TSCM Quarterly
ISSUE Q1 2018
REI®
WWW.REIUSA.NET

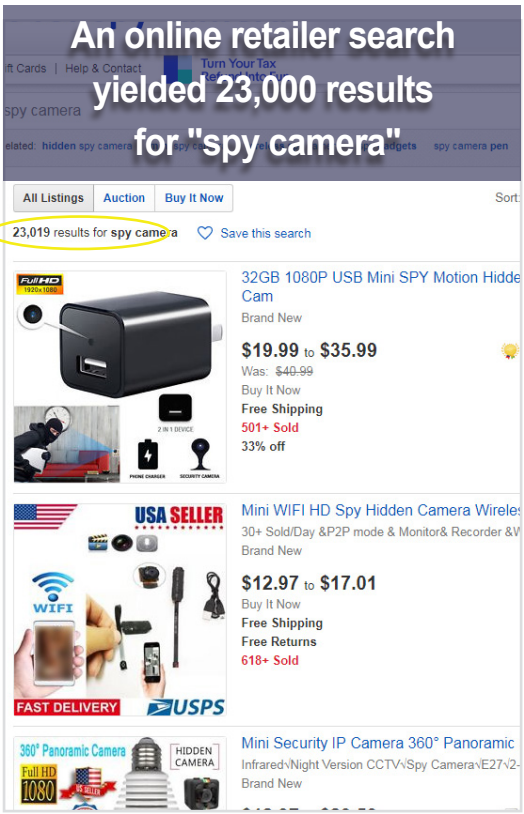
WHAT'S INSIDE

Research Electronics International
455 Security Drive Cookeville, TN 38506 USA
+1 931 537-6032 | 800-824-3190 (US only)
Fax +1 931 537-6089
www.reiusa.net

USING SPECTRUM ANALYZERS TO LOOK FOR UNKNOWN SIGNALS

Integrated Spectrum Analyzers like OSCOR combine capabilities from multiple types of analyzers to locate signals, not just detect them.

In the last few decades, the volume of RF spectrum activity has exploded and shows no indication of slowing as the demand for wireless information transmission grows insatiably. The opportunity to use free airspace for good is equal to the ability for it to be used as a weapon. RF safety and security efforts will face significant challenges in coming years to keep pace with increased opportunity for abuse.



One particular area of RF exploitation that is demonstrating significant expansion is illicit surveillance. Availability of cheaper and highly advanced surveillance products at the consumer level has taken technology that was once reserved for an elite field of intelligence specialists, and made it accessible to the average individual. Easy to use video and audio recording transmitters can be disguised and hidden in the most common, ordinary off the shelf products. These malicious devices are being produced in volume and marketed commercially with little restriction. A quick search for "hidden camera" on your favorite online retailer site may yield surprising results.

This article will explain how integrated spectrum analyzers, like the REI OSCOR, draw characteristics from several types of analyzers to make it uniquely qualified to detect, analyze and locate illicit transmitters. Some spectrum analyzer manufacturers and software developers focus on analyzing signals for precise signal characteristics. In security applications like TSCM (Technical Surveillance Countermeasures), it is equally important to find the source of the transmission. Knowing there's a thief in the neighborhood isn't good enough. You're going to want to catch him.

Continued >

SPECTRUM ANALYZER OVERVIEW

Spectrum analyzers use antennas to collect RF signal activity and display amplitude (signal strength) as it varies by signal frequency. The frequency appears on the horizontal axis, and the amplitude is displayed on the vertical axis. Every product has different levels of signal display and analysis capability, either integrated with the receiver or processed through computer based software.

For many years, spectrum analyzers have been used for lab measurements of electromagnetic emissions, safety and compliance testing, spectrum monitoring, and many other applications:

- Regulatory Compliance
- Research & Development
- Manufacturing testing and calibration
- SIGINT (Signal Intelligence)
- Wi-Fi testing and analysis
- Spectrum Management
- Security

There are many applications and technical requirements that make it impossible to build a spectrum analyzer that does everything superbly. It is necessary when choosing one to determine the application needs, not just product specifications. Relying only on speed or sensitivity may not contribute to the optimal outcome for your application.

