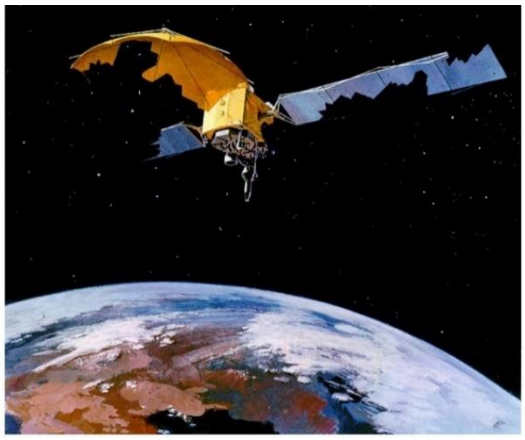
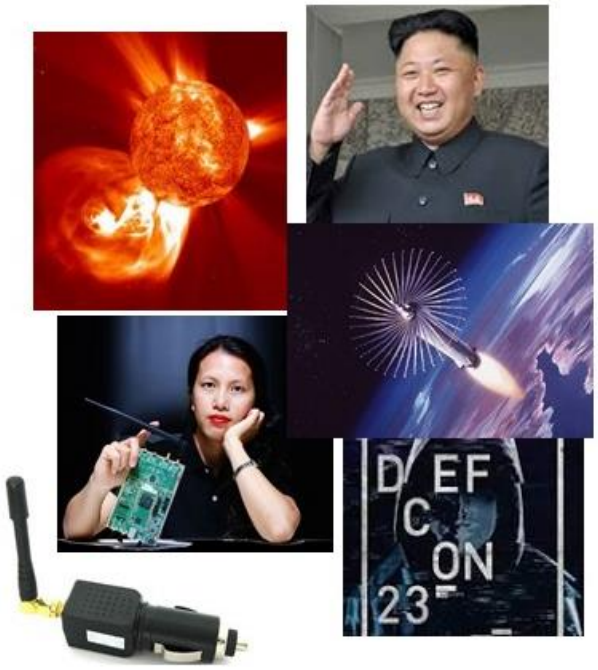
PRIORITIZING DANGERS TO THE UNITED STATES FROM THREATS TO GPS

Ranking Risks and Proposed Mitigations





WHITE PAPER

This paper examines risks to the United States, its Global Positioning System (GPS) and GPS signals. Other Global Navigation Satellite Systems (GNSS) have very similar characteristics as GPS. This high-level risk model may be of use when considering risks to other nations and to GNSS more generally.

RESILIENT NAVIGATION and TIMING FOUNDATION

The Resilient Navigation and Timing Foundation is a 501(c)3 educational and scientific charity registered in Virginia.

This paper is available on line at www.rntfnd.org/Library

Executive Summary

The US Department of Homeland Security has called the Global Positioning System "a single point of failure for critical infrastructure." This is because GPS signals are essential to virtually every networked technology but are exceptionally weak.[1] Civil GPS signals can be easily jammed or spoofed. Exacerbating the problem, receiver performance is not standardized and many users purchase based on low price instead of required capability or resilience to disruption.

Many efforts have been proposed, and some undertaken, to reinforce and protect GPS signals and the positioning, navigation, and timing (PNT) services they provide. This analysis takes a high level qualitative look at many of the threats to these services, and the danger or risk to the nation posed by each. It then examines how some of the more commonly discussed mitigation efforts might reduce the risk from one or more threat vectors.

Key findings include:

- Of all the threat vectors to GPS that were considered, the greatest danger to the US is from jamming. This includes:
    - The cumulative impact of thousands of low power jammers used by criminals and privacy seekers each day across the nation.
    - Terrorist jamming that would create damage on its own, or would aid and abet another malicious act
    - Military-style jamming (a jamming attack by a foreign power, either directly or through proxies)
- Most risk reduction measures examined address only one or some threat vectors and do not mitigate most of the risk from those vectors.
- Of the methods examined, the two most effective in reducing the danger or risk to the nation are:
    - Requiring owners and operators of critical infrastructure to be able to operate for 30 days without signals from GPS or similar space systems, and
    - Establishing a complementary and backup capability for GPS, such as the proposed eLoran system.

[1] See for example: http://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation

PRIORITIZING DANGERS TO THE UNITED STATES FROM THREATS TO GPS

Ranking Risks and Proposed Mitigations

Introduction

The Global Positioning System (GPS) is essential to virtually every networked technology. Within the United States the lack of a similarly ubiquitous complementary and backup system has caused government officials to describe GPS as a "single point of failure for critical infrastructure."

But not all threats are equal. Some could seriously damage the nation, but have little chance of ever being carried through. Other threats cause only minor damage, but that damage is inflicted every day in many locations. Making informed public policy decisions requires that all the threat vectors be normalized in terms of the risk they pose to the nation. This allows them to be compared to each other and mitigation actions prioritized.

The National Space-based Positioning, Navigation and Timing Advisory Board has periodically called for development of a "threat model" as a way of evaluating threats to GPS, the risk they pose, and to help prioritize measures that could mitigate the risk. This paper offers such a model.

The model, at its essence, is a method for organizing judgements and examining their cumulative results. It is intended to stimulate deliberate thought and discussion, and to support, not to be a substitute for, thoughtful decision making.

It is clear that any threat to GPS satellites or signals is a threat to America. This is also true for other nations that are similarly dependent upon GPS/GNSS.

The model is flexible enough to be used in classified and unclassified settings, by senior policy makers and highly technical analysts, and can be modified to include new threat vectors or exclude ones previously considered.

This paper provides both the model and its results when using input from subject matter experts associated with the Resilient Navigation and Timing Foundation. The authors encourage others knowledgeable in the field to similarly use the model as a way of methodically examining the issues and considering ways to protect GPS services and users.

