dualos

Military C5ISR  Acronyms

Alphabet Soup

Anyone that interacts with our Military already knows they have their own language, and that ***they love using acronyms***. This paper isn't going to list every acronym, just the most common ones used in **C5ISR**.

So, let us start with this as our first acronym:

- **C5ISR** – Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance, is the framework used to describe the systems and operations in gathering, processing, and distributing information to support decision-making and operations. It builds upon the older and more well-known C4ISR with the addition of the 'Cyber' element to address the importance of cybersecurity in modern warfare.

  C5ISR is the integration of all these elements creating a synergistic effect which assures dominance on the battlefield by providing enhanced situational awareness, faster decision making, more effective actions, improved operational success, and reducing risks.
  - Command – the leadership which sets objectives, assigns missions, and provide guidance
  - Control – the process of managing and coordinating forces and resources
  - Computers – the hardware and software systems used to process and store information
  - Communications – the means to securely transmit and receive information
  - Cyber – the security of all digital systems and networks
  - Intelligence – the collection, analysis, and dissemination of information about threats
    - HUMINT (Human Intelligence) – information obtained from human sources
    - SIGINT – (Signal Intelligence) – intercepted communications and electronic emissions
    - IMINT – (Imagery intelligence) – visual information from aerial and satellite photography
  - Surveillance – the continuous monitoring of areas of interest
  - Reconnaissance – the process of gathering information on a target or area of interest

- **AFC** – US Army Futures Command, is focused on modernizing our Army, via six essential areas:
  - Concepts – develop innovative ideas and approaches for future warfare
  - Experimentation – testing/validating concepts and technologies via simulation/field exercises
  - Integration – coordinating efforts across various parts of the Army and external partners
  - Operational environment – assessing the evolving landscape of the future battlefield and threats
  - Requirements – defining specific capabilities needed to address identified gaps
  - Research – investing in innovative technologies and scientific advancements

- **CANES** – Consolidated Afloat Networks and Enterprise Services, consolidates multiple Warship networks into a single integrated system, simplifying management, and reducing costs

- **CCDC** – Combat Capabilities Development Command C5ISR Center (formerly CERDEC) was created under US Army Futures Command – is the US Army information technologies and integrated systems center headquartered at Aberdeen Proving Grounds, MD. It collaborates with the Army, DoD and other stakeholders to provide C5ISR models, simulated architectures and automated tools in support of requirement definition, design and engineering, manufacturing, and test and evaluation.

- **CERDEC** – Communications Electronics RD&E Center (known now as CCDC)

- **CI** – Counterintelligence, refers to all activities and measures undertaken to protect against espionage, sabotage, and other harmful activities – a crucial component for our National Security

- **CIC** – Combat Information Center, is a crucial dedicated space on Warships or AWACS aircraft that functions as the tactical Command and Control center, essentially the 'nerve center' for information gathering, analysis, and dissemination
  - AWACS – Airborne Warning and Control System, refers to a sophisticated military aircraft with a powerful radar system used to detect and track targets

- **COMSEC** – Communications Security, are measures implemented to prevent unauthorized personnel from accessing sensitive communications and information

- **COTS** – Commercial Off-the-Shelf, readily available hardware/software for sale to the general public

- **CR** – Cognitive Radio, a type of radio that can intelligently sense and adapt to its surrounding RF environment

- **C2** – Command and Control, represents how our military makes operational decisions via the use of five variables: Who, What, When, Where, and How
  - by Who's authority
  - What is required to assure a successful mission (manpower and hardware)
  - When – timeline
  - Where – geographic
  - How – technical elements of mission

- **Cybersecurity** - Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation (DoDI 8500.01)

- **DF** – Direction Finding, is a method for learning the bearings of RF emitters by use of a highly directional antenna along with a display instrument

- **DISA** – Defense Information Systems Agency, is responsible for ensuring the continuous operation and security of global C2 capabilities

- **DISN** – Defense Information Systems Network, is an integrated network, managed by DISA, to provide dedicated point-to-point, switched voice/data, imagery, and video teleconferencing services for all DoD activities

- **DoD** – Department of Defense, includes the Army, Navy, Air Force, Marine Corps, and Space Force – while the Coast Guard falls under the Department of Homeland Security (DHS)

