

INSIDE THIS ISSUE

**New Hand-held
ANDRE Quickly Detects
Transmitters**

**Are You Being
Overheard? (pg. 3)**

**Spectrum Analyzer
Sweep Speed (pg. 4)**

**South Africa TSCM
Courses (pg. 5)**

**Export Restrictions
Lifted (pg. 5)**

**TSCM In the News
(pg. 6)**

**Tradeshows & Seminars
(pg. 6)**

**Training Calendar
(pg. 6)**

Questions, comments, suggestions, or to add someone to the REI Newsletter mailing list, please e-mail: newsletter@reiusa.net



NEW HAND-HELD ANDRE QUICKLY DETECTS TRANSMITTERS

Research Electronics International is pleased to announce the **ANDRE™ Advanced Near-field Detection Receiver**, a hand-held broadband receiver that detects and assists in locating nearby RF, infrared, visible light, carrier current and other types of transmitters.

Advantages

The ANDRE detects signal activity in its vicinity and displays changes in signal strength over time, allowing users to quickly locate the source of transmissions. The ANDRE's frequency counter provides quick frequency information of the strongest signal and outputs additional information to an automatic signal list generator.

Antenna probes included with the ANDRE can be used to sweep rooms and objects in search for known, unknown, illegal, disruptive, or

interfering transmitters from 10 kHz to 6 GHz.

A 3.5-inch touch screen displays all of the operation controls and frequency activity. The frequency chart provides advantages over other RF detectors by showing rising and falling signal strength over time. Eight displayed time intervals can be selected ranging from 5 seconds to 24 hours. This helps identify pulsing signals and shows historical peaks, to ensure nothing will be missed. Manual and automatic threshold settings notify the user when a signal exceeds defined strength levels with haptic, audible, and visual alerts.

The ANDRE automatically recognizes connected probes and displays the appropriate frequency band on the time chart. When there are no probes attached, the ANDRE's built-in visible light/IR probe is active.

Continued on next page



INTRODUCING THE ANDRE (Continued)

(Continued)

The ANDRE also has a built-in AM audio demodulator that allows users to listen to signals. Ten second audio clips can be recorded for reporting.

A built-in frequency counter registers the strongest signal and displays the frequency. Output from the frequency counter can automatically generate a signal list with additional details such as received signal strength, attenuation and gain settings, and information about the

shots of any of the screens and audio files. A USB port and cable provides the means for transferring files and recharging batteries in the unit.

Applications

Access to eavesdropping and electronic bugging devices is becoming easier and more affordable. Broadband receivers, like the ANDRE, provide mobile RF search capability to help locate these and other transmitters quickly and discretely.

RF investigators will find the ANDRE a valuable asset and affordably priced to complement advanced analysis equipment, like the OSCOR spectrum analyzer. It can also be used independently to acquire quick, non-alerting RF detection and location.

In addition, the ANDRE can be used by wireless industry developers, RF hobbyists, and educational institutions for RF research and development. Commercial and corporate applications include performing site surveys, installing and maintaining RF systems, and emissions detection of illicit transmitters.



communication band classification. Band identification will help classify detected signals based on the FCC frequency allocation the signal falls within.

As the signal list builds, stronger signals rise to the top of the list and weaker signals fall within the list. The signal list displays the frequency, date/time and the option to designate the signal as Friendly; Threat; or Unknown. The ANDRE also has the option to capture and store screen

The ANDRE replaces the discontinued CPM-700 Broadband detector. REI will continue to support the CPM-700 with parts and service as long as parts supplies last.

Visit the [REI website](#) for more information about the ANDRE Advanced Kit.



ANDRE ADVANCED KIT

INCLUDED PROBES/ANTENNAS:



ARE YOU BEING OVERHEARD?

The Threat

Arguably one of the biggest threats of confidential conversations leaving a room or area of a facility is the ordinary loudspeaker or well-shielded microphone. When conducting a proper TSCM investigation, it is important to inspect all building wiring to ensure that no conductors are being used to transport stolen audio or video information. It is fairly simple for someone to attach a microphone to any two existing conductors present in an area and pass audio through a speaker “down the line” to be received elsewhere.