Different types of spectrum analyzers generally have particular qualities by which they can be compared:

- Benchtop - high precision and accuracy, speed, signal analysis
- SDR (Software Defined Radios)- in-place continuous monitoring, less expensive, hardware is generalized and not optimized for specific application, software based
- Portable- in-field measurement, detecting unknown signals, mobile and agile
- Integrated- combine characteristics from all others, detecting unknown signals, spectrum view and analysis, speed, mobile/agile, integrated antenna system

In security applications, spectrum analyzers are used to investigate for RF transmitters that may be stealing corporate, private or government information, or simply in violation of security or privacy policies. Hidden microphones and cameras can record and/or transmit stolen information via RF or other mediums to remote receivers. GSM devices allow users to dial into a device for real-time monitoring, view recordings or transfer recorded files. Finding transmitters like these in the RF environment can be like finding a needle in a stack of needles. Traditional spectrum analyzers are used to look at and analyze specific signals. TSCM is different because they are used to look for unknown and often disguised signals anywhere in the spectrum. This requires a certain set of skills.

> Opportunity to use free airspace for good is equal to the ability for it to be used as a weapon.

PORTABILITY

When looking for hidden transmitters, portability should be a key analyzer feature and there's more to portability than just being able to move the product from one location to another. In this situation, portability is about effectively, quickly, and discretely collecting data from different locations and comparing the differences to provide important information for locating transmitters.

The results achieved by walking around are based on the physics of transmitting RF energy. Because of the expanding radiation pattern, energy levels being transmitted from a single source will decrease as an exponential power of 2. This means that energy level changes as a function of the range squared, from the source of the transmission.

For example, when comparing RF energy 1 foot from a target versus 20 feet from the target, the energy level is 400 times stronger at one foot than at 20 feet. By simply walking around, you can increase the sensitivity of your search by a large factor.

Continued >

In order to do this, the spectrum analyzer needs to be compact and light enough to carry and operate while moving about. Many receivers and handheld analyzers may be smaller than the OSCOR, but after you include antennas, cables, laptop/tablet, and other accessories required to adequately capture comparable signal activity across a large frequency span, they aren't very portable. The display, control center, and 24 GHz auto switching antenna system built into the OSCOR make it easy to move around and analyze data simultaneously.

The best way to know a system's portability is to test it by walking around a facility for 30 minutes collecting RF measurements. Try it with different products and see which one has the portability and provides the most information to locate RF energy.

SWEEP SPEED

While the OSCOR can sweep 24 GHz a second, there are spectrum analyzers that claim faster sweep times. However, other spectrum analyzer sweep speed specifications are typically referring to the receiver's processing speed when tuned to a single narrow acquisition bandwidth and NOT the time it actually takes the receiver to sweep a span from 10 kHz to 24 GHz (which would require changing/switching antennas). The OSCOR can actually sweep from 10 kHz to 24 GHz, switching through multiple built-in antennas in less than 1 second, displaying a single trace for this wide span.

Determine the application needs, not just product specifications when choosing a spectrum analyzer.

PROBABILITY OF INTERCEPT

POI is often referred to in spectrum analyzer specifications. Many spectrum analyzers are quoting a 100% probability of intercept (detection) for a specific burst duration (for example, one competitor system claims their unit has a 100% probability of detecting a 125µsec burst event). However, this specification assumes that the receiver is tuned to a single instantaneous bandwidth block (also called the acquisition bandwidth, maybe 40MHz wide depending on the model/manufacturer), which means the frequency of the signal being tuned to is already known.

