RESILIENT
NAVIGATION
and TIMING
FOUNDATION

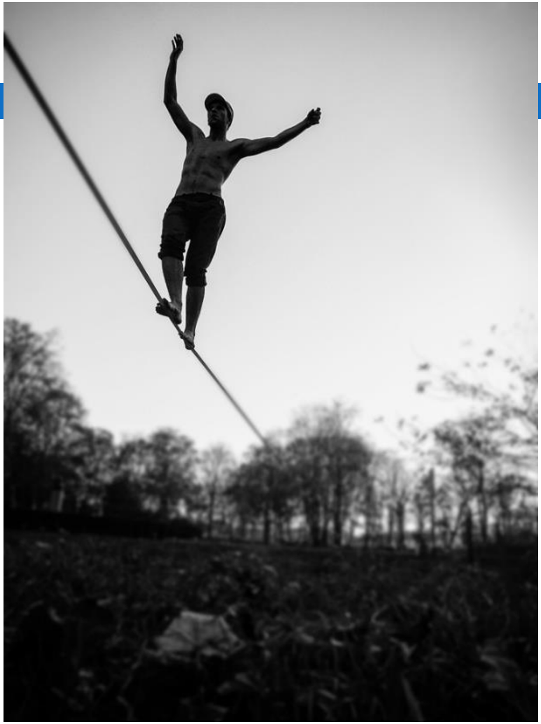
Prioritizing Dangers…

DECEMBER 2016

US National PNT Advisory Board

California Cool

Danger, or Risk



Adverse External Event? (Threat)

How likely it will matter? (Vulnerability)

What bad thing will happen? (Consequence)

Risk from external event =

Threat x Vulnerability x Consequence

or

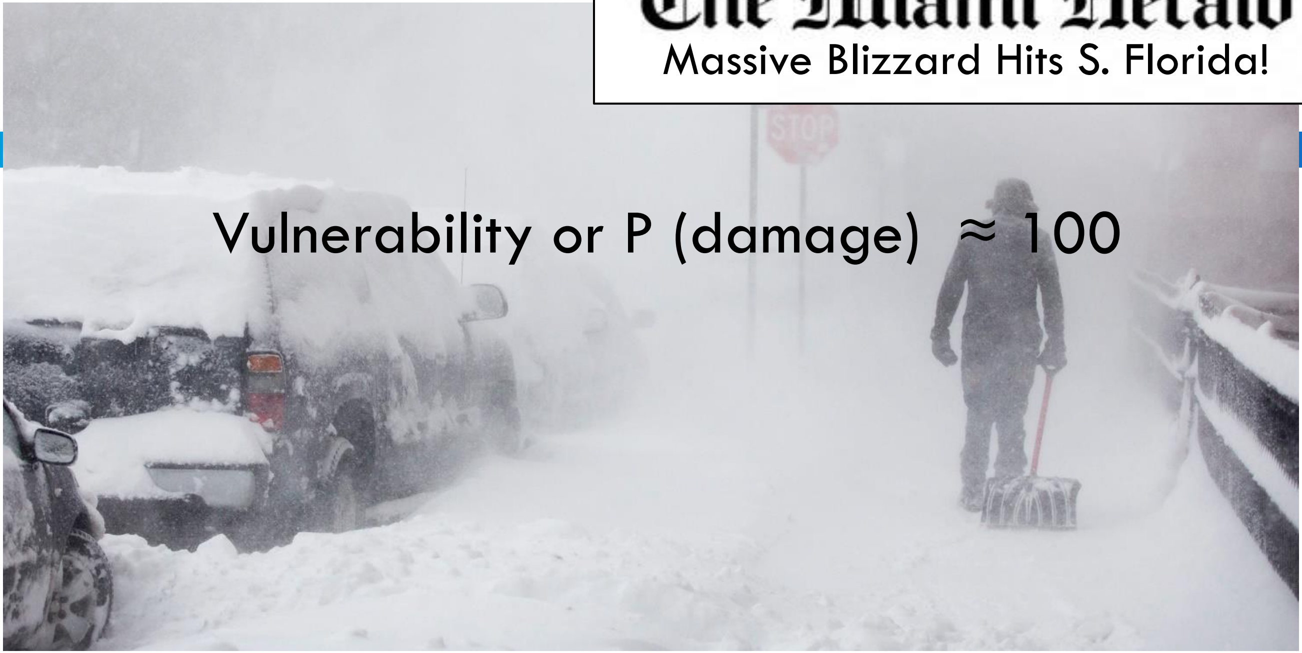
P(vector) x P(damage) x Damage

The Miami Herald

Massive Blizzard Hits S. Florida!

