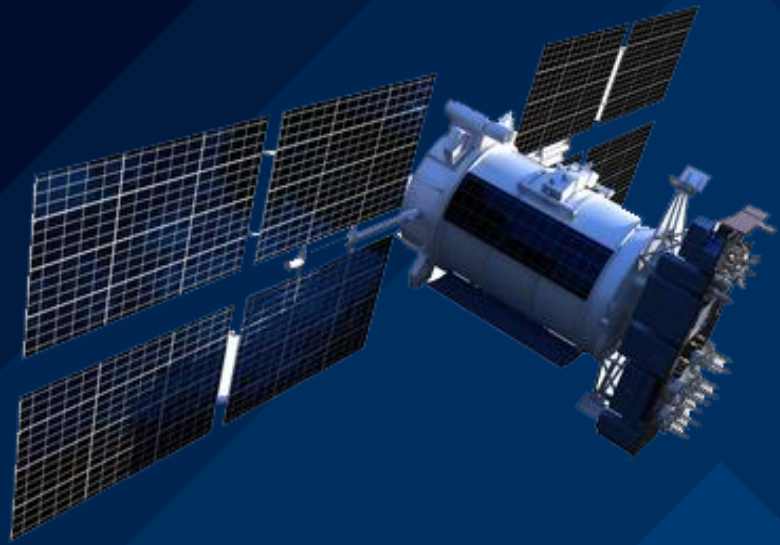
SPACE EW
A PRACTICAL APPROACH



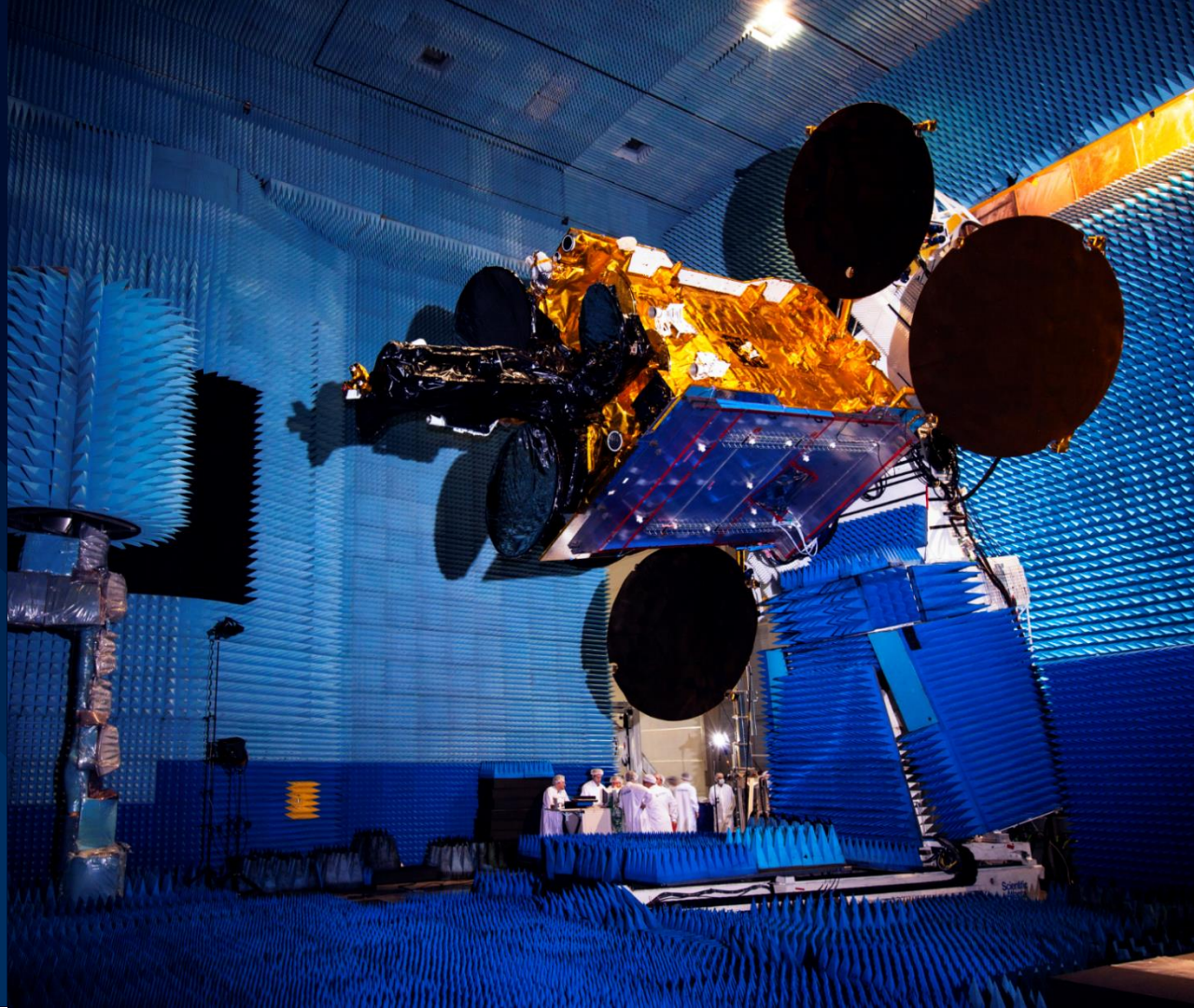
Tim Fountain
Market Segment Manager, RADAR & EW

All information was acquired from publicly available sources

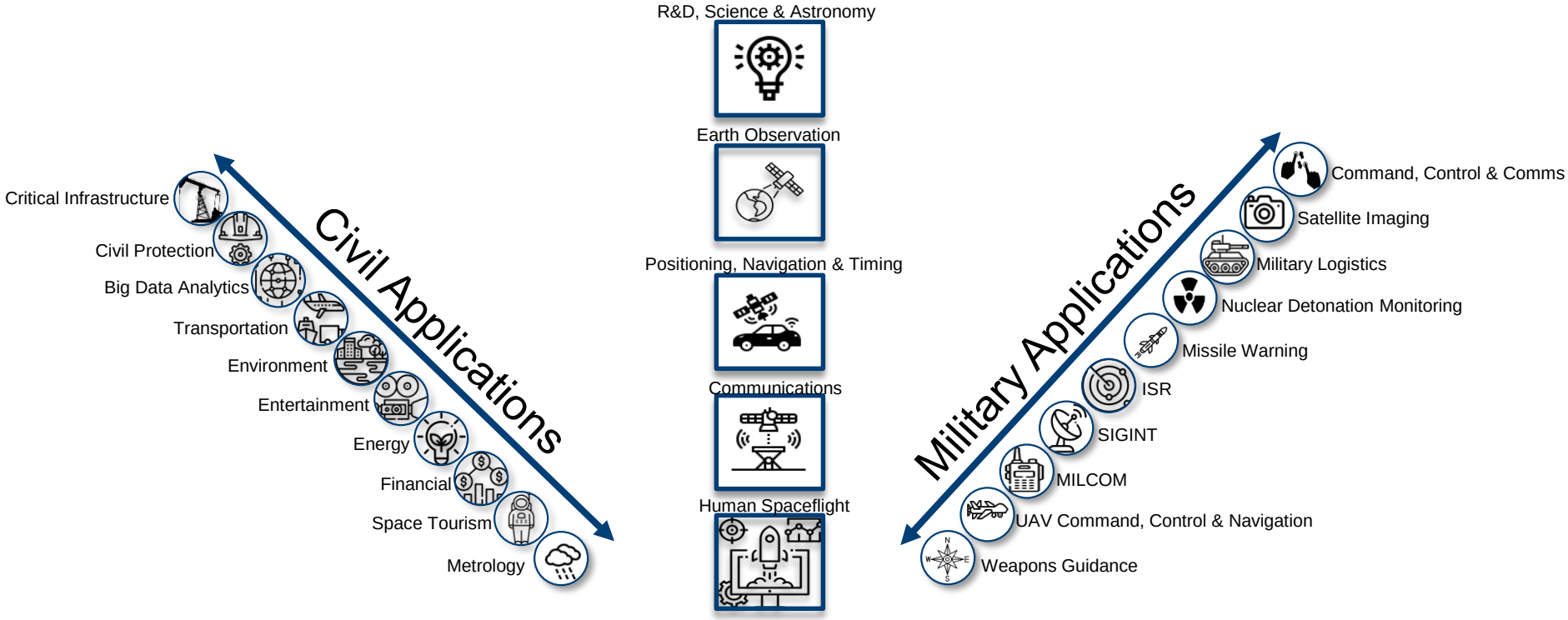
ROHDE&SCHWARZ
Make ideas real

AGENDA

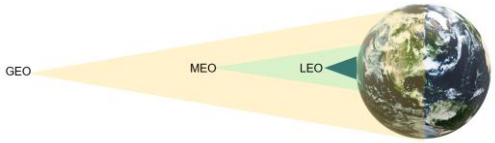
- Space Domain Ecosystem
- Definition of Space EW
- Orbits & Segments
- Satellite Communication Overview
- Offensive EW
- Defensive EW
- Examples of operational Space EW systems
- Technologies for Space EW
  - Link Budgeting & Link monitoring
  - Interference Hunting
  - Signal Generation, Analysis & Power Measurements
- Conclusion