Background

The threats and risks to America's (and the world's) all-important Global Positioning System (GPS) services are numerous.

Threats addressed in this paper have the potential to deny or degrade GPS service to some portion of the global user group. Denial of service, or jamming, is complete disruption of GPS signals by another radio frequency source, be it the sun, privacy seeking citizens, or belligerent nations. Denial of service can have very serious impacts, depending upon the number and type of affected users, duration of the disruption, etc. Degradation of service can be more insidious. User equipment may continue to function, but with less precision. Or it may appear to be functioning normally, but instead be providing hazardously misleading information. Service degradation can result from many causes varying from multi-path reflections of GPS signals in urban canyons, to deliberate "spoofing" by malicious actors intending harm to a user or group or users.

Many efforts are underway and proposed to address the numerous threats to GPS satellites and signals. For example, the Department of Defense is investing billions of dollars in offensive and defensive space capabilities to deter kinetic attacks on US satellites.[2]

A more holistic approach to protecting GPS and the important positioning, navigation and timing (PNT) services it provides has become known as "Protect, Toughen and Augment" (PTA). "Protect" the satellites and signals, "Toughen" users and equipment, and "Augment" GPS signals with other navigation and timing systems.

- Protecting satellites and signals includes efforts such as the Air Force's efforts to deter attacks on satellites mentioned earlier, and regulatory efforts to ensure broadcasts in frequencies adjacent to those used by GPS do not interfere with GPS signals.
- Toughening users and equipment includes encouraging users to have multiple, independent sources of PNT, and to ensure their equipment is resistant to jamming and spoofing.
- Augmenting GPS services includes establishment of a wide area complementary and backup system such as the eLoran network the US Deputy Secretaries of Defense and Transportation described in a letter to five members of Congress in 2015.

The multi-faceted PTA approach involves many initiatives to reduce risk to the American people. Whenever multiple efforts to reduce risk are considered, it is important to prioritize the most effective measures and execute them first. This ensures economy of effort, the most risk reduction is realized as soon as possible, and the greatest return on investment.

[2]"Air Force to Boost Budget to Prepare for Conflicts in Space" Stew Magnuson, National Defense Magazine, June 2015, pg 35

The Risk Model

The purpose of this risk model is to compare risks posed by various vectors. Knowing these relative risks can inform decision making about risk mitigation measures.

A high level risk model often used by the US Department of Homeland Security considers risk as the product of (1) threat, or the probability of an adverse event, (2) vulnerability, or the probability the system or facility under consideration would be damaged, and (3) consequence, or the damage to the system or facility. More simply:

Risk = Threat x Vulnerability x Consequence, or

Risk = P(vector) x P(damage) x Damage

Thus, the risk of a Category Five hurricane breeching levees and damaging New Orleans is the product of the probability there will be such a storm, the probability there will be damage, and the amount of that damage. If such a storm is forecast to strike the city every five years (20%/yr), the levees have a 50% probability of being breeched each time, and $5B in damage would result, the risk could be computed as:

Risk = .2/yr x .5 x $5B = 500M/yr

This risk score may then be compared to that from other threat vectors to inform decision making. Note that, while risk scores may be expressed in recognizable units, such as the dollars/year example above, this is not necessary. All that is needed to compare various threat vectors and risks with each other is a consistent methodology.

Threat vectors that are deliberate malicious acts (criminal, terrorist, military attack) are considered similarly. In these cases, though, the definition of "threat," or P(vector), is the product of (1) intent, or how seriously the bad actor wants to and is willing to carry out the act, and (2) capability, whether the bad actor has the wherewithal and is able to carry out the act. For malicious acts:

P(vector) = Intent x Capability

A terrorist eager to destroy a surveillance satellite, for example, would be assigned a very high score for intent, but might not be considered a threat if they had no ability to reach into space or compromise a ground control system.

The model used in this paper assesses threat, vulnerability, and consequence, for each risk vector on a scale of one to five (see criteria in Appendix 1). These numbers are then multiplied to produce a risk score. For Malicious Vectors the model fuses scores[3] for Intent and Capability. This is to enable the risk scores of Malicious Vectors to be compared to those of Accidents and Natural Vectors.

[3]Intent and Capability scores for Malicious Vectors must be fused to get Threat scores that are comparable to those for Unintended/Natural Phenomena. This is done by taking the square root of the Intent score and of the Capability score, and then multiplying the results to get a score for Threat.

Risk Vectors

The analysis examined **22 threat vectors** for GPS that have been discussed in the industry press over the last three years. Each was assessed as to the likelihood of the vector, how vulnerable GPS users or the system were, and the severity of the consequences.

Tables 1 and 2 show the results of that analysis.

Threat Vectors Considered

Natural/Accidental

1. Built structure obstruction
2. Terrain obstruction
3. Foliage (pines, hvy canopy)
4. Solar Activity – mild
5. Solar Activity - moderate
6. Solar Activity -powerful
7. Human Error/software
8. Satellite malfunction
9. Control Segment Failure
10. Space Debris
11. Unintentional RF

Malicious Acts

12. Privacy seeker (1 event)
13. Criminal Jamming (1 event)
14. Criminal + Privacy 1 Yr Total
15. Criminal Spoofing (1 event)
16. Terrorist Jamming
17. Terrorist Spoofing
18. Military-style Jamming
19. Nat. Agent Spoofing
20. Attack on Satellites
21. Attack on Control Segment
22. Cyber Attack on Control Segment

