S C A N N E R S

# THE URBAN DX'ER

S H O R T W A V E

Vol. 4 No.9
September, 2000
NYDXA@Hotmail.com

Established 1984

***SCANNING IN SYDNEY***

Here's an interesting letter that was sent to Rich Wells at http://www.strongsignals.net

With the Sydney Olympic Games drawing to a close, I thought you and the Strong Signals readers might be interested to know how it has been from a scanning enthusiast's perspective. Many months prior to the start of the Olympic Games, all Australian radio amateurs were informed that a portion of their 70cm UHF band would be used for the Sydney Olympic Radio Network (SORN). We were told that the 421MHz to 432MHz band would be used until December 31, 2000 and that all Amateurs must avoid operating in this band within 150 kilometers of the Sydney Olympic Stadium. The SORN is an encrypted ASTRO Motorola SmartZone network. 12,000 Motorola XTS3000 portable radios, (re-badged as Samsung radios to fulfill sponsorship obligations) were in use for all Olympic security communications.

Then a few months before the games began, we were told that another portion of the 70cm band, 440MHz - 450MHz, would be "taken" from us temporarily as well; mainly for the use of the international media. These frequencies were used for analogue 2 way communications and studio audio feeds. Other international media frequency allocations appeared in the 150MHz, 410MHz and 500MHz bands.

Some of the best monitoring to be had was listening to (and watching on TV live) the broadcast directors calling the camera shots and being able to hear all the behind the scenes action as well. During the sailing events on Sydney Harbour, it was possible to listen in as the director co-ordinated 9 Helicopters to get the different camera angles. It was also a spectacular sight watching the helicopters maneuver into their positions as he called the shots - very Acopalypse Now!!. Most broadcast director/camera communications at the various Olympic venues around Sydney were in the 500MHz band at low RF power outputs, so it was necessary to be nearby to hear the action.

Monitoring the emergency services was not difficult considering the high level of security at these games. Although most of the sensitive police and security communications were on the ASTRO SORN, NSW Police were still using conventional analogue transmissions in their 65 channel, 468Mhz allocation, mainly for traffic co-ordination and crowd control. DVP and ASTRO transmissions were also heard popping up in the police band.

Ambulance, fire brigade and bush fire brigade communications are part of the NSW Government Radio Network (GRN), a large 400MHz Motorola SmartZone/Omnilink system covering most of the state. This is an analogue network and all that was needed to track it was a 245xlt, which have been released here with Australian specifications. It was possible to listen to any site in the Sydney region and hear the talk groups associated with the Olympic Games.

The NSW Ambulance and Fire Brigade had setup new talk groups specifically for Olympic related communications, including the transporting of injured athletes and spectators and for fire protection. A talk group was also setup for disaster co-ordination in the event of a major incident. Talk groups had also been assigned to the co-ordination of buses used to ferry athletes and spectators from, and to, the Olympic Venues around Sydney. The 800MHz Motorola SmartNet site at the Olympic Stadium was still active, carrying mainly venue services communications including food and drink staff and maintenance services.

The Australian Communications Authority (ACA) had a team of radio technicians at the Olympic site who's purpose was to resolve any RF interference issues and to track down any illegal frequency use. These ACA Techs were using a talk group on the NSW GRN for their communications and it was interesting listening to say the least. One of the biggest problems they encountered was from international organizations who had brought their own radios and were causing interference with local users. FRS radios from Europe and the USA also

caused problems by transmitting close to the SORN and media allocations. These techs would track down sources of interference with mobile radio direction finding gear hooked up to a laptop computer.

Some of the radio equipment used which they mentioned over the air included AOR AR3000 and AR5000 scanners and Hewlett Packard spectrum analyzers.

So, as you can see Rich, given the high level of security at the Sydney Olympic Games and with the increased use of digital transmission modes, it was still possible to monitor a great deal of the radio action with a simple conventional scanner and a 245xlt....all is not lost!!

