GPS in 2030

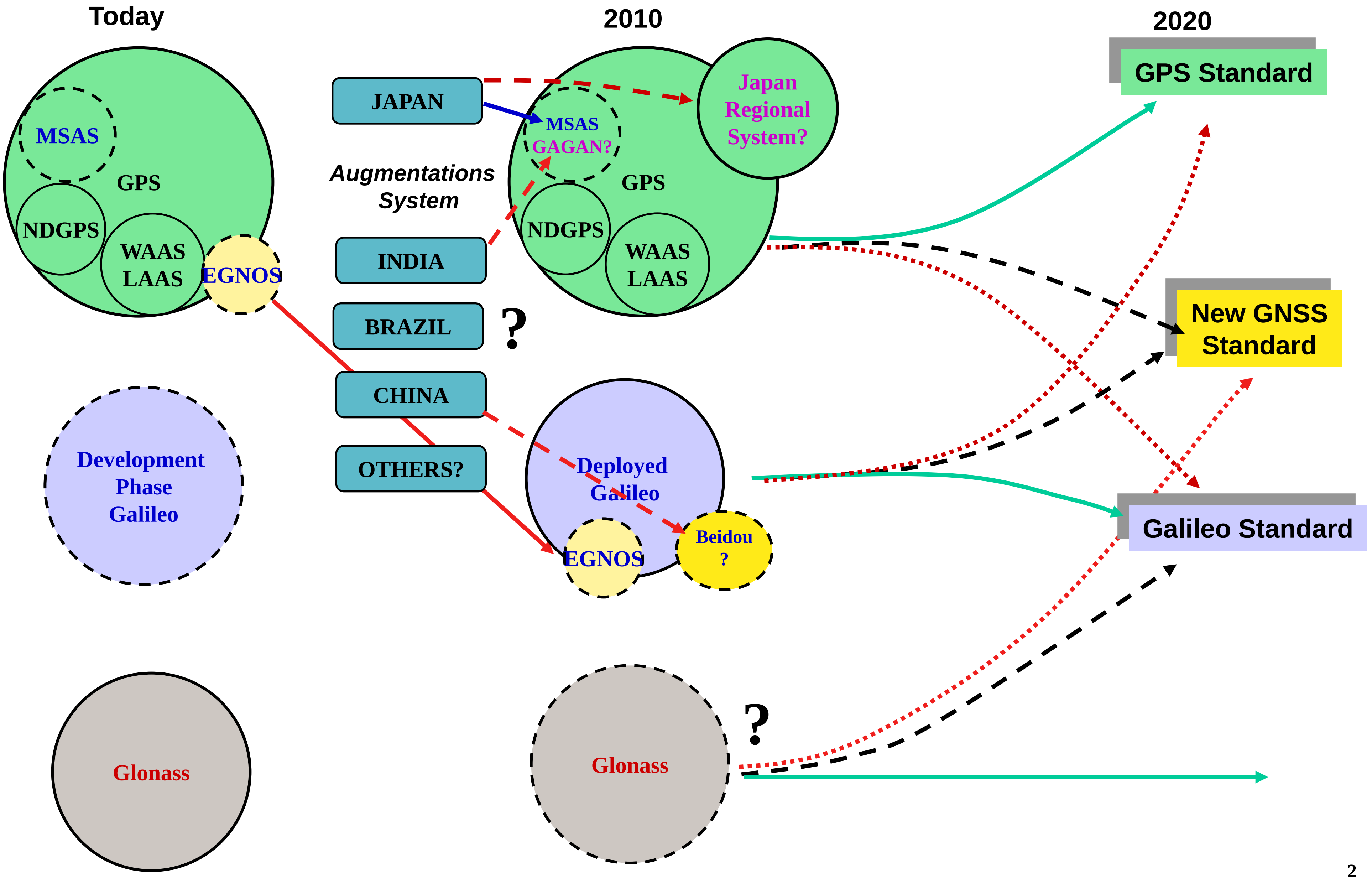
Operating in a Multi-National, Multi-GNSS Environment

Steve Moran
Director, GPS Mission Solutions
Raytheon Company

7 May 2013

Possible GNSS futures

GPS INDEPENDENT ASSESSMENT TEAM INTERNATIONAL STUDY – AUGUST 2002



Today

MSAS

GPS

NDGPS

WAAS LAAS

EGNOS

Development Phase Galileo

Glonass

JAPAN

Augmentations System

INDIA

BRAZIL

?