Total Risk to GPS Services & US National and Economic Security Table - 1						
	Vector	Vulnerability	Consequence	Threat		Risk Score
				Intent	Capability	
I. Natural & II. Accidental	1. Built structure obstruction	1	2	5		10
	2. Terrain obstruction	1	2	5		10
	3. Foliage (pines, hvy canopy)	1	1	5		5
	4. Solar Activity – mild	1	1	5		5
	5. Solar Activity - moderate	3	2	4		24
	6. Solar Activity -powerful	5	5	2		50
	7. Human Error/software	5	1 5	3		15-75
	8. Satellite malfunction	1	1	4		4
	9. Control Segment Failure	5	5	1		25
	10. Space Debris	1	4	2		8
	11. Unintentional RF	5	1 4	5		25 - 100
III. Malicious	12. Privacy seeker (1 event)	5	3	√5	√5	75
	13. Criminal Jamming (1 event)	5	3	√5	√5	75
	14. Criminal + Privacy 1 Yr Total	5	5	√5	√5	125
	15. Criminal Spoofing (1 event)	4	3	√4	√4	48
	16. Terrorist Jamming	5	5	√5	√5	125
	17. Terrorist Spoofing	4	4	√3	√4	55
	18. Military-style Jamming	5	5	√5	√5	125
	19. Nat. Agent Spoofing	3	4	√4	√4	48
	20. Attack on Satellites	5	5	√1	√1	25
	21. Attack on Control Segment	1	1	√1	√2	1.4
	22. Cyber Attack Control Segment	2	5	√3	√2	24

A Note on Risk Scores

The purpose of this model is not to evaluate the benefit/cost ratio of various mitigations. Its risk scores have no intrinsic meaning. They serve only to help compare one threat to another and examine:

- Which threat vectors pose the greatest risk, and
- Which are impacted by various mitigation efforts.

Sorting the results in **Table 1** by Risk Score to produce **Table 2**, we find a clear prioritization of the vectors.

Mitigation measures are available for each vector. For example, the Air Force is in the process of deploying a $1.6B "Space Fence"[4] to watch for space debris and other objects that could damage satellites. This will partially mitigate the risk posed by threat vector 10, "Space Debris," in our analysis by informing the Air Force of pending collisions and the need to reposition satellites, if possible, to avoid them.

Mitigation measures that address multiple events are generally more economical and effective in achieving the higher-level goal of protecting GPS services and PNT users.

Table 3 lists a variety of Protect, Toughen, and Augment measures discussed in the industry press over the last three years and provides a high-level assessment of their effectiveness in mitigating the risk associated with the 22 vectors.

Appendix 2 provides the assessments conducted for each vectors and details the rational for each of the model inputs used in this analysis.

Table 2 - Vectors by Risk Score	
14. Criminal + Privacy 1 Yr Total	125
16. Terrorist Jamming	125
18. Military-style Jamming	125
11. Unintentional RF	25 - 100
7. Human Error/software	15 - 75
13. Criminal Jamming (1 event)	75
12. Privacy seeker (1 event)	75
17. Terrorist Spoofing	55
6. Solar Activity - powerful	50
19. Nat. Agent Spoofing	48
15. Criminal Spoofing (1 event)	48
20. Attack on Satellites	25
9. Control Segment Failure	25
22. Cyber Attack Control Segment	24
5. Solar Activity - moderate	24
2. Terrain obstruction	10
1. Built structure obstruction	10
10. Space Debris	8
3. Foliage (pines, hvy canopy)	5
4. Solar Activity – mild	5
8. Satellite malfunction	4
21. Attack on Control Segment	1.4
Colors added to show natural groupings	

[4] http://www.lockheedmartin.com/us/products/space-fence.html

Table – 3

Proposed and Ongoing Mitigation Measures Vs Risk Vector

Vector	Risk Score	**Protect –** Space Fence for debris detection	**Protect –** Offensive (anti-Satellite weapons (deterrence)	**Protect –** Quiet adjacent bands, no authorized in-band terrestrial transmissions	**Protect –** Legal changes to counter jamming and spoofing equipment and use	**Protect –** Establish jamming detection systems & enforcement capability	**Toughen –** Improve receivers standards, implement better receivers	**Toughen –** Improve GPS signal., supplement with other GNSS signals	**Toughen –** Require critical users to be able to operate 30 days w/o space-based PNT	**Augment –** Provide 2nd Wide Area PNT signal (e.g. eLoran) for US free to users**
14. Criminal + Privacy Jamming (1 Year)	125									
16. Terrorist Jamming	125									
18. Military-style Jamming	125									
11. Unintentional RF	25 - 100									
7. Human Error/Software	15 - 75									
13. Criminal Jamming (1 event)	75									
12. Privacy Seeker (1 event)	75									
17. Terrorist Spoofing	55									
6. Solar Activity - Powerful	50									
19. Nat. Agent Spoofing	48									
15. Criminal Spoofing (1 event)	48									
20. Attack on Satellites	25									
9. Control Segment Failure	25									
5. Solar Activity - Moderate	24									
22. Cyber Attack on Control Segment	24									
2. Terrain Obstruction	10									
1. Built Structure Obstruction	10									
10. Space Debris	8									
3. Foliage (pines, hvy canopy)	5									
4. Solar Activity - Mild	5									
8. Satellite Malfunction	4									
21 Attack on Control Segment	1.4									
Some Risk to US Security/Economy Mitigated*				Most or All Risk to US Security/Economy Mitigated*						

*Risks will be mitigated as indicated once measures are widely adopted. It is essential that public policy be structured around encouraging adoption of available mitigation measures.