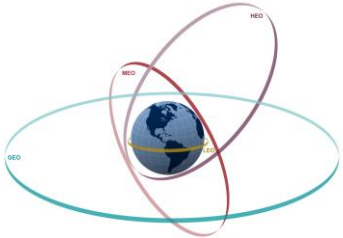


SPACE DOMAIN ECOSYSTEM



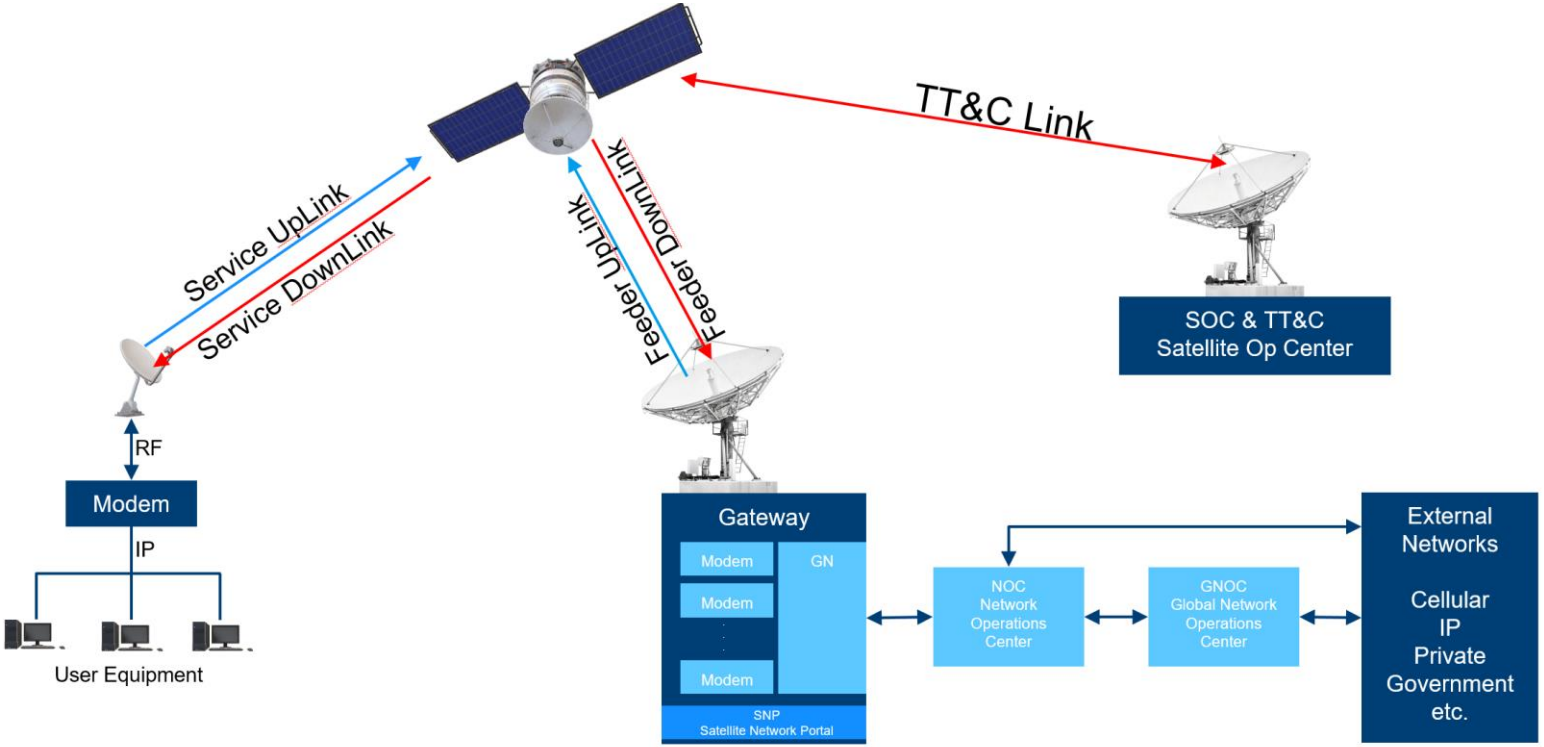
GEO, MEO, LEO,HEO OVERVIEW



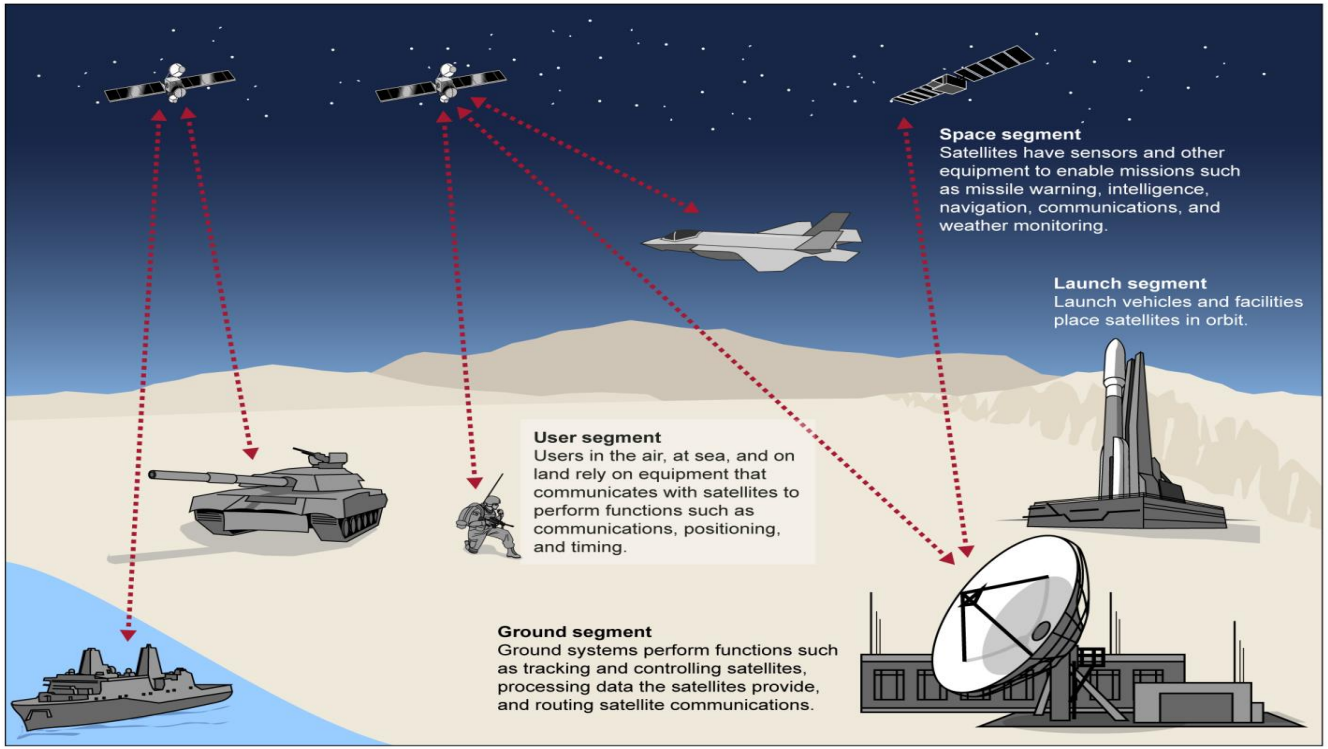


Orbit	Distance (Miles)	Advantages	Disadvantages	Example
LEO	1,200	• Global Coverage • Low latency	• Traffic switching between satellites • Large numbers of satellites needed for full coverage	StarLink, Iridium
MEO	1,200 – 22,000	• Global Coverage • Predicable Locations	• Traffic switching between satellites	GPS, Galileo, SpaceLink
HEO	25,000 at Apogee	• Polar Coverage • Lower # of Satellites	• Traffic Switching between satellites • Variation in distance/coverage • Radiation in Van Allen Belt • Variable Latency	SirusXM QZSS
GEO	22,000	• Stationary Ground Equipment • Can cover 1/3 of the Earth with a single satellite	• Limited polar Coverage • Large signal path loss • Large Latency	DirecTV MUOS AEHF