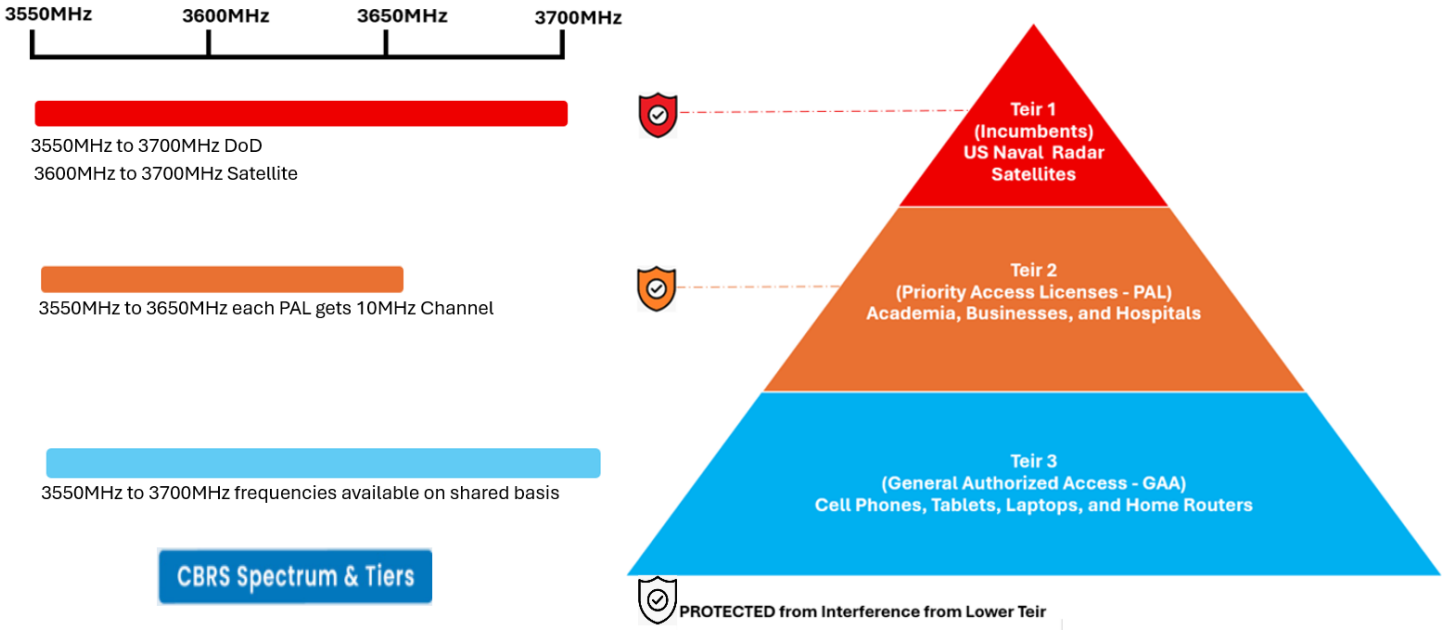
- **DoDD 3222.04** – DoD Directive 3222.04, establishes EW policies

- **DoDD 5100.20** – DoD Directive 5100.20, establishes SIGINT policies in combination with Executive Orders (EO 12333) and National Security Agency/Central Security Service (NSA/CSS Policy 12-3 Annex C)

- **DoDI 8500.01** – DoD Instruction 8500.01, establishes the Cybersecurity Risk Management Framework for DoD Network Systems

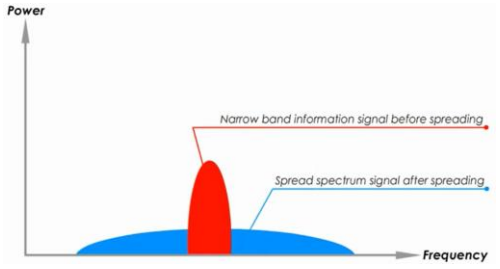
- **DoDISS** – Department of Defense Intelligence Information System, the combination of DoD personnel, procedures, equipment, computer programs, and supporting communications that support the timely and comprehensive preparation and presentation of intelligence and information to military commanders and national level decision makers

- **DSS** – Dynamic Spectrum Sharing, is a technique to maximize spectrum utilization, mitigate spectrum interference, and enable our military to benefit from commercial wireless technologies (like 5G/6G), in areas such as augmented reality (AR/VR), smart bases, and smart hospitals



CBRS Tiered DSS model is one example of how multiple users can coexist over shared frequencies

- **DSSS** – Direct Sequence Spread Spectrum, is a modulation technique that spreads a signal across a wider bandwidth to improve resistance to interference. In addition, Pseudo noise (PN) code is mixed onto the transmitted signal to encode it, at the receiver the encoded signal gets demodulated



