications. GPS users have seen a largely unconstrained increase in unregulated use of the civil GPS signal, which currently provides a world-wide source for PNT services to many users in multiple applications. The utilization of GPS has become widespread among sectors listed as “critical infrastructures” by the U.S. Government. Through recommendations from the DOT Research and Special Programs Administration Center (disestablished in 2005, and now the Research and Innovative Technology Administration), the transportation industry and in particular, aviation, endorsed and mandated measures establishing standards, procedures and requirements for GPS use and integration. While the criticality of safe navigation is self-evident, the use of precise timing and frequency sources is also critical to many business sectors. The U.S. Government has for some time attempted to publicize the impact of GPS interference through the efforts of the Civil GPS Service Interface Committee (CGSIC) at various events. The IDM Plan will implement a multi-layered approach to GPS interference that ensures that CI equipment is properly designed and integrated and that interference is detected and mitigated promptly.

### Spending Link – 2 billion

#### Plan costs 2 billion dollars

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Because the technologies for the improvements included in this option have already been developed, it should be possible to field receivers incorporating those technologies relatively quickly. The services have already begun to develop, and in some cases, field, advanced antennas to be used on specific aircraft and weapon systems.12 Because such systems have been designed and tested, improved antennas and INSs could be purchased starting in 2013 and integrated into existing platforms thereafter. CBO estimates that the total cost to purchase the needed hardware and to integrate it into existing or future GPS receivers would be $2 billion. Of that total, $1 billion would be needed before 2017 to purchase enough equipment to upgrade roughly half of the GPS receivers currently fielded by the services. An additional $1 billion would be needed from 2017 through 2021 to purchase the remaining hardware (see Table 3-2 on page 21).

### Neg – Spotbeams Turn

#### Plan trades off with spotbeam technologies on the new GPS systems - this hurts our anti-jamming abilities

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

By forgoing the improvements provided by the GPS IIIC satellite program, however, Option 1 would have two major disadvantages when compared with DoD’s plan. First, under this option, users would not benefit from the greatly improved accuracy that could be realized with the introduction of the high-speed cross-link antennas on the IIIC satellites. The ability to update all GPS satellites every hour that comes with those antennas and the upgraded ground control system would be forfeit, along with the much more accurate data that could be transmitted by the satellites. Thus, the GPS program under Option 1, by relying on IIIA technology and once-daily satellite updates, would yield accuracies in determining location of about 3 feet, rather than the 6 inches that might be possible under DoD’s plan. Such pinpoint accuracy might not be important for most applications, but it could be useful when trying to establish the exact position of landmines or unexploded ordnance. The second disadvantage, which all three of CBO’s options would have, results from the loss of the planned spotbeam signal on the IIIC satellites. That higher power focused signal—100 times stronger than the signal transmitted by current IIF satellites—would improve the ability of GPS receivers to operate in a jamming environment even without the improvements to receivers considered in this option. Thus, for receivers that cannot incorporate a larger antenna or an INS because they are limited by size or power constraints (such as those for use by personnel operating on foot or for use in small munitions or unmanned vehicles), the antijamming advantage provided by the IIIC’s stronger signal would not be available. That drawback might be mitigated, however, by the widespread availability on the commercial market of small versions of improved antennas and inertial measurement units and navigation systems. One commercial vendor offers antijam antennas for the DAGR’s predecessor, the Precision Lightweight GPS Receiver, and another offers inertial measurement units small enough to fit in munitions.

#### Plan eliminates critical spotbeams included in the DoD – key to landmine detection

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Another disadvantage common to the options is that they would forgo the improvements offered by the IIIC satellites, so military users would not benefit from the increased power of the M-code signals within the spotbeam. Those signals, which would be roughly 30 times stronger than those transmitted by IIIA satellites, could be advantageous for users who could not handle the added weight and power needed for improved antennas or who could not take advantage of the iGPS program. Forgoing the IIIC satellites would also mean the loss of the ability to determine position to within about 6 inches for civilian users under all of the options and for military users under Option 1. In those cases, GPS users would have to rely on the less accurate signals from the IIIA satellites, allowing them to determine their position to within about 3 feet. The addition of iGPS in Options 2 and 3 would allow military—but not civilian—users to determine their position to within 8 inches—almost as accurately as would be the case under DoD’s plan. That increased accuracy might not be important for most applications, but it could be useful when items need to be located precisely, such as in the case of land mines or unexploded ordnance.