BASIC SATELLITE COMMUNICATION



SEGMENTS



Source: GAO analysis of Department of Defense (DOD) documentation. | GAO-20-80

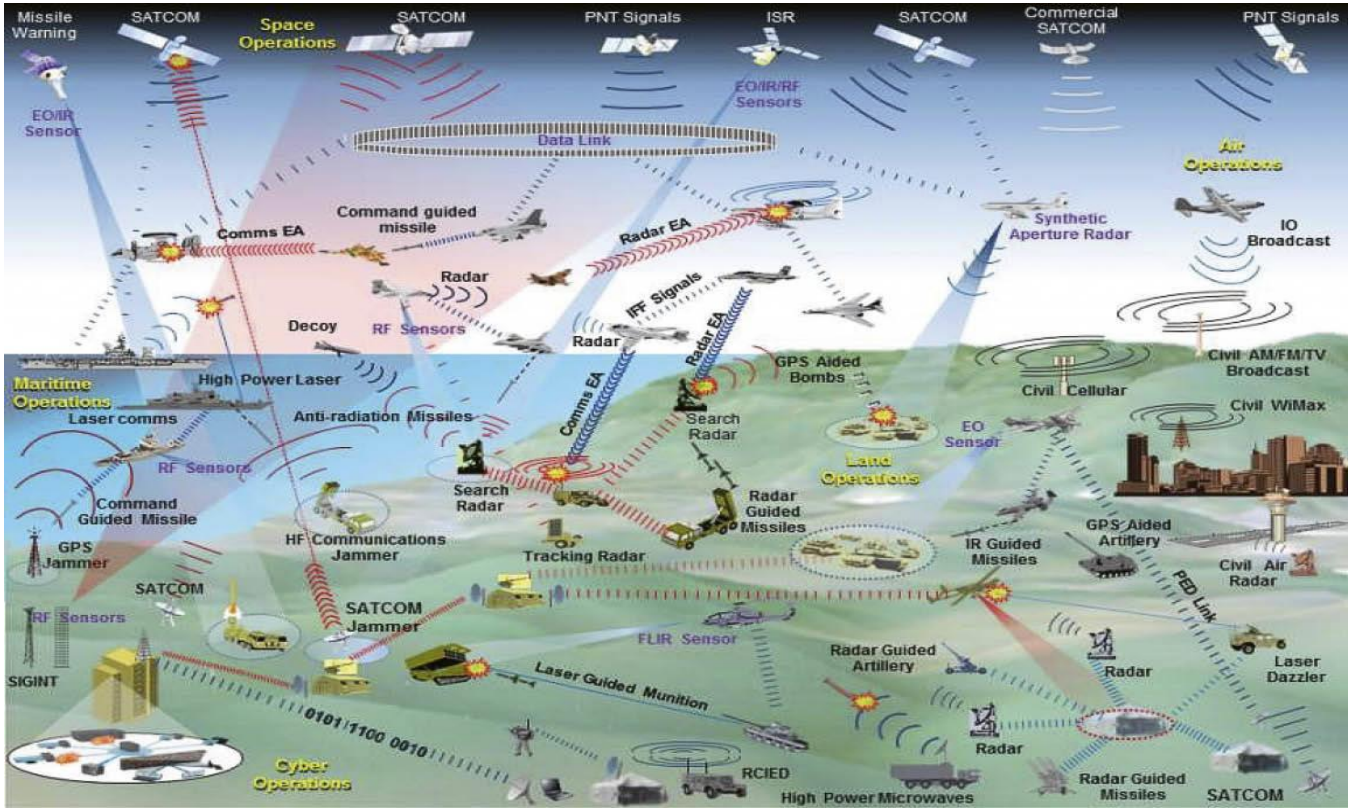
EW OVERVIEW

- EW is **any action involving the use of the electromagnetic spectrum** (EM spectrum) or directed energy to control the spectrum, attack impeded an opponent. The purpose of electronic warfare is to deny the opponent the advantage of—and ensure friendly unimpeded access to—the EM spectrum

- EW Comprises 3 main areas:
  - **Electronic Attack**
    - Actions taken to prevent or reduce an adversary's effective use of the EMS through the use of electromagnetic energy
  - **Electronic Protect**
    - Actions taken to ensure effective friendly use of the EMS despite the adversary's use of electromagnetic energy
  - **Electronic Support**
    - Actions taken to search for, intercept, locate, record, and analyze radiated electromagnetic energy for the purpose of exploiting such radiations in support of military operations

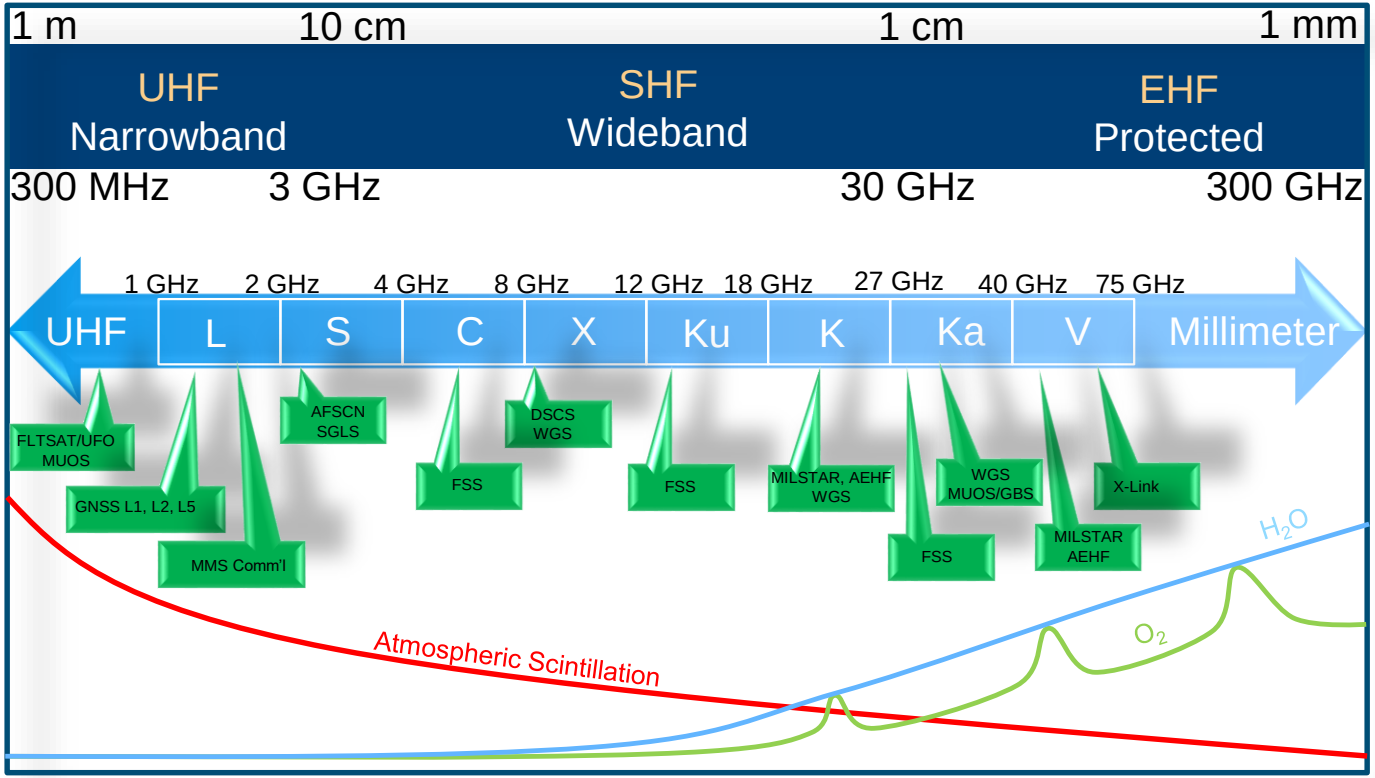
- Space is just another EW domain
  - Traditional domains include land, sea and air
- Space EW is most commonly associated with satellites and their communication links

IW IS A COMPLEX AREA



Source – Electronic Warfare, the forgotten discipline, Commander Malte von Spreckelsen, DEU N, NATO Joint Electronic Warfare Core Staff

MILITARY SATCOM IN THE EMS



OFFENSIVE SPACE EW

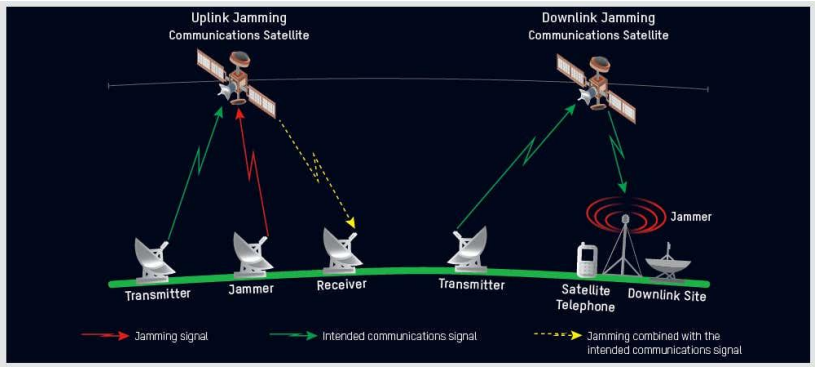


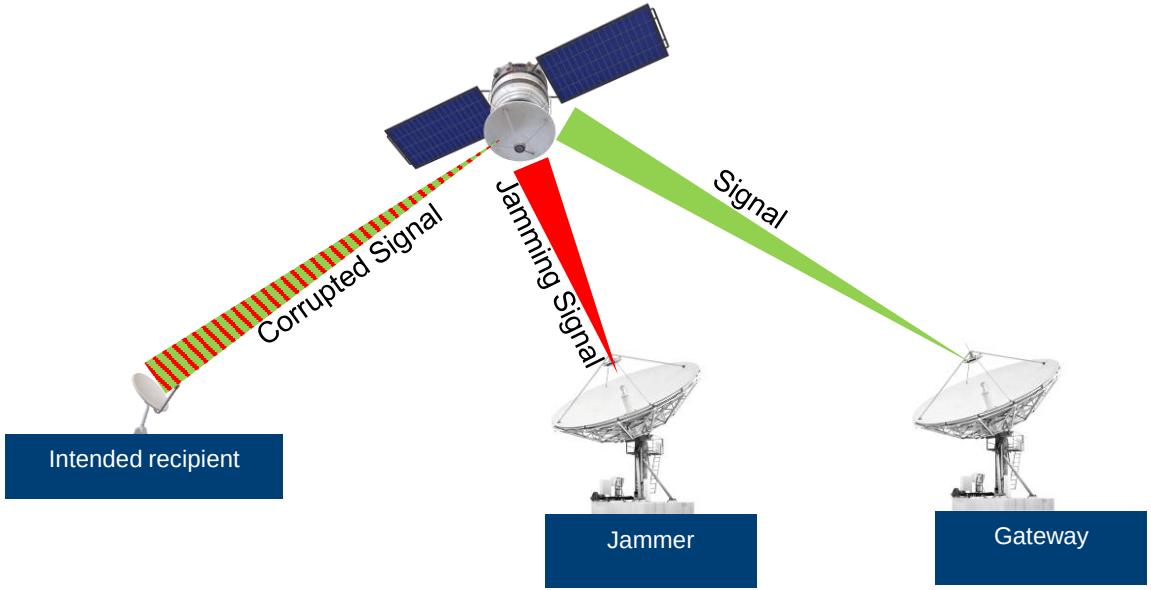
Image – Defense Intelligence Agency

- Electromagnetic Attack
  - Jamming actions against uplink
  - Jamming actions against downlink
  - Jamming actions against crosslink (satellite to satellite)
  - Jamming actions against TTC Link
  - High Power Electromagnetic Energy – disable or destroy satellite