While POI could be useful when analyzing a specific burst signal at a known frequency, in a TSCM sweep, neither the existence nor the frequency of a suspect signal is yet known. For unknown signals (TSCM applications), the POI has more to do with how quickly the receiver can actually cover a very wide band (i.e. 8 GHz or more) and a reasonable resolution step size (i.e. 12.2 kHz) to actually capture evidence of an unknown signal.

Is POI Helpful for Finding Unknown Transmitters?

EXAMPLE: Product X claims to have 100µsec POI in 40MHz bandwidth.

This means that any signal duration longer than 100µsec will have 100% POI in the 40MHz span (small blue bar). What is not explained in the specification is that signals of any duration outside the 40MHz span have ***0%*** *POI because the receiver is blind to this area. POI offers little value in this narrow a span if you are looking for unknown transmitters.*

KNOWN vs. UNKNOWN SIGNALS

If you were to compare spectrum analyzers to the telescope, the telescope focuses on a narrower field of view in order to magnify a subject. A system of lenses or mirrors allows the viewer to see distant objects more clearly by magnifying them or by increasing the effective brightness of a faint object. This is great for looking at known stars and planets or observing relatively small segments of the sky, but what if you had to find a single unknown stationary object somewhere in the entire sky looking only through the telescope. It would be impractical at best. Even worse, suppose the unknown object didn't reflect light all the time, but was only visible some of the time as is the case with burst transmitters. The likelihood of finding the subject would be very small and would require an immense amount of time.

In the same sense, many spectrum analyzers display relatively small segments of the spectrum at one time, often limited by the antenna input or frequency span of the equipment. Changing antennas may change the frequency span, but it would still display a limited span.

Continued >

The OSCOR's antenna array continuously sweeps and displays 24 GHz of frequency spectrum, with the ability to also zoom in on any segment of the frequency while still sweeping. OSCOR was designed for applications where the user does not know the frequency of the signal of interest. This is a totally different perspective than spectrum analyzers designed for bench top test analysis or field analysis of a known frequency or band, or general purpose software defined radio where the user adds laptop/tablet, software, antennas/cables, and any other hardware for their specific application.

The bottom line is, to identify and locate unknown signals, you need the right tool for the job, and the right specifications. Specifications that relate to your specific application.

For more information on the OSCOR Spectrum Analyzer, visit the REI website.

GSM BUGS

GSM stands for Global System for Mobile communication and is a standard digital cellular network used in Europe and much of the world. GSM phones use removable SIM cards (Subscriber Identity Module) containing network access configurations. A GSM bug is a wireless listening device fitted with a SIM card using the GSM network, and can be accessed and controlled anywhere by a telephone call. GSM bugs can be concealed in common consumer products, appliances, electronic accessories, lamps, preferably items with access to unlimited power, but can also be battery powered. Reasons they are common:

- **Simple design** - conveniently made to be concealed in cars or buildings. They are usually very small devices with microphone, GSM transceiver and battery (if not powered by the housing). All that is needed is a SIM card. Turn it on and a number is assigned to the bug and the network enabled. It's activated by calling the assigned phone number.

- **Range** - many can hear up to 30-50 ft. (10-15 m). Because they are GSM they also have tracking capability.

- **Inexpensive and easy to acquire** -easily purchased on the internet with a large variety of disguises for less than U.S. $40.

Most GSM bugs have settings that can be easily changed remotely by sending a simple text message: voice activation, microphone sensitivity level, anti-detection function, and more. They can often be set to call or text the eavesdropper when voice or motion is detected, or store recordings directly to a memory card for future download. As a manufacturer of counter-surveillance equipment, it is a tricky exercise to educate users without going into too much detail how illicit surveillance products work. It's important to know, however, the types of threats that may be encountered in order to defend and protect information. Unless you accidentally stumble across a GSM bug, it will take special skills and equipment to detect and locate one.