  - Narrow band signals are easily jammed or interfered with, to overcome this the operator must increase the output power
  - After spreading, the narrow band signals now occupy more bandwidth, the output power remained the same, but the power density has spread resulting in a lower power profile close to the noise floor, making the signal harder to detect, thus reducing jamming or interference

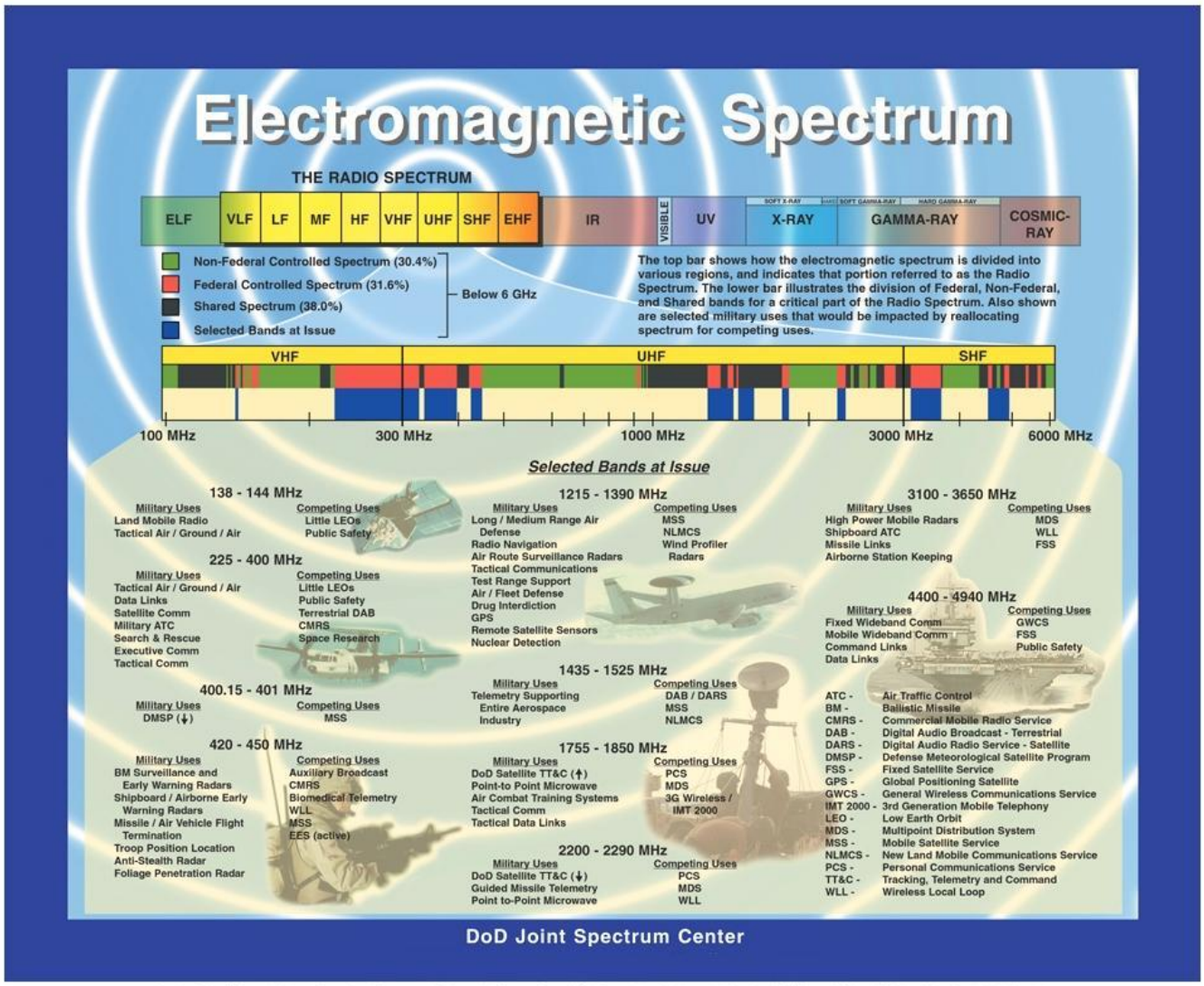
- **ECM** – Electronic Counter Measures, **offensive EW technique** used to disrupt enemy use of the EMS via jamming, deception, or other electronic means