***TROUBLE IN PARADISE***
Cops Take Radio Complaints to Airwaves

**HONOLULU (APBnews.com)** -- The hills and valleys of the island of Oahu are part of its charm, eternal reminders of the volcanic activity that created the Hawaiian islands. But Honolulu police officers say the topography -- along with bureaucratic inaction -- threatens their safety.
For the past two years, the city police union has been complaining that new police radios fail in areas where signals are blocked by mountains. And for two years, nothing happened.

Then, last week, police employees put $5,000 worth of advertisements on commercial radio stations, urging citizens to carry cellular telephones so officers can borrow them when their two-way radios fail to work. "We got a little frustrated," said Alexander Garcia, Oahu chapter chairman of the State of Hawaii Organization of Police Officers.

Within hours, the city and police department said they would install new antennas to eliminate the dead spots. $19.5 million system The problems began in 1998, when the city spent $19.5 million to convert its radios from a Motorola to Ericsson system, Garcia said. The new system was not designed to work in a mountainous area, where hills block the signals, he said.

Dead spots, which were not accessible by radio, cropped up in each of the island's four quarters, he said. The city and county of Honolulu are combined and cover the entire island of Oahu.

"You can't talk to each other," he said, and many officers had to turn to their own cellular phones to communicate with headquarters. "Having a radio is a lifeline," said Garcia, a violent crimes detective. "You have to be able to communicate not only with dispatch but also with your fellow officers. The big difficulty is not having that direct communication."

What price safety?

The union chapter, which represents 2,000 officers, complained to no avail. "For the last two years, the city engineers and administration have been trying to correct this, but nothing happened," Garcia said. The police union decided to take its concerns to Oahu's one million residents. The union planned to spend as much as $50,000 on three radio ads, Garcia said. "What price do you put on officer safety? If we could save one life, $50,000 is nothing," he said. One ad starkly warned citizens to "not be alarmed" if an officer approaches and asks to borrow a cellular phone. "If you're in trouble, need help or have an emergency, make sure you have your cell phone with you," says a male voice in one ad. "Your Honolulu Police Department needs to be able to call on your cell phone."

Police actually have not had to ask residents for their cellular phones. "We did the ads to show how difficult it could be," Garcia said. "I know the public would have lend them to us if we had asked."New antennas on way" The day the ads appeared, police and city officials held a news conference to say that the problems were being addressed. Police officials declined to comment, but a spokeswoman confirmed that new antennas would fix the dead spot problem. The city official in charge of the antenna system did not return repeated calls seeking comment. Garcia said he had mixed feelings about the quick response. "I wish they could have done it a couple years ago," he said. "They didn't realize how important it was."

But officers will not bear a grudge, he said. Late last week, the union changed the content of the ads. "We said thank you to the public and the administration of the police department for their fast response," Garcia said.

Randy Dotinga is an APBnews.com West Coast correspondent (randy.dotinga@apbnews.com )

***COMMENTS ON THE OPTO SCOUT***

Optoelectronics recently had a sale on the Opto Scout. I've been borrowing Dave, WI2Q's so often that I thought it was time I buy my own! For those of you who have owned one, Optoelectronics made some changes to increase its reliability. For starters, the battery charging circuit has been simplified and it no longer heats the batteries up. Older Scouts also turned on when the battery was being charged. The new units can be turned on while charging, but will not turn on automatically.

After using it I've made some observations that led me to doing some serious experimentations. Optoelectronics recommends the "miracle baby" antenna made by Comet. Comet claims it's a "10 band" antenna, but I've determined that it actually resonates best at about 819 mhz. This accounts for the superb performance in that region. I called Optoelectronics and they confirmed my findings. They also agreed that the small antenna is marginal at 450 mhz and almost "ineffective" at 150 mhz.