This USB charging/data cable has a hidden high sensitivity microphone and GSM SIM card. The user can activate the device with a GSM call and listen to audio within 15m. Retail U.S.$6.

The REI Training Center offers regularly scheduled countersurveillance courses including certification in RF and telephony. Visit the REI website for complete schedule and course information.

UPCOMING SEMINARS IN D.C. AND OTTAWA

REI will be hosting four free seminars in May. The first two in Ottawa, Canada, and the next two near Washington, DC. Each seminar will discuss the risks posed by electronic eavesdropping and illicit surveillance. There will be an overview of modern threats and eavesdropping techniques, as well as the countermeasures and equipment used to combat intelligence theft.

HANDS-ON PRODUCT DEMONSTRATION

OTTAWA SEMINARS

REI is partnering with Contretron, Inc., to host the Ottawa seminars. The Government/Law Enforcement seminar will take place Tuesday, May 15 and the Corporate/ Commercial seminar will take place Wednesday, May 16. Each will begin at 1:00 PM and conclude at 5:00 PM at the Infinity Convention Center.

REGISTER

HANDS-ON PRODUCT DEMONSTRATION

WASHINGTON D.C.-AREA SEMINARS

In addition to the topics already mentioned, the Washington D.C. seminars will include hands-on ANDRE exercises. The Government/Law Enforcement seminar will take place Tuesday, May 22 and the Corporate/ Commercial seminar will take place Wednesday, May 23. Each will begin at 9:00 AM and conclude at 4:00 PM at the Holiday Inn- Old Town Alexandria.

REGISTER

REI

RECORDING AUDIO WITH VPC 2.0

TECH NOTE

Not only can the VPC 2.0 capture video while in use, it also features a built-in microphone. This microphone adds the ability to provide voice descriptions of what the user is seeing. Pairing the audio along with the captured video provides essential context when reviewing the footage at a later time.

The VPC 2.0 is an effective physical search tool when needing to visually inspect hard-to-reach areas. With a minimized footprint due to its physical size, users can get in and out of a sweep location more efficiently without carrying additional bulky items like a ladder.

Visit the REI website for more information about the VPC 2.0 Video Pole Camera.

2018 TRAINING CALENDAR

Countermeasures Core Concepts Level 1
April 2 - 6

RF OSCOR Course Level 2
April 9 - 13

TALAN Telephone Countermeasures Course Level 2
April 9 - 13

TALAN Certification Level 3
April 16 - 20

RF OSCOR Course Level 2
April 16 - 20

VoIP Course Level 3
April 23 - 27

Countermeasures Core Concepts Level 1
April 30 - May 4

TALAN Telephone Countermeasures Course Level 2
May 7 - 11

RF OSCOR Course Level 2
May 7 - 11

Advanced Equipment Use Course Level 3
May 14 - 18

Countermeasures Core Concepts Level 1
June 4 - 8

TALAN Telephone Countermeasures Course Level 2
June 11 - 15

RF OSCOR Course Level 2
June 11 - 15

VoIP Course Level 3
June 18 - 22

Countermeasures Core Concepts Level 1
July 30 - August 3

CLICK HERE TO REGISTER

TSCM IN THE NEWS

MIDEAST HOMELAND SECURITY MARKET SET TO DOUBLE IN FIVE YEARS TO REACH $19.7BLN
Source: The Saudi Gazette
Article: http://bit.ly/2CsstGY

HOW TO SWEEP FOR BUGS AND HIDDEN CAMERAS
Source: WIRED
Article: http://bit.ly/2E7eQx8

BOMBSHELL LETTER EXPOSES UBER'S CORPORATE SPY TACTICS
Source: Forbes
Article: http://bit.ly/2BrXgpz

WIND POWER LEADER DENIES SPYING ON OKLAHOMA STATE LAWMAKER
Source: US News
Article: http://bit.ly/2suzoi2