The wiring used can be AC power lines, telephone wiring, speaker wiring, HVAC wiring, access control, intercom, etc. Generally, any two copper conductors will provide the path that the eavesdropper needs. Also consider that the hard work has already been done for your adversary; the wires already exist and microphones are already in place (intercom, video projectors, fire alarm, telephones). The only thing our bad guy has to do at this point is to exploit the existing vulnerabilities that have already been installed.

Keep in mind that in the above examples a spectrum analyzer or broadband detector will not detect the attack because there are no free-space RF emanations. Additionally, a non-linear junction detector will have a difficult time locating a well-shielded microphone.

The Solution

The [CMA-100 Countermeasures Amplifier](#) is the ideal tool to analyze miscellaneous wiring for analog audio and video content. In addition to detecting stolen audio, the CMA will allow the user to hear and identify the synchronization pulses of any video content present on the wires. The CMA is a multi-functional, high gain audio amplifier that has a built in AC/DC digital voltmeter, selectable audio filters, and an extremely wide dynamic range. The CMA has a balanced and unbalanced high impedance input that provides connectivity to a variety of suspect wiring.

It is a common practice to utilize electret-type microphones for audio surveillance which require a voltage supply in order to function. Therefore, when evaluating suspect wiring, if the wiring does not have any voltage on the line, it is recommended to apply a DC bias voltage to activate



any potential microphones. The CMA-100 also provides the ability to apply bias voltage, which is adjustable between +/- 14.5V DC. This feature can be used to activate these types of voltage-dependent devices.

The CMA-100 can be a powerful testing tool in the hands of a trained TSCM technician. Its small size, combined with the audio grabbing capabilities which have made it known the world over, make it a valuable piece of equipment for your TSCM toolkit.

The CMA-100 comes equipped with a unique set of test leads which are well suited for testing phone connection blocks, AC power wiring, or insulated and non-insulated wiring. Additionally, the unit's optional acoustic leakage probe allows the user to test various surfaces (window glass, HVAC ducts, electrical conduits, overhead steel beams, etc.) for the presence of structure-born audio – or audio that is traveling naturally from one room to the next through acoustically susceptible surfaces.

For more information on the CMA-100 Countermeasures Amplifier, [visit the REI website](#).

SPECTRUM ANALYZER SWEEP SPEED

One of the most common specifications for comparing spectrum analyzers is sweep speed. It is important to understand exactly what resolution is being considered when specifying sweep speed. To start the discussion, let's look at the OSCOR Spectrum Analyzers which sweep from 10 kHz to 24 GHz in 1 second. Therefore, the sweep speed is 24 GHz/sec with a frequency resolution of 12.2 KHz. This means that every second, it produces a trace of 24 GHz span with 2,000,000 data points. Consequently, if you are using an OSCOR and only sweeping 8 GHz, then the sweep speed is 24 GHz/sec, but now the unit covers the 8 GHz span 3 times in one second.

Let's compare this to a different spectrum analyzer, which we will call Product Z, that is a little larger in size to the OSCOR. This particular unit is advertised as the "World's Fastest Countersurveillance Receiver" and "scans 20 GHz in 20 ms (1000 GHz/sec)." Let's take a closer look at these claims.

To begin, Product Z has only a single antenna input. It is not practical to sweep 20 GHz with a single antenna and have good coverage over the full band. In contrast, the OSCOR has an array of built-in antennas and automatically switches through these antennas as it covers the entire spectrum providing powerful sensitivity that is balanced across the spectrum. In the case of Product Z, the real question is how fast can the user manually change antennas? If you cannot do it faster than five times per second, then Product Z is not faster than the OSCOR when sweeping the full span.

Product Z's frequency resolution is not advertised. However, it does specify a data processing rate of 5,000,000 samples/sec. Granted, this is faster than the OSCOR, but the real problem with Product Z is the resulting frequency resolution when sweeping the full 20 GHz.

If the unit can only process 5,000,000 samples per second, this means that the frequency resolution is only 100 MHz when sweeping 1,000 GHz/sec! A 100 MHz resolution means that while the unit is sweeping very, very, fast, it cannot resolve any individual signals that are within 100 MHz of each other. Meaning it cannot distinguish between different FM radio stations or Wi-Fi channels. Figure A illustrates the multitude of individual signals that could be missed inside a 100 MHz span. Having a super-fast sweep speed, but an incredibly poor measurement resolution, is not useful when searching for unknown signals. In this mode, the sensitivity of Product Z is reduced by almost 40 dB compared to the OSCOR because of the tremendous noise bandwidth introduced into the unit.