CHINA

OTHERS?

2010

MSAS GAGAN?

Japan Regional System?

GPS

NDGPS

WAAS LAAS

Deployed Galileo

EGNOS

Beidou ?

Glonass

?

2020

GPS Standard

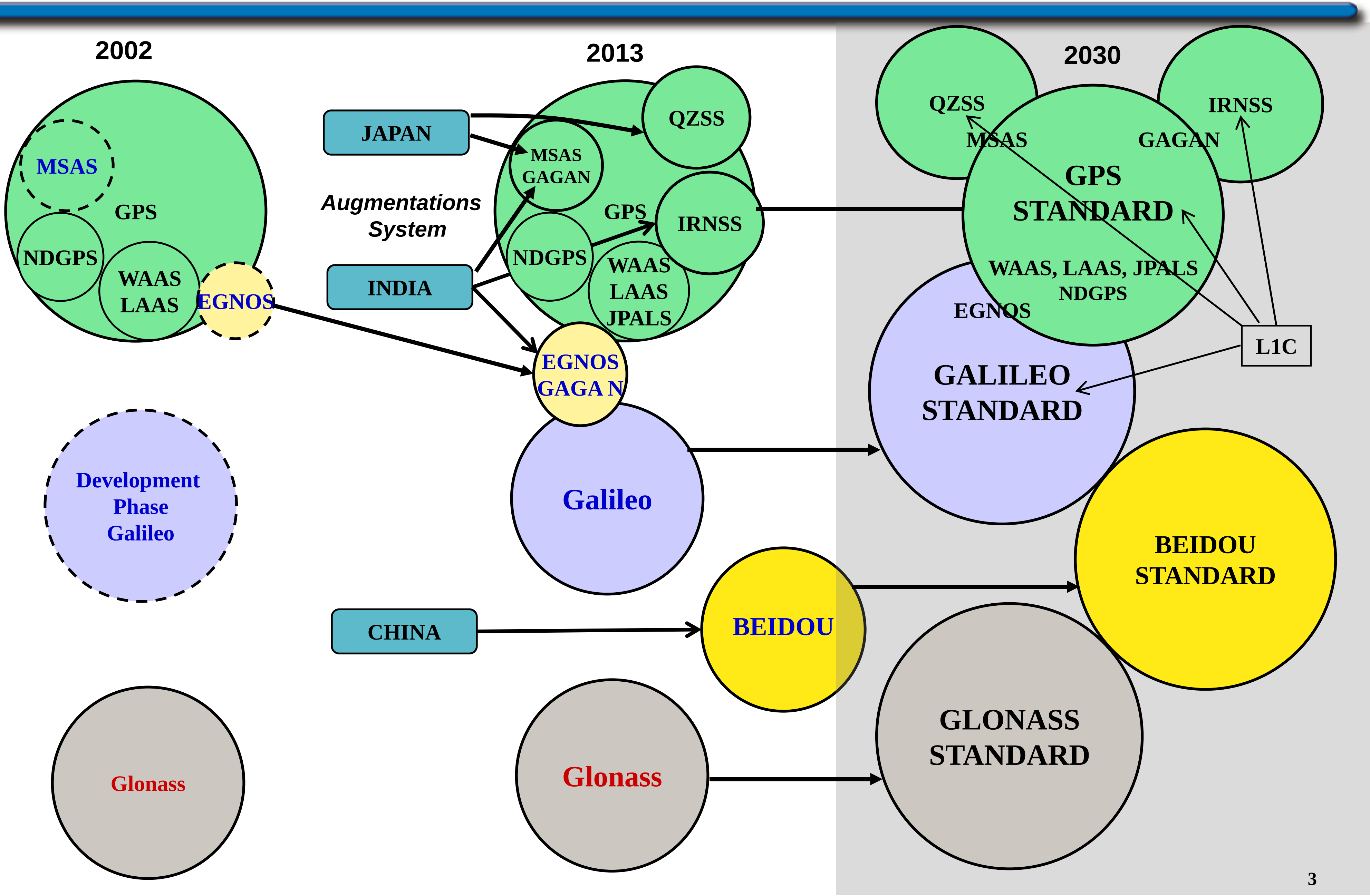
New GNSS Standard

Galileo Standard

What will determine the future?

