



TECHNICAL SURVEILLANCE COUNTERMEASURES (TSCM) “DEBUGGING”

ADVANCED CORPORATE SOLUTIONS (ACS)

31 YEARS OF SERVICE



HOW TSCM DETECT THE INVISIBLE

Countering wireless surveillance threats with expert-led TSCM methodology

01

RF Spectrum Analysis

Full-band radio-frequency “debugging” detect active transmitters, including covert Wi-Fi, Bluetooth, GSM, and sub-GHz devices operating in your environment.

02

Wireless Network Audit

Identification of rogue access points, unauthorised devices on corporate networks, and misconfigured protocols that create eavesdropping vulnerabilities.

03

Physical & Electronic Inspection

Systematic inspection of all hardware — conferencing equipment, smart devices, power outlets, and fixtures — for implanted wireless transmitters.

04

Mobile Device Identification and Analysis

Control and Analysis of devices brought into sensitive areas for Bluetooth-activated spyware, tracking applications, and remote-access malware.

YOUR TSCM TICK-BOX



TSCM Physical “Debugging”



RF Spectrum & Signal Detection



Wi-Fi Rogue Device Scan



Bluetooth Vulnerability Assessment



VoIP & Conferencing System Audit



Mobile Device Forensic Analysis



Penetration & Vulnerability Testing



Safety & Security Risk Audit

Eavesdropping has evolved.
So have we !!