FRUMEL HISTORY AVAILABLE IN THE NATIONAL ARCHIVES OF AUSTRALIA

By Nick England and Doug Tilley

For those interested in the history of the Fleet Radio Unit Melbourne (FRUMEL) outpost at Adelaide River, information is now available through the National Archives of Australia (NAA). Doug Tilley lives very near the remains of the Adelaide River receiver site in Australia. He sent me the following information about the construction and post-war removal of the facility. The interesting thing is that the Australian National Archives seem to have digitized dang near every scrap of paper from WWII! So anyone interested in FRUMEL and Australian SUPRAD history may want to make use of this on-line archive.

This is the NAA response to Doug's request for information:

To: Doug Tilley
Mt Bundy Station
Adelaide River
Northern Territory, Australia

Thank you for your request for an online copy of the following record held by the National Archives of Australia (NAA). Archives series and Item control symbols: MP1049/5, 2037/3/187, Adelaide River, Northern Territory - combined United States Navy/Royal Australian Navy, wireless telegraph station

Record Search barcode: 504893. Your request for this particular record has been processed by the North Melbourne office of the NAA - please send any queries about it to ref@naa.gov.au referring to Order No: North Melbourne/ 372068. If you requested more than one online copy, you will receive a notification for each record as it is completed from the office in which the record is located. Photocopy requests will be processed according to the applicable standard of service: records previously cleared for public access (Open & Open With Exception) within 30 days and items not previously cleared (Not Yet Examined) within 90 days.

HOW TO VIEW THE ONLINE COPY:

To go directly to the record, click on the link below. http://naa12.naa.gov.au/scripts/SearchOld.asp?O=I&Number=504893. If you are having technical difficulties or would prefer not to use the direct link, go to the Record Search homepage of the NAA website **www.naa.gov.au** and follow the instructions at "How to view online images." Information about other services, products and events for the public and for Australian Government agencies can be also found on our website.

⚓

www.usncva.org

COMMUNICATIONS ON NAVSECGRUDETS IN THE MED

By Jack Mirabelli

In the late 1950s and 1960s, Naval Security Group Detachments (NAVSECGRUDETs) were assigned to the two carriers operating in the Mediterranean on a six month TAD basis. The DET was composed of personnel from Naval Communications Station (NCS) Morocco, DET 28 Karamursel, Turkey, NSGA Bremerhaven, Germany, and later on from Rota, and also from NSGA Edzell, Scotland. The DET was manned with two CTOs, two CTIs, two CTRs, 1 CTM, and one CTA. A Chief or First Class was the leading petty officer. The OIC of the DET was either an Ensign or LTJG from one of the above NSG Activities. The mission was to support the embarked COMCARGRU Staff with Special Intelligence either obtained onboard or through Intelligence Reports received from military and national intelligence agencies. Ironically, the only cleared personnel other than DET personnel were the Admiral, Chief of Staff, Flag Meteorologist, and the CO of the carrier. Depending on the type of carrier, the DET spaces were located in Supplementary Radio on the 03 level, portside near Main Communications. The DET would spend at least three months on one carrier and when that carrier was relieved the DET would transfer to the relieving carrier. I had the pleasure of serving on the USS FORRESTAL (CVA-59) and USS ENTERPRISE (CVAN-65) in 1962 and 1963.

Before Satellites and on-line encryption systems (KW-7, KW-26, KW-37), all messages to and from the NAVSECGRUDET had to be off-line encrypted or decrypted. Incoming messages were encrypted at the SECGRU Activity at Morocco and later at Rota prior to transmission over HF broadcast frequencies. These signals were rebroadcast on different frequencies to cover the entire Med. Morocco, Greece, and Spain had the HF transmitter sites. The site in Greece was composed entirely of mobile vans and antennas. Their transmitters were consistently reliable and had the best signal strength. The ship's radiomen would copy these broadcasts and deliver a tape and hard copy to the DET. The messages had an RU routing indicator, date time group, system indicator, and message indicator followed by the encrypted text. Most of the messages were over 1,800 characters. The Python cryptosystem less the key tapes were carried onboard by DET Personnel. The Python key tapes and Adonis key lists were obtained from the ships' CMS Custodian. The "O" brancher would take the encrypted tape and based on the date time group and system indicator take out a Python cryptographic key tape for that day. Using a special TD (transmitter distributor, a B-2 or CSP 2599), that had dual tape gates. One gate for the encrypted text and the other gate for Python key tape. The received encrypted tape start point was at the message indicator and the crypto tape start point was on the system indicator for that day. The TD would be turned on and hopefully decryption would happen. A printer and tape reperforator would be turned on and the "O" brancher could watch the message decrypt. This was a very demanding job since you had to

Continued on page 19

COMMUNICATIONS ON NSG DETS...