In summary, a 1,000 GHz/sec sweep speed specification is not useful when there are antenna issues and the unit sensitivity and resolution is being reduced to a non-meaningful value. Be aware when comparing sweep speeds and make sure that you have a good understanding of the frequency resolution and antenna switching capabilities associated with quoted specifications when searching for a new spectrum analyzer.

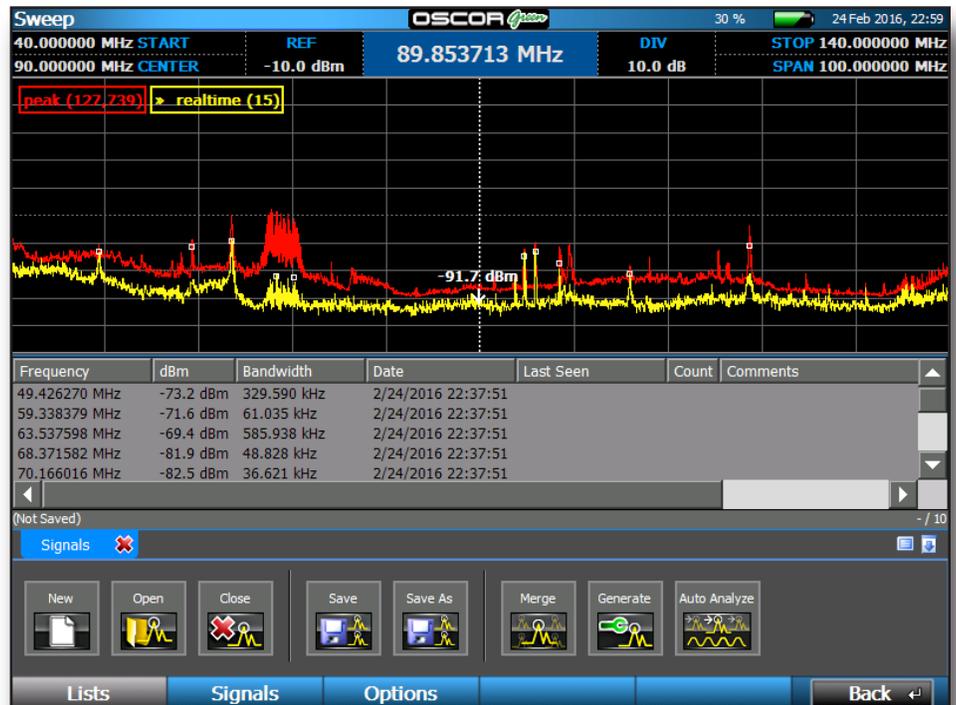


Figure A - 100 MHz span highlighting real time signals above a -10dB threshold

SOUTH AFRICA TSCM TRAINING COURSES

REI is pleased to announce a training partnership with [Eavesdropping Detection Solutions \(EDS\)](#) to present technical security countermeasure (TSCM) training courses on a regular basis in South Africa. The strategic partnership between REI and EDS means that many TSCM practitioners from outside of the USA who cannot afford to travel to the United States, or for whom it is inconvenient, will be able to receive the same high level training and certification in South Africa.



EDS has a dedicated training facility in Centurion, approximately fifteen kilometers south of Pretoria, South Africa. Attendees to the new training will receive the same training performed at REI's headquarters in Cookeville, Tennessee.

Attendees who have previously completed Level 1, Level 2 or other basic training in the USA will be able to attend the next levels of training courses in South Africa. Attendees who attend REI's Level 1 or Level 2 courses in South Africa will be able to attend further courses in the USA. The following courses will be presented in South Africa during May and June 2017:

Level 1 – Countermeasures Core Concepts

28 May – 02 June 2017

Level 2 – RF OSCOR Training

05 – 09 June 2017

Level 2 – TALAN Telephone Countermeasures

12 – 16 June 2017

Level 3 – TALAN VoIP Course

19 – 23 June 2017

[Click here to visit the EDS website and register for the new courses.](#)



EXPORT RESTRICTIONS LIFTED

REI General Manager, Tom Jones recently met with Tennessee Senators Lamar Alexander and Bob Corker in Washington DC, along with Stacie Oliver, Senior Professional Staff Member, Senate Committee on Foreign Relations, to discuss export control reform. The meeting also provided Jones an opportunity to express his appreciation for their help on behalf of REI.