The Scout detects a signal that is about 12-15 db above the ambient RF noise floor. This means that if an efficient is used, strong signals such as NOAA weather and paging transmitters may artificially mask out nearby signals. Ideally, we need a "nearfield" antenna resonate in the 150 and 450 mhz region. As I'm writing this, I'm waiting for one of the "stubby" antennas used by NASCAR scanner listeners. Using an "FM" trap in line with the antenna will also mask out FM broadcast stations that may effect the Scout's overall sensitivity. I also E mailed my conclusions to Bob Grove at Monitoring Times and received this answer...

Hi, Bob:
You're right on all counts. Intuitively, I think you've answered your own questions.

By keeping the general RF field density low, the counter responds only to near field signals which it interprets as being the strongest, so you don't get false products. But by substituting a resonant 155 Mhz rubber duckie, you'd encourage the detection of nearby 152/158 MHz pager signals, NOAA weather broadcasters, and other powerhouses that could give false readings in a near-field environment.

An FM trap will certainly reduce those broadcasters by 30 dB or so."

Continuing, I also related the following story to Bob Grove....

I had the need to sit with someone for several hours in the emergency room of a local hospital. The hospital had countless signs informing visitors that cell phones were not permitted as they can interfere with the equipment in the hospital. Interesting that my Scout got 20 separate hits from cell phones that the staff was using. I asked one of the Bio-med people why such signs were posted, yet the use of the staff's phones had no effect. His response was that they house phones were on a "safe frequency." I pulled out by Scout, demonstrated how it worked. I wondered if he was just singing the hospital's policy or if he simply had no knowlege of RF? His lack of a response said more than any explanation he could provide!

To this, Bob Grove commented, " yes, there is no difference in the "safe" frequencies used by the hospital staff cell phones than those used by walk-in clients unless the hospital is using their own system, but you showed him this wasn't the case. I recall isolated instances in which patient monitoring telemetry was affected by nearby cell phones, but this doesn't forgive the use by the staff unless they have demonstrated there are safe ZONES rather than FREQUENCIES on the grounds."
Bob Grove

***COLORADO SCANNING....***

Colorado law enforcement had no quams in switching to digital modes and announcing it to the world. Check this page out!
http://www.state.co.us/gov_dir/gss/cits/comm/dtrs/media.htm

"With the transition of many public safety radio systems to the Cooperative Communications Network of Colorado (CCNC) digital trunked radio system, it will no longer be possible for unauthorized monitoring of radio traffic. The CCNC realizes that granting permission for the news media and certain non-government agencies to monitor specific channels may benefit the public. This policy will define the process and requirements to obtain permission to monitor along with how to obtain and activate the equipment.

All requests for permission shall be in writing signed

by a senior level official from the agency requesting permission. Request should be sent to:

Cooperative Communications Network of Colorado
c/o State of Colorado, ITS 2452 W 2nd Ave. #19
Denver, CO 80219

The request should contain the following information:

C Name, address, Email and telephone number

C Specific channels to be monitored

C Quantity and type of radios requested (Base, Airborne or Portable)

C Purpose for monitoring Users of the equipment

Once a request has been received, the CCNC Board will contact the public safety agency whose channels are being requested to clear the request. Once the agency has approved or denied the request, the requesting agency will be contacted with the status of their request. If the request is approved, the CCNC will provide an agreement form to be completed by the requesting agency. Once the form is completed and returned, the CCNC the will provide information on how and where to purchase the necessary equipment, along with how and where to get the equipment programmed.

The maximum number of radios authorized to a single agency will be 2, one newsroom or fixed location and one airborne unit. Newsroom units will be capable of monitoring only. Airborne units may be granted permission to transmit for official public safety activities only. Decisions of the CCNC Board are final."

***FLAWS IN CELL PHONE TECHNOLOGY***
Cell Phone Flaw Opens Security Hole

Your cell phone may be multilingual - and that could be detrimental to your privacy. Computer security researchers said a design flaw in the protocol used in global system for mobile communication cell phones could allow eavesdropping. The trick: Just make the cell phone think it's somewhere else. Only 6.5 million people in North America use global system for mobile communications cell phones - through providers such as Pacific Bell Wireless and VoiceStream Wireless - but worldwide, it's the most widely used standard, accounting for 65 percent of the total wireless digital market.