#### (\_\_) Outweighs nuclear use

BBC July 31, ‘98, Landmine facts and figures, http://209.85.173.132/search?q=cache:fwQ84O8eFisJ:news.bbc.co.uk/1/hi/uk\_politics/142895.stm+landmines+facts+AND+nuclear+chemical&hl=en&ct=clnk&cd=1&gl=us

The Red Cross has estimated that over the last 50 years landmines have probably inflicted more death and injury than nuclear and chemical weapons combined.

#### (\_\_) Turns their– ( ) Poverty advantage ( ) Environment advantage ( ) Food prices advantage

ENS ‘4

[Dec 2, “Countries Gather to Lighten the World's Burden of Landmines”, http://www.ens-newswire.com/ens/dec2004/2004-12-02-03.asp]

"In addition to immediate risks for the local population and returning refugees after the conflicts, mines and UXO's are also posing a threat to the wildlife and to the use of nature protection areas such as National Parks and wildlife reserves," Slotte said. Klaus Toepfer, UNEP's executive director, said, "Land mines are among the horrendous legacies of war that play their deadly role in perpetuating poverty. The direct threat to people from these seeds of misery must be our first concern but it is clear that the environment, upon which local people depend for items such as food, shelter and natural medicines suffers, too." "Land mines effectively bar people from productive land forcing them to clear forests and other precious areas for agriculture with consequences for the fertility of soils, accelerated land degradation and loss of wildlife," said Toepfer. "We need more initiatives like this Roots of Peace and Conservation International project in Angola that not only remove these discarded weapons but replace them with the chance for local people to earn a sustainable livelihood."

### Neg – Private Investment CP

#### **Companies are already investing in GPS augmentation alternatives**

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Iridium Communications Inc. is a mobile satellite communications company that operates a constellation of 66 active satellites and a number of in-orbit spares.18 The Iridium constellation operates from a low-Earth orbit at an altitude of 485 miles (in contrast with the GPS constellation, which operates at medium-Earth orbit at an altitude of about 12,500 miles). Satellite launches for the Iridium network began in 1997 and continued through 2002. Iridium has recently obtained financing to launch a replacement constellation called Iridium NEXT.19 A total of 72 Iridium NEXT satellites—enough to replace all 66 working satellites and some of the spares in the present constellation—will be launched starting in 2015, and the network will start operating by 2017. The Iridium network provides a high-power signal that can help specially modified GPS receivers acquire and lock on to much weaker GPS signals. The Iridium satellites receive data regarding the location of GPS satellites within view of a receiver from an iGPS reference station located within 750 miles of the receiver. The Iridium satellites can then relay that data to the GPS receiver, which uses the data to shorten the time it needs to locate the GPS satellites and lock on to their signals. The iGPS program has four main components (see Figure 3-2):  The Iridium satellite network operations center in Leesburg, Virginia, which feeds Iridium data to the iGPS reference stations. Those data, known as ephemeris data, include information about where the Iridium satellites are located at a particular point in time. The iGPS reference stations also receive similar data about the location of the GPS satellites.  An iGPS reference station, located within 750 miles of the GPS ground user, which transmits navigation data, differential corrections, and time references to the Iridium satellite;20  An Iridium satellite within the field of view of the GPS ground user that can provide GPS satellite location data via its high-power signal;  The ground user operating a GPS receiver that has been modified to detect the Iridium signal and augmented with a miniature INS module. For military users, the receiver would be a modified version of the DAGR, which would include the addition of an iGPS receiver, a closely integrated INS, and an iGPS antenna. (See Appendix B for a picture of the earlyproduction version of the iGPS module.) To operate, iGPS first establishes a one-way data link from the network of Iridium satellites to the iGPS ground user. The transmitted data provide initial geolocation information to the iGPS user on the basis of the location of the nearest Iridium satellite. The satellite also transmits data to the iGPS user that aid in finding the best path to acquire the GPS signals. That information is then used to help the modified DAGR acquire and lock on to the GPS signals. Once that has happened, GPS tracking begins. Information transmitted by the Iridium satellite also helps the receiver to maintain that tracking in the presence of jamming by continuing to provide information about the location of GPS satellites in the receiver’s field of view.