- Optical Attack
  - Laser – Dazzle CCD or CMOS imaging sensors on reconnaissance satellites
  - Laser – Damage CCD or CMOS imaging sensors on reconnaissance satellites
  - Laser – Damage satellite or subsystems, requires very high power laser

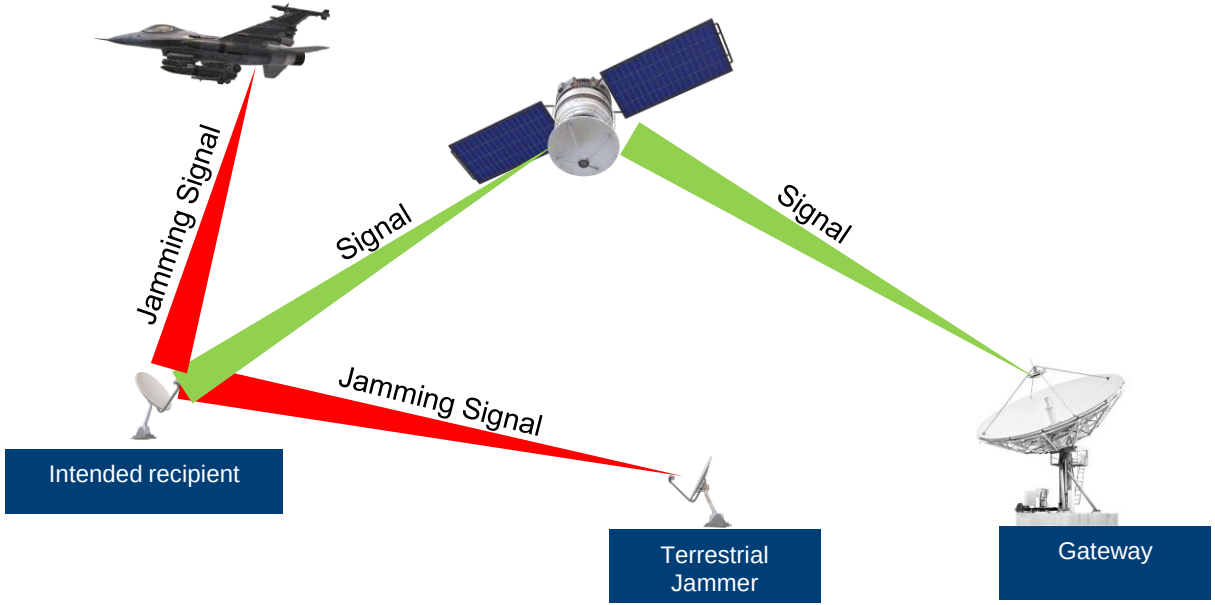
UPLINK JAMMING

- Uplink jamming interferes with the signal going from a ground station or user terminal to the satellite
- An RF signal of the same frequency as the targeted uplink signal is transmitted to the satellite, aiming to limit the satellite transponder from differentiating between the jamming signal and the actual signal
- Uplink jamming requires significant RF power to reach satellite transponder
- Uplink jamming degrades the signal for all recipients



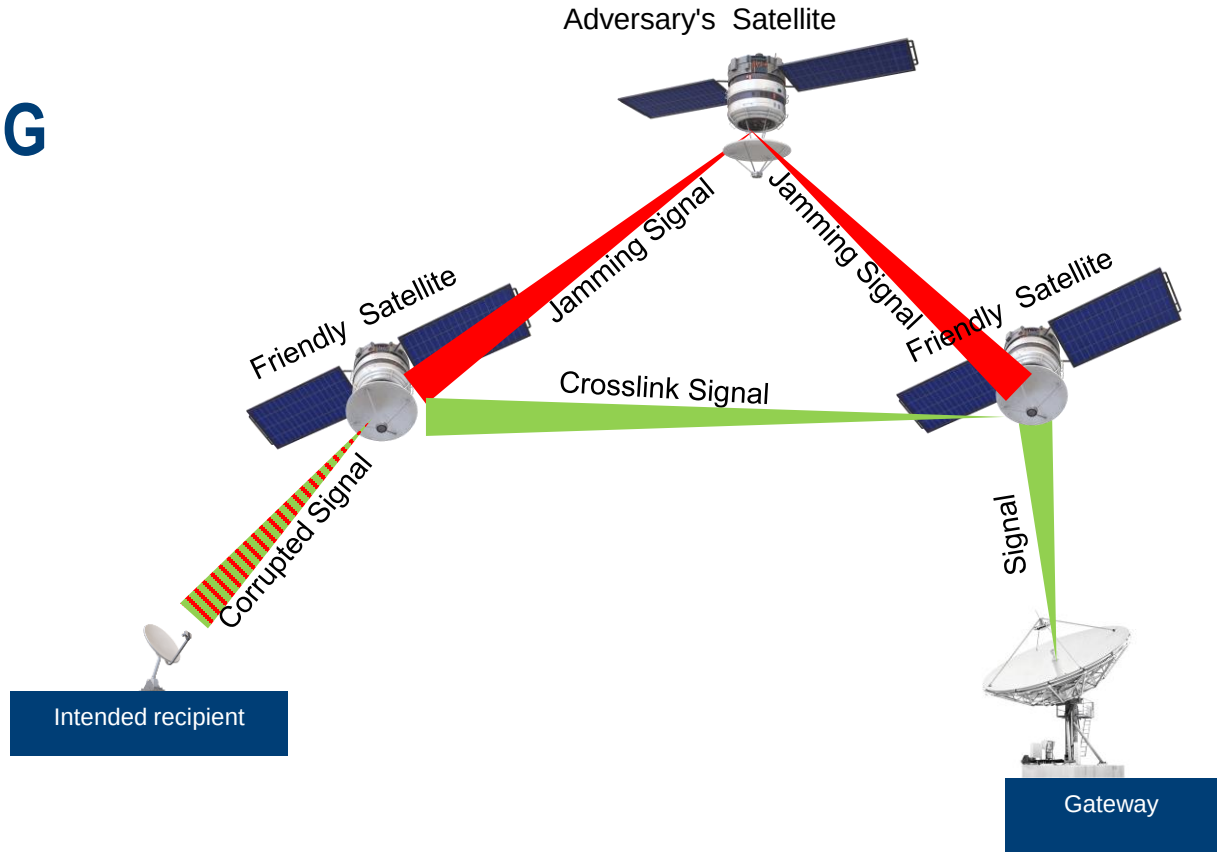
DOWNLINK JAMMING

- Downlink jamming disrupts transmissions sent from the satellite to ground-based or airborne receivers using RF signals that mimic the frequency of the downlink signal
- It inhibits ground users from receiving transmissions from the satellite and RF jamming power can be relatively low
- Downlink jammer may be terrestrial or airborne
- The downlink jammer needs line of sight of the intended receiver
  - Could be problematic in a conflict zone



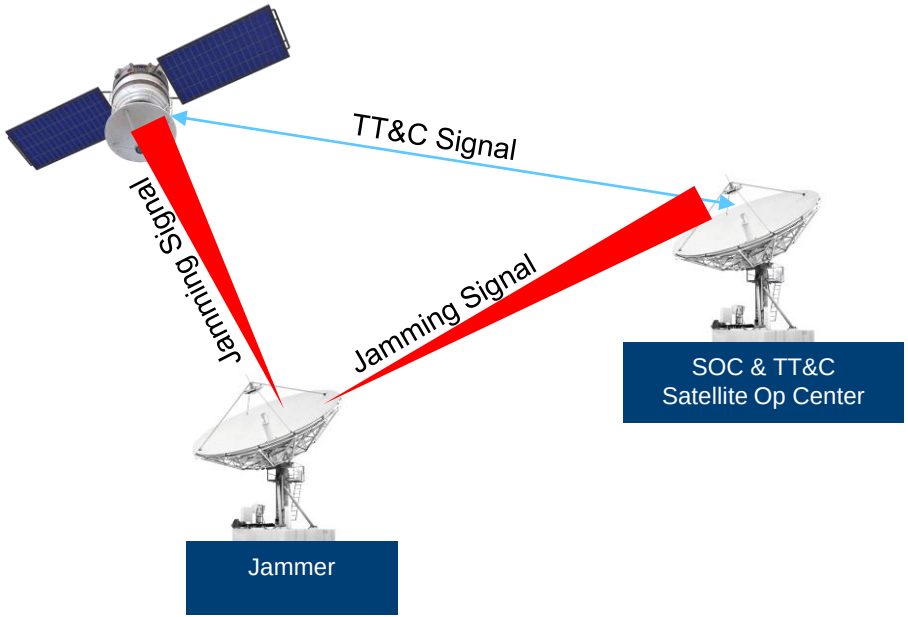
CROSSLINK JAMMING

- In crosslink jamming, an adversary's satellite is positioned such that it can jam the crosslink/relay signal between two friendly satellites
- All satellites need to have line of sight of each other
- Phased array antennas can limit the effectiveness of an adversary's jamming signal
- The crosslink signal could be RF but could also be an optical link
- Jamming of optical links is considered more challenging
- Positioning of adversary's satellite can be difficult to achieve in a timely manner