- **ECCM** – Electronic Counter-Countermeasures, **defensive EW technique** designed to mitigate the effects of the enemy's ECM attempts to ensure our forces have continued use of the EMS. Techniques include DSSS, FHSS, LPD, LPI, LPG, Anti-jamming, Advanced Algorithms Filters

- **EMBM** – Electromagnetic Battle Management, is the dynamic monitoring, assessing, planning, and directing of joint EMS operations in support of the mission

- **EMI** – Electromagnetic Interference, is any electromagnetic disturbance – induced intentionally or unintentionally – that obstructs, or otherwise degrades/limits the effective performance of electrical and electronic equipment

- **EMS** – Electromagnetic Spectrum, is the continuous range of all possible frequencies of electromagnetic radiation – the new battlefront



- **EW** – Electronic Warfare, regards your ability to control, exploit, deny, or deceive your adversary's use of the EMS (DoDD 3222.04)
  - EA (Electronic Attack) – offensive use of the EMS to attack your adversaries, by disrupting their ability to communicate, navigate, or use their electronic systems
    - Jamming your adversary's communications and radar systems
  - EP (Electronic Protection) – defensive use of the EMS to protect from your adversaries
    - Using frequency agility to rapidly change your RF signals making you harder to intercept
    - Employing FHSS techniques
    - Implementing sidelobe-blanking to reduce interference from unintentional RF signals
    - Using advanced algorithms and SDR technology for discrimination against electronic threats
  - ES (Electronic Support) – supportive use of the EMS
    - Employing a DF system to pinpoint the location of harmful RF signals
    - IFF – Identification Friend or Foe systems, the use of RF transponders and RF interrogators to distinguish between friendly and hostile entities
    - Using advanced SIGINT technologies to intercept, identify and analyze your adversary's RF communications
    - Using a Radar Warning Receiver (RMR) to detect your adversary's incoming radar signal

- **FHSS** – Frequency Hopping Spread Spectrum, is a method of transmitting radio signals by rapidly changing the carrier frequency

- **LPD** – Low Probability of Detection, is where your enemy's EW systems cannot detect your electronic emissions

- **LPI** – Low Probability of Intercept, whereas your electronic emissions are detected; however, your enemy is unable to gain any intelligence from your emission

- **NOTE:** of the two **LPD** is more critical in tactical scenarios; because if your electronic emissions are not even detected, it makes sense that they also cannot be intercepted

- **LPE** – Low Probability of Exploitation, refers to RF Communication signals designed to be difficult for an unauthorized receiver to exploit
  - ISI – Inter-symbol Interference, intentionally introducing interference between symbols to hinder an unauthorized receiver from accurately estimating the symbols or recovering the bit sequence
  - Noise-Shaping – shaping the RF signal with artificial noise to appear more like noise, thus making it difficult for an unauthorized receiver from demodulating and analyzing

  - Signal Obfuscation – techniques like dirty constellation algorithms to hide the actual RF signal within a background of noise

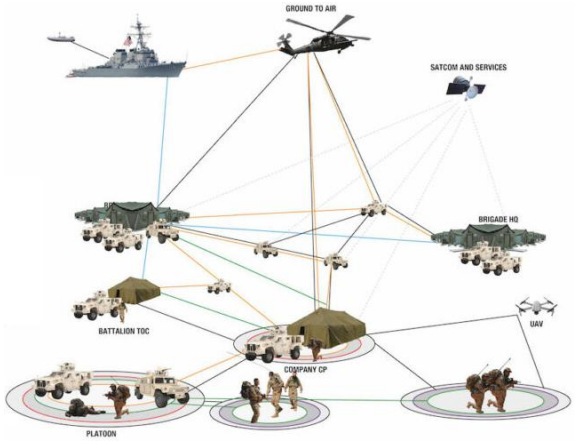
- **LPG** – Low Probability of Geolocation, where it's difficult to determine the location of a RF emitter due to the characteristics of the RF signal or the surrounding environment
  - Signal characteristics – operators can use waveforms with irregular autocorrelation properties to prevent accurate geolocation
  - Surrounding environments – densely populated urban areas can cause signal interference, reflections, and blockage all complicating geolocation. Also, mountainous, hilly, forested, and areas near large bodies of water can complicate geolocation. Atmospheric conditions like solar storms or atmospheric absorption can affect RF signal propagation thus impacting accuracy

- **MACE** – Multi-Access Cellular Extension, is intended to unify commercial wireless to meet military communication requirements, even when a cellular base station is not available