The Miami Herald

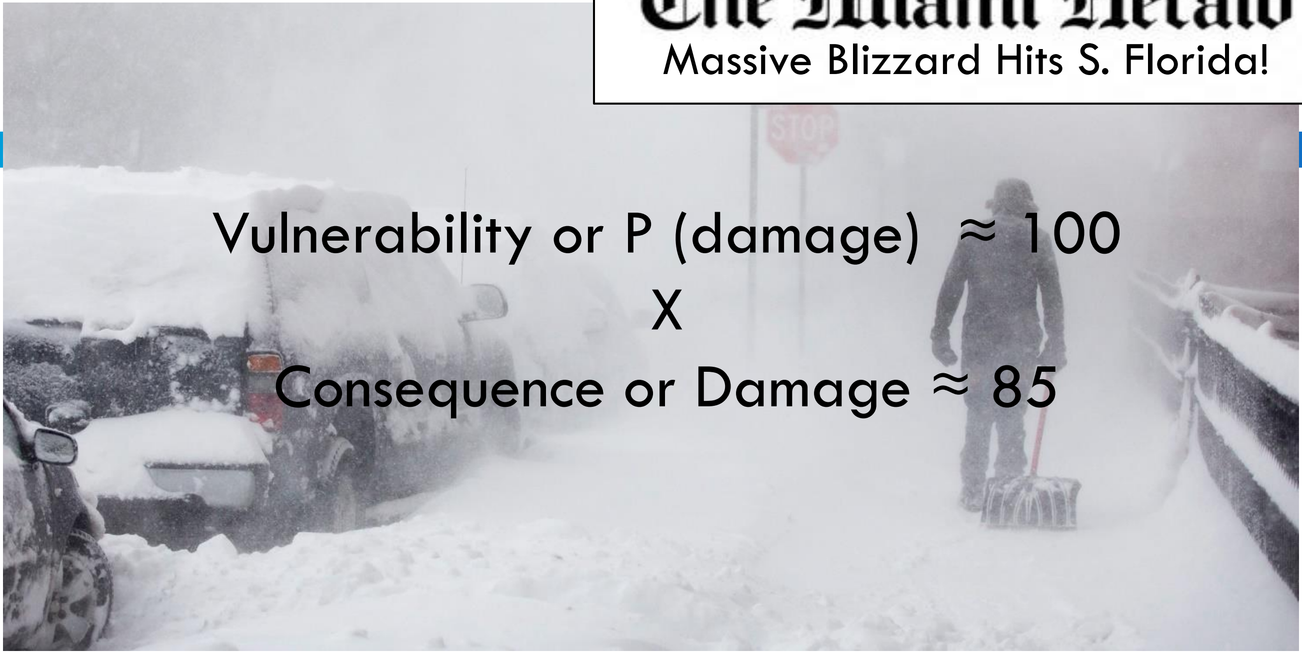
Massive Blizzard Hits S. Florida!



Vulnerability or P (damage) ≈ 100

The Miami Herald

Massive Blizzard Hits S. Florida!