#### Iridium iGPS program would solve need for federal action

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

The iGPS program has had several demonstrations of signal acquisition and tracking by GPS receivers under jamming conditions. On the basis of those demonstrations, OASD(R&E) claims that iGPS capability will attain operational status during 2012. However, to provide that capability to military users, several components of iGPS—primarily the network of reference stations and modifications to Defense Advanced GPS Receivers— would have to be fielded. DoD has already purchased 55 reference stations—enough, according to OASD(R&E), to provide global coverage—and plans to begin deploying them worldwide in 2012.21 Although the reference stations are unmanned, they must still be placed in secure locations and maintained. OASD(R&E) plans to develop the ability to cross-link the signals from the reference stations in the future so as to reduce the overall number of stations required. To receive the Iridium signal, DAGRs would need to be modified. Those modifications would require the addition of software and hardware, including an iGPS core module and an antenna to receive the Iridium signal and the GPS signals. OASD(R&E) had proposed that the modifications to DAGRs could be made when the upgrade to receive M-code signals occurred, but such an upgrade might not happen for 10 or more years, according to DoD’s current schedule. If iGPS capability is to be fielded in the next few years, then the necessary hardware needs to be produced and fielded before any planned Mcode upgrades to current receivers are made. At present, OASD(R&E) estimates that approximately $3,000 would be needed to purchase one iGPS module and upgraded DAGR that could receive and process the Iridium signal. Because the current iGPS module is significantly larger than the DAGR itself, this option would limit the iGPS upgrades to the 200,000 or so DAGRs mounted in vehicles.

#### Saves 3 billion dollars over the SQO

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

CBO estimates that the total investment cost to carry out Option 2 would be $18.9 billion from 2012 through 2025, a net savings of more than $3 billion compared with DoD’s plan. The acquisition costs to implement iGPS, which would pay for improvements to the GPS receivers, would be approximately $1 billion from 2012 through 2025. CBO’s estimate includes research and development funds needed to convert the prototype receivers into fieldable iGPS units as well as the cost to purchase 200,000 modified receivers so that they can take advantage of the signals from the Iridium satellites.

#### Solves Jamming

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Demonstrations of iGPS during the OASD(R&E) program have shown that it can reduce the effectiveness of jammers against the DAGR. Using an iGPS-augmented receiver, a user could lock on to and track a GPS signal in a jamming environment within approximately 120 seconds of turning on the receiver.22 Furthermore, according to data provided by the iGPS program office, integrating a DAGR with iGPS and an inertial navigation system would reduce the effectiveness of enemy jammers by 99 percent.23 That improvement in capability would mean that the range at which a 10-watt jammer could cause the iGPS-augmented DAGR to lose track of the signal would drop from 55 miles with current equipment to about 0.6 miles (see Figure 3-1). Additional improvements in capability would follow when 18 IIIA satellites were put into orbit and when large numbers of M-code-capable receivers were fielded. By 2026, when CBO estimates that a full constellation of IIIA satellites would be in orbit and roughly half of military receivers would be M-code-capable (including those attached to iGPS modules), those enhancements would reduce the effective range of a 10-watt jammer even further— to 0.14 miles (see Figure 3-1 and Table 3-3). Thus, when all the improvements introduced by this option are in the field in sufficient number, the effective range of 10watt enemy jammers should be reduced by 99.7 percent, from 55 miles to 0.14 miles.

