TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

NETWORK ANALYSIS CENTRE

Making Network Sense of the encryption problem Roundtable

[redacted] Head of GCHQ NAC

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

GCHQ metadata

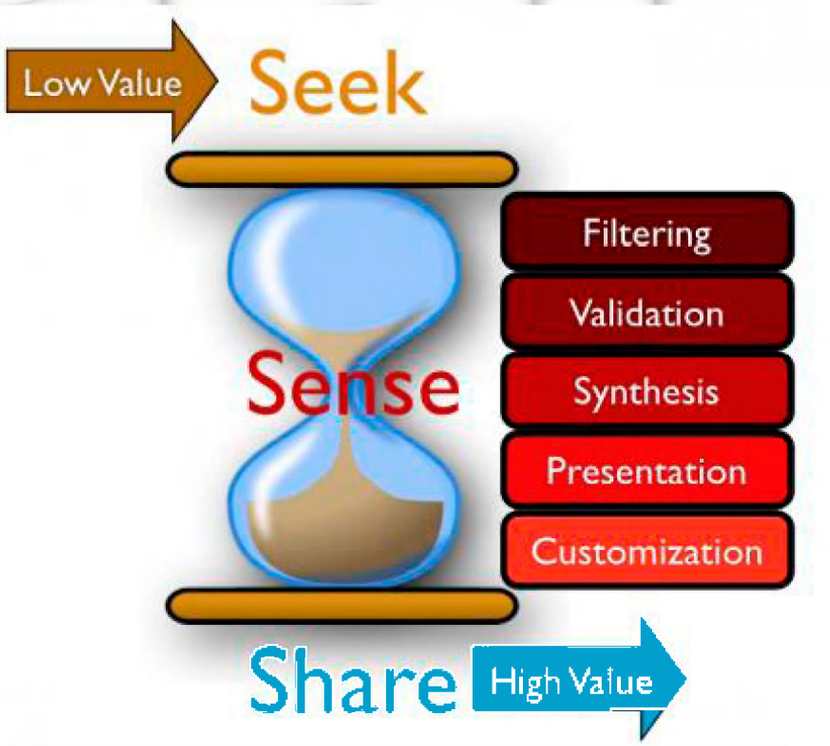
- GCHQ now creating metadata on:
  - SSL / TLS
  - IKE
  - OpenVPN
  - SSH
  - SQUEAL signatures (Various crypt packages)
- Data available in BEARDED PIGGY and/or the CLOUD

NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

How can Network Analysis help ?

- Can NAC help make sense using network knowledge of the volumes of data to isolate that which we want to decrypt…



NAC
NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

The Seed Approach

- Intercepted documentation reveals details of VPN set up…

[redacted]

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

The Seed Approach

- Turn Seed IP into network block
- Query on network block against metadata
- Chain outwards / fuzzy subnet logic
- Basis of NTAT developed tradecraft:
  - IRASCIBLE HARE
  - IRASCIBLE RABBIT
  - IRASCIBLE MOOSE
  - IRASCIBLE EMITT

.

