Full-Spectrum Cyber Effects

---

name redacted
Head of JTRIG

name redacted
SD Effects Lead

SIGINT Development as an enabler for GCHQ's "Effects" mission

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Effects

Destroy | Deny | Degrade | Disrupt | Deceive | Protect

Computer Network Attack (CNA)
Computer Network Information Operations (CNIO)
Disruption

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Effects in GCHQ

- Definition: having an impact in the real world
- Key deliverers: JTRIG and CNE
- Now major part of business – 5% of Operations
- Across all target types
- Continuous innovation of new tools and techniques

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNIO

Computer Network Information Operations

- Propaganda
- Deception
- Mass messaging
- Pushing stories
- Alias development
- Psychology









This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Disruption / CNA

- Masquerades
- Spoofing
- Denial of service
  - Phones
  - Emails
  - Computers
  - Faxes



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Call "bombing"

Hotel Attack

Maritime Cyber

Critical Infrastructure

Individual/Enterprise Low Impact

EFFECTS

Country wide High impact

WiFi DoS

Email/SMS Spoofing

PSYOP (social networks /phone/ email)

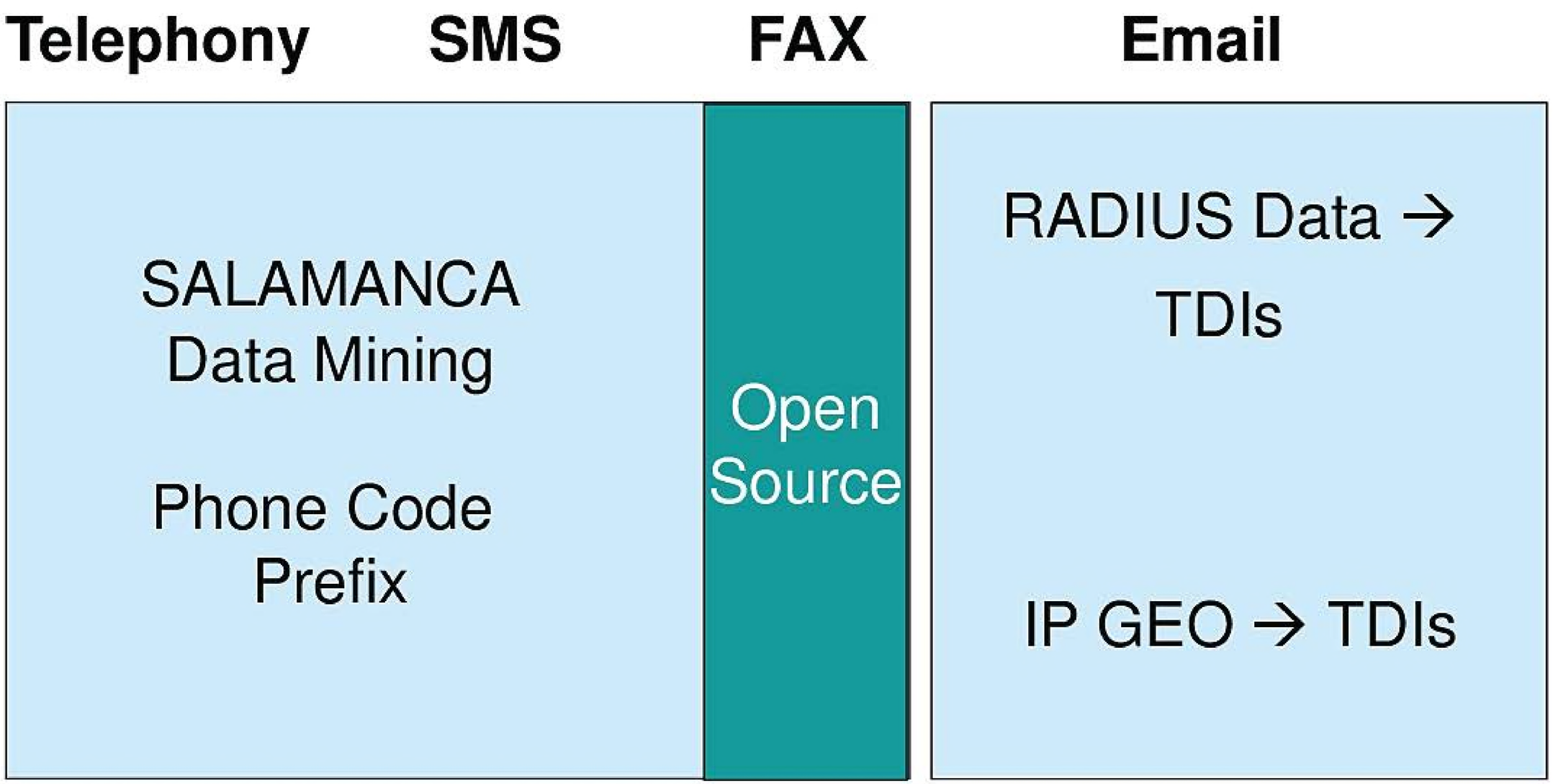