**Assumes complementary and backup system for GPS has different phenomenology and failure modes than GPS/GNSS

Appendix 1

Vector Assessment Criteria		
Vulnerability		
1	Low	Vector able to impact less than 5% of users
2	Moderate	Difficult for this vector to impact overall GPS service, or more than 10% of users
3	Significant	Fairly easy for this vector to impact many unsophisticated users and high performance users
4	High	Fairly easy for this vector to impact all or most users
5	Severe	Very easy for this vector to impact all or most users
Consequence		
1	Low	No noticeable economic losses, unlikely impact to safety of life
2	Moderate	Probable economic losses, possible safety of life impacts
3	Significant	Documented economic losses, probable safety of life impacts
4	High	Economic losses > $1B, injuries, probable loss of life
5	Severe	Economic losses > $5B, and/or loss of life
Threat of Natural Phenomena & Accident = Probability of Occurrence		
1	Low	Probability/history of occurrence < once every 100 years
2	Moderate	Probability/history of occurrence ≥ once every 100 years
3	Significant	Probability/history of occurrence ≥ once every 50 years
4	High	Probability/history of occurrence ≥ once every 10 years
5	Severe	Probability/history of occurrence ≥ once every year
Threat of Malicious Acts = Bad actor intent x Bad actor capability		
Intent		
1	Low	No expressed desire or interest
2	Moderate	Rarely expressed desire or interest
3	Significant	Repeat expressions of interest, some attempts, possible successes
4	High	Repeat expressions of interest, some attempts, some successes
5	Severe	Repeat expressions of interest, many attempts, many successes
Capability		
1	Low	No known ability to access and use this method
2	Moderate	Available to some nations & sophisticated actors (global criminal networks, terrorist organizations)
3	Significant	Available to all nations & sophisticated actors
4	High	Available to moderately sophisticated actors (individual technologists, criminals, etc.)
5	Severe	Available to unsophisticated actors (low cost, easy to access or build and use)

Appendix 2

Analysis by Risk Vector

This section examines each of the 22 identified risk vectors by how vulnerable GPS services are to that vector, the consequences of disruption, and the probability the vector will occur.

I. Disruption Due to Natural Phenomenon

1. Built structures – GPS service disrupted because man-made structures block some or all signals, or cause multipath/reflections that disrupt receivers.

Vulnerability GPS signals are exceptionally weak compared to other radio broadcasts and have difficulty penetrating any significant distance indoors. They are also subject to reflection off built structures causing receivers to sense two or more sources for the same signal (multi-path). However, most users to not need to rely on GPS services while indoors or in urban canyons.
Low – Vector able to impact less than 5% of GPS users

Consequence This risk vector is well understood and there are numerous local/indoor positioning systems in use to supplement GPS indoors. Unmitigated impacts include frequent transient service disruptions in urban canyons. Mitigation measures and unmitigated impacts result in economic impacts.
Moderate - Probable economic losses, possible safety of life impacts

Threat The lack of reliable GPS services in locations without a clear view of the sky has been reliably and well documented. This is experienced daily in major metropolitan areas, indoors.
Severe - Probability/history of occurrence ≥ once every year (every day)

1. Built Structures	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	Moderate (2)	Severe (5)	10

2. Terrain– GPS service disrupted because some or all signals are blocked or disrupted by terrain

Vulnerability Similar to problems in urban canyons, GPS services in natural canyons and at high latitudes are well documented. Canyons and other natural land forms can block signals and/or generate multipath problems. At high latitudes the number of satellites in view and their geometry is less favorable, and scintillation is more likely.[5]
Low - Vector able to impact less than 5% of GPS users

Consequence Disruptions to unsophisticated users in impacted areas are usually transient. High performance/sophisticated users understand the vulnerability and find alternative methodologies incurring additional cost and effort.
Moderate - Probable economic losses, possible safety of life impacts

[5] See for example: http://gpsworld.com/blms-new-gnss-protocols-may-set-undesirable-precedent/

Threat The lack of reliable GPS services in locations without a clear view of the sky and challenges in high latitudes has been reliably and well documented. This is a constant in impacted areas.
Severe - Probability/history of occurrence ≥ once every year (every day)

2. Terrain	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	Moderate (2)	Severe (5)	10

3. Foliage – Pines, Heavy Canopy – GPS service degraded by foliage that blocks or disrupts signals.

Vulnerability Triple canopy foliage often blocks signals as effectively as a building's roof for users indoors. Also, some studies have shown a single pine canopy can be problematic for some users.[6] Impacted areas are typically remote and the number of user disruptions is very low relative to the entire user base.
Low - Vector able to impact less than 5% of GPS users

Consequence Mitigation is often as simple as relocating a short distance to obtain a clear view of the sky.
Low – No noticeable economic losses, unlikely impact to safety of life.

Threat The lack of reliable GPS services in locations without a clear view of the sky has been reliably and well documented. This is a constant in impacted areas,
Severe - Probability/history of occurrence ≥ once every year (every day)

3. Foliage	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	Low (1)	Severe (5)	5

Note on Solar Activity (next three vectors): Solar activity occurs across a broad and continuous spectrum and has many facets which may or may not impact GPS service. It is a complex topic upon which many lengthy papers have been written. For the purposes of this study we consider three different levels of impact on GPS equipment and signals.

4. Solar Activity - Mild – GPS service degraded by levels of solar activity to be expected each year.

Vulnerability GPS equipment is designed to easily withstand such activity and signals in most areas are unaffected. Constellation geometry and atmospheric effects (scintillation) at high latitudes degrades service for some users.
Low - Vector able to impact less than 5% of GPS users

Consequence Satellites and most receivers are designed so as to avoid being impacted.
Low – No noticeable economic losses, unlikely impact to safety of life.

[6] See for example http://web.ics.purdue.edu/~sfei/documents/Bettinger2010.pdf

Threat Mild solar activity occurs at least once a year.
Severe – Probability/history of occurrence ≥ once every year

4. Solar Activity - Mild	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	Low (1)	Severe (5)	5

5. Solar Activity - Moderate – GPS service degraded by levels of solar activity that prevent use in some portions of the world. For the purposes of this category we consider the solar activity that caused service disruptions on the 7th of September 2005, 5th of December 2006, and 13th of September 2014 to be "moderate." The assessments below are based upon those events.