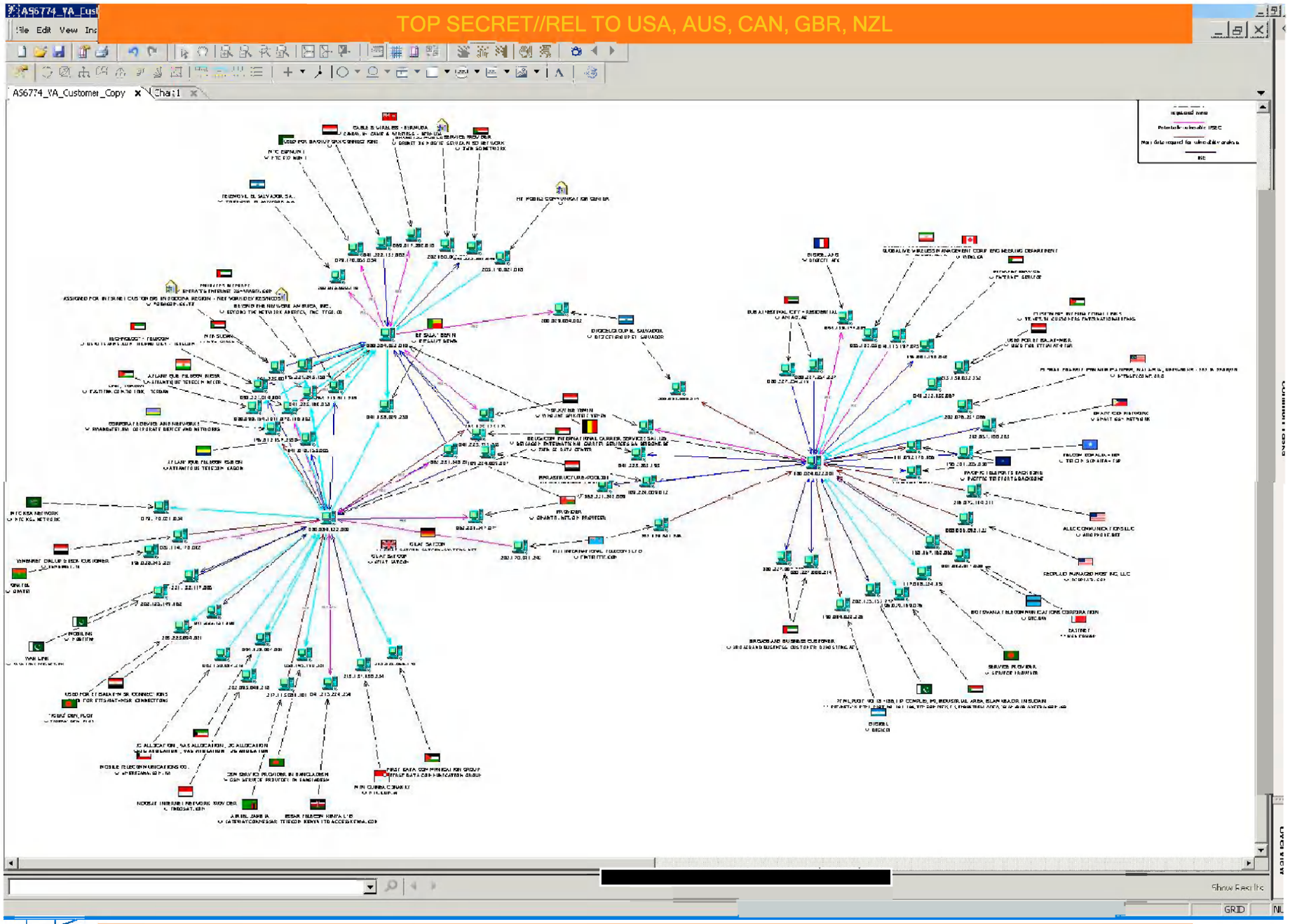
NAC
NETWORK ANALYSIS CENTRE

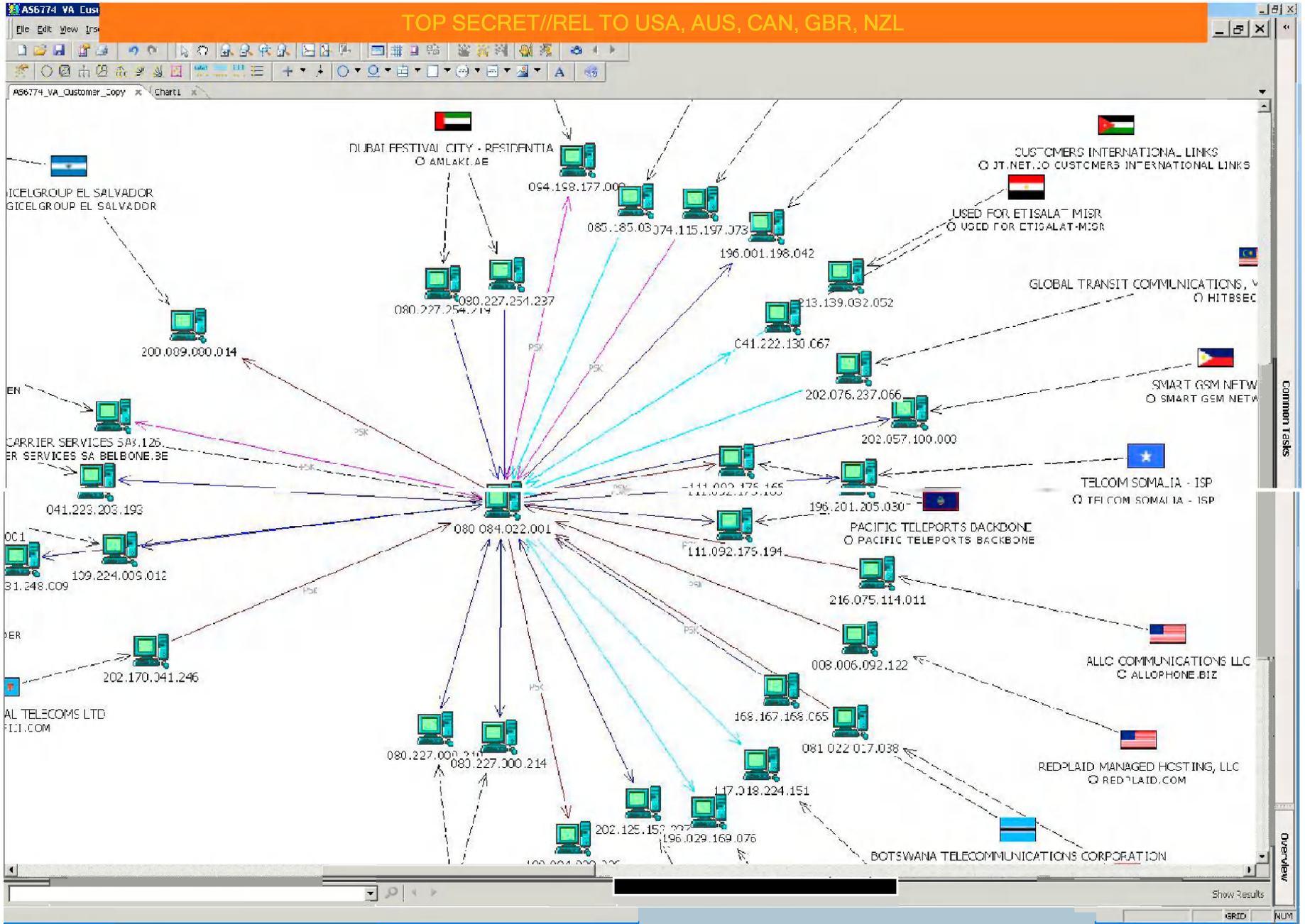
TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Known usage

- Target known to use encryption
  - Identify target subnet
  - Select on subnet against metadata
- Or…
  - Start with an AS – look for most interesting wheel
  - BELGACOM - AS6774 – known to run GRX links to MNO over VPN

NETWORK ANALYSIS CENTRE


A56774_VA_Customer_Copy
Chart1
File Edit View Ins
[redacted]
Show Events
GRID


AS6774_VA_Customer_Copy
Chart1
DUBAI FESTIVAL CITY - RESIDENTIA
O AMLAKI.AE
CUSTOMERS INTERNATIONAL LINKS
O JT.NET.JO CUSTOMERS INTERNATIONAL LINKS
USED FOR ETISALAT MISR
O USED FOR ETISALAT-MISR
GLOBAL TRANSIT COMMUNICATIONS,
O HITBSEC
SMART GSM NETW
O SMART GSM NETW
TELCOM SOMALIA - ISP
O TELCOM SOMALIA - ISP
PACIFIC TELEPORTS BACKBONE
O PACIFIC TELEPORTS BACKBONE
ALLO COMMUNICATIONS LLC
O ALLOPHONE.BIZ
REDPLAID MANAGED HOSTING, LLC
O REDPLAID.COM
BOTSWANA TELECOMMUNICATIONS CORPORATION
080 084.022.001
080.227.251.237
200.089.080.014
041.223.203.193
109.224.005.012
202.170.041.246
111.092.175.194
196.201.205.030
202.076.237.066
202.057.100.000
041.222.130.067
216.075.114.011
008.006.092.122
168.167.168.065
081 022 017.038
117.018.224.151
080.227.300.214
196.029.169.076
196.001.198.042
Common Tasks
Overview
Show Results
GRID
NUM