Internet Routing

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Information Operations

INFINITE CURVATURE/MOUNTAIN SLOPE

Sending messages across the full spectrum of communications



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

ROYAL CONCIERGE

A SIGINT driven hotel reservation tip-off service

From: reservations@expensivehotel.com
To: new-target@mod.gov.xx

"Thank you for reserving……"



ROYAL CONCIERGE exploits these messages and sends out daily alerts to analysts working on governmental hard targets

What hotel are they visiting?
Is it SIGINT friendly?

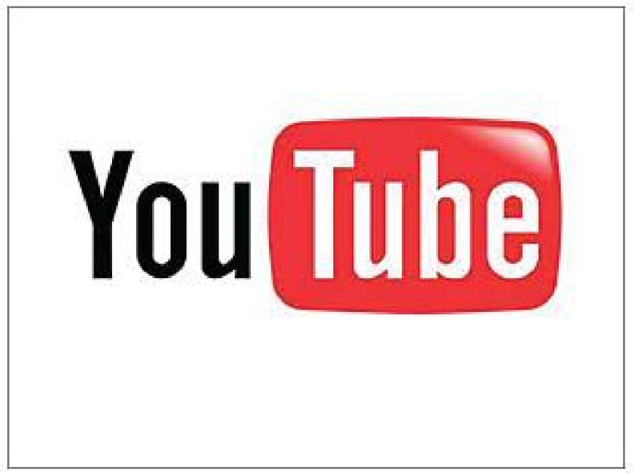
An enabler for effects – can we influence the hotel choice? Can we cancel their visit?

We can use this as an enabler for HUMINT and Close Access Technical Operations

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Information Operations: The Social Web









Deliver messages and multimedia content across Web 2.0

Crafting messaging campaigns to go 'viral'

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNIO

Twitter TDI Development

Need SIGINT coverage across protocols,
Not necessarily consistent with *target* SIGDEV priorities



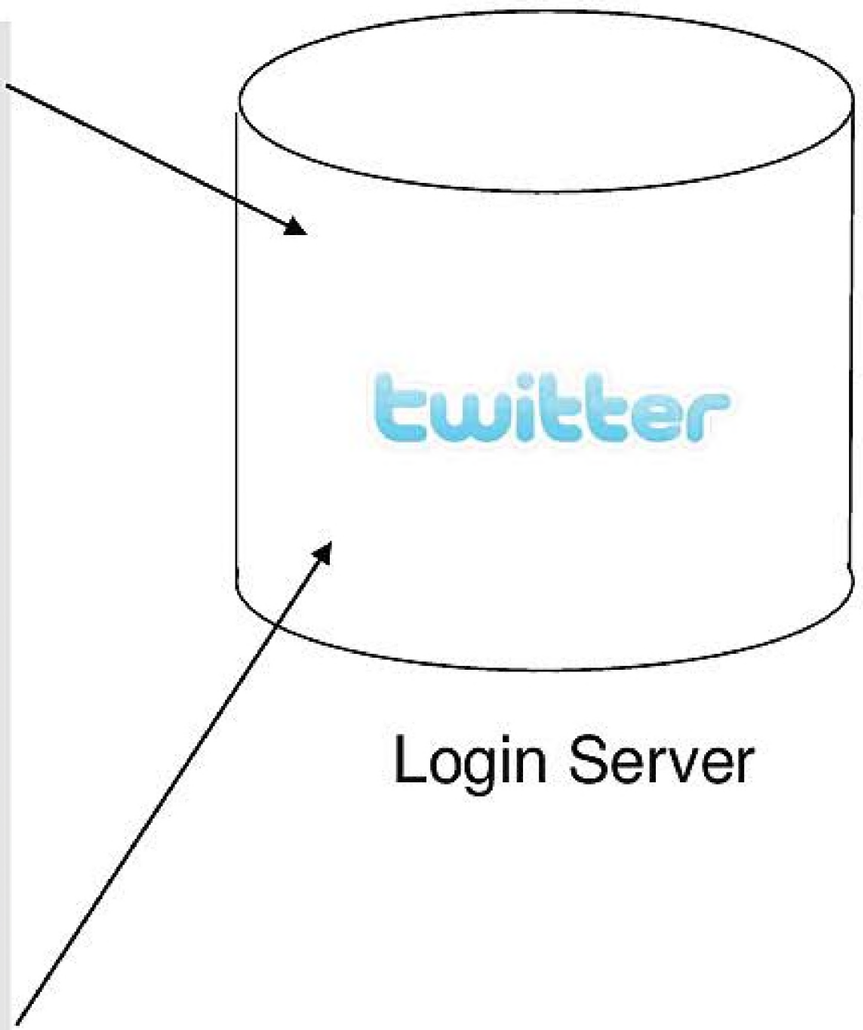
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNIO

Twitter TDI Development

Base64 + double encoded URL

```
0000000 004  \b   {  016   :  023   p   a   s   s   w   o   r   d   _   t
0000020   o   k   e   n   "   -   a   a   0   b   7   d   9   4   9   9
0000040   b   5   2   d   9   d   3   3   3   2   a   7   6   9   9   2
0000060   6   3   4   c   f   f   3   f   9   4   3   c   b   d   :  \f
0000100   c   s   r   f   _   i   d   "   %   6   f   b   4   a   5   9
0000120   9   d   5   d   2   9   d   2   a   a   7   e   8   d   7   3
0000140   9   c   6   e   a   f   4   7   9   "   '   s   h   o   w   _
0000160   d   i   s   c   o   v   e   r   a   b   i   l   i   t   y   _
0000200   f   o   r   _   s   o   l   o   _   o   n   l   y   0   :  025
0000220   i   n   _   n   e   w   _   u   s   e   r   _   f   l   o   w
0000240   0   :  021  t   r   a   n   s   _   p   r   o   m   p   t   0
0000260   :  \t   u   s   e   r   i  004 003 331   0  001  "  \n   f   l
0000300   a   s   h   I   C   :   '   A   c   t   i   o   n   C   o   n
0000320   t   r   o   l   l   e   r   :   :   F   l   a   s   h   :   :
0000340   F   l   a   s   h   H   a   s   h   {  \0  006  :  \n   @   u
0000360   s   e   d   {  \0   :  007  i   d   "   %   a   d   4   e   8
0000400   c   6   6   c   4   f   4   d   3   e   6   4   b   9   d   f
0000420   f   0   b   f   8   e   c   d   8   4   2   :  017  c   r   e
0000440   a   t   e   d   _   a   t   l   +  \b   e  202  %   .   '  001
0000460
```



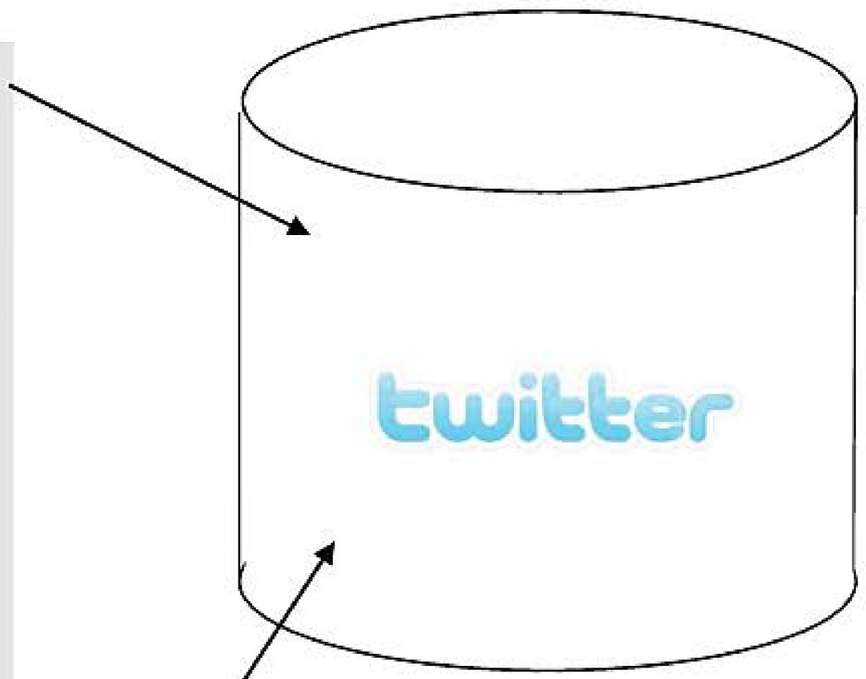
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNIO

Twitter TDI Development

PPF application across 10G Environment

1272671024 **81.169.145.25**
128.242.240.20 6 55489 80 Login-
twitter.com 31 **solo_only@twitter.com**
TDI-Scope 4 User Route 13
81.169.145.25 HHFP-Hash 8 38
4646d4 User-Agent 52 Twitter Tools
Geo-IP-Src 28
49.00;8.39;**KARLSRUHE;DE**;5MVV
Geo-IP-Dst 33 39.0062;-
77.4288;STERLING;U
S;7LLM Event-security-label 6 10007F
Stream-security-label 10 400023E0FF

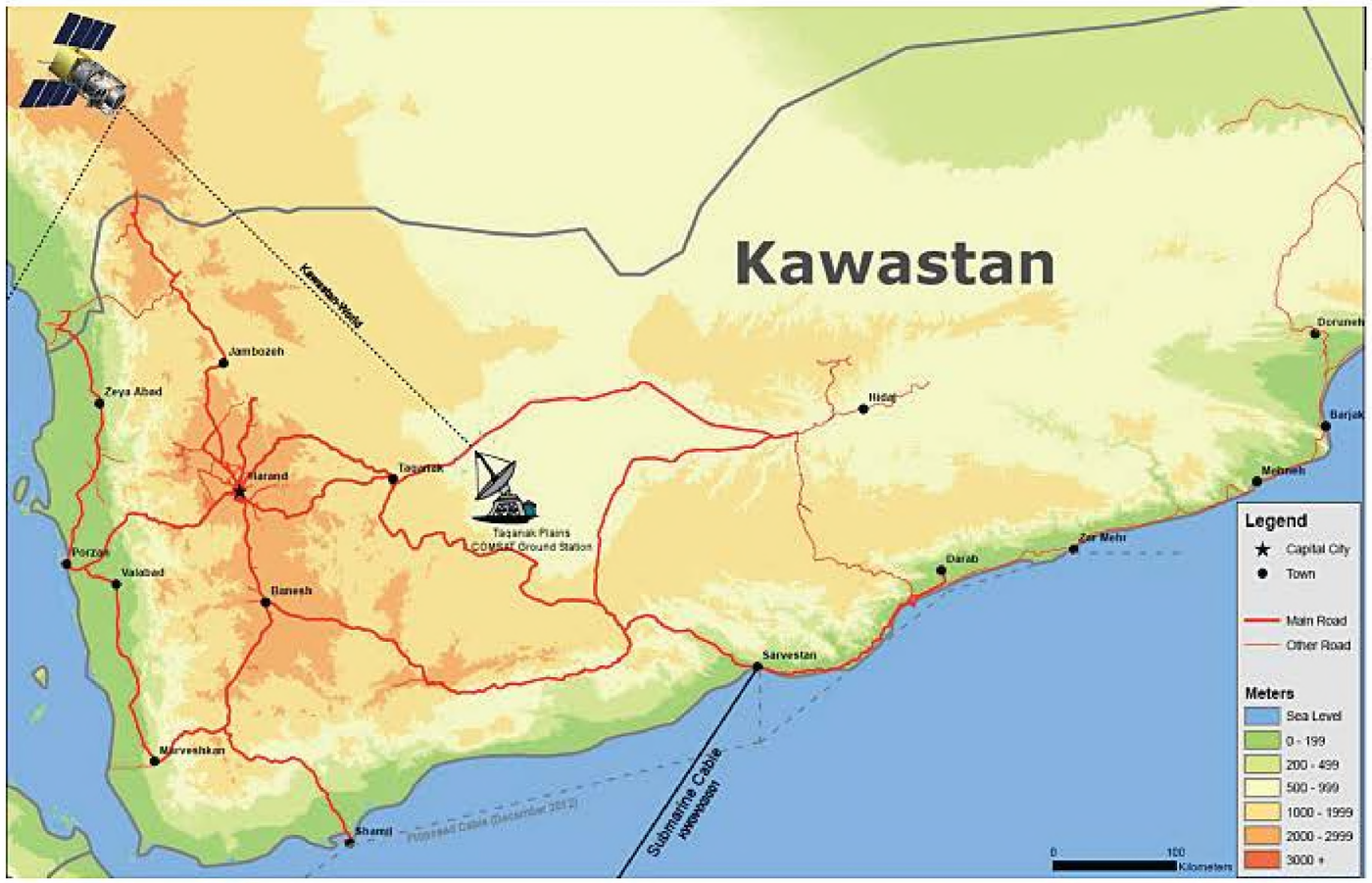


Millions of events per day feeding BLACKHOLE

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNIO

Twitter TDI Development



Given a country:

Who are the top Twitter Users?