GSM phones are increasingly popular in the U.S. because they allow roaming in Asia and Europe upon insertion of the appropriate smart card. Since western Europe can't export encryption products to certain countries, such as targets of United Nations sanctions, the default version of the GSM protocol does not use encryption. This in itself isn't necessarily a problem, said David Wagner, a professor of computer science at the University of California-Berkeley, but GSM also does not authenticate its base stations, the hardware that communicates with the handsets - and that is potentially troublesome.

Experts said it is possible to build a phony base station that jams the signal from the real base station and forces the cell phone to connect to it. The base station then tells the cell phone, in essence, "You're in Iraq, don't use encryption," and the call proceeds unprotected with the false base station relaying information between the real base station and the handset.

A handful of researchers have been aware of the loophole for several years now, but it's been "a well kept secret," Wagner said. Security experts call this a "man-in-the-middle" attack because the phony base station sits between the handset and the real base station, intercepting their communications, but neither the real base station nor the handset knows it's there.

"We know about it as a technical issue, but we haven't seen it demonstrated," said James Moran, fraud and security director at the GSM Association. He added that building an interception device would require considerable technical skill. Moran said the next GSM standard would address the problem. Other cell phone standards probably don't authenticate base stations either, Wagner said, perhaps because their designers were more concerned with preventing handset cloning, which allows someone to bill his or her calls to someone else's number. But the phony-base-station trick is a particular problem for GSM, because different strengths of encryption are used in different places. "Whenever you have to support both weak and strong cryptography, one very real risk is that you

end up with "least common denominator" security,"
Wagner said. Cracking different pieces of the cryptography that protects GSM cell phones from eavesdropping has long been a favorite pastime for computer security researchers. Just last December, two Israeli researchers announced that they had found a fast method of cracking the A5/1 algorithm, the strong encryption used to protect GSM phone calls in Europe and the U.S. But the phony-base-station strategy obviates the need for any encryption busting.

***INCREASE IN MILITARY ACTIVITY RESULTS IN INCREASED SATELLITE ACTIVITY***

As a result of recent events in the Persian Gulf area and typical of crisis related situations, increased analog FM-SCPC communications has been monitored at my central Virginia location from the INMARSAT Atlantic Ocean Region-East satellite 15 Degrees West and to a lessor degree from the INMARSAT Atlantic Ocean Region-West satellite 53 Degrees West in the 1,535-1,542 mhz. range.

The INMARSAT AOR-E satellite east-west approximate median latitude footprint covers from the Persian Gulf to the USA Mississippi river area. The INMARSAT AOR-W satellite east-west approximate median latitude footprint covers from central Europe to the USA west coast.

VHF SATELLITE FREQUENCY UPDATES

| FREQ(MHz) | Use |
|---|---|
| 137.00000 | ISKRA-1 |
| 137.02000 | Symphonie-1 |
| 137.03500 | FY-1 F1, F2 |
| 137.05000 | Ariel-4 OTS-2 Orbcomm-X DCS-1 VSUME |
| 137.08000 | SSU Precursor-2 Meteosat-1, -3 |
| 137.10000 | METEOR 1-29 |
| 137.11000 | ATS-6 |
| 137.14000 | Aurora-1 NOAA-4,- 5 |
| 137.15000 | METEOR 1-24, 1-25, 1-26, 1-27, 1-30, 1-31 Magion-1, -3, -5 |
| 137.17000 | Explorer-43 MARECS-1, -2 |
| 137.17500 | Bhaskara-2 |
| 137.19200 | APPLE |
| 137.20000 | ESRO-4 GEOS-1, -2 ESA Bhaskara-2 |
| 137.22000 | Bhaskara-2 |
| 137.22500 | Orbcomm-A2, -F21, -F22, -F23, -F24, -F25, -F26,-F27,-F28 SAFIR-2 |
| 137.23000 | Explorer-51, -54, -55 |
| 137.25000 | Orbcomm-F21, -F22, -F23, -F24, -F25, -F26,-F27,-F28 |
| 137.26000 | Aeros-1 |
| 137.28000 | Kosmos-1602 |
| 137.28750 | Orbcomm-A8 |
| 137.29000 | Explorer-38 Aeros-2 |
| 137.30000 | METEOR 1-23, 2-2, 2-3, 1-29, 2-4, 2-5, 2-7, 2-8, 2-9, |
| 137.31250 | Orbcomm-A5 |
| 137.33000 | Kosmos-1602 |
| 137.35000 | ATS-1,-2, -3, -4 |
| 137.36000 | ATS-5 |
| 137.38500 | Timation-2 |
| 137.40000 | NOAA-3 METEOR 2-6, 2-10, 2-12, 3-1, 2-13, 2-15, 2-16, 2-21 |
| 137.41000 | Explorer-30 S69-4 |
| 137.42000 | Rohini-1B |

