Significant TRF TROODOS stories over past 6 months

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- Regular collects of Heron TP carrying weapons
- [redacted]
- [redacted]

Success against Syria

- 17th Feb 2012 collection on an undocumented frequency of 1208MHz.
- Ababil III (Iranian manufactured) UAV from Shayrat Airfield.
- Tip-off procedures facilitated co-incident collect from Golf, E Section and MHS on 9th March.

- Site made a further recording on 11th March.
- Presidential level interest in further video samples.

ISUAV Video Descrambling

Author: [redacted]
Version: 1.0

Introduction

Analogue video from Israeli UAVs has been intercepted in both clear (i.e. unencrypted) and scrambled (i.e. encrypted) formats. Processing clear video using M2Extra is relatively straightforward, the method being described in Anarchist training Module 4. For scrambled video the capability exists to exploit the content using a combination of image processing tools and scrypts on Mutiny Jaguar.

Background

Interception of scrambled analogue video signals at Anarchist has a long history, with the earliest examples dating back to 1998.

The Signal

The appearance of the encrypted signal in the frequency domain is virtually indistinguishable from the clear video signal. A comparison of the Post-D data for an example of clear video, and an encrypted example from a few seconds later (figs 1a & 1b) show that, apart from a subtle modification to the envelope, the signals appear very similar. The most noticable effect is an increase in energy at lower frequencies, consistent with the detail in the image being smoothed out by the scrambling process.

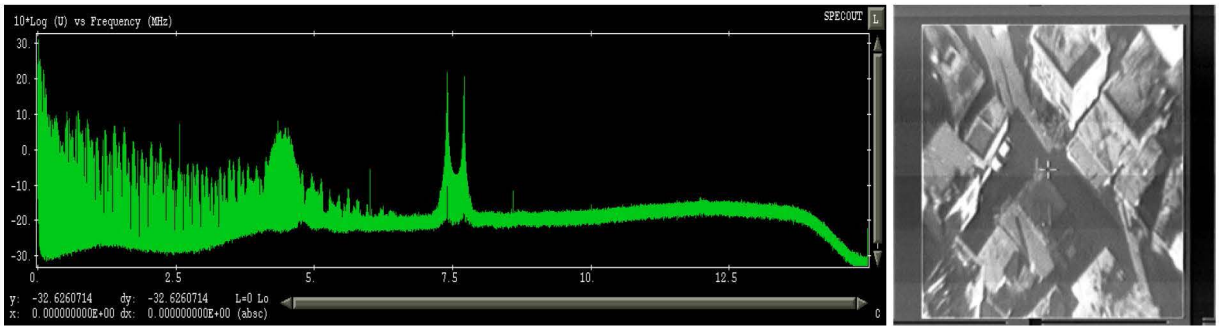

Fig. 1a: Post-D spectrum and video image for a clear S455e video signal

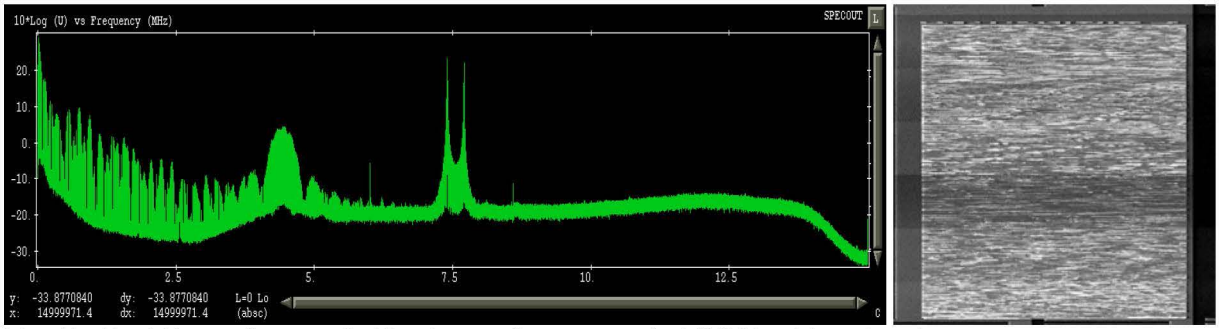

Fig. 1b: Post-D spectrum and video image for a encrypted S455e video signal

Scrambled Imagery

As can be seen by examining an example of a frame of scrambled video (Fig.2) the video frame is unchanged by the scrambling method. In addition to the image seen in clear video there is also two lines of digital information encoded in the teletext area at the top of the screen. This is presumed to be information relating to the scrambling, e.g. a cryptographic 'key' to enable the original image to be reconstructed.