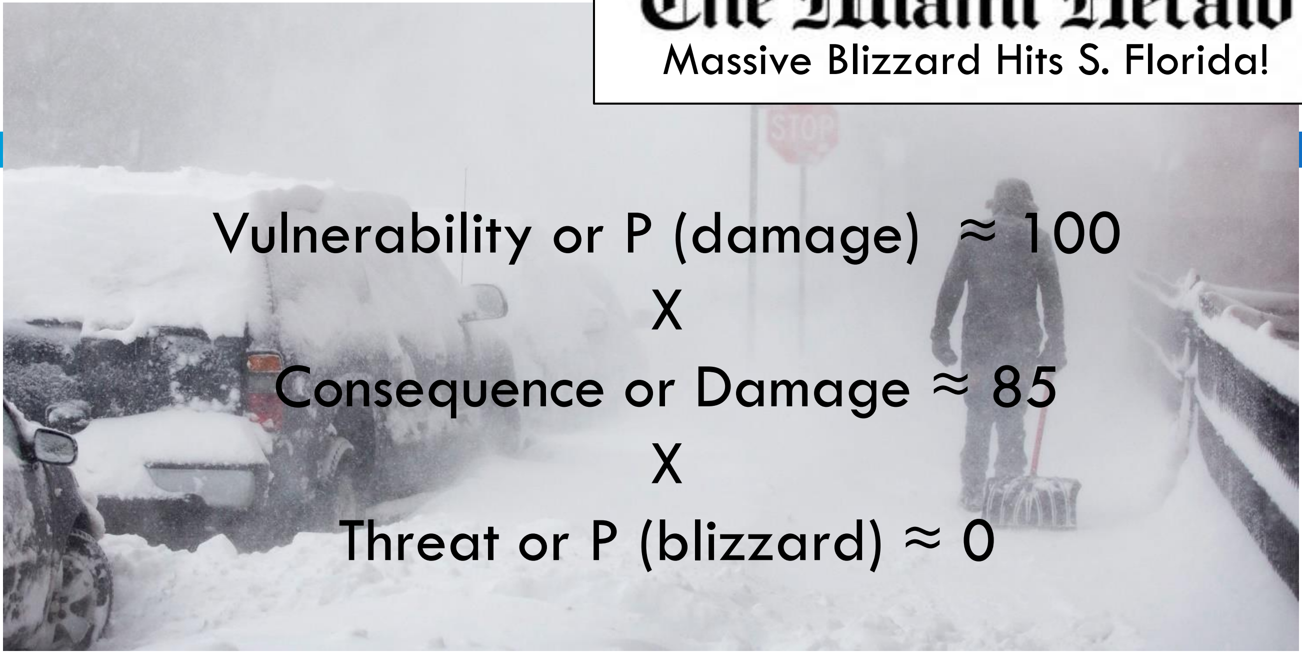
Vulnerability or P (damage) ≈ 100

X

Consequence or Damage ≈ 85

The Miami Herald

Massive Blizzard Hits S. Florida!



Vulnerability or P (damage) ≈ 100

X

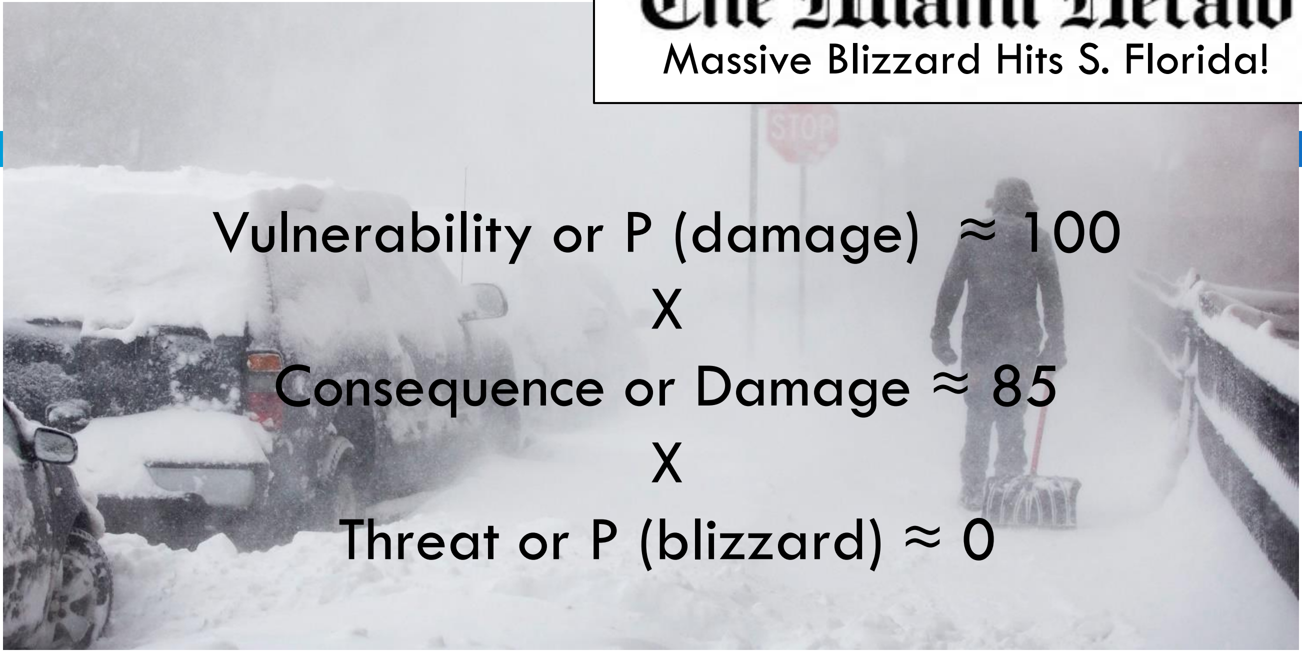
Consequence or Damage ≈ 85

X

Threat or P (blizzard) ≈ 0

The Miami Herald

Massive Blizzard Hits S. Florida!



