

TOP SECRET STRAP 2

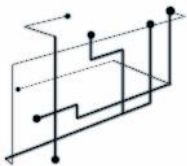


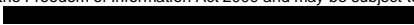
Mobile Networks in



World

 Head of GCHQ NAC

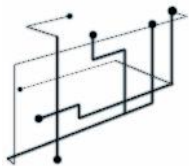
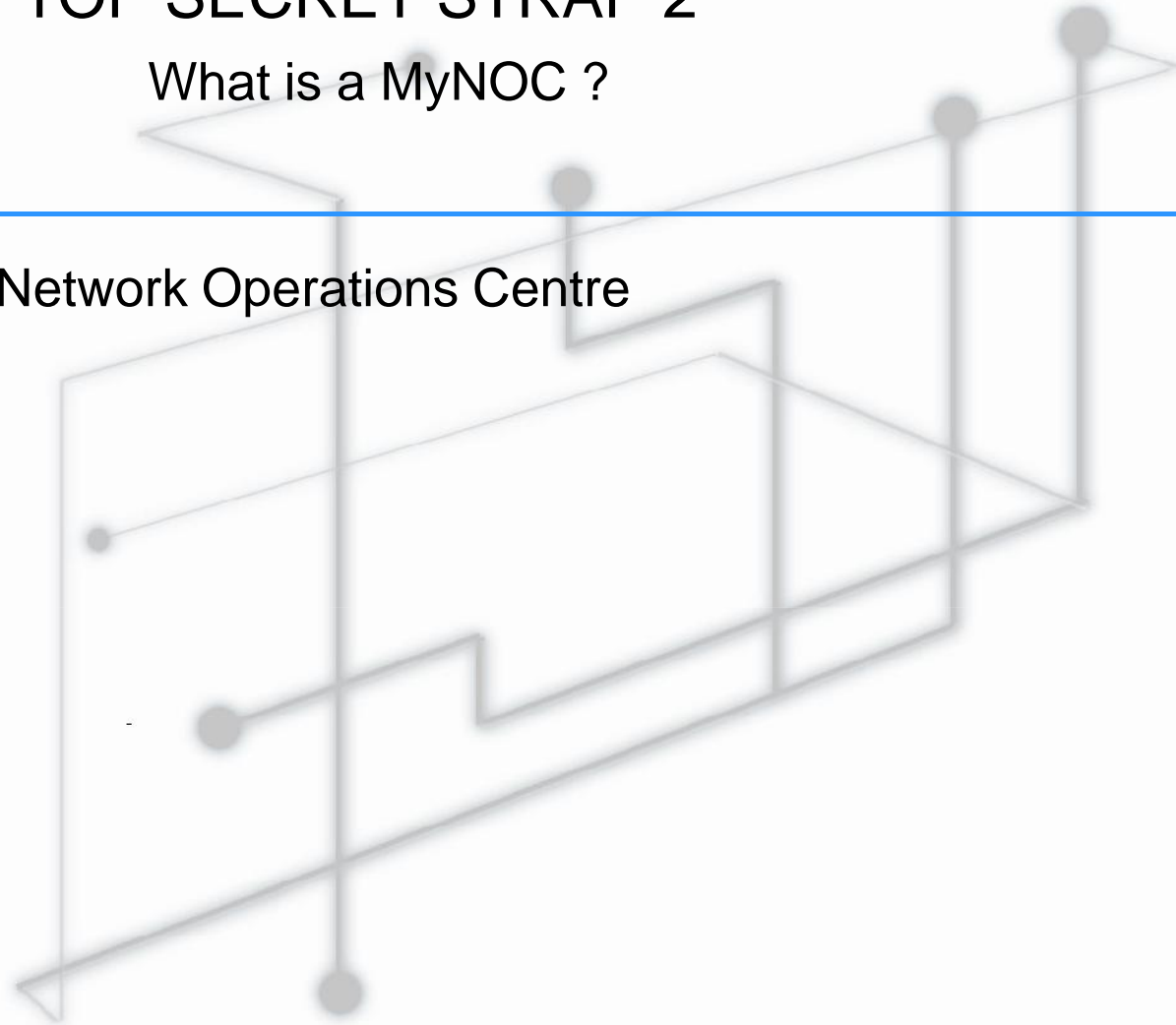


This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or 

TOP SECRET STRAP 2

What is a MyNOC ?

