## WARRIORS ACADEMY - DEFENCE TECHNOLOGY SERIES:

# MODERN COMMUNICATIONS ELECTRONIC WARFARE

### *SYNOPSIS:*

**In a nutshell, this course covers the intercept, analysis, geo-locating, jamming & spoofing of tactical military communications and their countermeasures (with lessons from Ukraine war, Middle East wars etc)**

In 1985, a prescient paper submitted to Joint Staff titled **"Precision warfare: GPS + Datalinks"** by the lecturer proposed the use of then-nascent digital technologies riding on Moore's law such as spread-spectrum communications, network-routing, GPS positioning-timing, target-detection & locating technologies, drones etc to improve battlefield efficiency.

The idea was to create a network-centric fighting force wherein information superiority enables precision warfare to be waged "remotely" with GPS-guided sensors & shooters/munitions, all navigating & sharing coordinates on a common GPS grid & connected via a secure communications network, with no fratricide to blue forces. All that came to pass, in large measure, in ensuing conflicts such as Iraq/Balkan/Afghan/Syrian wars

The latest war in Ukraine brought to fore the continuation of this trend but now in an epic existential battle of tech equals. Two superpowers & their allies are now attacking each other's network-centric strategies & comms assets with the best asymmetric countermeasures their best minds can devise, with and without the luxury of time. Therein lies the bolts & nuts, heart & soul of modern communications warfare ushered in by the Ukraine war.

This course, from a hands-on industry pioneer in communications EW & navigation warfare, is a rite-of-passage for military users of modern communications & comms EW. It is for users who have a professional imperative to understand their craft from first principles, thereby enabling them the requisite competence & asymmetric mindset to break new ground, to stay way ahead of one's competitors/adversaries in this evolving cat & mouse game

This course will first provide theoretical foundations to understand design rationale & operation of various comms & EW assets & their vulnerabilities. The lecturer will then discuss various techniques to exploit these vulnerabilities and counter-counter measures to mitigate them.

The lecturer has a knack for original, first-principle ground-breaking reasoning, elegantly connecting the dots, making complicated things simple and interesting for professionals from any background. It offers fresh perspectives and non-trivial insights to understanding various associated issues not found in public literature, often leading to new breakthroughs in solutioning to old problems & disrupting the complacent status quo, like it did so very often for the lecturer

## COURSE CONTENTS:

| | |
|---|---|
| Day 1 | **1. MOTIVATIONS FOR COMMS EW**<br>1.1 Comms Warfare Tactics through the ages<br>1.2 Revolution in Military Affairs – Role of info and Network-Centric Warfare<br>1.3 Building Blue-force/Red-force Picture – Role of GPS/Sensor Networks<br>1.4 Battle of OODA, Sensor-shooter loops – Role of Secure Comms & EW<br>1.5 Comms EW and Comms Intelligence - Exploiting Vulnerabilities of Comms Networks in Modern Battlefields (with examples from Ukraine war, Middle East wars etc)<br><br>**2a. INTRODUCTORY CONCEPTS ON WIRELESS COMMS**<br><br>2.1 Concepts of info representation, time vs frequency domain, phasors, Constellation diagran<br>2.2 Concepts of EM waves –, properties of EM waves, bands, usage<br>2.3 Concept of modulation, phasors, constellation diagram , different types & use cases<br>2.4 Concepts of antennas – waves & radiation patterns , different antenna types, properties, u<br>2.5 Concepts of power & gain calculations - link budget, range equations, S/N , decibels<br><br>**2b. INTRODUCTORY CONCEPTS ON COMMS EW**<br><br>2.1 Role of Secure Comms and Information Efficiency<br>2.2 Role of Comms Intelligence<br>2.3 Role of Counter Comms Intelligence<br>2.4 Role of Comms Denial<br>2.5 Role of Counter Comms Denial<br>2.6 Role of Comms & Nav Spoofing and Deception<br>2.7 Role of Civilian Comms Assets – Opportunities and Vulnerabilities<br>2.8 Role of Open-Source/ Crowd-Sourced Intelligence<br><br>**3. FUNDAMENTALS OF ANTI-JAM/ LPI SPREAD SPECTRUM COMMS**<br>3.1 Direct Sequence (DS) Spread Spectrum<br>3.2 Frequency Hopping (FH) Spread Spectrum<br>3.3 Orthogonal frequency division multiplexing - OFDM<br>3.4 Hybrid Spread Spectrum Systems<br>3.5 Signal Acquisition and Tracking of FH , DSSS etc<br>3.6 Case Study: Building a FH and Direct Sequence Radio<br><br>**4. INTERCEPT AND ANALYSIS OF SPREAD-SPECTRUM COMMS**<br>4.1 Intercept and Analysis of frequency-hopping radios<br>4.2 Hopping parameters to Track and Analyze<br>4.3 Hop-Phase Diagram and Radio-Net Association<br>4.4 Dehopping /Demodulation<br>4.5 Hop-grouping for wideband Target Position-Fixing<br>4.6 Intercept and Analysis of Direct-Sequence Radios<br>4.7 Intercept & analysis of OFDM systems<br>4.7 Intercept and Analysis of Hybrid Systems<br>4.8 Case Study : Inventing the hop-phase diagram & radio net-association |