Vulnerability or P (damage) ≈ 100

X

Consequence or Damage ≈ 85

X

Threat or P (blizzard) ≈ 0

Risk ≈ 0

Threat (malicious acts) =

Level of Intent

x

Level of Capability

Vulnerability ≈100

Vulnerability ≈100

X

Consequence ≈ 100

Vulnerability ≈100

X

Consequence ≈ 100

X

Intent ≈ 100

Vulnerability ≈100

X

Consequence ≈ 100

X

Intent ≈ 100

X

Capability ≈ 0

Vulnerability ≈100

X

Consequence ≈ 100

X

Intent ≈ 100

X

Capability ≈ 0

Risk ≈ 0

Risk =

Natural event/ Accident:

P(vector) x P(damage) x Damage

Malicious Act:

(Intent x Capability) x P(damage) x Damage

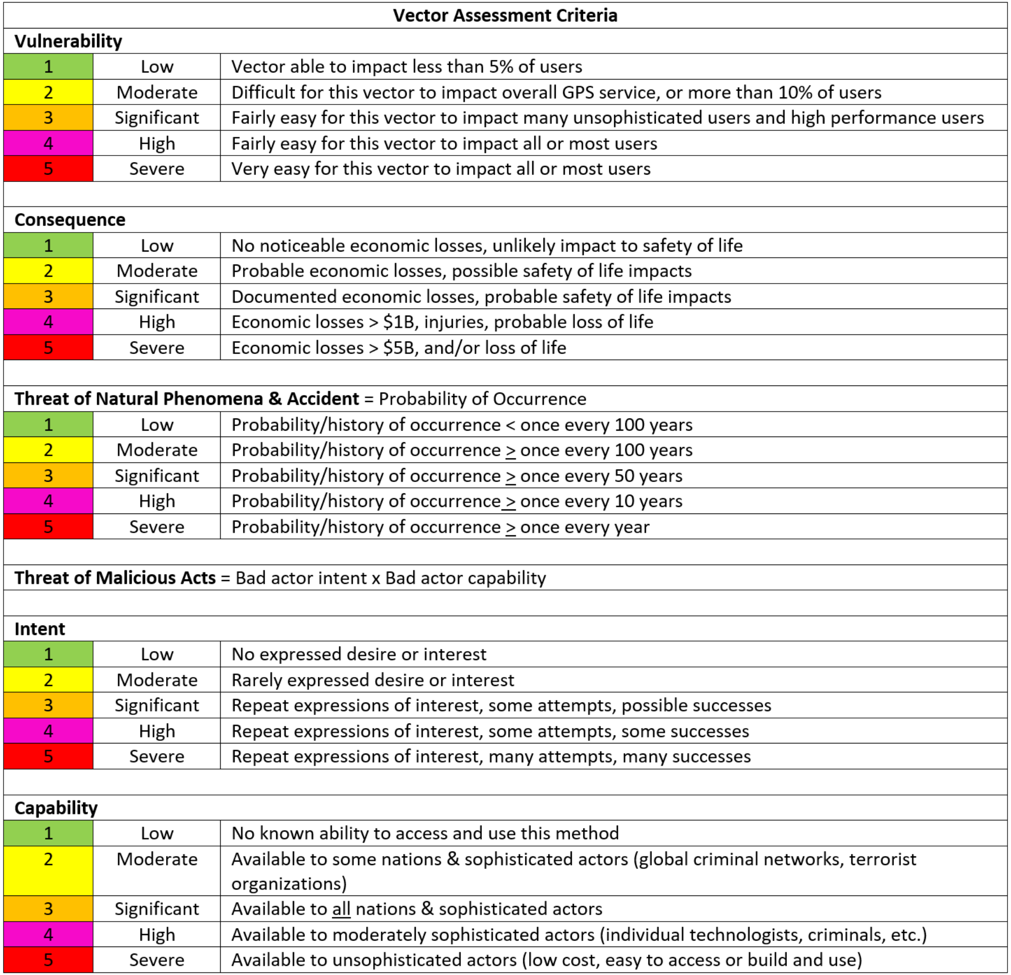
Threat Vectors for GPS

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



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)

Example:

5. Solar Activity – Moderate   Risk Score = 24

Vulnerability - 3

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 - 2

Events in Sept 2005, Dec 2006, Sept 2014 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 – 4

There have been three events in the last 11 years.