- MyNOC – My Network Operations Centre
 - A Space
 - A Concept



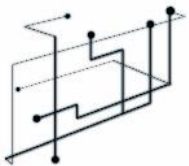
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

A Space

- Analyst Desktop X 10
- Un-attributable internet X 10
- JTRIG Desktop
- HIGHNOTE – CNE Toolsuite
- COPPERHEAD – CNE Attack box
- NEXUS (BSS Desktop)
- CADDIS (SIS Desktop)
- NRT Tipping Display
- 65” VTC/Collaborative Monitor and Projector
- Virtual Whiteboarding tool and Whiteboard
- Secure telpehony / storage



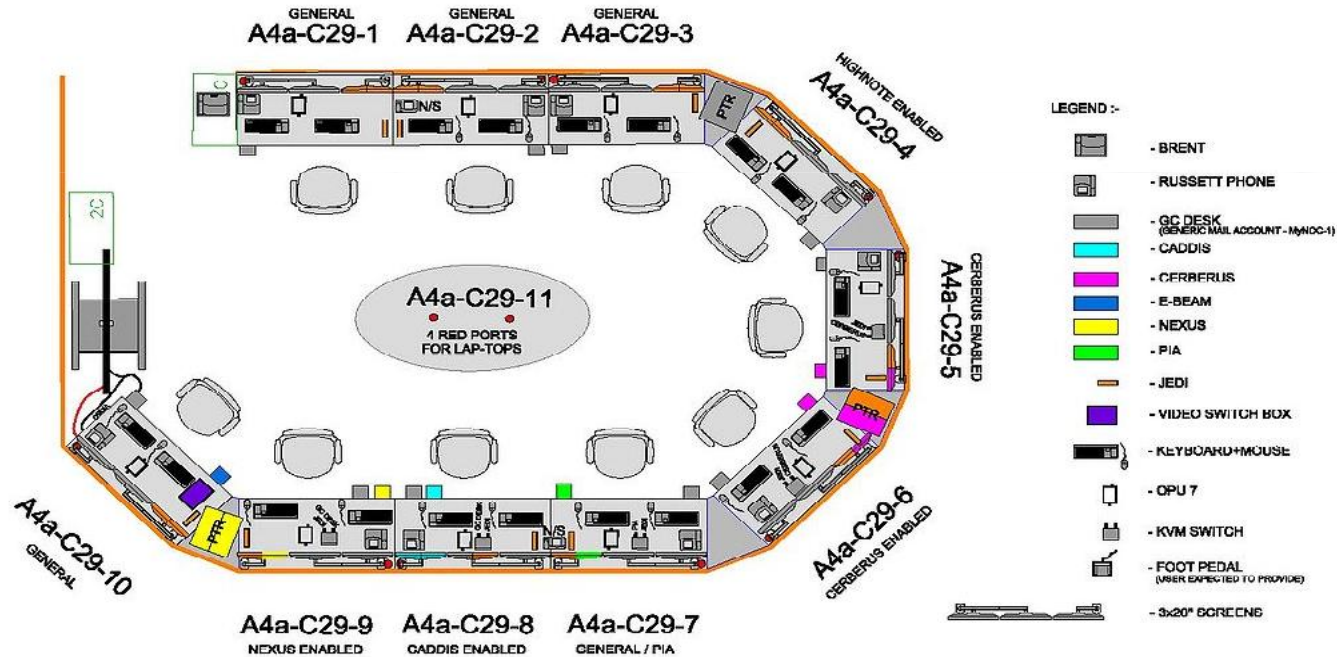
TOP SECRET STRAP 2

A Space

MyNoc Locations

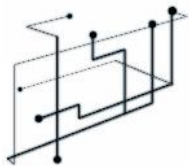
The MyNocs are located as follows and contain the following capabilities:

- MyNOC1 A4a,
- MyNOC2 C4c,
- MyNOC3 B4d
- MyNOC4 C4d
- MyNOC5 A4f



TOP SECRET STRAP 2

Interlopers in A Space



NAC
NETWORK ANALYSIS CENTRE

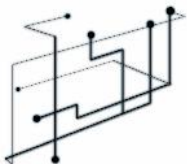
This information is exempt from disclosure under the Freedom of Information Act 2000 and the Freedom of Information (Scotland) Act 2002. Refer disclosure requests to GCHQ or [REDACTED]

exemption under other UK information

TOP SECRET STRAP 2

A Concept

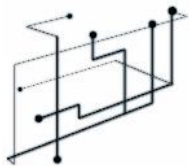
- **Collaboration** environment bringing together capability from **across GCHQ**.
- Appropriate **resources** identified / Appropriate **prioritisation**
- Formalised planning process
 - Clear **Focused** objectives
 - Selection of **Operations Manager**
 - **Preparation**
 - Review
- Assessment and feasibility
- Professional Operations Manager
 - Ensure operation is focused on stated objectives
 - Ensures operation is legal
 - Protects information equities



TOP SECRET STRAP 2

MyNOC & NAC

-
- NAC tasked with development of “greater good” capability in Mobile/Mobile Internet environment.
 - Due to lack of progress decision made to sponsor three MyNOC events:
 - OP WYLEKEY – Exploitation of International Mobile Billing Clearing Houses
 - OP SOCIALIST – Exploitation of GRX Operator
 - OP INTERACTION – Development of in-depth knowledge of Mobile Gateways.



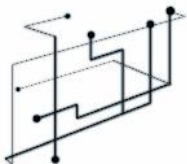
nac
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

MyNOC Team assemble

- Operations Manager
- Network Analysts (NAC Cheltenham, NAC Bude & NAC Cyprus)
- Dataminer (GTAC)
- Open Source Specialist
- JTRIG Analysts (Cheltenham & Bude)
- CNE Operators (Cheltenham CNE & Scarborough CNE)
- VPN Expert (Crypt SD)
- EREPO Expert (CNE)
- Protocol Analyst (GTE)
- Production Tasking Co-ordinator (PTC)
- Trainee Ops Managers



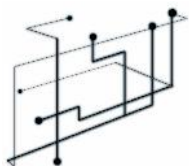
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

One Month Later – OP SOCIALIST

- Scoping session conducted – main focus to be on enabling CNE access to **BELGACOM GRX Operator**
- **Ultimate Goal – enable CNE access to BELGACOM Core GRX Routers from which we can undertake MiTM operations against targets roaming using Smart Phones.**
- Secondary focus – breadth of knowledge on GRX Operators
- Operations Manager assigned, team assembles



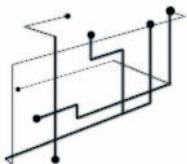
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

Preparation work

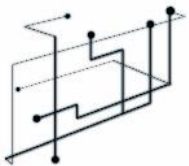
- Identified static web gateways and IP range used by engineers and tasked for QUANTUM operations
- Identification and tasking of optimal bearers
- TDI data mining identified potential for exploitation of LinkedIn as a vector for QI – QI capability developed for LinkedIn
- WOODCUTTER logs analysed for usage by BELGACOM.



TOP SECRET STRAP 2

MyNOC Focus

- Expand **collection and capability** to enable better exploitation of Belgacom.
- Identify **key staff at BICS**, and selectors used by these individuals for QI.
- **Map the network** to better understand the Belgacom Infrastructure.
- Investigate **VPN links** from BICS to other telecoms providers.
- Investigate the vulnerability of the **MyBICS** Reporting Tool.