Vulnerability The great preponderance of GPS receivers in use across applications are relatively unsophisticated and subject to disruption by moderate solar activity. Moderate events are of limited duration and only some users were exposed and impacted.
Significant– Fairly easy for this vector to impact many unsophisticated and high performance users

Consequence The three events cited above were well documented, but none resulted in resulted in reports of significant economic damage or impact to safety of life. This may change as use of GPS equipment and signals continues to increase and broaden, but there is no documented history of significant impacts.
Moderate - Probable economic losses, possible safety of life impacts

Threat There have been three events in the last 11 years.
High – Probability/history ≥ once every 10 years

5. Solar Activity - Moderate	Vulnerability	Consequence	Threat	Risk Score
	Significant (3)	Moderate (2)	High (4)	24

6. Solar Activity - Powerful – GPS service degraded by levels of solar activity that prevent use over 25% or more of the Earth's surface.

Vulnerability GPS and other satellites are engineered to withstand the impact of many coronal mass ejections, though their degree of resilience is not well publicized. The 1859 Carrington event was sufficiently powerful to induce currents in wires that set telegraph offices on fire. It is likely that a similar event would damage much equipment in space and on the ground. Even if space assets survived unscathed, it is likely the ionosphere would be disturbed for a week or more making GPS services unavailable. Space-based and ground-based equipment vulnerabilities aside, the ionosphere is easily disrupted by geo-magnetic storms.
Severe - Very easy for this vector to impact all or most users.

Consequence Powerful solar activity will impact some if not all equipment and prevent reception of signals. If it is of sufficient duration, or severity, the impacts could be global. For example, even if equipment damage (in space and on the ground) from a Carrington-like event was limited to the exposed parts of the earth and satellite constellations, disruption of the ionosphere could be global and impact all users and services. All modes of transportation

would immediately slow, have less capacity and accident rates would rise. Other critical infrastructures would degrade or fail as backup timing systems began to desynchronize.
Severe - Economic losses > $5B, and/or loss of life

Threat

NASA estimates the threat of a powerful, Carrington-like event to be 12% every ten years[7] or 72% every 100 years.
Moderate – Probability/history of occurrence ≥ once every 100 years

6. Solar Activity - Powerful	Vulnerability	Consequence	Threat	Risk Score
	Severe (5)	Severe (5)	Moderate (2)	50

[7] http://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm/ The only good 100+ year data set for solar activity is observation of sunspot activity. This can be used as a proxy for coronal mass ejections, some of which could damage electronic equipment and/ or disturb the ionosphere and disrupt GPS signals. Sunspot activity peaked in the late 1830's (the famous "Carrington Event" was in 1859) and again in the late 1950's. This was before first satellite navigation system, the US Navy's TRANSIT, became operation in 1964. At that point solar activity had fallen to near minimum. A "super storm" coronal mass ejection in July of 2012, estimated by NASA to have been at least as powerful as the Carrington Event, would have had catastrophic impacts for much of the earth. Fortunately, the Earth had moved along its orbit and out of the line of fire a week earlier.

II. Disruptions Due to Accident/Malfunction

7. Human Error/Software – Human error maintaining and operating satellites or ground systems, or aspects of software and programming that have unanticipated negative impacts to the system as a whole. This does not include errors involving one or two satellites, such as improper positioning after launch.

Vulnerability Systematic problems typically impact all users
Severe - Very easy for this vector to impact all or most users.

Consequence Impacts will vary by the type of systematic error and the sophistication of user equipment. For example, a relatively minor GPS system "timing glitch" of 13.7 microseconds in January 2016 disrupted service for some receivers across industries and applications around the globe. Other receivers and applications were unaffected.
Low to Severe – Depending on type and duration of error

Threat On the first of January 2004 human error resulted in the GPS system broadcasting, in the words of the US Air Force, "hazardously misleading information" for about three hours with location errors of approximately 16km. On the 25th and 26th of January 2016 almost half the GPS constellation broadcast signals that were in error by 13.7 microseconds. On the first of April 2004 the Russian satellite navigation system, GLONASS went completely off air for 11 hours due to human error. Another outage of shorter duration happened later that same month.
Significant – Probability of occurrence $\geq$ 50 years.

	Vulnerability	Consequence		Threat	Risk Score
7. Human Error/Software	Severe (5)	Low (1) to	Severe (5)	Significant (3)	15 - 75

8. Satellite Malfunction – Improper operation or positioning of one satellite.

Vulnerability Almost all users are able to receive usable signals from more than four GPS satellites at any given time. Problems with one satellite are very unlikely to impact overall service.
Low – Vector able to impact less than 5% of users

Consequence Experience has shown that problems with one satellite have very little impact on overall GPS service.
Low – No noticeable economic losses, unlikely impact to safety of life.

Threat In spite of constant monitoring and attention, GPS, Galileo and other GNSS have had multiple instances of individual satellites that were poorly positioned, transmitted bad information or malfunctioned.
High – History/Probability of occurrence ≥ every 10 years

8. Satellite Malfunction	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	Low (1)	High (4)	4

9. Control Segment Failure – GPS service degraded or interrupted by failure of control system equipment. The GPS constellation requires regular monitoring and maintenance to retain its effectiveness. This is done through the Control Segment.

Vulnerability GPS service depends upon the proper functioning of the ground control system, known as the "Control Segment."
Severe - Very easy for this vector to impact service to all or most users.