OLYMPICS VIP SECURITY TEAM TO RELY ON CUTTING-EDGE TECHNOLOGY
Source: The Korea Bizwire
Article: http://bit.ly/2EpZCUA

STALKER-ASSISTING SPY DEVICES: BUGS & HACKING SOFTWARE SOLD ONLINE FOR £20
Source: Reuters
Article: http://bit.ly/2Buq4O0

QUESTIONS OVER LISTENING DEVICE FOUND AT FORMER HOME OF SENIOR REPUBLICAN
Source: The Irish News
Article: http://bit.ly/2EZxMyw

AURORA POLICE: MAN SPIED ON EX-GIRLFRIEND WITH HIDDEN CAMERAS, TRACKED VEHICLES
Source: Daily Herald
Article: http://bit.ly/2FvK2bb

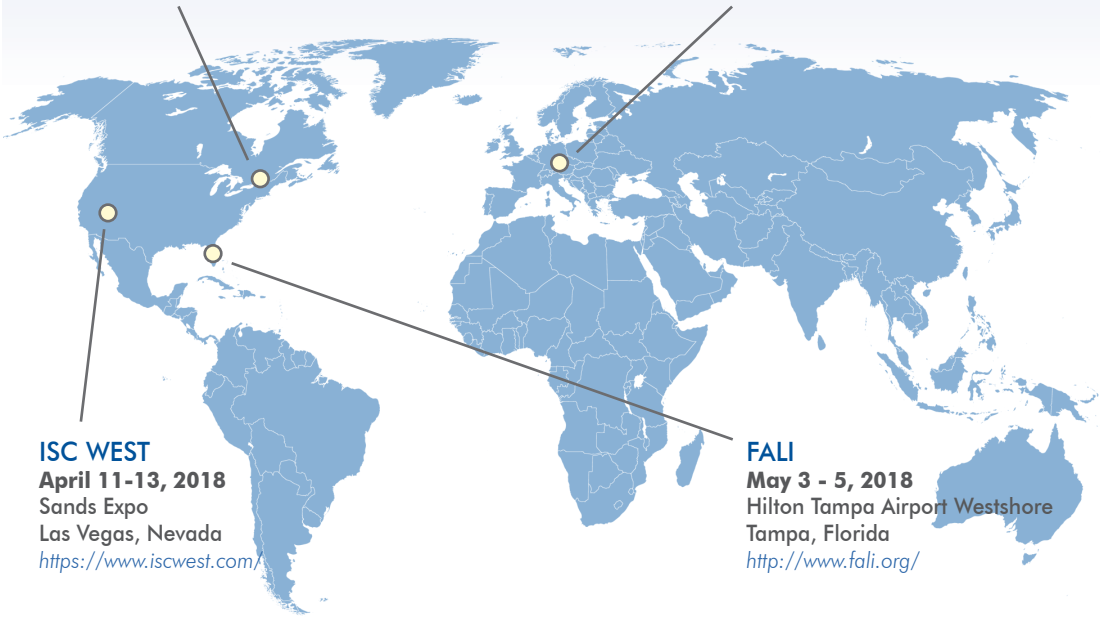
REI is on Twitter!

Want to keep up with REI's latest developments and get more #TSCM in the News stories? Follow us @REI_TSCM

TRADESHOWS & SEMINARS

CONTRETRON COUNTER-SURVEILLANCE SEMINARS
May 15 - 16, 2018
Ottawa, Ontario, Canada
https://reiusa.net/news/canada-corporate-seminar/

LEA-DER
May 15-16, 2018
Muzeum Stará Čistírna
Prague, Czech Republic
http://www.lea-der.org/



ISC WEST
April 11-13, 2018
Sands Expo
Las Vegas, Nevada
https://www.iscwest.com/

FALI
May 3 - 5, 2018
Hilton Tampa Airport Westshore
Tampa, Florida
http://www.fali.org/

REI®

For questions or comments, or to subscribe, please email newsletter@reiusa.net.