Investigation of the data has determined the method by which the video is scrambled. The method used is a 'cut & slide' technique whereby each line is cut at a location and the two halves are transmitted in the opposite order. This technique was originally used by Sky TV to protect their analogue transmissions before they switched to digital, the system being known as VideoCrypt.

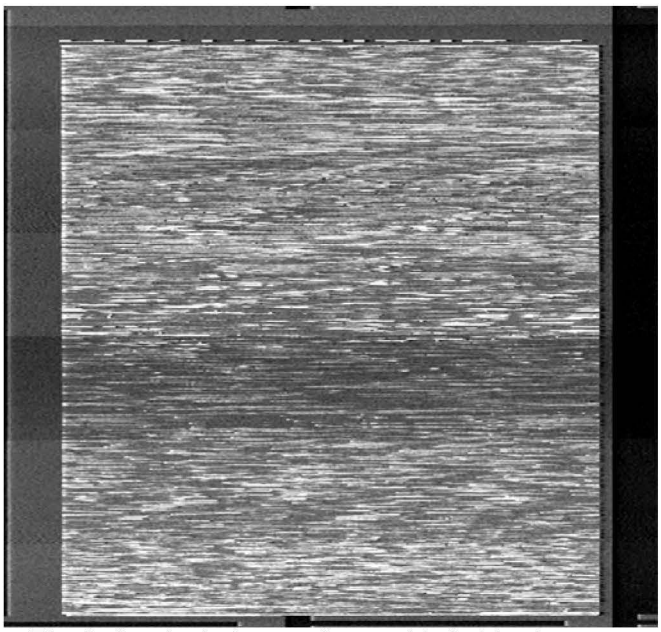

Fig. 2: An single frame of scrambled video imagery

Exploiting Scrambled Video Images

Having determined the technique used to scramble the video imagery a number of known attacks are available from open source material. One technique in particular offers a brute force way of reconstructing the image, without requiring any knowledge of the generating algorithim.. This technique, and the source code needed to employ it is freely available on the internet.

The computing power needed to descramble the images in near real time is considerable without the use of dedicated hardware such as a video capture card that can record uncompressed images. It is still possible to descramble individual frames to determine the image content without too much effort.

Method

The method involves capturing a video frame in bitmap (.BMP) format using M2Extra. The video data should be processed as described in the M2Extra video processing guide. When the quality of the video image is good a snapshot can be made of the data in the *Event Processing* window. Pause the processing and use the left mouse button to zoom in to the scrambled image to exclude the frame.

From the file menu in the top left hand corner of the Event Processing window select *Snap . . . (CTRL-S),* and choose .BMP as the format.

Start *Martes* in a terminal window with the command *martes,* and launch the *Image Magick* tool from a terminal window with the command *magick_display*

Fig. 3: Image Magick and the file browsing menu

Select the bitmap image from the file menu, right click on the image and select *Save …* The image format can be set by pressing the Format button at the bottom of the window. There are a huge number of different formats to select from. The format required is *PPM* format (portable pixmap).

In a terminal window at a command line prompt type

antisky –bc input.ppm output.ppm

This will now have descrambled the image using the program *antisky.* The descrambled image can be viewed using the *Image Magick* tool and converted to a more convenient format if desired.

The initial results from running antisky with the default settings as above may not produce particularly good results depending on the image being descrambled. This is because there may be part of the non-scrambled frame of the image included in the descrambling which corrupts the results. To improve the descrambling there are two more option which force the program to ignore the left and right hand sides of the image. Using the –l and –r (for left and right) flags and experimenting with different values may produce better results. The descrambled image first obtained with the default settings is shown in Fig. 4, whilst the image obtained with the command

antisky –bc –l15 –r3 input.ppm output.ppm

is shown in Fig. 5 and is considerably clearer.

There is no quick way of discovering the optimum settings for Antisky other than stepping through the parameter space of values and selecting the one that gives the best results.