TT&C JAMMING

- Telemetry, Tracking & Command (TT&C) signals can be jammed or spoofed by an adversary
- TT&C jamming can either be against the ground based Op center or the receiver on the satellite
- The effects of jamming TT&C can be catastrophic, resulting in deorbiting of the satellite, or movement from the intended orbit
- TT&C jamming can also result in communication failure due to loss of timing and control signals
- Spoofing of TT&C is more challenging as the link is encrypted
- Ground based jamming of the TT&C link needs Line Of Sight (LOS) to the op center and uses lower power
  - Can be challenging to be LOS to adversary's op center
- Ground based jamming of the TT&C link on the satellite needs line of site to the satellite and higher power



SPACE-BASED ANTI-SATELLITE OPERATIONS

- Space-based A-SAT can be based on:
  - High power microwaves that disable or destroy the satellite
  - RF jamming
  - High powered lasers that dazzle, disable or destroy the satellite
  - Chemical sprays that disable the satellite
  - Robotic kill vehicle that can damage the satellite through kinetic methods
  - Robotic mechanisms that can capture another satellite

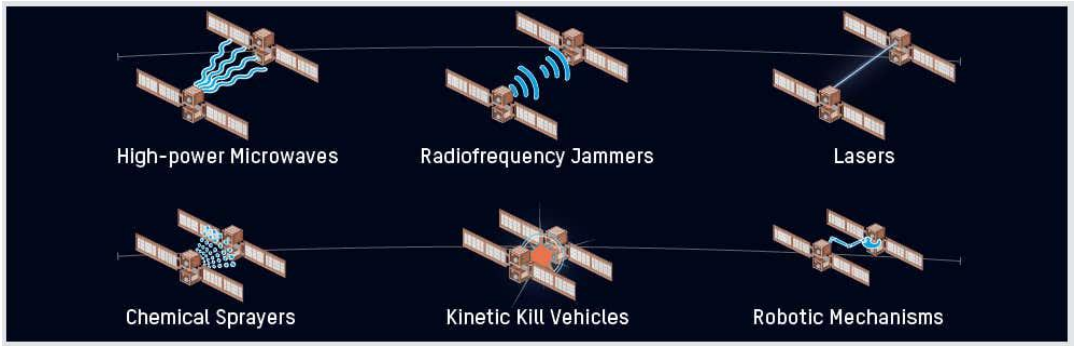


Image – Defense Intelligence Agency

OFFENSIVE SPACE EW

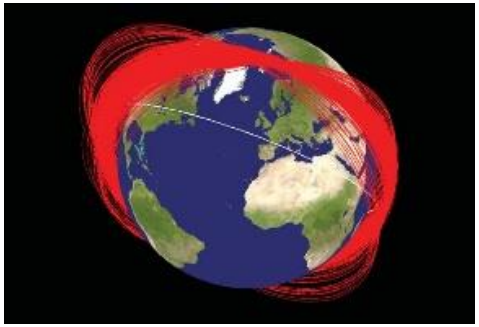


Image - NASA Orbital Debris Program Office - http://www.orbitaldebris.jsc.nasa.gov/newsletter/pdfs/ODQNv11i2.pdf

- Kinetic Attack
  - Direct Ascent Anti-Satellite (ASAT) Missiles
    - Ground launched missile is targeted towards satellite where it either collides with the satellite (hard to do) or detonates close to target
  - Co-Orbital ASAT Missiles
    - Space based weapon is positioned in a similar orbit, maneuvered close to target and detonated

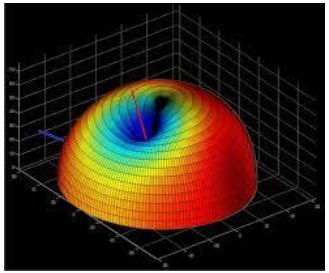
- Kinetic attack is not usually preferred as it leads to space debris that compromises other space vehicles including friendly and neutral assets
  - In 2007 China launched a DF-21 multi-stage ballistic missile from the Xichang Satellite Launch Center against a Chinese FY-1C polar orbit weather satellite weighing 1,650 lbs
  - The DF-21 was traveling at 8 Km/s or ~17,000 MPH
  - The destruction of the FY-1C lead to 10,000 pieces of debris, of which more than 2,800 are still in orbit

CYBER OFFENSIVE

- SATCOM systems are primarily tasked at moving data on a network from one place to another
- Offensive Cyber employs the idea that you can take action through the use of those networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves
- Primarily related to the ground segment of network operations, but could include TT&C links
- Primary types of cyber offensive attacks include
  - Computer Network Exploitations (CNE) compromise the network to which a ground station is connected to through poorly configured or vulnerable technologies and phishing
  - Backdoor attacks through cloud infrastructure
  - Data corruption either at-rest or during communication
  - Supply chain attacks – malware inserted into software, tools and common components
  - Unpatched, outdated or legacy COTS software
- Can also include misinformation, disinformation etc.

NAVIGATION WARFARE

- Navigation Warfare (NAVWAR) are deliberate offensive and defensive actions to assure friendly use of, and to prevent an adversary's use of positioning, navigation and timing information
- Most commonly applied to GNSS/GPS signals
- NAVWAR is mainly concerned with jamming and spoofing ground assets
- Mitigation
  - Monitoring and AI/ML to detect jamming/spoofing
  - Alternate Position, Navigation & Timing when GNSS/GPS unavailable
  - Hold-over clocks to keep timing
  - CRPA antennas to minimize ground-based jamming
  - DoD & friendly nations can use Military GPS User Equipment (MGUE) that utilizes GPS M-code to detect jamming & spoofing
  - GPS Block-3 satellites can use beam forming to increase S/J by +20dB to spot points on earth



OPERATIONAL CHALLENGES IN OFFENSIVE EW

- In a terrestrial jamming scenario, the ideal situation is to position the jammer close to the target
  - In a space environment, this is not possible
  - You cannot control the trajectory of a satellite, but it can be predicted
- Getting enough power on target
  - Free space losses and distances involved can lead to large jamming power requirements
    - Received power decreases with the square of the distance ($1/R^2$)
    - E.g. GPS (20,200 km) ~ -182 dB
  - Conversely ground based jamming can be very effective, requiring a lower margin of J/S
- Logistical requirements
  - Need to be physically co-located within Line of Sight (LOS) to adversary's ground
    - Problematic in a conflict zone
    - Jammer can easily be geolocated & eliminated with kinetic effects
- Obtaining actionable intelligence on adversary's assets is always challenging

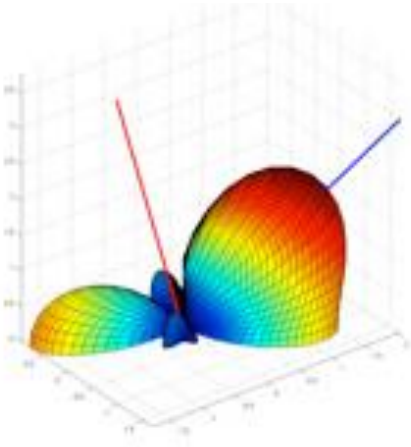
DEFENSIVE SPACE EW

- Mitigation of jamming
  - Phased Array antennas using space-time adaptive processing to form nulls against jamming
    - Phased array antennas & beam steering can provide spot focus of RF power on a specific area
      - e.g. BLK 3 GPS satellites and provide an addition 20dB of power to any point on earth to mitigate jamming – “Regional Military Protection”
  - Detect & Destroy
    - Geolocate and counter to ground based jammer
  - Detect & Decoy
    - For ASAT Missiles it may be possible to deploy IR, RF to jam terminal guidance
  - Employ frequency agile schemes
    - Harder to jam a wideband frequency hopping signals
  - Cryptography
    - Utilization of cryptographic techniques to detect degradation & corruption of signal & data
    - Limits intercept by 3rd parties

PHASED ARRAYS

- Phased arrays can be used to mitigate the effects of jamming
  - Enables directionality of antenna array through electronic steering of the signal
  - Energy from the separate elements add together to increase the far-field power in a desired direction and suppress radiation in undesired directions
  - Reduces effectiveness of interference outside of the main lobe on receiver antenna
    - Flat plane arrays give high immunity to interference at right angles to the plane
- Imperfections such as side lobes will still allow some amount of off-beam transmission & reception
- Directional antennas are still useful!