Consequence A control segment failure could quickly result in loss of control of the GPS constellation and impact virtually every critical infrastructure in the United States.
Severe – Economic losses > $5B, and/or loss of life

Threat We can find no open source reports of GPS, or GNSS, Control Segment failure. This is likely due to designs that include multiple redundant components and locations to prevent a component or site failure from impacting the Control Segment as a whole. In the absence of any failure history, and considering concerted efforts to ensure system redundancy and update the Control Segment, we assess the probability of future failure to be low.
Low – Probability/history of occurrence < once every 100 years

9. Control Segment Failure	Vulnerability	Consequence	Threat	Risk Score
	Severe (5)	Severe (5)	Low (1)	25

10. Space Debris – GPS service degraded or interrupted because of damage a satellite by space debris.

Vulnerability Individual GPS satellites can be easily damaged by space debris. However, there are 31 satellites and damage to one is unlikely to impact service as a whole.
Low – Vector able to impact less than 5% of users

Consequence Impacts to the system from space debris damage to one satellite would be minimal. The overall cost to replace the satellite and restore the constellation would be in excess of $1B.
High – Economic losses > $1B

Threat There have been no reports of satellite or system damage due to space debris. The amount of debris in orbit increases each year, though initiatives like the Air Force Space Fence seek to minimize its impact. Additionally, debris is not normally found in the GPS orbital plane.
Moderate – Probability/history of occurrence ≥ once every 100 years

10. Space Debris	Vulnerability	Consequence	Threat	Risk Score
	Low (1)	High (4)	Moderate (2)	8

11. Unintentional RF Interference – GPS service disruption due to unintentional radio frequency interference from all sources. These include: malfunctioning/poorly configured electric and radio equipment; accidental transmissions on GPS frequencies; and intentional transmissions on GPS and adjacent frequencies not intended to disrupt GPS services.

Vulnerability GPS signals are very weak. Weaker than signals from other satellites and weaker than the cosmic background noise. Very low power terrestrial transmissions are able to disrupt reception of GPS signals. One experiment using a 2 watt transmitter on the cliffs of Dover disrupted GPS reception across the width of the English Channel.
Severe - Very easy for this vector to impact service to all or most users.

Consequence The location, frequency, strength, and duration of the interfering signal will determine the impact on GPS service. For example, a high power signal on GPS frequencies, in a major metropolitan area, that continues for several hours will have much more impact than a high power signal on an adjacent frequency.
Low to High – Depending on factors listed above.

Threat The literature contains many reports of unintentional RF interference with GPS services. Two notable examples that had wide area implications were US Navy transmissions that accidentally disrupted service in San Diego in 2007 and in Norfolk in 2013. Poorly configured antennae and sparking electric motors are among other examples that challenge users daily. Proliferation of authorized in-band and near-band transmissions makes future disruptions more likely.
Severe – Probability/history of occurrence ≥ once every year

11. Unintentional RF Interference	Vulnerability	Consequence		Threat	Risk Score
	Severe (5)	Low (1) to	High (4)	Severe (5)	25 - 100

III. Intentional Disruption (For intentional acts Threat = Intent x Capability)

12. Privacy seeker (one event, local impact) – GPS service disruption due to the use of an illegal-to-use, but legal-to-own (in the US) "personal privacy device." Such transmitters are typically low power, highly portable, and disrupt GPS service within radii of 50 feet to a quarter mile.

Vulnerability The very weak nature of GPS signals makes the great majority of GPS receivers vulnerable to this type of jamming. More expensive and sophisticated receivers with directional antennae can be less impacted, but they are not immune and are a very small portion of receivers in use.
Severe - Very easy for this vector to impact service to all or most users.

Consequence Low power means that these devices have a limited range. Use in vehicles often limits the time they are in the vicinity of critical GPS receivers and applications. Service disruption is often prevented by backup clocks or oscillators. Personal privacy devices have been responsible for idling a seaport container terminal and causing an airport landing system to malfunction. They may have been responsible for more egregious impacts, but none have been reported in the press.
Significant – Documented economic losses, probable safety of life impacts

Intent Multiple surveys have shown these devices to be in regular use by thousands of Americans. Sampling in some areas have shown 25% to 30% of commercial trucks using such devices, and thousands of signals a month in metropolitan areas. Multiple press reports have recounted their use by individuals seeking to avoid surveillance or tracking by others.
Severe – Repeat expressions of interest, many attempts, many successes

Capability Devices are available from numerous websites and easily obtained for less than $100. See for example http://www.jammerall.com/. The devices require no special knowledge to use and often function with the activation of a switch.
Severe – Easily available to unsophisticated actors.

12. Privacy Seeker (x 1 event)	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Significant (3)	Severe (√5)	Severe (√5)	75

13. Criminal Jamming (one event, local impact) – Use of GPS jamming technology as an aid in another criminal act. As an example, jamming a GPS enabled tracking device embedded in high value cargo to facilitate theft.

Vulnerability See vector 12. Privacy Seeker
Severe - Very easy for this vector to impact service to all or most users.

Consequence Single instances of cargo theft and other criminal acts abetted by jamming technology can result in significant losses for individuals and companies.
Significant – Documented economic losses, probable safety of life impacts

Intent The US Federal Bureau of Investigation has issued a notice identifying GPS jammer use as a tool used by cargo thieves. Similar use has been reported in other countries.
Severe – Repeat expressions of interest, many attempts, many successes

Capability See vector 12. Privacy Seeker, above.
Severe – Easily available to unsophisticated actors

13. Criminal Jamming (x 1 event)	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Significant (3)	Severe (√5)	Severe (√5)	75

14. Total Criminal & Privacy Seeker Jamming Each Year – Individual jamming incidents result in dropped cell phone calls, less efficient fleet management, temporary disruption to others' navigation systems, more efficient and effective thefts, and a myriad of other technical ills and inefficiencies. This type of GPS jamming is rarely detected or detectable. It is virtually impossible to tell whether a cell phone call is dropped because the phone lost sight of a tower, or because someone with jammer stopped at a traffic light at the base of the tower. Tens of thousands of low power devices are estimated to be in daily use in the United States.