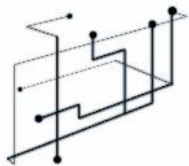
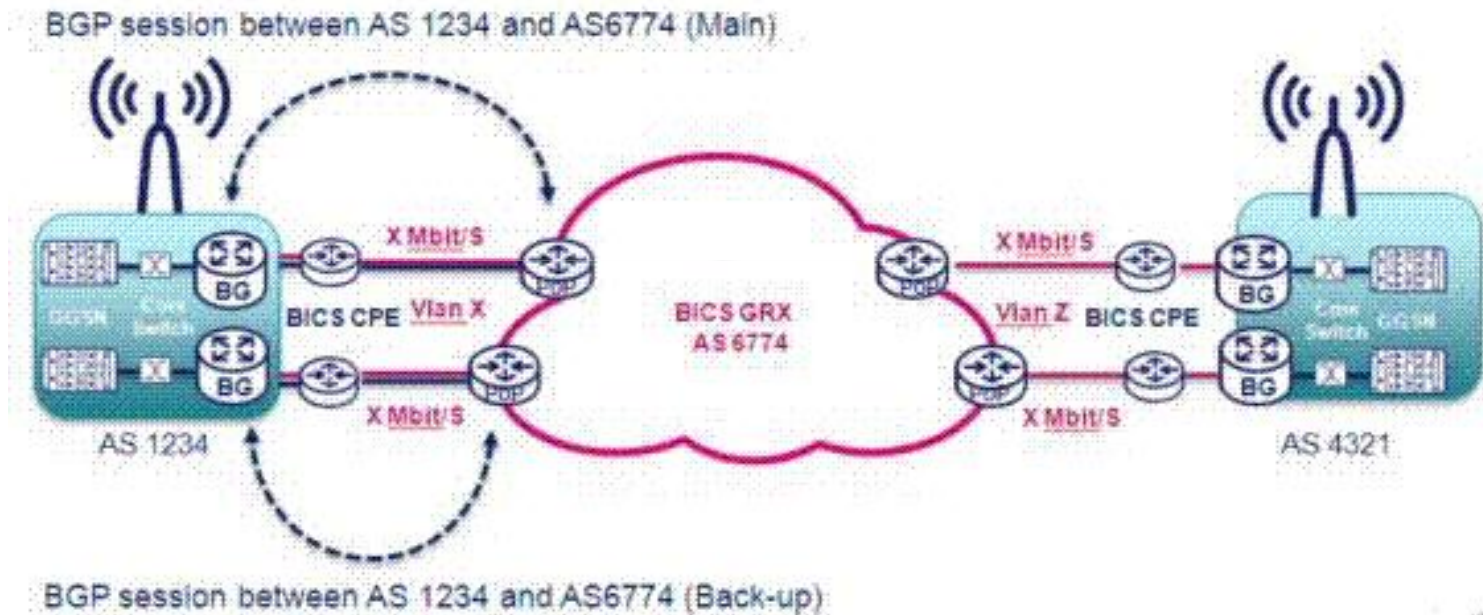