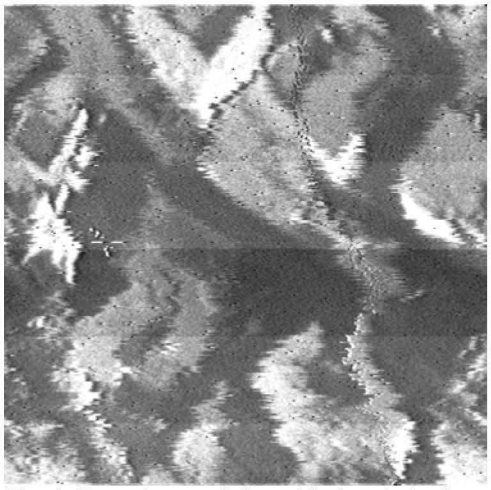

Fig.4: Running antisky with the default settings

Fig. 5: Running antisky with optimised settings

As can be seen from Figs 4 & 5, for a good quality signal and optimal settings near perfect image construction can be achieved.

published March 2008

MHS FISINT Successfully Collects Israeli F-16 Heads-Up Display (S//SI//REL)

[redacted], Menwith Hill Station (F77)

(S//SI/TK//REL) During the recent unrest in the Gaza Strip in January, Menwith Hill Station FISINT operators collected video for the first time from the cockpit of an Israeli Air Force F-16 fighter jet. The day before, MHS FISINT operators collected video from an Unmanned Aerial Vehicle (UAV). The UAV appeared to still be on the ground, which prompted the site to go back to the area again the next day. As a result, MHS collected the F-16 heads-up display that showed a target on the ground being tracked. MHS worked closely with a GCHQ site in Cyprus for tip-offs.

(S//SI//REL) Reacting to the unrest in the Gaza Strip, MHS conducted ad hoc range surveillance. On 3 January, the site collected the aircraft video from an Israeli F-16 fighter. The 14-second long video showed an "unbroken line" running through the targeting display, indicating that the target being tracked was on the ground.[1]

(S//SI//REL) Heads-up display from an Israeli F-16 fighter over the Gaza Strip. The target being tracked is located inside the circle.

(U//FOUO) POC: [redacted] ([redacted])

(U) Notes:

[1] (U//FOUO) Open-source reporting indicated that the Israeli Air Force was involved in at least five airstrikes over the Gaza Strip killing two militants.

(U//FOUO) This article is reprinted from MHS's Horizon newsletter, February edition.

S455N – Israeli UAV Digital Video

Golf Section, JSSU(CYP)

Analyst: [redacted]

CONTENTS

1. INTRODUCTION

1.1 This report covers analysis of S455N a High Data Rate (HDR) signal emanating from an Israeli UAV. The Signal of Interest (SOI) was first intercepted in April 2009 however, the original recording was too weak for full analysis. This report is based on the analysis of a recording made in April 2010.

1.2 S455N is a complex signal utilising a number of error correction and detection techniques to successfully convey Internet Protocol (IP) data carrying streaming digital video.

2. MODULATION

2.1 The SOI employs FSK modulation and is keyed at 9.11MBauds occupying approximately 10MHz bandwidth. Demodulation of the SOI was attempted using various demodulators including m2Extra however, the resultant bits were poor quality. The SOI was successfully demodulated using an FM demod in Black Magic.

2.2 Data is NRZL and frames consist of 4140 bits with a 44 bit synchronisation pattern – 11101011010101001101001101110011011111110000.

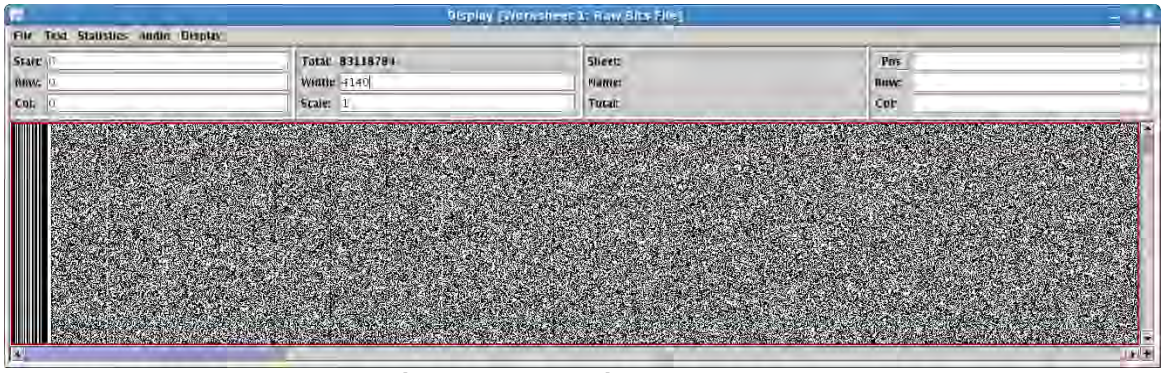

Fig 1: DVT Sync'd Data Frames

3. FORWARD ERROR CORRECTION (FEC) AND ERROR DETECTION

3.1 FEC and EDAC are achieved utilising a block interleaver and a two dimensional Turbo Product Code (TPC). The interleaver is a 64x64 bit block interleaver used to spread the data to improve the performance of the TPC. The TPC is a (64, 57)*(64,57) 2 dimensional code employing parity with a generating polynomial of:-