Vulnerability See vector 12, Privacy Seeker, above.
Severe - Very easy for this vector to impact service to all or most users.

Consequence Boston Consulting Group estimated that geospatial services are responsible for $1.4T/yr in economic efficiency in the United States alone.[8] Even a half of one percent reduction would be a negative annual economic impact of $7B/yr. This does not include cost of the crimes committed, nor the impact of timing disruptions that cause dropped cell calls, burden IT networks, etc.
Severe – Economic losses of > $5B/yr, and/or loss of life.

Intent See vector 13, Criminal Jamming, above.
Severe – Repeat expressions of interest, many attempts, many successes

Capability See vector 12, Privacy Seeker, above.
Severe – Easily available to unsophisticated actors

14. Total Criminal & Privacy Seeking Jamming (each year)	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Severe (5)	Severe (√5)	Severe (√5)	125

15. Criminal Spoofing (one event) – Transmitting false GPS-like signals so as to introduce hazardously misleading information. The target receiver displays a false location/course/speed, a false time, and/or false data is incorporated into information systems. Introducing a false time signal into financial systems, for example, could enable cyber-theft or fraud.

Vulnerability The great majority of GPS receivers are susceptible to spoofing, though the process is more complex than jamming. Papers and demonstrations (notably by Prof. Todd

[8] http://www.directionsmag.com/entry/google-shares-oxeras-report-on-impact-of-geospatial-services-on-the-wo/306916

Humphrey's at the University of Texas, and Prof. Mark L. Psiaki at Cornell) have shown vulnerabilities in various modes of transportation, financial systems, the electrical grid, and cell phone networks.
High - Fairly easy for this vector to impact all or most users.

Consequence Spoofing is has more serious potential outcomes than jamming for targeted GPS users. Rather than no information, users have hazardously misleading information. Criminal spoofing is almost always to misdirect and deprive persons of their property or security and poses serious risk to safety of life.
Significant – Documented economic losses, probable safety of life impacts

Intent The US Department of Homeland Security has reported that drug cartels have spoofed surveillance drones used by Customs and Border Protection on the southwestern border of the United States. While this is the only report we have found, one goal of such deceptive practices is to remain undetected. Experience has shown that criminal enterprises are quick to adopt new technologies to frustrate authorities. There is every reason to believe that criminal spoofing is or is becoming a common practice
High – Repeat expressions of interest, some attempts, some successes

Capability Step by step instructions for building a GPS spoofer were published at the 2015 DefCon hackers' convention in Las Vegas and kits were on sale for about $300.
High – Available to moderately sophisticated actors

15. Criminal Spoofing (one event)	Vulnerability	Consequence	Intent	Capability	Risk Score
	High (4)	Significant (3)	High (√4)	High (√4)	48

16. Terrorist Jamming in US – Use of jamming technology to support terrorist operations or goals. Includes local use to disable first responder capabilities and across broader areas to disrupt economic activity, put safety of life at risk, and shake confidence in government.

Vulnerability See vector 12, Privacy Seeker, above.
Severe - Very easy for this vector to impact service to all or most users.

Consequence Unlike criminals who jam with limited goals and seek to remain undetected, terrorists seek to inflict maximum damage and may desire to have it attributed to their group. Jamming to impact/damage transportation and other critical infrastructure and cause loss of life could be the attack itself. Jamming could also be used to aid another attack by disabling first responder navigation and communications systems.
Severe – Economic losses > $5B and/or loss of life

Intent Multiple terrorists in Europe and the Middle East have been apprehended with jamming devices. Terrorist websites have discussed using GPS jamming as a tool or weapon.[9]
Severe – Repeat expressions of interest, many attempts, many successes

Capability See vector 12, Privacy Seeker, above.
Severe – Easily available to unsophisticated actors

16. Terrorist Jamming	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Severe (5)	Severe (√5)	Severe (√5)	125

17. Terrorist Spoofing in US – Use of spoofing technology to support terrorist operations or goals. Includes misdirecting authorities, misdirecting potential victims/targets, and introducing hazardously misleading data into information systems. Introducing a false time signal into electrical control systems, for example, could cause equipment malfunction and damage.

Vulnerability See vector 13, Criminal Spoofing, above.
High - Fairly easy for this vector to impact all or most users.

Consequence The goal of terrorist spoofing would be to support or achieve an attack that inflicted as much economic damage and loss of life as possible. While it is impossible to predict the results of an attack, loss of life is highly probable.
High – Economic losses > $1B, injuries, probable loss of life

Intent We were unable to find any open source documentation for use of spoofing by terrorists. However its use by criminal networks, along with use of and expressions of interest by terrorist networks in jamming technology, point to this being a capability that terrorists organizations are undoubtedly very interested in deploying.
Significant – Repeat expressions of interest, some attempts, possible successes

Capability See vector 13, Criminal Spoofing, above.
High – Available to moderately sophisticated actors

17. Terrorist Spoofing	Vulnerability	Consequence	Intent	Capability	Risk Score
	High (4)	High (4)	Significant (√3)	High (√4)	55

9 See for example: 25 May 2013 – Steal This Drone, Is Obama Too Late? http://121contact.typepad.com/my_weblog/television/ "… a message on the Ansar al-Mujahideen forum suggested that jihadists use the simpler method of jamming the signal.

> "The idea is very simple and could be applied with great success, Allah willing, and this is due to the remoteness of the main source of the signal - the satellite - and its relative weakness. All we need to implement this attack is a jamming device for the "GPS" frequencies, which makes the plane lose control and forces it to land, like what happened in North Korea when it forced an American drone to land through jamming"

18. Military-style Jamming in US – Disrupting GPS reception over local to broad areas with military style equipment and/or techniques by nation states or proxies to advance their military and political goals.