Beamforming towards a particular satellite



DEFENSIVE SPACE EW

- Jamming Mitigation
  - Air relay
    - Avoid ground based jamming by utilizing intermediate high-altitude relay aircraft or UAV
    - UAV mesh relay
    - Can link to airborne asset in a completely different geographical direction and different frequencies
  - Space Relay
    - Avoid ground based jamming by utilizing secondary relay satellite
    - Utilize photonic satellite-to-satellite links to mitigate against RF effects
      - Narrow beam makes jamming difficult
- Cognitive techniques
  - One of the major challenges is to identify that you communication link is degraded
  - Requires specific link monitoring, spectrum sensing and quality of service measurements
  - Cognitive & machine learning can be applied to build a library of threats
  - Once threats are understood by the AI system, mitigation schemes can be developed & deployed

COUNTER COMMUNICATION SYSTEM (CCS)

- Deployable ground-based system that is used to jam adversary's SATCOM
- Utilizes Modular Open Standard Architectures (MOSA)
- Operates across C, Ku & X-bands
- Primarily targets are geostationary communications satellites

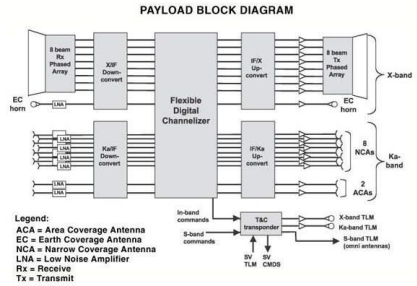
Image – USAF

OPERATION SILENT SENTRY

- System started as a spectrum analyzer and parabolic dish
- Reponses to Iraqi attempts to jam SATCOM & GPS during Operation Desert Storm
- Deployed in Qatar & in other undisclosed locations
- Utilizes Rapid Attack Identification Detection Reporting System (RAIDRS)
  - Provides near real-time detection, characterization, geolocation & reporting of RF interference signals

Image – USAF

MAJE & WGS

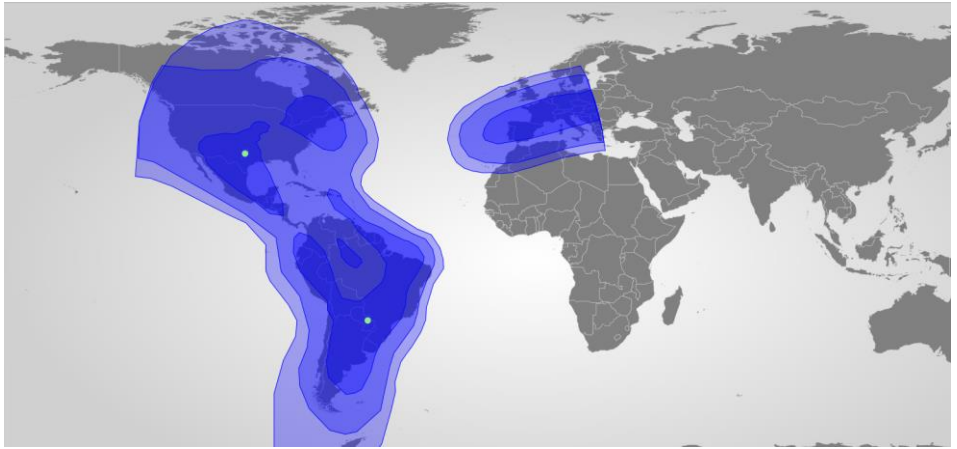


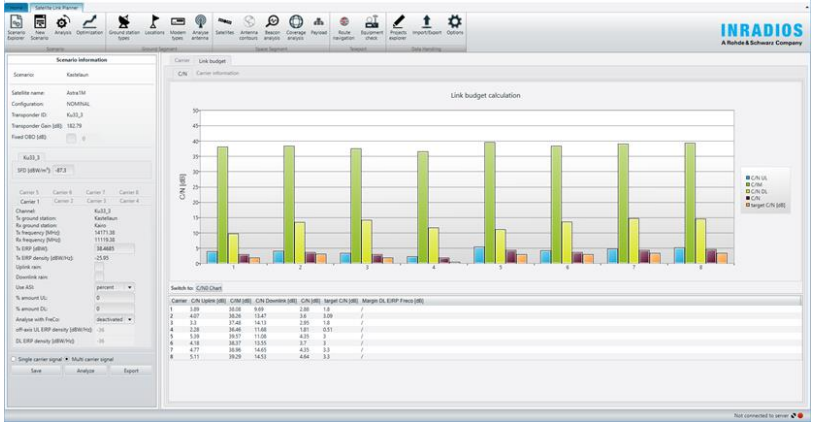
Images: Boeing

- MAJE – Mitigation & Anti-Jam Enhancement
  - Upgrade to Wideband Global Satcom (WGS)
    - X-band (7.9 gigahertz/GHz to 8.4GHz uplink/7.25GHz to 7.75GHz downlink)
    - Ka-band (26.5GHz to 40GHz uplink/18GHz to 20GHz downlink)
    - 4.875 GHz of IBW
  - Software and hardware upgrades for the Army-operated Global SATCOM Configuration Control Element (GSCCE) ground system
  - Performs detection, identification, geolocation and mitigation of unwanted RF interference on the WGS satellites
  - Jamming geolocation, beam forming & adaptive modulation techniques are employed

SATELLITE LINK PLANNER

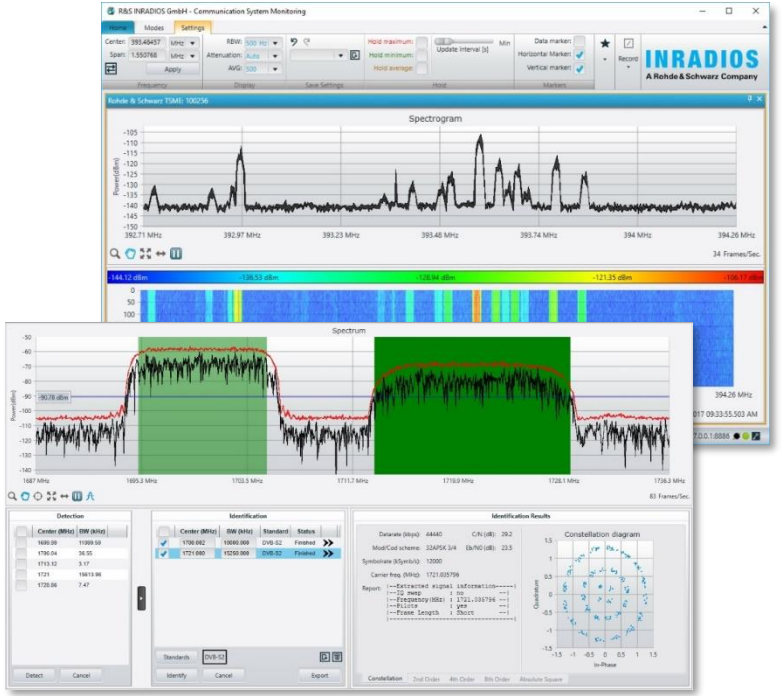
- Planning of satellite links in all bands
  - C-, X-, Ku- and Ka-band
- Planning of satellite links for
  - Point-to-point connections
  - VSAT networks
  - LEO constellations
- Support of scenarios with mobile terminals
- Analysis and optimization of complex setups
- Open interface to monitoring & control system





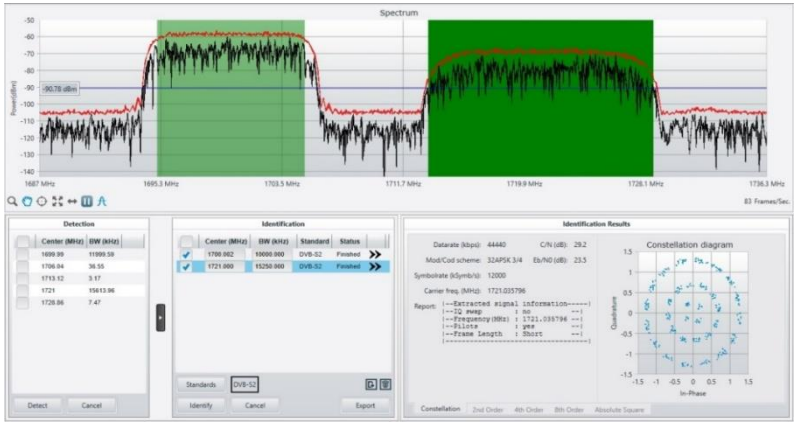
COMMUNICATIONS SYSTEM MONITORING

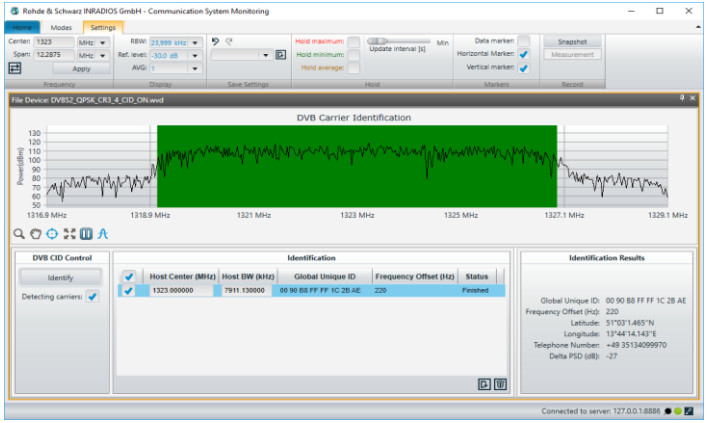
- Spectrum scanning and carrier identification
- Continuous carrier monitoring
- Classification of various satellite standards
- Distributed server-client architecture
- Support of various R&S Analyzers and Sensors
  - Including MSR-4, FSW & SMBV100A Analyzers



SIGNAL ANALYSIS

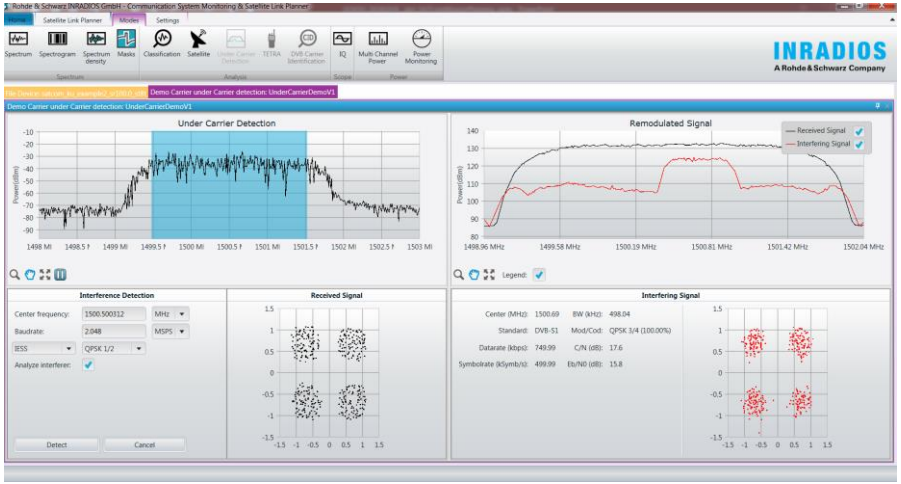
- Automatic detection of carriers in the spectrum
- Visualization of constellation diagrams and signal parameters
- All common types of modulation supported
  - QPSK, 8QAM, 8PSK, 32APSK, etc.
- All common satellite standards supported
  - DVB-S, DVB-S2, IESS, etc.
- Bursted transmissions supported
  - e.g. VSAT reverse channels
- DVB Carrier ID
  - Detection of PCMA/Carrier-in-Carrier
  - Autonomous detection and identification of CID for DVB-S and DVB-S2 signals
  - Continuous spectrum scanning to identify all CID in a certain frequency band entirely
  - Clear visualization of CID parameters
    - Global Unique ID, GPS coordinates, etc.