Continued from page 18

monitor the entire decryption. If an extra letter or characters caused by atmospherics were in the encrypted tape then the message would garble and you had to start or find a good start point. Some of the radiomen who did not understand this system would provide us tapes that were stapled together because they ran out of tape and had to place a new roll in the tape factory. It might be five feet of missing characters and impossible to decrypt. When asked about it, they said, "What difference did it make, it was all garbled anyway." So, when decrypting, you would stop the TD and draw a line over the two tapes that allow you to go back to a good point. By moving the encrypted tape one character at time then turning on the TD, the message would start decrypting. With the decrypted message and tape, the operator would try to piece together to create a good tape and page copy so the Admiral and his staff would receive a readable message. After six months, my relief came on board and did not have that much experience with the Python System. So, I explained the procedures. While he was breaking a message it started to garble so he stopped it and yelled for help. I told him to pull back the encrypted tape and crypto tape to the last marked point. He did and it worked till it hit the bad part. He pulled the encrypted tape one, two or three characters but no luck. I came over and pulled that tape at least five or six inches and turned on the TD. To my surprise, it commences to decrypt properly. I couldn't believe it. The chances must have been a million or two to one for that to happen. I laughed and told him that. However, before I left he tried to do what I did and of course it didn't work. Outgoing messages from the DET were rare. Personnel messages on our travel or orders were via the ship's Personnel Office. SI messages or test messages had to be encrypted using the Adonis Cryptosystem (KL-47) devices. Classified messages were hand typed on the KL-47 keyboard. This cryptosystem was composed on a Base KLB-47 and a basket (KLK-47) of eight rotors that had to be set daily. An encrypted tape (white with black letters) came out in five letter code groups. These messages were delivered to Main Comm for transmission via Morse code. In the mid 1960s, the Python System was replaced with the Jason Cryptosystem (KWR-37) which the DET copied itself via HF frequencies from Morocco, Greece and Spain. Outgoing messages were still encrypted in the Adonis off-line system. One of the most exciting event on my six month cruise, that probably happened to others, was the issuing of a CRITIC test message from the DET. In those days, there were six message precedence - ZZ Flash, YY Emergency, OO Operational Immediate, PP Priority, RR Routine and MM Deferred to be used for military messages. The CRITIC test message was received from DIRNSA via ARFCOS addressed to the DET. At a certain time, we were to encrypt the message in the ADONIS system and deliver this Flash precedence to Main Communications with the DIRNSA address, I believe with an R routing indicator. It was a test to evaluate the handling time from our DET via the ship to the shore base facility, and finally to DIRNSA. We were instructed not to divulge that it was test. The Duty Officer in Main Comm said only the Commanding Officer could release a Flash message. He called the Comm Officer, who called the OPS Boss, who called the XO, who finally called the Commanding Officer. Our poor young Ensign had to run to the bridge and explain the message. Flash messages indicated attacks or combat actions. It took almost one hour before the CRITIC was sent via Manual Morse to a shore station. This system stayed around through the 1980s and was finally retired. One of the reasons was the infamous John Walker, a retired CWO, who sold cryptographic keying materials to the Soviets for money over a period of 20 years. He is currently serving time and is due for parole around 2020.

Needless to say, today's communications are via satellites and are delivered to the ships via secure high speed circuits. Ships receive them and place them on separate local area networks depending on their classifications and addressees.

⚓

Please Note:

Henceforth please send all notices of death and/or obituaries to our membership secretary and to our new obituary editor:

Richard C. Carlson
1109 N. MAIN ST
Winterport, ME 04496-3418
carlson3302@roadrunner.com

CYBER WARRANT OFFICER COMMUNITY ESTABLISHED

The Navy has established the cyber warrant officer (743X) community, recently announced in NAVADMIN 139/10.

Designated as warrant officers in the ranks of Chief Warrant Officer-2 (W-2) through Chief Warrant Officer-5 (W-5), the program will identify, develop, and commission technically proficient sailors to operate, analyze, plan and direct on-net cyber operations. In addition to the normal Chief Warrant Officer commissioning program requirements, candidates must be currently certified as apprentice interactive network collection operators Navy enlisted classification (NEC) 9308.

FY-10 743X accessions will come in the form of re-designating qualified 744X officers (who have already earned the 9308 NEC). Starting in FY-11, all selections will be made via the annual Chief Warrant Officer and Limited Duty Officer selection board. Current plans are to access two 743X officers annually.

⚓