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Network Knowledge enrichment

- Internet Registry information
- IP Geolocation
- DNS
- Data derived from network device configuration files (routers/Firewalls etc)
- Network information on surrounding IPs (i.e. rest of subnet is MNO related)
- ……

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

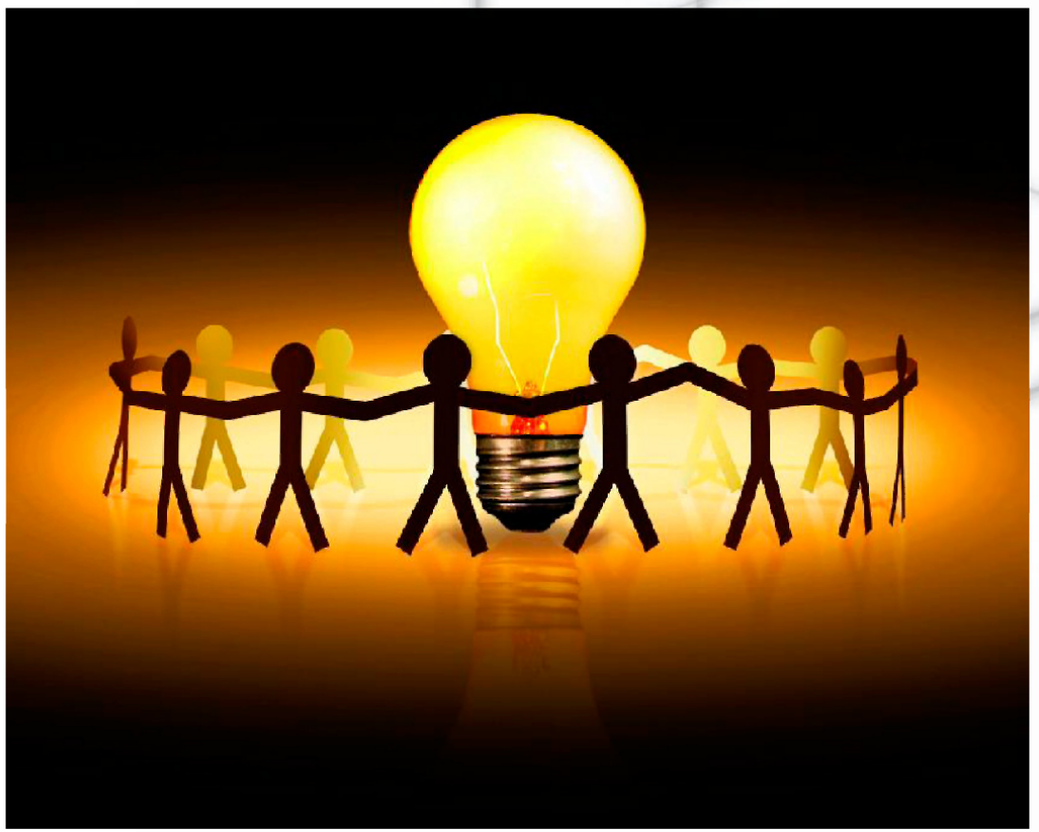
Access Optimisation

- A given role of Network Analysis is optimising access for a given problem – in this case enabling two-ended collection
- Or….. Identifying opportunities to get at the data before it is encrypted therefore no need to make sense of encrypted data. Can do this both:
  - Passive
  - Active

NETWORK ANALYSIS CENTRE

TOP SECRET STRAP 2 // REL TO USA, AUS, CAN, GBR, NZL

Your Idea's Please



NETWORK ANALYSIS CENTRE