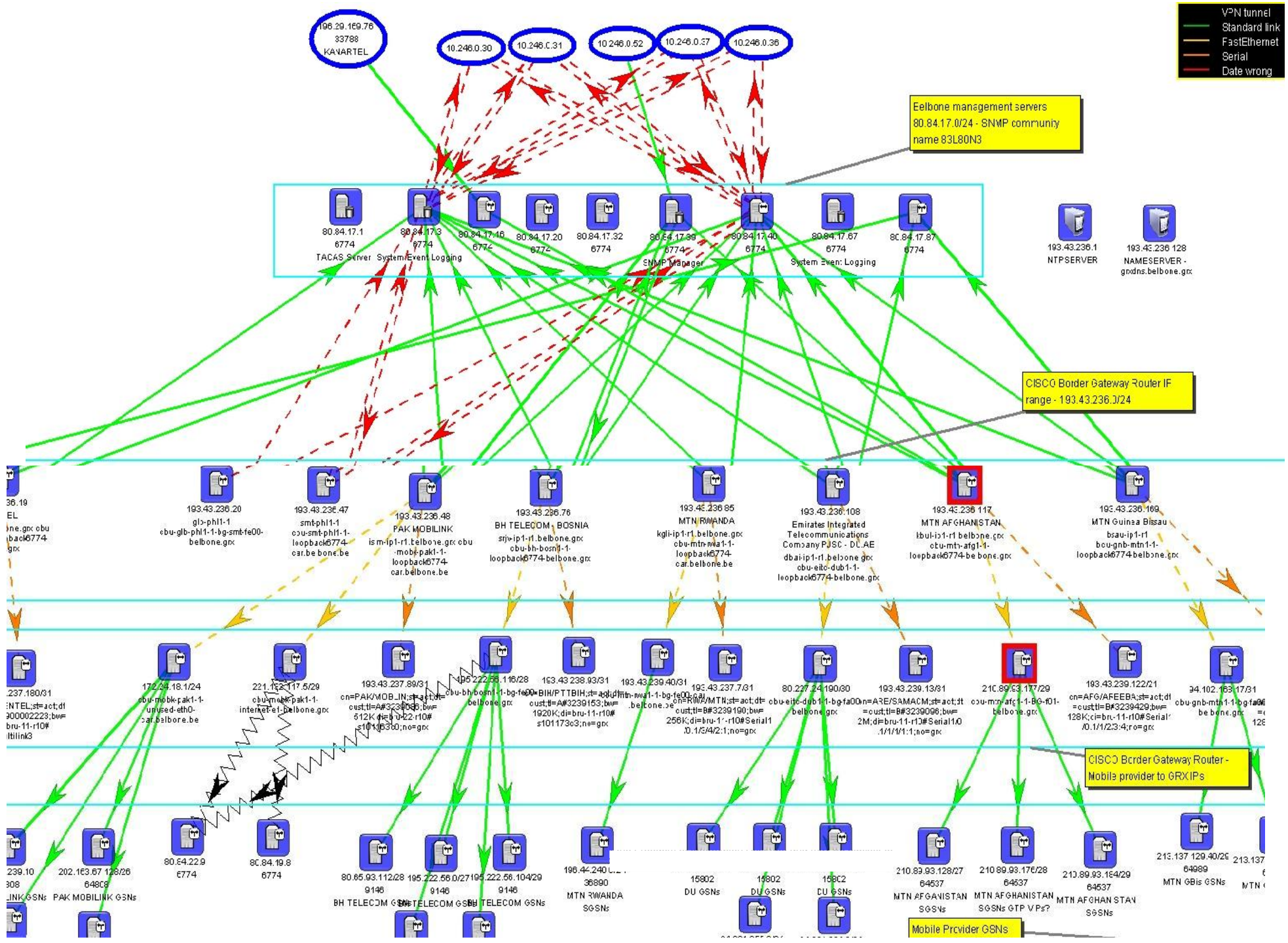
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

Infrastructure

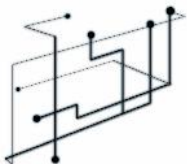




TOP SECRET STRAP 2

Key BELGACOM staff

- Identify Belgacom employees
 - NOC staff
 - In areas related to maintenance or security
- Selectors to enable QUANTUM targeting
 - Use of LinkedIn noted
 - Use of Slashdot.org noted
- MUTANT BROTH used to identify TDI/Selectors coming from identified range/proxy
- QI capability enhanced to allow shots on LinkedIn
- QI capability enhanced to allow 'white listing' when shooting on proxy



TOP SECRET STRAP 2

NOC IP range search in MUTANT BROTH

MUTANT BROTH

Identifier Search

IP Address Search

Password Search

IP Prefix Search

Legal Context

- This is a powerful technique that allows you to pull back presence events for an IP network.
- You **must** make sure that your HRA justification (Reason) clearly explains why you are querying on an IP network, as you are more likely to retrieve the communications of innocent individuals as well as targets.
- Your queries will be logged for audit.
- You should use Traceroute or DNS look up first so that only IP prefixes registered or associated with the target networks are queried.
- If you suspect that the IP prefix is dynamic, you must **either** combine this search with another filter eg an HHFP **or** limit the query length to 60 minutes.
- If after running the query, it is clear that the IP prefix is dynamic, you should not look at the results as they are unlikely to relate to your target.

Search for IP address prefixes

- Enter the set IP address prefixes.
- The IP address range must be specified as: < dotted decimal IP >/< prefix length >
- Example: 172.16.17.0/23
192.168.4.5
192.168.128.0/17
- Prefix lengths of less than 16 bits will be ignored.
- Absent lengths are assumed to be 32 bits.
- Optionally enter the HHFP or the time period start and search length in minutes.