- **MANET** – Mobile Ad-hoc Networks, makes possible independent communication networks between soldiers, vehicles, ships, planes, and headquarters

  MANET supports radio links in operational areas where fixed infrastructure or line-of-sight communications are not available, enabling our warfighters to share info 'anywhere – anytime'

  MANET are self-forming and self-managing, eliminating the need for intensive central management



- **PNT** – Positioning, Navigation and Timing, refers to the capability of determining location, direction, and time by the use of satellites
  - Positioning – uses latitude, longitude, and altitude to determine the location of an object
  - Navigation – uses positioning data to guide/control an object's movement
  - Timing – the ability to acquire and maintain accurate and precise time from a standard (UTC) anywhere in the world
  - GNSS – Global Navigation Satellite System, four major systems (USA, Europe, China, and Russia) with two regional systems (India and Japan)
    - GPS – Global Positioning System, is specific to the USA
    - Galileo is specific to Europe
    - BeiDou is specific to China

  - GLONASS is specific to Russia
  - NavIC – Navigation with Indian Constellation (formerly IRNSS) is specific to India
  - QZSS – Quasi-Zenith Satellite System is specific to Japan
- UTC – Coordinated Universal Time, is the recognized time standard used around the global

- **PTW** – Protected Tactical Waveform, is a frequency-agnostic waveform designed for secure and resilient military RF communications. It provides specifications for: baseband framing, modulation, coding, and security features to ensure data protection and resistance to jamming

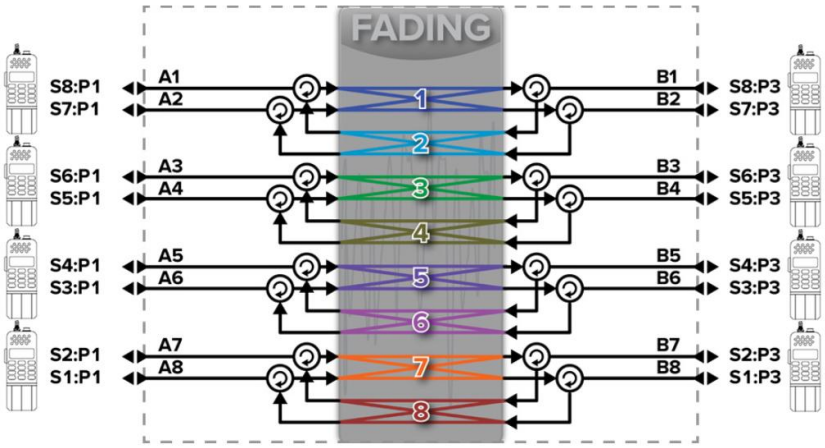
- **RFCE** – RF Channel Emulator , an advanced instrument that accurately replicates the comprehensive noise and spatial conditions of complex RF over-the-air channel propagation. It offers innovative capabilities which enable users to emulate **real-world RF environments in the lab**, making it possible to easily isolate, control, identify performance issues, and make repeatable measurements

Spirent Vertex RF Channel Emulator
supports EW, SIGINT, MESH and Satellite/Aeronautical applications

- User defined **modular**, **scalable** architecture
- RF Input: frequency and waveform agnostic
- Operating Freq: 30MHz to 6GHz
  - Up/Down Converters to extend Op Freq
- Channel BW: 40MHz to 1200MHz
- Doppler Shift: ±4kHz, ±12kHz, or ±2MHz
- Delay: 4msec, or 1sec (0.1nsec resolution)
- Relative Phase: 0° to 360° (0.1° resolution)
  * *Relative Phase accuracy important for* ***Direction Finding*** *scenarios*
- Built-in AWGN: C/N Ratio -40 to +40dB
  Accuracy: ±0.1dB
  Bandwidth: up to 400MHz
  Selectable Modes: C/N, Eb/N, and N

  - Modularity: each RF Module has an independent Local Oscillator (LO) allowing Vertex to support multiple carrier frequencies in one instrument
  - Scalability: Vertex is user defined for a broad range of RF applications, as each RF module offers both two Bidirectional I/O ports and two Uni-directional Outport ports, the user can test basic RF applications – all the way up to complex MESH, large scale MIMO, and Phased Array Antenna applications in one instrument
- HF Upconverters: 300kHz to 65MHz / LO Freq: 125MHz (Conversion Loss 10dB typical)
- mmWave Downconverters, Dual Channel (Conversion Loss 10dB typical):
  - RF Out: 6 to 20GHz / LO Freq: 6 to 20GHz / IF Freq: 1 to 10GHz
  - RF Out: 6 to 30GHz / LO Freq: 6 to 30GHz / IF Freq: 1 to 8GHz
  - RF Out: 24 to 44GHz / LO Freq: 24 to 44GHz / IF Freq: 0.1 to 14GHz