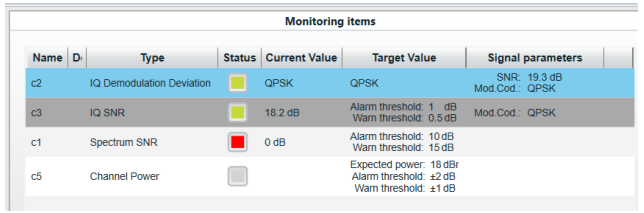
INTERFERENCE HUNTING

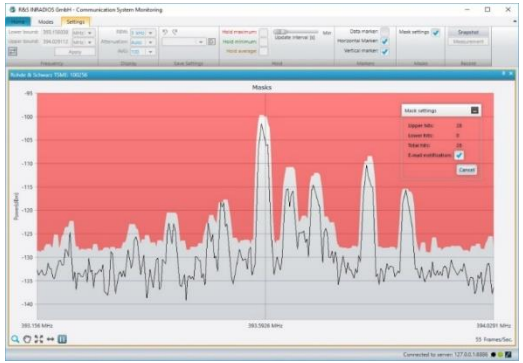
- Detection of Undercarrier Interference
- Source for interference might be:
  - Other satellite signals
  - Terrestrial signals
  - Intentional or Unintentional
- Demodulation, decoding and subtraction of wanted signal
- Underlying interfering signal is displayed and classified



CARRIER MONITORING WITH OR WITHOUT MASKS

- 24/7 Autonomous monitoring
- GUI alarming and email alerts
- Carrier defects:
  - ES/N0 dropping
  - Changes in modulation
  - Carrier off
  - Power levels
  - Etc.





DEDICATED CSM WITH MSR4

- Up to: 4 x Rx: 500MHz .. 3000MHz, each Input with 200MHz IQ BW
- 2 x Tx: 900MHz .. 2500MHz for play-out purposes
- Compact size, industrial standard, for stationary and mobile use (1RU)
- Software Defined / Cognitive Radio SATCOM functionality
- Can run CSM server – no extra computing HW required

SIGNAL ANALYZERS

- **Uses for Signal Analyzers**
  - Track & monitor interference
  - Insight into jamming effects
  - Demodulate signals of interest
  - Streaming interface to record signals of interest
  - Autonomous Monitoring of Uplink & Downlinks

- **Characteristics**
  - Up to 90 GHz Frequency Coverage
  - Up to 8.3 GHz Analysis Bandwidth
  - High dynamic range enables tracking of small signals
  - Integrated preselection to reject out-of-band signals

FSW

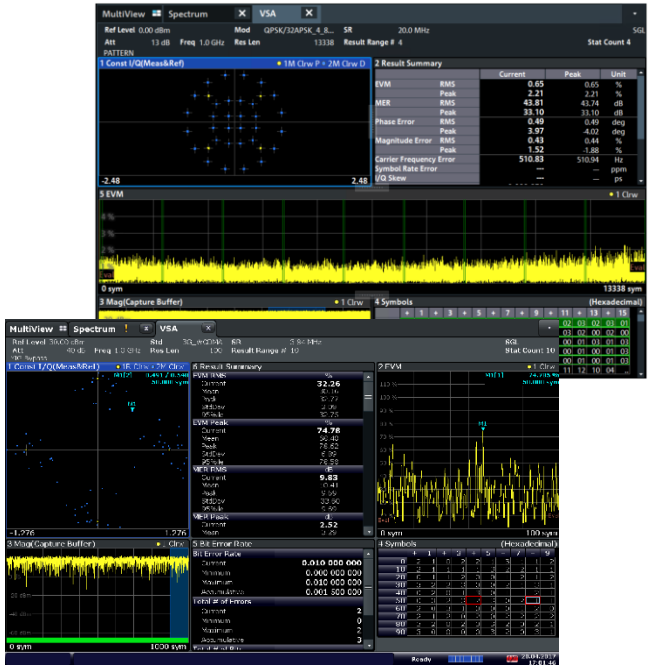
2 Hz → 90 GHz

FPL

5 KHz → 26.5 GHz

MONITORING SATELLITE COMMUNICATIONS LINKS

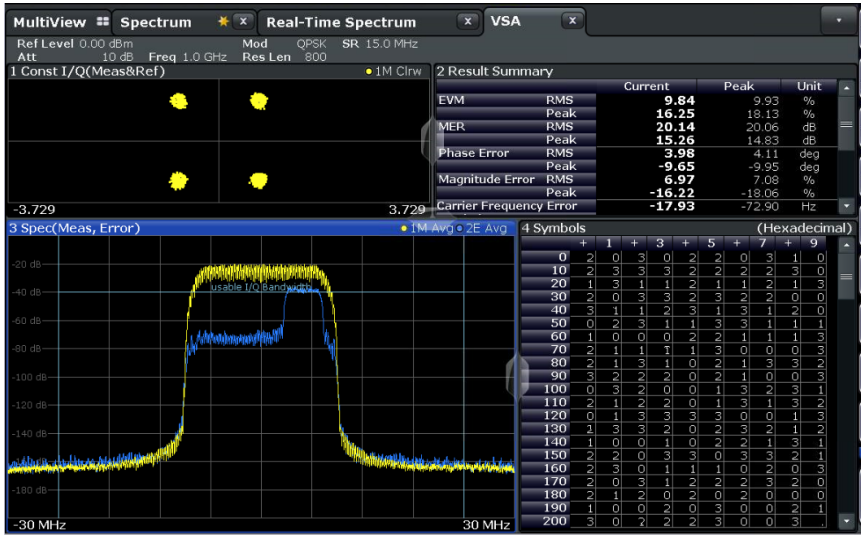
- Vector Signal Analysis down to bit level
- Up to 64k symbols, 8.5 GHz analysis bandwidth
- Display amplitude, frequency, phase, I/Q, eye diagram, phase or frequency error, constellation & vector
- DVB-S2X Measurements
  - Measurement of raw bit error rate (BER) on PRBS data up to PRBS23
  - Frame detection
  - Demodulation of header and payload parts of the signal
  - QOS & BER measurement with user-defined bit sequences
  - Multi-carrier analysis



INTERFERENCE MEASUREMENTS

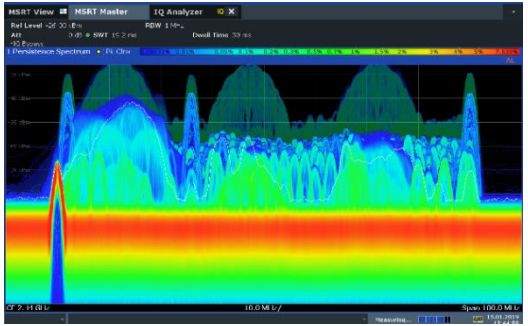
- **Carrier in Carrier Measurement**
  - The error spectrum (blue) clearly shows increased EVM where the interference signal is located
  - The EVM trace has the shape of the underlying carrier

- **Example:**
  - 2 Two QPSK signals overlayed 15 MSym/s QPSK and 5 MSym/s (-20 dB, 5 MHz offset)

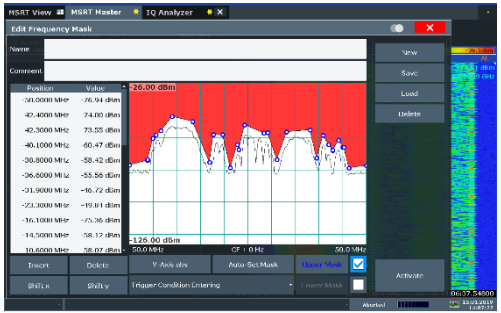


CAPTURING SHORT EVENTS & INTERFERENCE

- Requires Real-time Spectrum Analysis (RTSA) capability
- Requires dedicated fast processing and triggering
- Probability of Intercept (POI) is key a metric
  - FSW will capture signals longer than 0.46us at 800MHz of BW
- Flexible triggering is crucial to capture these short-duration events