#### Solves spoofing and jamming

CBO 11

Congressional Budget Office Study, “The Global Positioning System for Military Users: Current Modernization Plans and Alternatives,” October 2011, Congress of the United States, [www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf](http://www.cbo.gov/sites/default/files/cbofiles/attachments/10-28-GPS.pdf)

Option 2 would have several advantages over DoD’s plan. One advantage is a greater improvement in the ability of GPS to operate in a jamming environment. Several other advantages stem from the capabilities of iGPS. First, iGPS can help navigate in locations where the direct line of sight to the GPS satellite is limited, such as in urban canyons and mountainous terrain. Because the Iridium satellites are operating at a lower orbit and thus move more quickly than GPS satellites across the sky, they are “seen” more often by modified GPS receivers. Second, because location data are received from both the Iridium and the GPS satellite systems, spoofing—intentionally transmitting false GPS data that appear authentic to the receiver—is much more difficult to achieve. Third, the iGPS program has the potential to provide greater accuracy in determining the receiver’s position—on the order of about 8 inches—compared with the accuracy of approximately 10 feet achievable with today’s GPS receivers and satellites. That amount of improvement is comparable to the accuracy of 6 inches that might be achievable under DoD’s plan. Finally, the cost to carry out Option 2—$18.9 billion through 2025—would be more than $3 billion (or 15 percent) lower than that necessary to implement DoD’s plan.

### Neg – Topicality

#### Authority for the plan is under the DoD – DHS policy clearly states that modernization and augmentation is part of the military responsibility

DHS 8

Department of Homeland Security, UNITED STATES POSITIONING, NAVIGATION, AND TIMING INTERFERENCE DETECTION AND MITIGATION PLAN SUMMARY, April 2008, [www.gps.gov/news/2008/2008-04-idm-public-summary.pdf](http://www.gps.gov/news/2008/2008-04-idm-public-summary.pdf)

Under the U.S. Space-Based PNT Policy, the Department of Defense (DoD) was assigned the following responsibilities that are applicable to this Plan: • Have responsibility for the development, acquisition, operation, security and continued modernization of the GPS, while facilitating appropriate civil and homeland security Department and Agency representation and participation in these activities, and any decisions that affect civil and homeland security equities. • Develop, acquire, operate, realistically test, evaluate and maintain navigation warfare (Navwar) capabilities and other capabilities required to: o Effectively utilize the GPS services in the event of adversary jamming or other interference. o Deny to adversaries PNT services from the GPS, its augmentations and/or any other space-based PNT systems without unduly disrupting civil, commercial and scientific uses of these services outside an area of military operations, or for homeland security purposes. o Identify, locate and mitigate, in coordination with Departments and Agencies, as appropriate, any interference on a global basis that adversely affects use of the Global Positioning System for military purposes.

### CP Solvency - XO

#### Highlighting the critical nature of GPS infrastructure solves the plan

PNT Advisory Board, 10

National Space-Based Positioning, Navigation, and Timing (PNT) Advisory Board, Jamming the Global Positioning System A National Security Threat: Recent Events and Potential Cures November 4, 2010, <http://www.pnt.gov/advisory/>

There is not any practical way to completely eliminate GPS interference. But steps can be taken to greatly reduce the frequency and impacts of such interference. Further, actions can be taken to insure that GPS receivers do not give false indications of position or time. Our recommendations are:. 1. National Focus. GPS is absolutely critical US National Infrastructure. This has not been formally recognized. GPS should be formally declared critical infrastructure by Executive Branch and managed as such by DHS. This is necessary to elevate the importance of GPS to our critical infrastructure and bring the needed attention to the interference problem. The various existing national interference programs must be coordinated and gaps must be filled with additional funded efforts (see later recommendations). Senior leadership must recognize the vulnerabilities of the current critical infrastructure and give high priority to budgets and solutions.