IP Ranges

80.84.19.0/24

HHFP

Time period start

Search length (minutes)

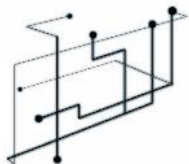
MIRANDA

JIC

Purpose

Reason

Execute



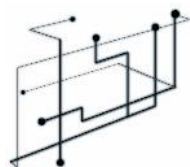
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ or [REDACTED]

TOP SECRET STRAP 2

NOC IP range – Target identifiers for QUANTUM INSERT

Source IP	User-Agent	Date	Time	Non Routine Source	Source IP:HHFP	Source IP Geo	Identifier Type	Identifier Value	Event Count (%)
80.84.19.9	Mozilla/5.0 (X								(4 %)
	Mozilla/5.0 (X	17/05/11	00:02:54		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LLM	Yahoo-B-Cookie		(4 %)
	Mozilla/5.0 (X								(2 %)
	Mozilla/5.0 (X	17/05/11	00:02:59		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LLM	Yahoo-B-Cookie		(0 %)
	Mozilla/4.0 (c								(1 %)
	Mozilla/5.0 (X	17/05/11	00:02:59		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LHV	Yahoo-B-Cookie		6 (16 %)
	Mozilla/5.0 (W								(4 %)
	Mozilla/5.0 (X	17/05/11	00:05:37		80.84.19.9:5eec974d	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		2 (14 %)
	Mozilla/5.0								(0 %)
	Mozilla/5.0 (X	17/05/11	00:16:18		80.84.19.9:7d9134a5	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		4 (28 %)
	Mozilla/5.0 (X								2 (18 %)
	Mozilla/5.0 (W	17/05/11	00:17:58		80.84.19.9:77387b02	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		(3 %)
		17/05/11	00:23:35		80.84.19.9:e4a90e3f	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:28:05		80.84.19.9:7d9134a5	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:37:34		80.84.19.9:b36815d3	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:39:55		80.84.19.9:fi2897e0	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:47:56		80.84.19.9:477c4721	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-Cookie		
		17/05/11	00:54:38		80.84.19.9:d23bad41	50.83;4.33;BRUSSELS;BE;7LHV	Google-PREFID-		



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

Real-time picture of QI

The screenshot shows the NRTA Dashboard for OPSOCIALIST. At the top, a red banner reads "TOP SECRET STRAP 2 UK EYES ONLY". Below this, the dashboard title is "NRTA Dashboard for RROC" and the specific view is "Alerts for OPSOCIALIST".

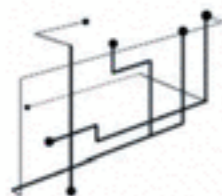
Target	TOI Type	Selector	IP addresses	Age	From	To	OS
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.149.99	1,860,000 ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63
[REDACTED]	LinkedIn-Memberid	[REDACTED]	Route: 93.184.209.38 Src: 93.184.209.38; Dest: 216.52.242.80	15,267,700 ago	[REDACTED]	[REDACTED]	Firefox 3.6.13
[REDACTED]	LinkedIn-Memberid	[REDACTED]	Route: 93.184.209.38 Src: 93.184.209.38; Dest: 216.52.242.82	15,177,700 ago	[REDACTED]	[REDACTED]	Safari 4.0
[REDACTED]	LinkedIn-Memberid	[REDACTED]	Route: 178.144.20.284 Src: 178.144.20.284; Dest: 216.52.242.89	20,111,500 ago	[REDACTED]	[REDACTED]	Safari 4.0
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 10.252.243.17 Src: 10.252.243.17; Dest: 10.225.01.102	22,367,000 ago	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.149.104	23,807,000 ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 10.252.243.5 Src: 10.252.243.5; Dest: 10.225.01.68	24,247,000 ago	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 10.252.243.11 Src: 10.252.243.11; Dest: 10.225.01.199	24,357,000 ago	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	Google-WEBID-Cookie	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 209.85.149.104	24,507,000 ago	[REDACTED]	[REDACTED]	Firefox 3.6.13
[REDACTED]	LinkedIn-Memberid	[REDACTED]	Route: 213.181.44.4 Src: 213.181.44.4; Dest: 216.52.242.80	26,147,000 ago	[REDACTED]	[REDACTED]	Chrome 6.0.472.63

GeoLookup reports IP address 213.181.44.4 as NICHOLEN (low confidence), BE (high confidence).
No results returned.