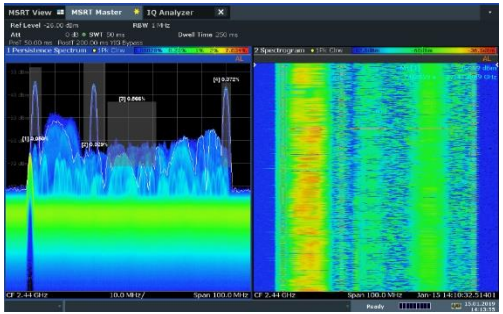


Frequency Mask Trigger



Trigger on any signal in mask area
Upper and lower masks possible

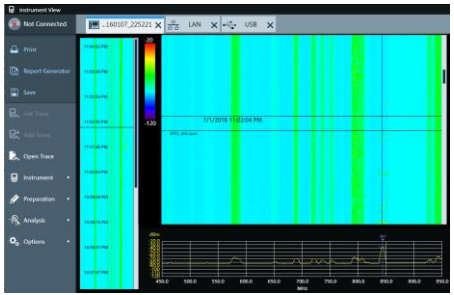
Probability Mask Trigger (up to 4 zones)



Trigger based on signal probability exceeding threshold within user defined area

HANDHELD INTERFERENCE HUNTING

- Handheld Spectrum Analyzer - R&S FPH
  - 5 KHz – 44 GHz
  - 6 hour battery life
  - Solid RF performance - DANL: typ. –163 dBm ,TOI measurement: +10 dBm
  - Interference hunting & signal strength with geolocated maps
  - Unique, high performance wideband directional antennas
- SATCOM Monitoring
  - Long term spectrum recording & logging
  - Monitoring Uplink & Downling bands for post analysis
  - Attended or unattended options
  - Automated measurement scripts with setup wizard
  - Instrument View SW helps to easily network instruments
  - Instrument View SW can help generate reports & document link outages



SIGNAL GENERATORS

SMW200A

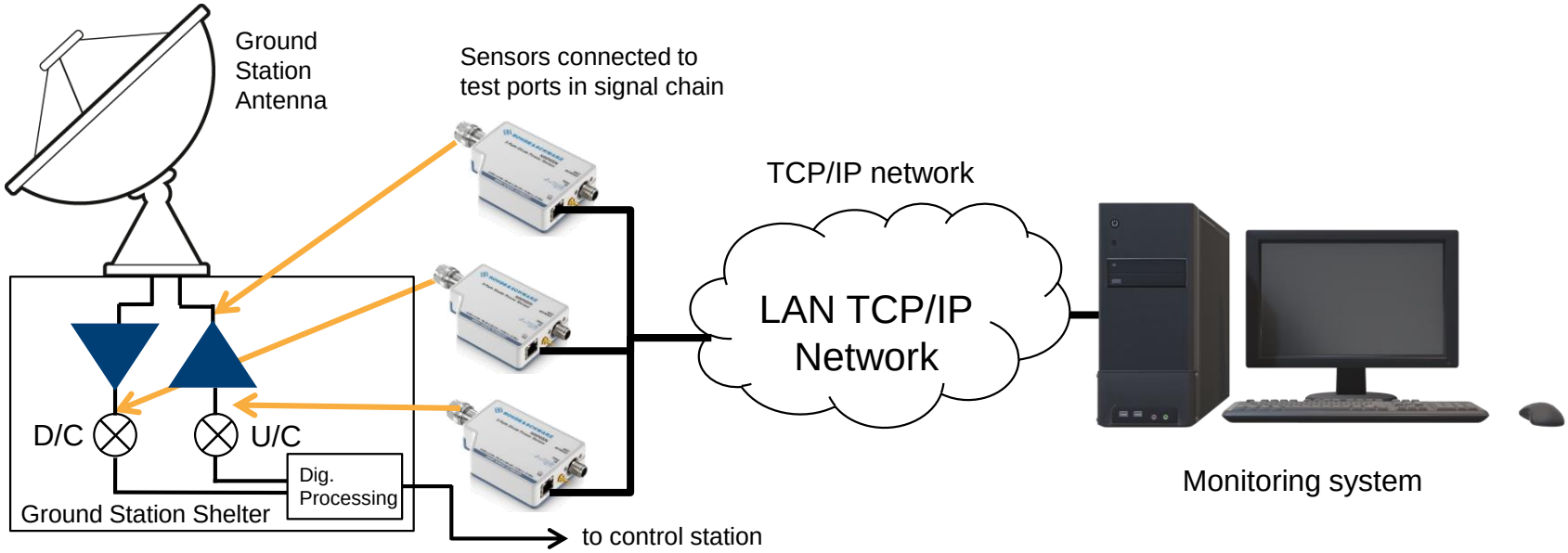
SMBV100B

- **Uses for Signal Generators**
  - Reference payload signal
  - Create realistic RF environments
  - Generate realistic jamming signals to measure effect on space vehicle during development
  - Generate wideband jamming signals with generator & solid-state power amplifier
  - 2 channels in single box - signal & interferers during simulation
  - Generate non-standard waveforms for proprietary modulation schemes

- **Characteristics**
  - Up to 67 GHz frequency coverage
  - Up to 2 GHz of generation bandwidth
  - Generation of complex modulated signals
  - High dynamic range

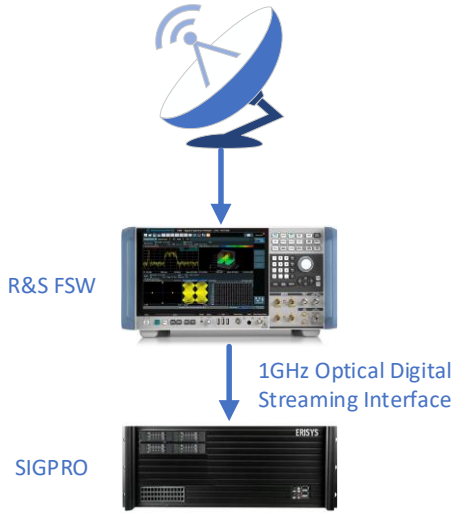
POWER LEVEL MONITORING OF SATELLITE GROUND STATIONS

- Remote, autonomous monitoring of RF signal levels via LAN controlled power sensors
- Bridging of longer distance from test point to control station



RF RECORDING - INTEGRATED RECORD, ANALYSIS & PLAYBACK SYSTEM (IRAPS)

- Turnkey system for RF recording in the lab & field
- Triggered recording of anomalies in Uplink, Download & TT&C
- Consists of
  - FSW Spectrum Analyzer
  - SigPro processing system
  - ZoomOut Application software
- Recording of up to 6 hours at full bandwidth
- Up to 1GHz of bandwidth
- SigpPro supports removable storage
  - Recordings can be taken back to lab for analysis
- Optical link enables large distance between FSW & SigPro
- Portable options for field measurements



SUMMARY

- R&S provides deep domain knowledge in EW, Communications and Satellite payload test to enable customers to solve their most challenging problems.

- We provide a set of targeted solutions for:
  - Link Modelling, Planning & Simulation
  - Communication Link Monitoring
  - RF Signal Analysis
  - RF Signal Generation
  - Power Measurement
  - Long-terms RF recording & visualization
  - Representative signals sets for all segments
    - Including environmental and jamming effects

THANK YOU FOR YOUR TIME

REFERENCES

- Cognitive Anti-jamming Satellite-to-Ground Communications on NASA's SCaN Testbed
  - S, Jayaweera, S. Feng, D. Mortensen, A. Holland, M. Piasecki, M. Evans, C. Christodoulou
  - https://ntrs.nasa.gov/api/citations/20190001548/downloads/20190001548.pdf
- WGS
  - Dr. Paul LaTour, Lieutenant Colonel, United States Air Force (USAF)
  - http://www.satmilmagazine.com/story.php?number=1909521651
- Rapid Attack Identification Detection and Reporting System (RAIDRS)
  - https://www.globalsecurity.org/space/systems/raidrs.htm
- Silent Sentry
  - Staff Sgt. Alexandre Montes, 379th Air Expeditionary Wing Public Affairs
  - https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/885152/operation-marks-10-years-of-interstellar-combat-support-protecting-centcoms-sat/
- Space EW
  - Massimo Annulli, EURODASS Consortium
  - https://www.emsopedia.org/entries/space-ew/

SOURCES

- Defense Intelligence Agency – US Security Challenges In Space
  - http://www/dia.mil/Military-Power-Publications/
- Declassified US national archives
  - https://www.archives.gov/files/declassification/iscap/pdf/2014-033-doc01.pdf
- **Electronic Warfare – The Forgotten Discipline,** Commander Malte von Spreckelsen, DEU N, NATO Joint Electronic Warfare Core Staff, Joint Airpower Competence Center
  - https://www.japcc.org/electronic-warfare-the-forgotten-discipline/
- **Pierluigi Paganini, Infosec**
  - https://resources.infosecinstitute.com/topic/hacking-satellite-look-up-to-the-sky/

FAIR USE STATEMENT

Disclaimer

Images used in this document are copyright their respective owners. No endorsement by Rohde & Schwarz of any company or product is implied or given. No endorsement of Rohde & Schwarz products by any company or product is implied or given.

Fair Use Act - Disclaimer

This document may contain copyrighted images, the use of which may not be specifically authorized by the copyright owners. In accordance with the educational and informational nature of this document, such material is made available to the reader to improve their comprehension and understanding of the Space EW market and the challenges and technologies used therein. Such material is used in the belief that it constitutes 'fair use' of any such copyrighted material as provided in U.S.C. 17 § 107. This document is distributed without profit, for research and educational purposes.

For further information on fair use legislation, please visit https://www.govinfo.gov/app/details/USCODE-2010-title17/USCODE-2010-title17-chap1-sec107. If you wish to use copyrighted material from this document for your own purposes that do not include fair use, you **must** obtain the permission of the original copyright owner, that permission is specifically not implied or given by the author of this document.

Removal of copyright material

Requests for the removal of copyright material may be made to tim.fountain@rsa.rohde-schwarz.com