| | |
|---|---|
| 137.43500 | Orbcomm-A3 |
| 137.44000 | Explorer-30 Miranda Aryabhata Solrad-2A |
| 137.44500 | MAGION-2 |
| 137.45000 | ATS-1 METEOR 1-29, 2-5 Kosmos-1484 Interkosmos-24, Aktivny |
| 137.46000 | Orbcomm-FM1, -FM2, -A4 |
| 137.50000 | ESSA-2, -4, -6 ITOS-1 MIKA NOAA-2, -3, -4, -5, -6, -7, -10, |
| 137.53000 | SRET-2 (MAS-2) |
| 137.56000 | Prospero X-3 Ariel-6 Solar Maximum Mission Orbcomm-A1, |
| 137.57500 | Explorer-49 |
| 137.62000 | ESSA-8 NOAA-1,- 2, -3, -4, -5, -7, -9, -10, -11, -13, -14, |
| 137.66250 | Orbcomm-A3, -A4, -A8, -F15, - F16, - F20 |
| 137.67600 | Hilat |
| 137.68000 | Ariel-5 P76-5 Orbcomm-FM2 |
| 137.68750 | Orbcomm-A5, -G1, -G2 |
| 137.71000 | Explorer-44 Orbcomm-FM1 |
| 137.71750 | Orbcomm-A1, -A2, -A5, -A6, -A7 |
| 137.72000 | TEMISAT |
| 137.73750 | Orbcomm-A6, -F14, -F19 |
| 137.74000 | GRAV GRAD 4 TD-1A SROSS-C |
| 137.77000 | NOAA-7, -9, -10, -11, -13, -14 |
| 137.79500 | FY-1 F2 (4 lines/sec APT) |
| 137.80000 | Interkosmos-18 Orbcomm-A7, -F13, -F17, - F18 |
| 137.82000 | S69-4 |
| 137.85000 | Interkosmos-19 METEOR: 2-8, 2-11, 2-14, 2-15, 2-16, 2-17, 2-18, 2-19, 2-20, 2-21 (2 lines/s APT + 20 lines/min IR) METEOR 3-1, 3-2, 3-3, 3-5 (2 lines/s APT + 2 lines/s IR) Kosmos-1809 FY-1 Magion-3 Resurs-01 4 |
| 137.86000 | Landsat-1, -2, -3 |
| 137.89000 | ANS-1 |
| 137.90000 | NUSAT |
| 137.92000 | Explorer-47 PEGSAT |
| 137.93500 | MEGSAT |
| 137.95000 | ISIS-1, -2 Explorer-45 MU-SAT |
| 137.95500 | UPM/LBSAT |
| 137.96000 | HETE |
| 137.98000 | GRAV GRAD 5 Explorer-50 |

***The Urban DX'er would like to thank all those who contributed to this months issue!***
Charlie - N2NOV, **"R"**, Joe Walc - K2JAW