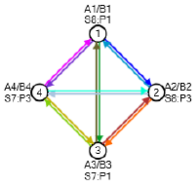
- MESH applications require each RF node to independently communicate with each other. From a RF Channel Emulator perspective this implies that each radio link needs to be emulated with a different fading profile simultaneously, placing heavy demand on the number of RF Antenna ports required, in addition to the internal processor load. Vertex supports up to 16x16 independent channel models in one instrument



MESH Radio Network for Radios with Dual-Antenna

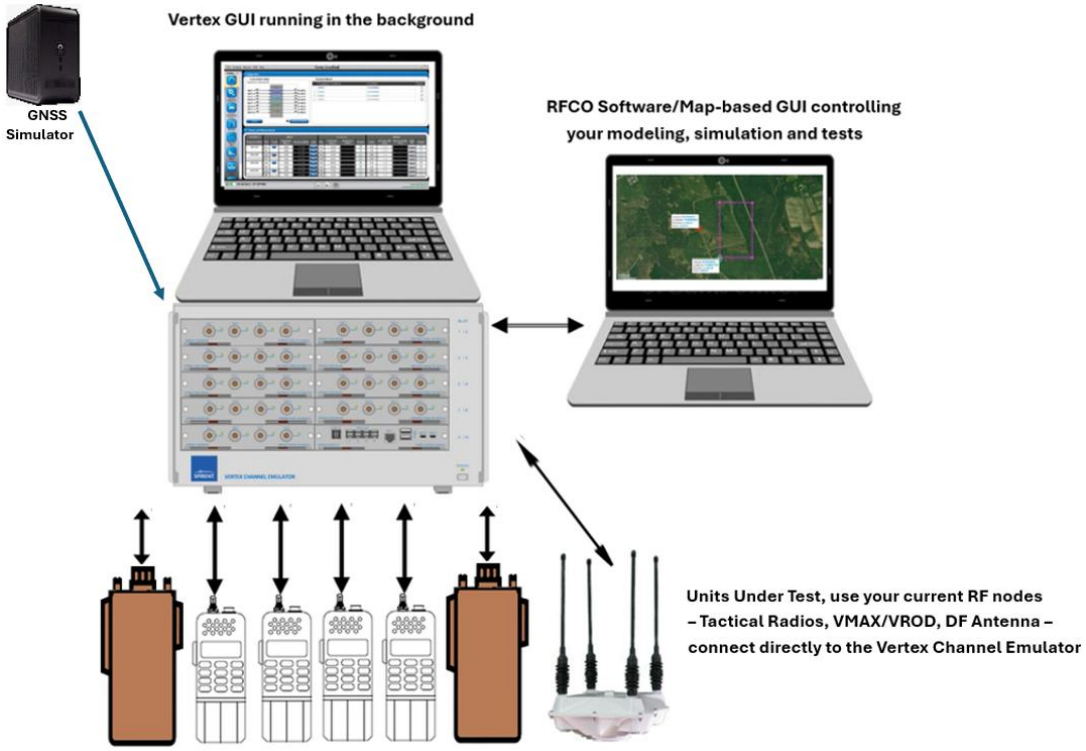
Vertex offers an optional MESH Builder software tool which enables users to quickly set up models and define radio link losses for each node – just 3steps:

1) Choose the number of nodes from the dropdown menu (1 to 16)
2) Define radio link path(s) per node
3) Define radio link loss (0 to -40dB)



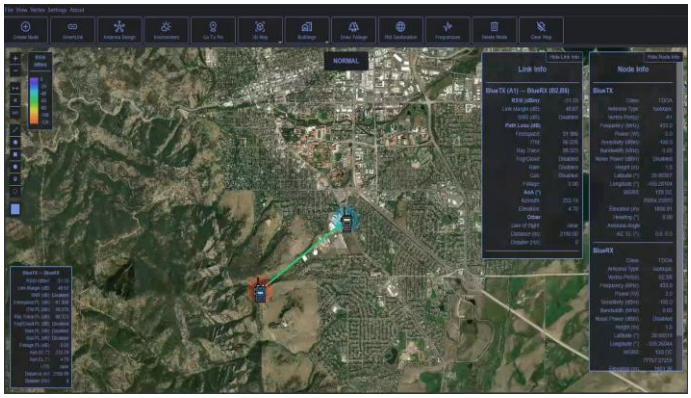
ex: 4-nodes MESH

- **RFCET** – RF Channel Emulator Testbed, is comprised of a (COTS) Vertex RF Channel Emulator controlled by the RFCO software – ***Electronic/RF Battlefield in a Box***