The OSCOR Blue Spectrum Analyzer was launched in 2010 for worldwide distribution. Due to the technological advances in the product, export regulators determined it needed to be restricted for export. Several years of negotiating and navigating export regulations resulted in the OSCOR Blue's successful removal from export restriction in 2016, thanks in large part to the support of the senators, and Oliver's personal involvement. The OSCOR Blue now has the same export control status as the OSCOR Green.



(L to R) U.S. Sen. Lamar Alexander, R-TN; Stacie Oliver; Tom Jones; U.S. Sen. Bob Corker, R-TN



2017 TRAINING CALENDAR

SPANISH COURSE PACKAGE

Spanish RF OSCOR/TALAN Level 1 & 2
March 13 - 24

Countermeasures Core Concepts Level 1
March 20 - 24

RF OSCOR Course Level 2
March 27 - 31

TALAN Telephone Countermeasures Course Level 2
March 27 - 31

Countermeasures Core Concepts Level 1
April 17 - 21

RF OSCOR Course Level 2
April 24 - 28

Advanced Equipment Use Level 3
May 1 - 5

Countermeasures Core Concepts Level 1
May 8 - 12

RF OSCOR Course Level 2
May 15 - 19

TALAN Telephone Countermeasures Course Level 2
May 15 - 19

Countermeasures Core Concepts Level 1
June 5 - 9

RF OSCOR Course Level 2
June 12 - 16

TALAN Telephone Countermeasures Course Level 2
June 12 - 16

TALAN Certification Level 3
June 19 - 23

Countermeasures Core Concepts Level 1
July 31 - August 4

TALAN Telephone Countermeasures Course Level 2
August 7 - 11

RF OSCOR Course Level 2
August 7 - 11



CLICK HERE FOR COURSE DATES & REGISTRATION

:// IN THE NEWS

ARE HI-TECH SPIES STEALING ALL YOUR FIRM'S SECRETS?

Source: BBC News
Article: <http://bbc.in/2bhyd9U>

EAVESDROPPING DEVICE FOUND IN ROOM FOR MITO CITY ASSEMBLY MEMBERS

Source: The Mainichi
Article: <http://bit.ly/2hBQepb>

SOME SCHOOLS SWEEP FOR HIDDEN CAMS AMID 'EPIDEMIC' OF SPYING, EXPERT SAYS

Source: NJ.com
Article: <http://bit.ly/2dLsLzN>

BUGGED SAMOVAR LEADS TO ARREST OF RUSSIAN OFFICIALS

Source: BBC News
Article: <http://bbc.in/2dKJv8t>

WHY THE SPY TRADE IS SUCH A BOOMING INDUSTRY

Source: CBC News
Article: <http://bit.ly/2kymff9>

HIDDEN CAMERAS EVERYWHERE?

Source: Fox 7 Austin
Article: <http://bit.ly/2k6LyYW>

5 SPORTS SCANDALS THAT INVOLVED ACTUAL ESPIONAGE

Source: USA Today
Article: <http://usat.ly/2hzjwVQ>

HOPKINSVILLE ATTORNEY INDICTED FOR EAVESDROPPING

Source: News Channel 5 Nashville
Article: <http://bit.ly/2jCqWnW>

TRADESHOWS & SEMINARS

REI BUSINESS INTELLIGENCE PROTECTION SEMINARS

March and April
Texas and Nevada

[REGISTER HERE](#)

SECURITY & POLICING

March 7 - 9, 2017
Farnborough International Exhibition and Conference Center
Farnborough, UK
<http://www.securityandpolicing.co.uk/>

EXPO SEGURIDAD

March 14 - 16, 2017
Citibanamex Center
Mexico City, Mexico
<http://www.exposeguridadmexico.com>

SECON

March 15 - 17, 2017
Kintex Exhibition Center
Seoul, South Korea
<http://seconexpo.com/2017/>



Research Electronics International
455 Security Drive • Cookeville, TN 38506 USA
TEL +1 931.537.6032 • FAX +1 931.537.6089
www.reiusa.net