Date	Time (UTC)	Source	Destination	Type	Description
11/02/11	14:56:23	213.181.44.4:80792659	193.125.115.181	HTTPFromPOST	POST to widget.samsungmobile.com/NP/UpdateMagerService/Service1.aspx/GetMatchNotify
11/02/11	14:56:14	213.181.44.4:96019290	46.137.114.64	HTTP	GET rainbow.mythings.com [REDACTED]
11/02/11	14:56:14	213.181.44.4:96019290	79.125.107.244	HTTP	GET pixel.rubiconproject.com/fap.php?tv=566011
11/02/11	14:56:03	213.181.44.4:80792659	193.125.115.181	HTTPFromPOST	POST to widget.samsungmobile.com/NP/UpdateMagerService/Service1.aspx/GetMatchNotify
11/02/11	14:55:59	213.181.44.4:96019290	46.137.114.64	HTTP	GET rainbow.mythings.com [REDACTED]
11/02/11	14:55:56	213.181.44.4:44149444	46.137.126.199	HTTP	GET smchv0bin.adswizz.com [REDACTED]
11/02/11	14:55:46	213.181.44.4:44149444	46.137.126.199	HTTP	GET smchv0bin.adswizz.com [REDACTED]
11/02/11	14:55:42	213.181.44.4:80792659	193.125.115.181	HTTPFromPOST	POST to widget.samsungmobile.com/NP/UpdateMagerService/Service1.aspx/GetMatchNotify

Expand all Collapse all Export CSV Export XML

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ at [REDACTED]



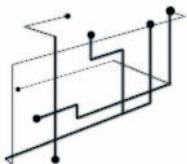
NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ at [REDACTED]

TOP SECRET STRAP 2

GTAC effort

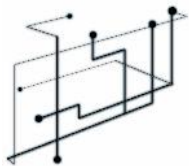
-
- IR21 extractions
 - Website research – domains visited from target gateway IPs
 - TDI harvesting
 - Identified owners of TDIs / finding new potential targets
 - Identified the FTP service
 - User agent analysis
 - Laptop identification
 - Mail server analysis
 - SSL research
 - GRX analysis



TOP SECRET STRAP 2

What MyNOC Priority gets you

- Dedicated resources
- Priority tasking of access
- Priority utilisation of CNE Operator resources
- Priority utilisation of CNE Developer resources
- Priority use of enabling community (GTE, GTAC, JTRIG)
- Priority time of legalities bodies



nac
NETWORK ANALYSIS CENTRE

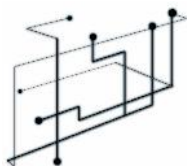
This information is exempt from disclosure under the Freedom of Information Act 2000 and related legislation. Refer disclosure requests to GCHQ or [REDACTED]

exemption under other UK information

TOP SECRET STRAP 2

OP SOCIALIST Outcome

- In MyNOC:
 - CNE Access to BELGACOM – MERION ZETA – 6 endpoints into Engineer/support staff IP range
 - 2 endpoints into BELGACOM DMZ (from prep VA work)
 - Optimal Bearers identified providing good access to BELGACOM proxy.
- Post MyNOC:
 - Optimal Bearers continue to allow QI against BELGACOM engineers/proxy
 - Internal CNE access continues to expand – getting close to access core GRX Routers – currently on hosts with access
 - NAC continue to support with Network Analysis of internal networks, network understanding research on credentials and identification of engineers/system administrators and their specific roles.

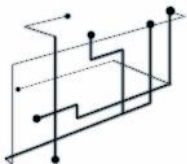




TOP SECRET STRAP 2

MyNOC leave behinds for NAC

- Focused working in small groups
- Regular Brainstorming sessions
- Professional Operational Management
- Network becomes Target – Target approach to Network Problems
- Awareness of JTRIG and Open-source information specialist capabilities and how they can support Network Analysis.
- Steerage of access for Network Analysis gain
- Closer working between NAC and CNE
- Joint working between NACs
- More NAC MyNOC/Focus efforts to come....

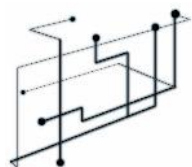


NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]

TOP SECRET STRAP 2

Questions ?



NAC
NETWORK ANALYSIS CENTRE

This information is exempt from disclosure under the Freedom of Information Act 2000 and may be subject to exemption under other UK information legislation. Refer disclosure requests to GCHQ on [REDACTED]