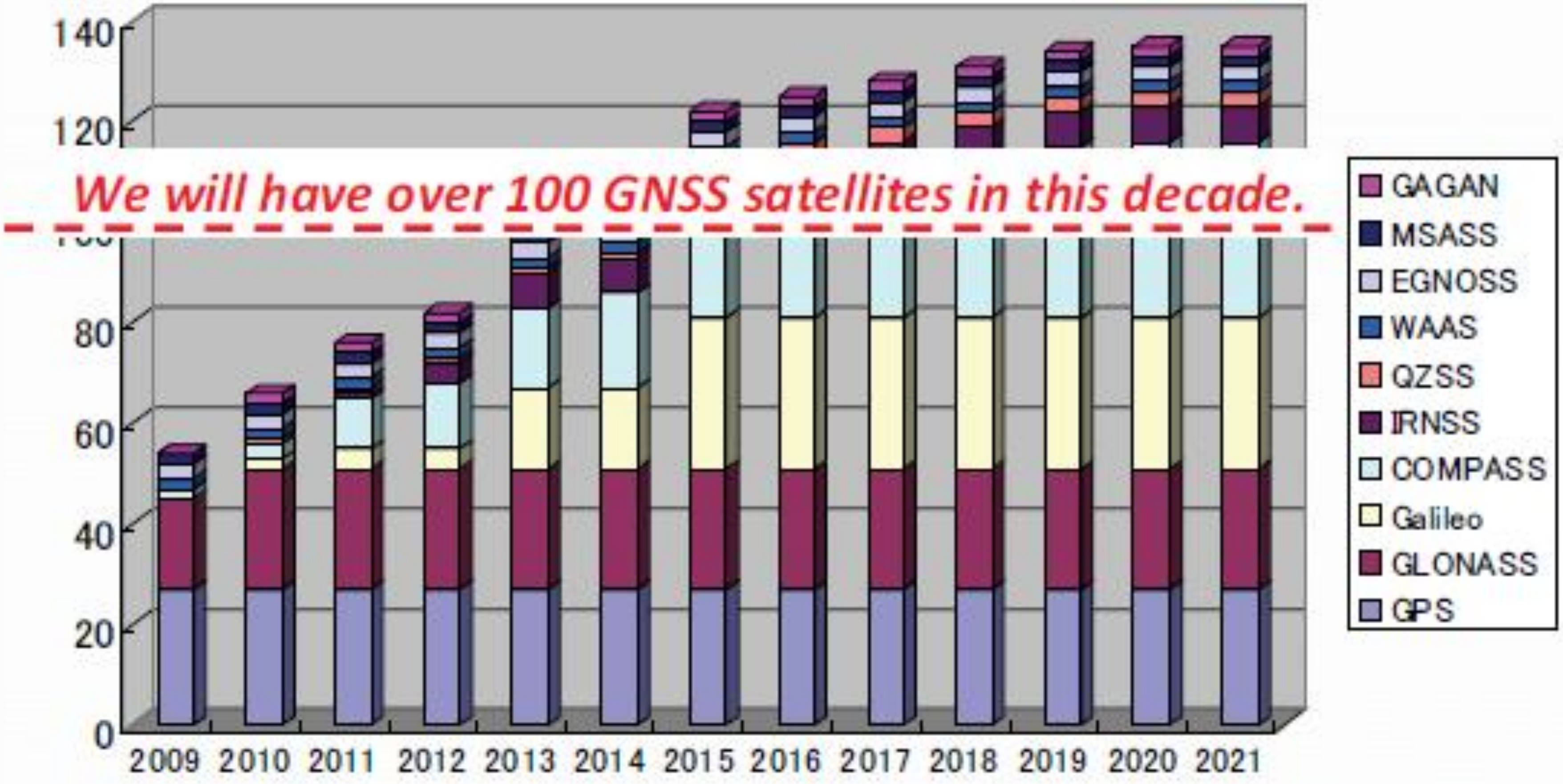
Possible GNSS futures

WE DIDN’T PREDICT THIS IN 2002 – WHAT ARE THE IMPLICATIONS?



Multi-GNSS

Total Number of GNSS Satellites



We will have over 100 GNSS satellites in this decade.