| | |
|---|---|
| | **5. GEOLOCATING OF TARGETS FROM EMISSIONS OF RADIOS**<br>5.1 Direction-finding Systems<br>5.2 Time-Difference of Arrival (TDOA) Position Fixing<br>5.3 Frequency-Difference of Arrival (FDOA) Position Fixing<br>5.4 Hybrid Position Fixing Systems<br>5.5 Case study 1: Position-Fixing of Tactical Frequency-Hopping Radios<br>5.6 Case study 2: Position-Fixing of Direct Sequence Radios<br>5.7 Case study 3: Space-Based (Satellite) Geolocation of RF Signals |
| Day 2 | **6. FOLLOWER JAMMERS AGAINST FH RADIOS AND COUNTER FOLLOWER JAMMING**<br>6.1 Follower Jammer System Analysis<br>6.2 Follower Jammer Time-Budget<br>6.3 Follower Jammer Signal intercept ,Sorting parameters, Analysis<br>6.4 How to defeat Follower Jammers<br>6.5 Case study 1: Building Follower Jammers against FH Radios<br>6.6 Case study 2: Defeating Foreign Follower Jammers in a Shootout<br>**7. ADAPTIVE TECHNIQUES TO COUNTER JAMMING**<br>7.1 Adaptive Waveforms<br>7.2 Adaptive Temporal Filters<br>7.3 Adaptive Spatial Filters: Adaptive Anti-Jam Antennas<br>7.4 Adaptive Space-Time Processing<br>7.5 Adaptive beamforming & MIMO<br>7.6 Adaptive Network Routing and Others<br>7.7 Case Study : Building Adaptive Anti-Jam antenna for Spread-Spectrum<br>**8. SATELLITES in WARFARE – OPPORTUNITIES AND VULNERABILITIES**<br>8.1 GEOSAT , LEOSAT comms – STARLINK, ONEWEB, IRIDIUM. GLOBALSAT, Kuiper<br>8.2 Space-Based Signal Detection and Geolocation<br>8.3 Space-Based Imaging Satellites – EO/Radar<br>8.4 Space-Based Navigation Satellites<br>8.5 Adversarial Attack on Satellites/Satcom Terminals & Countermeasures<br>8.Pseudo Satellites<br>**9. COUNTER COMMS INTELLIGENCE AND COUNTER COMMS DENIAL**<br>9,1 Directional Antennas<br>9.2 Adaptive Waveform<br>9.3 Comms spoofing<br>9.4 Other techniques<br>**10. EW in Gray Zone Ops**<br>10.1 EW against drone attacks – detection , geolocation, ES & EA<br>10.2 Intercept & use of civilian comms – EA/ ES<br>10.3 Protection of drone comms & nav - EP<br>10.4 EW attacks on critical civilian infrastructure - EA/EP |