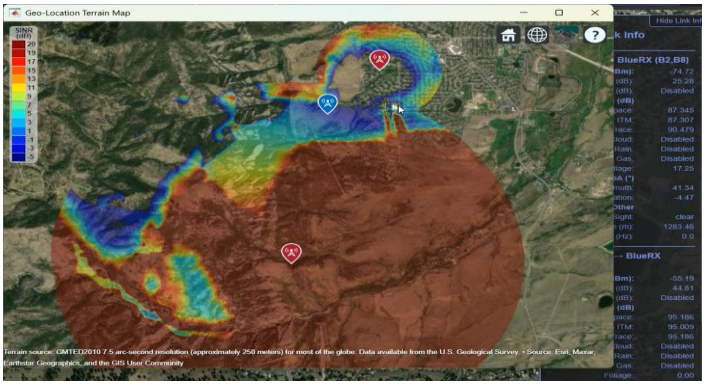


RFCO – RF Channel Orchestrator software, is a **proprietary** map-based Graphical User Interface (GUI) which controls a (COTS) RF Channel Emulator to model, simulate, and test realistic EW, SIGINT, DF, and Communication applications – ***offered exclusively by Dualos and our partner Aspen Consulting Grp***

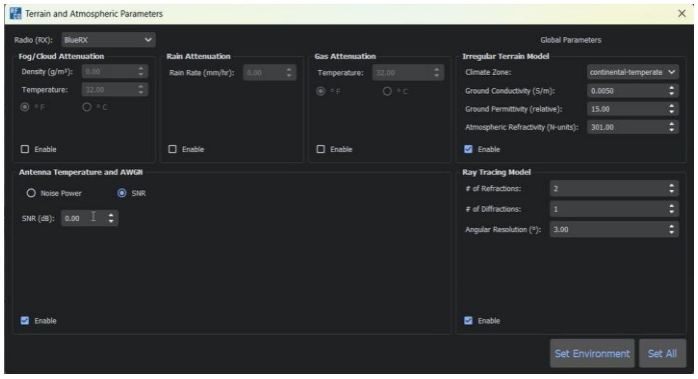
RFCO home screen
bring any location into your lab or classroom



add and place your RF nodes
limited to available Vertex RF Channels



Geolocation Terrain Map



setup Terrain and Atmospheric parameters

– RFCO example screenshots –

- **RIC-U** – Radio Interoperability Capability-Universal, is an analog-to-digital voice bridge to enable encrypted communications between our warfighters and their allied peers, where each party can utilize their native radio equipment, unique encryption, and frequency-hopping techniques

- **SDR** – Software Defined Radio, where software runs FPGAs and DSPs to replace traditional hardware components

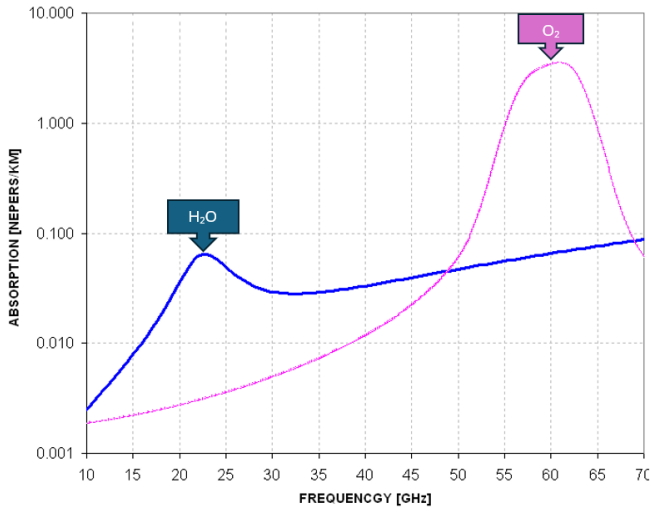
- **SIGINT** – Signal Intelligence, is the gathering of intercepted RF signals for analysis and interpretation to gain insights about adversaries or potential threats – encompasses COMINT, ELINT, and FISINT (DoDD 5100.20, EO 12333, NSA/CSS 12-3 Annex C)
  - COMINT – Communications Intelligence, is the process of collecting, analyzing, and interpreting intercepted communications – a crucial component of SIGINT