2011/9/22 ION GNSS 2011 Session P3: Global and Regional Satellite System Providers & the United Nations ICG

24th International Technical Meeting of the Satellite Division of
The Institute of Navigation, Portland OR, September 19-23, 2011

Satoshi Kogure, ION GNSS 2011

GNSS in 2030: Key Assumptions & Implications

- **Globally ubiquitous, high-quality GNSS signals will be available free of direct user fees**
  - Average users won’t know or care where their PNT information comes from
  - Safety of Life users will employ all signals that can be trusted
  - Military users will employ all signals available to cope with A2AD environments
- **The cost of sustaining and modernizing GNSSs will continue to increase**
  - GNSS provider nations will seek the minimum level of independent GNSS needed to maintain sovereignty at affordable cost
- **Cyber attacks will become more frequent, sophisticated, and successful**
  - GNSSs will be targeted by cyber attacks, some will survive and others won’t
- **PNT S&T will continue to advance at a rapid pace**
  - Other sources of PNT will be integrated with GNSS at the user equipment level

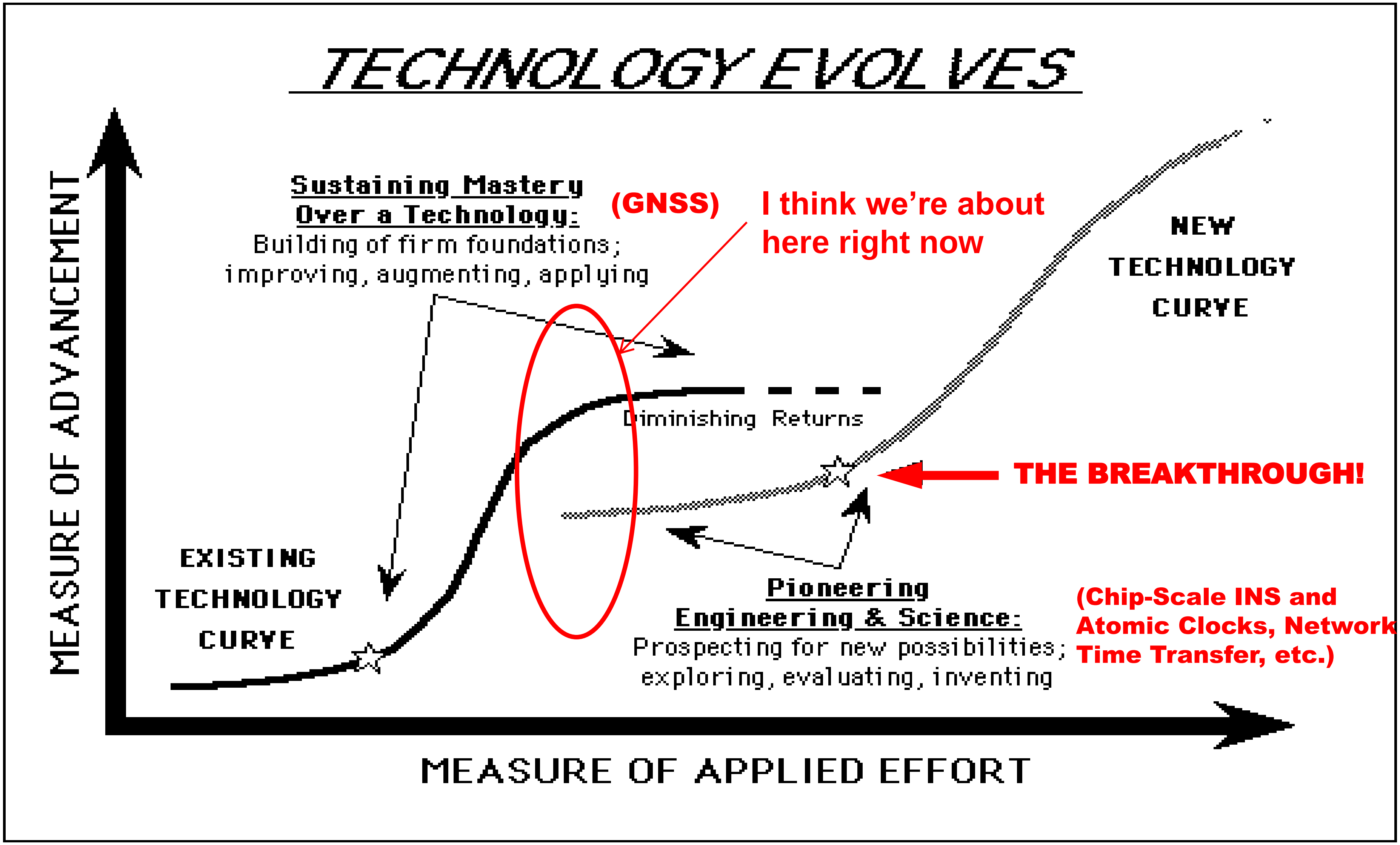
GNSS in 2030: Key Risks & Mitigations

- **Average users won’t know or care where their PNT information comes from**
  - Users will become dependent on services that may not be trustworthy
  - Civil signals will require some level of authentication and verification
- **Safety of Life users will employ all signals that can be trusted**
  - Definition of trust will need to be determined by international organizations
  - GNSSs will continue to require monitoring and national or regional augmentation
  - Information Assurance will become increasingly visible and important
- **Military users will employ all available GNSS signals to cope with A2AD environments**
  - Military user equipment will be integrated with net-connected comms, will receive all GNSS signals, and will employ state-of-the-art jam/spoof resistance
  - Military users will require knowledge about which GNSS signals can be trusted
  - In-theater monitoring of GNSSs will be needed to provide PNT Situational Awareness to warfighters

GNSS in 2030: Key Risks & Mitigations

- **GNSS provider nations will seek the minimum level of independent GNSS to maintain sovereignty at affordable cost**
  - Minimum GNSS level will depend on national priorities
  - Systems will become more collaborative to achieve optimum performance
  - Regional augmentations will evolve to meet specific user needs
- **GNSSs will be targeted by cyber attacks, some will survive and others won't**