| | |
|---|---|
| | **OBSERVATIONS AND LESSONS FROM RUSSIA-UKRAINE WAR, Middle-East Wars :**<br>a. EW & drones in Hamas-IDF war<br>b. Intel Collection from Russian Soldier Comms with AI Tools<br>c. Starlink/LeoSat for BVR Sensor-Shooter Loop, BVR Drone Guidance<br>d. Russian Satcom Jamming - Countermeasures from Starlink etc<br>e. Decoy Ops<br>f. Locating of Russian Comms and Jammers<br>g. Skyjack – Jamming & Spoofing of Drones<br>h. Robustification of Commercial Drones<br>i. Attacks on Static & Mobile Comms Nodes and Countermeasures<br>k. Russian modifications on Iranian & Chinese Drones<br>l. Ukrainian OSINT<br>n. Russian GPS jamming of JDAMs, GLSDB, GMLRS as per Pentagon Leaks & Countermeasure<br>plus others etc |

## ***ABOUT THE SPEAKER:***

**BILL ENG** graduated from Cambridge University with Honors in Physics in 1982 and Masters in 1986. He started his foray into anti-jam comms in mid-1980s with converting then-legacy USAF ARC182 & ARC164 tactical radios into frequency-hopping (FH) radios albeit @ very slow hop rates. At that same time, he also built the early direct-sequence spread-spectrum radios such as GPS receivers

Bill achieved a comms-EW break-through in 1995 when he became first (against fierce competition from top global vendors) to build a smart follower-jammer capable of selectively jamming (thus avoiding fratricide or collateral damage to own-force radios) against tactical FH radio networks. This pioneering work earned him a tech excellence award.

As encore, Bill invented & built an asymmetric counter-measure to follower-jamming which won a shoot-out contest neutralizing smart follower-jammers from various vendors.

The smart follower-jammer work led Bill into target identification & target geolocation of spread-spectrum & frequency-hopping radios. To sort out the hops coming from a FH radio in a noisy environment containing many other radios, Bill invented the hop-phase diagram (still used to this day by EW community) & radio-net association where unique radio signatures can be identified and tracked for location.

In 2000, Bill developed an adaptive anti-jam antenna array for GPS which was successfully flight-tested against powerful Russian GPS jammers (which posed a big nuisance to unprotected guided-munitions such as JDAM-ERs & GMLRS in Ukraine, according to Pentagon Leaks of 2023 ) . This pioneering work won a tech excellence award and proved to be mission-critical in GPS-guided drones/munitions, so pervasive in Ukraine war. It was later also extended to providing adaptive anti-jam beam-forming capability for communications datalinks as well.

In 2005, Bill invented & demonstrated precision-targeted GPS spoofing, anticipating the navigation warfare community & industry by 6 years before Iran famously hijacked a CIA drone with GPS spoofing/com-jam in 2011. Besides steering guided drones/munitions off-course, this pioneering work can potentially disrupt synchronization of comms networks( eg. Starlink ) and comm-intelligence sensors. Bill has also collaborated with LTA on studying the implication of GPS spoofing/jamming on ERP toll collection.

Bill is also a fintech entrepreneur, winning the prestigious MAS fintech awards twice (2016, 2020) and collaborated with many renowned financial institutions on AI solutions to capture & extract conversational intelligence from social chats, predicting market turning points etc amongst other things. More information can be found in https://finchat.tech/finchat-tech-news

## ***WHO SHOULD ATTEND:***

This course is designed for operational users & decision makers (military officers & civil servants), practising engineers and technicians, technical managers, system integrators, procurement officers, researchers and students who need to acquire up-to-date robust first-hand knowledge on various aspects of military comms, threats and countermeasures. This course will also benefit technical staff pursuing military communications research and development.

Please email enquiries to:
bill@fin.Chat
Tel: (65) 93690937 WhatsApp

For latest updates, go to https://warriors.academy/courses/