$$g(x) = x^6 + x^1 + 1$$

3.2 The FEC can be utilised to correct the data using magyk or removed by applying a t3648s448 to remove the vertical dimension and a t57s7 to remove the horizontal dimension.

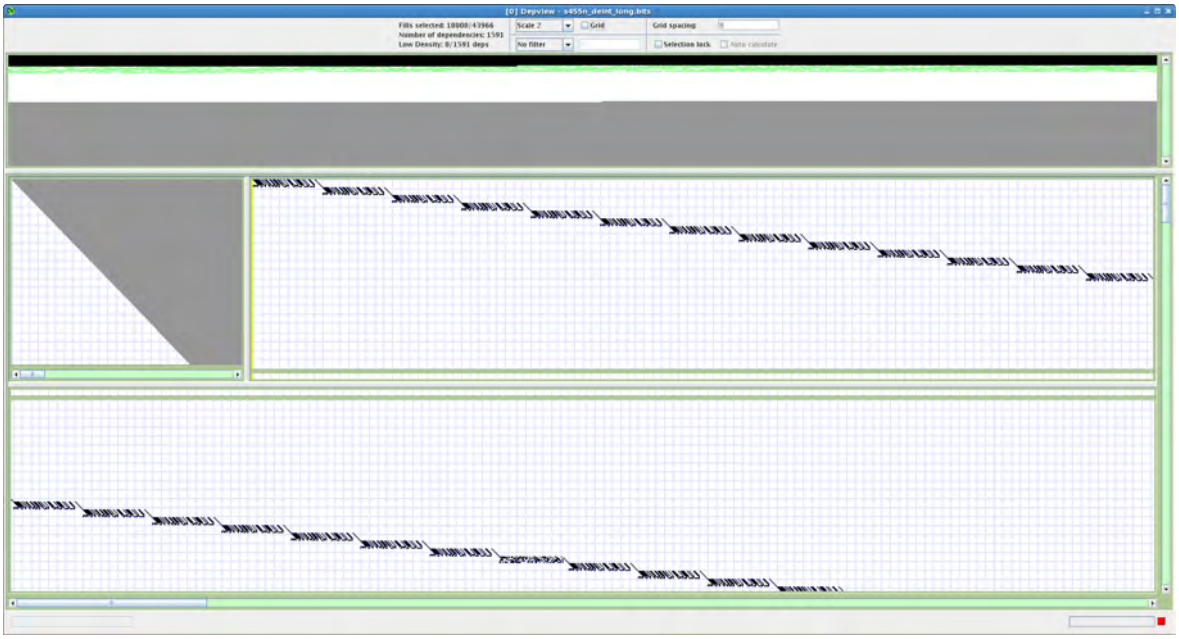

Fig 2: Depview showing horizontal dimension

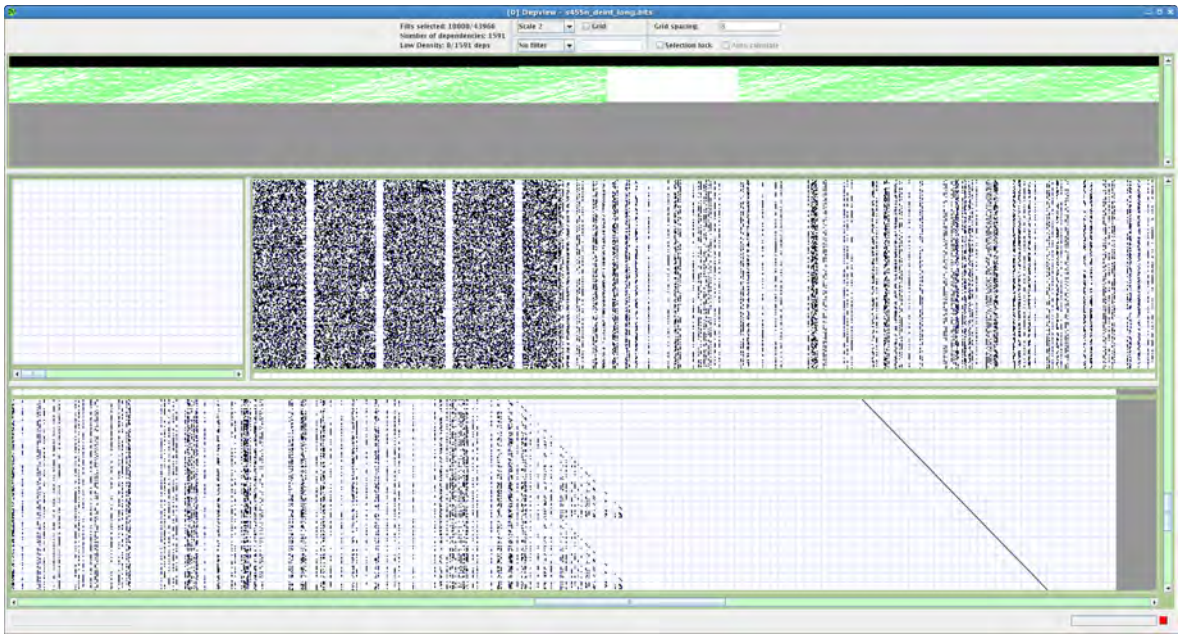

Fig 3: Depview showing vertical dimension

4. RANDOMISER

4.1 After deinterleaving the data and removing the FEC the frame width should be 3249 (57*57). The frame begins with a 10 bit sync except on every third frame where 10 bits of data are sent. These 10 bits of data raster on a width of 512 and conform to S455E. Removal of the 10 bits of sync/S455E from each frame will result in a frame width of 3239. The remaining data is randomised using a feed through randomiser F15(0,1,15).