Vulnerability Military-style jamming is typically overt and high power, denying use of GPS signals through brute force. No receivers are able to operate in such an environment.
Severe - Very easy for this vector to impact all or most users.

Consequence US credibility, security and economic interests are regularly harmed overseas by military jamming. A military-style jamming attack on the US homeland could last for several hours or more before a sufficient response was mounted and it was defeated. The results could be catastrophic.
Severe – Economic losses > $5B and/or loss of life

Intent North Korea has regularly jammed GPS signals in South Korea for short intervals and at low power since 2010. Jamming has been used by eastern forces to defeat international treaty monitoring in the Ukraine, and is a common occurrence in conjunction with military actions in the Middle East.
Severe – Repeat expressions of interest, many attempts, many successes

Capability Military jamming equipment is overtly manufactured and sold. It is available at varying levels of quality and price from numerous vendors and requires little training to operate. It is a capability of every national military.
Severe – Easily available to unsophisticated actors

18. Military- style Jamming	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Severe (5)	Severe (√5)	Severe (√5)	125

19. National Agent Spoofing - Use of spoofing technology by foreign agents to support their national operations or goals. Includes misdirecting adversaries, and introducing hazardously misleading data into information systems. Could be used against adversaries' critical infrastructure, military, first responder and other capabilities. Spoofing is a more targeted, precise and covert tool than jamming.

Vulnerability Spoofing is covert and typically carried out by specifically trained personnel. Many military and other sophisticated receivers are very resistant to spoofing. These make up a very small percentage of the total number of receivers in use.
Significant – Fairly easy for this vector to impact many unsophisticated users.

Consequence Spoofing can be directed at specific targets of national interest. It can be used to embarrass another nation or to achieve a specific military goal
High – Economic losses > $1B, injuries, probable loss of life

Intent Russia and other nations are reported to be using spoofing as defensive measures. Iran is known to have spoofed and captured a US drone in 2011. While there have been no publicized reports of such activity in the US by national agents, there has been activity by criminal organizations. In 2015 a Chinese national demonstrated how to build a spoofing device at the DefCon convention in Las Vegas and sold kits for about $300. These cause us to infer intent is high.
High– Repeat expressions of interest, some attempts, some successes (inferred)

Capability See vector 13, Criminal Spoofing, above.
High – Available to moderately sophisticated actors.

19. National Agent Spoofing	Vulnerability	Consequence	Intent	Capability	Risk Score
	Significant (3)	High (4)	High (√4)	High (√4)	48

20. Attack on Satellites – A simultaneous kinetic or directed energy attack on one to five GPS satellites.

Vulnerability Orbiting 12,500 mile above the earth, satellites are susceptible to damage from attack by any adversary able to access the domain. To effectively impact GPS service, four or five satellites would have to be destroyed simultaneously.
Severe – Very easy for this vector to impact all or most users.

Consequence Depending upon the number and location of satellites damaged, service could be degraded or temporarily halted for some parts of the world. The damage to the constellation would take billions of dollars to repair.
Severe – Economic losses > $5B, and/or loss of life

Intent No nation has expressed interest in damaging GPS satellites. US space domain awareness capabilities would be able to identify any nation that did so enabling a rapid retaliatory response.
Low – No expressed desire or interest

Capability Few nations have the capability to damage satellites in space and fewer are potential adversaries.
Low– Available to only a few nations

20. Attack on Satellites	Vulnerability	Consequence	Intent	Capability	Risk Score
	Severe (5)	Severe (5)	Low (√1)	Low (√1)	25

21. Attack on Control Segment – A kinetic attack on portions of the Control Segment responsible for operations and maintenance of the GPS constellation.

Vulnerability The control segment has multiple and geographically dispersed redundancies and components. These are well protected by physical security.
Low – Very difficult for this vector to impact GPS services

Consequence An attack on one portion of the control segment would have little consequence for GPS services
Low – No noticeable economic losses (nationally), unlikely impact to safety of life (for users)

Intent No nation or group has expressed interest in damaging the control segment.
Low – No expressed desire or interest.

Capability Overcoming physical security measures to damage one component of the control segment could be within the capability of some terrorist group. However, they would need to be to identify the physical components of the control segment and select one within their capability to damage.
Moderate – Available to some nations and sophisticated actors.

21. Attack on Control Segment	Vulnerability	Consequence	Intent	Capability	Risk Score
	Low (1)	Low (1)	Low (√1)	Moderate (√2)	1.4

22. Cyber Attack – Disrupting GPS service by cyber penetration of the Control Segment.

Vulnerability The Control Segment is a relatively closed system carefully guarded by the United States best cyber defenses and personnel. However, the system is dated and requires replacement.
Moderate – Difficult for this vector to impact overall GPS service.

Consequence If an attack was fully successful, it could easily degrade or terminate GPS service.
Severe – Economic losses > $5B, and/or loss of life

Intent Numerous US officials have expressed concern about this vector in light of high profile and destructive cyberattacks on other systems. The control segment is one of the most challenging and attractive targets imaginable for high capability hackers. As a result, the OCX control segment upgrade for GPS includes improved protections against cyberattack.
Significant – Repeat expressions of interest, some attempts, possible successes

Capability A successful cyberattack on the GPS control segment would require the utmost sophistication and be exceptionally difficult to achieve.
Moderate – Available to some nations and sophisticated actors.

22. Cyber Attack	Vulnerability	Consequence	Intent	Capability	Risk Score
	Moderate (2)	Severe (5)	Significant (√3)	Moderate (√2)	24