- ELINT – Electromagnetic Intelligence, focused on non-communication RF signals like from Radar and EW systems to assess enemy air defense capabilities – a crucial component of SIGINT
- FISINT – Foreign Instrumentation Signals Intelligence, focuses on collecting, analyzing, and interpreting telemetry and signals from foreign weapon systems – not crucial, just additional data
- IMINT – Imagery Intelligence, is focused on extracting meaningful information from imagery collected from satellites and sensors – compliments SIGINT
- MASINT – Measurement and Signature Intelligence, is a specialized discipline that goes beyond simply intercepting signals. It involves analyzing the unique physical characteristics (signature) of signals and other phenomena to identify and characterize objects and activities. MASINT can use data from SIGINT, ELINT, and IMINT sensors – so it aligns with SIGINT

- **TDL** – Tactical Data Links, are the secure communication systems used by our military and allies to exchange tactical information across various platforms and commands. They enable effective situational awareness and C2 across land, air, and sea operations. TDLs facilitate real-time data sharing and enhance C2 decision-making capabilities during military operations
  - TDL-11 is primarily used by naval forces
    - Operates in the HF-Band (3-30MHz) providing omni-directional coverage over long distance
    - Channel size is 6kHz in HF and 25kHz in UHF
  - TDL-16 is primarily used for Line Of Sight (LOS) Communications
    - Is the language used on JTIDS/MIDS for communications, situational awareness is achieved using SADL
    - JTIDS – Joint Tactical Information Distribution System, is a secure, high-capacity, LOS tactical data link
    - MIDS – Multifunctional Information Distribution System, is the backbone of TDL-16 for facilitating secure and jam-resistant communication
    - MIDS-LVT – MIDS Low Volume Terminal, smaller more affordable version of the older JTIDS
    - MIDS-JTRS – MIDS Joint Tactical Radio System, is a software-defined radio (SDR) that replaces legacy radios and adds new capabilities like additional waveforms
    - SADL – Situational Awareness Data Link is a secure jam-resistant tactical data link that enables real-time, LOS communication between friendly forces. Used by the US Air Force for air-to-air, air-to-ground, and ground-to-air tactical data exchange
    - Operates in the L-Band (960-1215MHz)
    - Uses anti-jam mode hopping over 51 frequencies spaced 3MHz apart
  - TDL-22 is primarily used for Beyond Line Of Sight (BLOS) Communications, also known as NILE (NATO Improved Link Eleven)
    - Operates in both the HF-Band (2-30MHz) for BLOS and UHF-Band (225-400MHz) for LOS communications

- **USSOCOM** – US Special Operations Command, is the only unified combat command comprising the Army, Navy, Air Force, and Marine Corp – *presently Space Force is not part of USSOCOM*. USSOCOM is headquartered at MacDill AFB, FL

- **V-band** (40 to 70GHz) communications offer **intrinsic LPD capability** due to the laws of physics, where the naturally occurring oxygen in our atmosphere resonates with RF signals specifically around 60GHz – this phenomenon is called oxygen absorption. Oxygen creates an incredible spike in attenuation that almost appears like a *cloaked wall* from a distance, thus creating a *curtain of invisibility* (LPD) between our warfighters and their adversaries



Laws of Physics impact on RF mmWave signals

RF mmWave signals >10GHz become subject to atmospheric molecular absorption, this is how rain and fog scatter (attenuate) RF signals

H_2O – water vapor absorption peak attenuation occurs near 22GHz (K-band)

O_2 – oxygen absorption peak attenuation occurs near 60GHz (V-band)

For optimum communications use frequencies where these attenuation peaks don't occur

  - V-band provides ultra-high-capacity, point-to-point, radio links over short distances, making it useful for small cell backhaul and high-density urban environments
    - (+) Data rates of up to 10 Gbps or more
    - (-) Radio links have a limited range of less than 1km in distance
    - (-) Radio links are highly susceptible to rain fade and other weather conditions
    - (+) Equipment required to operate is much smaller in size than for other communication bands operating below 40GHz resulting in lower costs

Author:

Claude Sweeton, Director of Test & Measurement Solutions, Dualos LLC
claude.sweeton@dualos.com
630.881.2288 Cell
linkedin.com/in/claudesweeton

- +45yrs in the Test & Measurement industry
- US Navy Veteran 1978-86