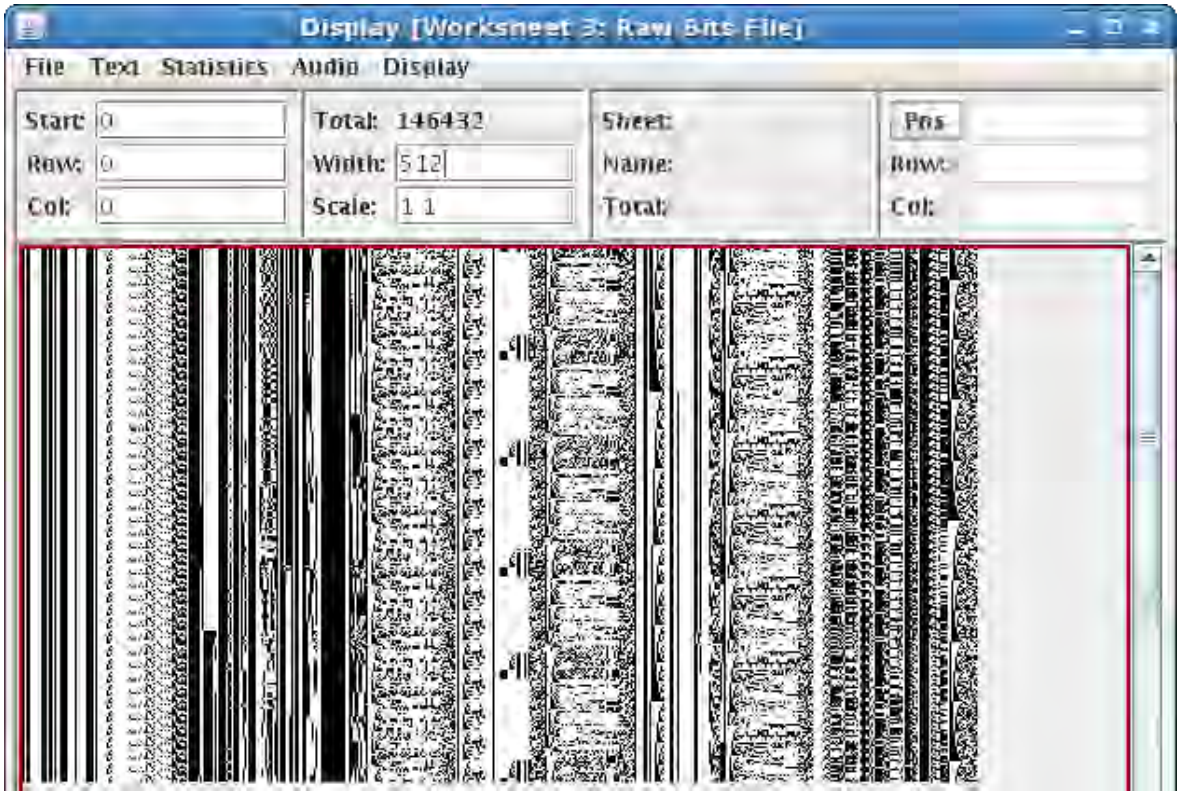

Fig 4: DVT Showing S455E Frames

5. PAYLOAD

5.1 Following removal of the randomiser the data was found to be HDLC. The packets contained IP data carrying Universal Datagram Protocol (UDP) conveying a number of different protocols. The main protocol in use was Real Time Protocol (RTP) and this was being used to carry MPEG 4 streaming video. Analysis of the video revealed multiple video streams from different cameras. The exact video encoding parameters have not been fully resolved and this should be taken in to consideration when viewing any outputted files.

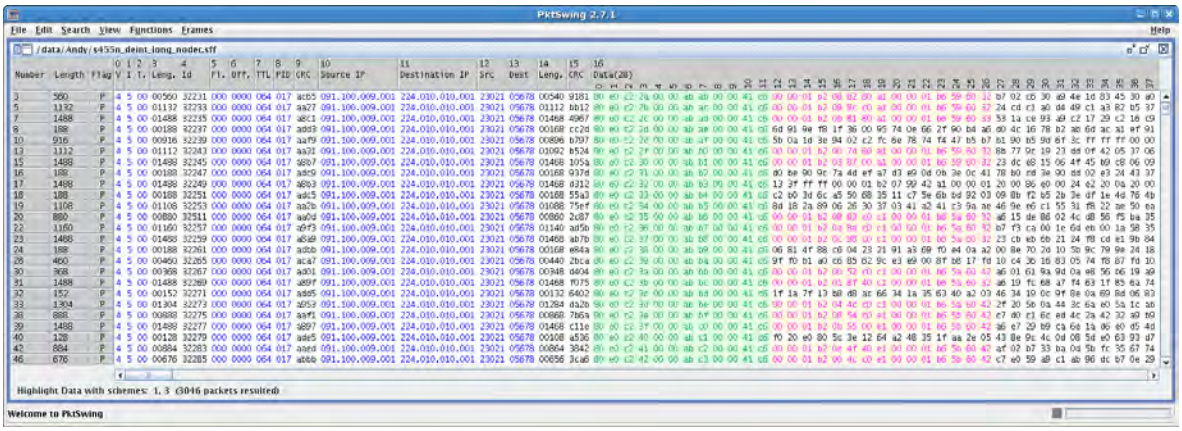

Fig 5: PktSwing showing IP packets carrying RTP conveying MPEG 4

6. VIDEO & S455E

6.1 The Video is MPEG 4 and appears to contain multiple streams; each stream appears to be capable of scanning through different camera views

Snapshots from Video

6.2 Telemetry is transmitted using normal S455E

Fig 6: GEO Plot extracted from S455E

7. CONCLUSION

7.1 A number of elements of this SOI need further analysis

- Video – Being analysed by OPC-SPF, GCHQ
- Remaining IP Data – They are a number of protocols in use that need resolving

7.2 This is potentially a significant upgrade to the normal analogue video we see, this new system adds the capability to see a number of video feeds simultaneously. We currently have no collection system capable of processing this signal due to the high data rate and complexity of the underlying data. There are a number of SIGINT collection solutions that would be more than capable of dealing with this signal should there be a requirement to do so.

Further information:

Intercept information and screen shots of associated S455A/E can be found on this wiki page:- [redacted]

This report was issued as:

TOP SECRET STRAP1 SPOKE

STRAP HANDLING NOTICE

(See Annexe H of the STRAP Security Manual for detailed guidance) SECRET STRAP reports may be seen by STRAP-inducted SC cleared readers who have a valid need-to-know. STRAP-inducted readers who hold a DV clearance may only see TOP SECRET reports at any STRAP level.

CONTACT:

Originator: [redacted],
OPA-AN
Non Secure: [redacted]

ACKNOWLEDGEMENTS:

[redacted]