High – Probability/history $\geq$ once every 10 years

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

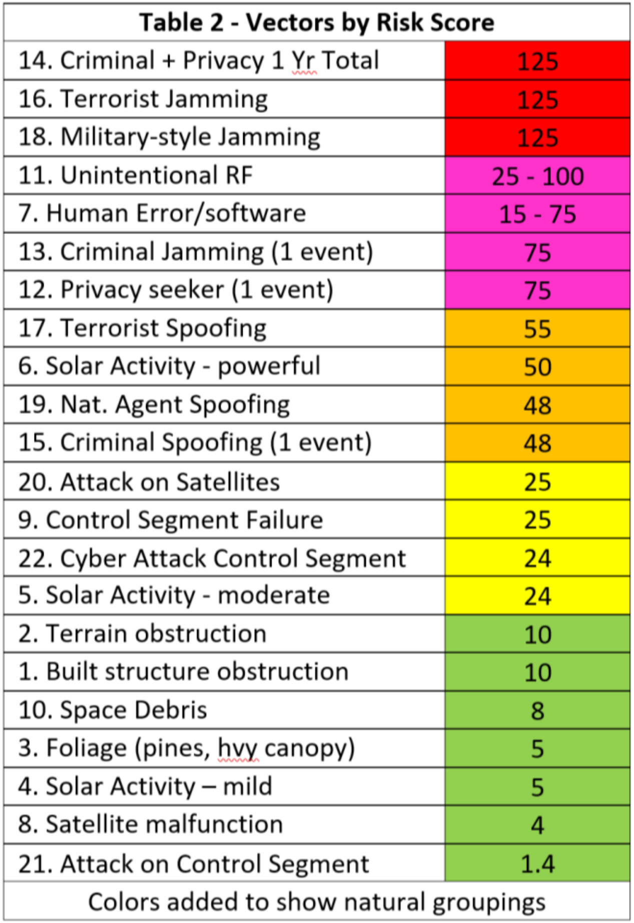


Table 2 - Vectors by Risk Score

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

Mitigations (in progress & proposed)

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 receiver 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

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 2^{nd} 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								■	■

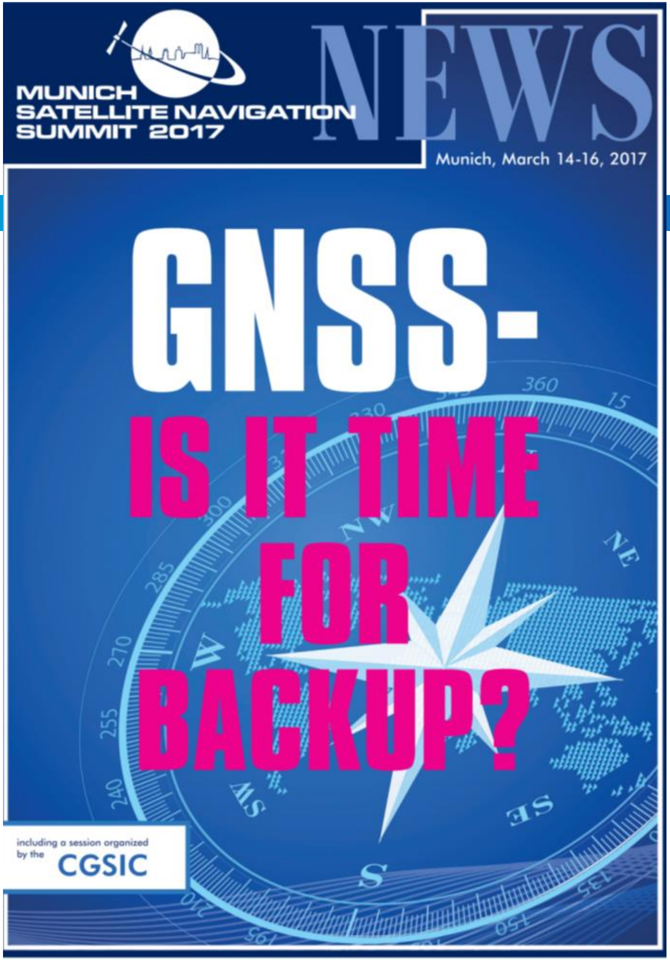
▨ Some Risk to US Security/Economy Mitigated*

■ Most or All Risk to US Security/Economy Mitigated*

RESILIENT NAVIGATION *and* TIMING FOUNDATION

Paper available at www.RNTFnd.org/Library

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


MUNICH SATELLITE NAVIGATION SUMMIT 2017
NEWS
Munich, March 14-16, 2017
GNSS-
IS IT TIME FOR BACKUP?
including a session organized by the CGSIC

Seeking Speakers/Panelists For “Yes” and “No”

15 March 2017

Contact: Info@RNTFnd.org

Register to attend at:
www.munich-satellite-navigation-summit.org/