  - Information Assurance will become critically important to GNSS survival
  - Agreement on level of IA protection required will be difficult to achieve, survival of the fittest may apply
  - Robust Information Assurance will be required of all GNSS
- **Other sources of PNT will be integrated with GNSS at the user equipment level**
  - Multi-source PNT will be embraced to achieve optimal user benefits
  - Other PNT technologies could become competitive with GNSS

Are we approaching The Breakthrough on PNT?


TECHNOLOGY EVOLVES
Sustaining Mastery Over a Technology:
Building of firm foundations; improving, augmenting, applying
(GNSS)
I think we're about here right now
NEW TECHNOLOGY CURVE
Diminishing Returns
THE BREAKTHROUGH!
EXISTING TECHNOLOGY CURVE
Pioneering Engineering & Science:
Prospecting for new possibilities; exploring, evaluating, inventing
(Chip-Scale INS and Atomic Clocks, Network Time Transfer, etc.)
MEASURE OF ADVANCEMENT
MEASURE OF APPLIED EFFORT

GPS in 2030: Operating in a Multi-GNSS Environment

- **Civil signals will require some level of authentication and verification**
  - UAS operations in controlled airspace
  - Civil signal validation through encryption and non-repudiation
- **GNSSs will continue to require monitoring and national or regional augmentation**
  - Multi-GNSS monitoring with anti-tamper, encryption, non-repudiation
  - PNT NavSats for resiliency
  - Impacts on Navwar ConOps
- **In-theater monitoring of GNSSs will be needed to provide PNT Situational Awareness to Warfighters**
  - Utilization of existing civil monitoring systems
  - Increased security posture of monitoring stations and networks
  - Impacts on Navwar ConOps

GPS in 2030: Operating in a Multi-GNSS Environment

- **Systems will become more collaborative to achieve optimum performance**
  - Signal interchangeability
  - Trusted global "PNT Grid"
  - Net-connected UE as PNT situational awareness sensors
- **Regional augmentations will evolve to meet specific user needs**
  - Coordination/integration with "foreign" augmentation systems
  - In-theater augmentations will be essential to military operations
- **Robust IA will be required of all GNSSs and augmentations**
  - International agreement on level of protection will be difficult
  - Remediation of existing systems will be difficult and expensive
  - IA will be a near-term discriminator for GPS
- **Other PNT technologies could become competitive with GNSS**
  - Watch S&T achievements closely, embrace multi-source PNT integration
  - Impacts on Navwar ConOps

Summary

“Trust nothing, use everything, come up with a solution that meets your needs at the time”

Jim Doherty, GPS IRT