WORKSHOP ON

JAMMING AND SPOOFING OF GNSS AND THEIR COUNTERMEASURES

SYNOPSIS:

GNSS positioning and timing solutions have become a ubiquitous utility in both civilian and military worlds. Civil safety-critical applications include aircraft/drone/ship navigation, autonomous driving etc. In military applications, GNSS is a critical game changer for battlefield efficiency/precision, potentially determining battlefield outcomes such as the Ukraine war. However, Jamming/Spoofing threats and other vulnerabilities can cause severe problems to GNSS users and it is a professional imperative for GNSS practitioners/users to acquire up-to-date robust first-hand knowledge on the various GNSS threats and countermeasures. This course will first provide the theoretical foundations to discuss the various vulnerable attributes of GNSS. Subsequently, the lecturer will discuss the various jamming and spoofing threats/techniques and also present the countermeasures to detect and mitigate jamming and spoofing attacks. Participants will benefit in both the theoretical and practical aspects in the area of GNSS operations, vulnerabilities and countermeasures from a hands-on industry expert and pioneer. The lecturer has a knack for original, outside-the-box reasoning, elegantly connecting the dots, making complicated things simple and interesting for students from any background and yet offers fresh perspectives and non-trivial insights to understanding the various associated issues not found in public literature, often leading to new breakthroughs in solutioning to old problems.

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

COURSE CONTENTS:

Day 1	**INTRODUCTION AND BACKGROUND** **1. MOTIVATIONS FOR GNSS & ATTACKS ON GNSS DEPENDENCIES (pg 7-45)** 1.1 GNSS as Critical Infrastructure in the Civilian World 1.2 GNSS as Critical Game Changer in Battlefield Outcomes 1.3 Actual Jamming and Spoofing Attacks on Civilian and Military Targets 1.4 GNSS guided munitions/drones in Ukraine War & countermeasures **2. INTRODUCTORY CONCEPTS ON GNSS (pg 46)** 2.1 Pre-GPS era Positioning and Timing Systems (Why study them?) 2.2 GNSS System Segments and Measurements a. Satellite and Signals b. Control Segments and Operations c. GNSS Measurements 2.3 Principles of Range-Based Positioning a. Measurement Modelling b. Error and Biases – ephemeris, ionosphere, multipath, clock errors, time dilations from special & general relativity etc c. Single Point Positioning d. Linearized Estimators of Position, Velocity and Time e. Differential GPS Estimator, Dual Frequency Estimator f. GPS system & augmentations

	3. FUNDAMENTALS OF GNSS SPREAD SPECTRUM TECHNIQUES (pg 104) 3.1 Direct Sequencing (DS)/ Frequency Hopping (FH) / Time Hopping (TH) (Why DS was chosen for GNSS?) 3.2 Construction and Properties of Spreading Codes (Old GPS Codes vs New GNSS Codes) 3.3 Signal Acquisition and Tracking **4. GNSS MODERNIZATION , RNSS & AUGMENTATIONS (pg 133)** **GPS Signal structure in frequency domain** GPS, GLONASS, GALILEO, BEIDOU, SBAS, QZSS, NaVIC, etc **5. VULNERABILIES OF GNSS SIGNALS AND RECEIVERS (pg 147)** 5.1 GPS L1 C/A Code as Paradigm: Spread Spectrum, Auto Correlation, Cross Correlation, Signal Levels, Multipath Performance 5.2 GPS Error Sources and Mitigation: Multipath, Earth Atmosphere, Receiver Noise , GPS Clocks, Orbit Data, Data Message Error 5.3 Receiver Architecture: Antennas, Correlators, Tracking Loops
Day 2	**JAMMING AND ANTI-JAMMING** **6. JAMMING SOURCES & Characterization (pg 162)** a. Jamming Sources and Signals b. Broadband and Narrowband Jamming c. Jamming Effects on different GNSS d. Jamming Detection using Time and Frequency Approach **7. JAMMING COUNTERMEASURES (pg 174)** a. Antenna Methods b. Jammer Geolocation Techniques c. Inertial Aiding d. Atomic Clocks & Quantum sensors e. Pseudolites, Nav Beacons and Other Techniques **SPOOFING AND ANTI-SPOOFING** **8. SPOOFING EFFECTS AND CHARACTERIZATION (pg 212)** a. Spoofing principles b. Meaconing, asynchronous & Synchronous spoofing **9. SPOOFING COUNTERMEASURES (pg 246)** a. Antenna Methods b. Receiver Algorithms

	c. Spoofer Geolocation Techniques c. Inertial Aiding d Atomic Clocks & Quantum sensors e. Pseudolites, Nav Beacons and Other Techniques **10. FUTURISTIC & SPECIAL TOPICS FOR FURTHER DISCUSSION** **- ALTERNATE RADIO NAV systems** **- QUANTUM POSITIONING SYSTEMS (pg 282)** **- Nav warfare issues in Ukraine-Russia War** **- Nav warfare issues in Hamas-IDF War**

WHO SHOULD ATTEND:

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

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

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