Or given a user:

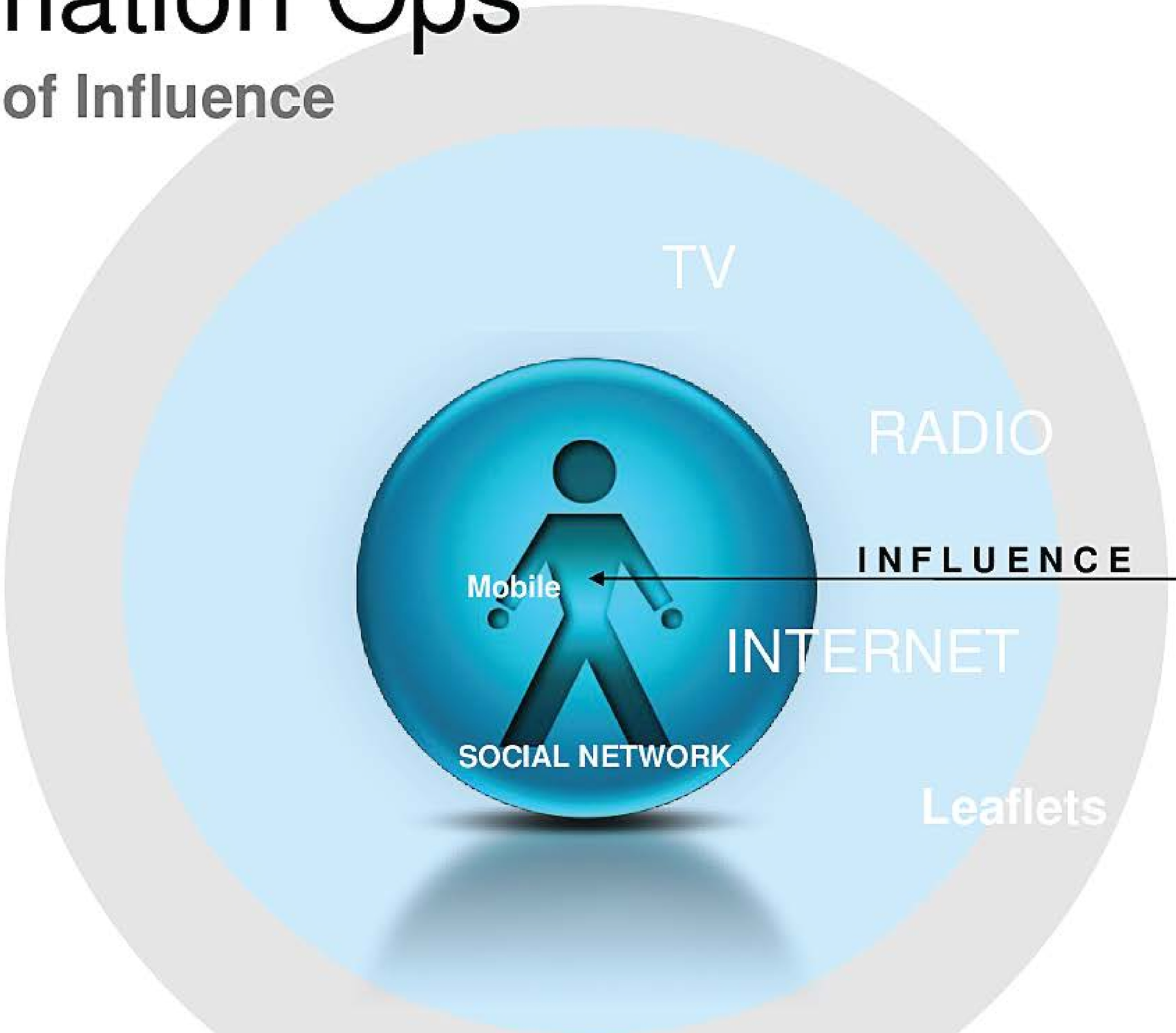
Are they really in Kawestan?

SIGDEV augments the IO process to aid targeting and takeup of message

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

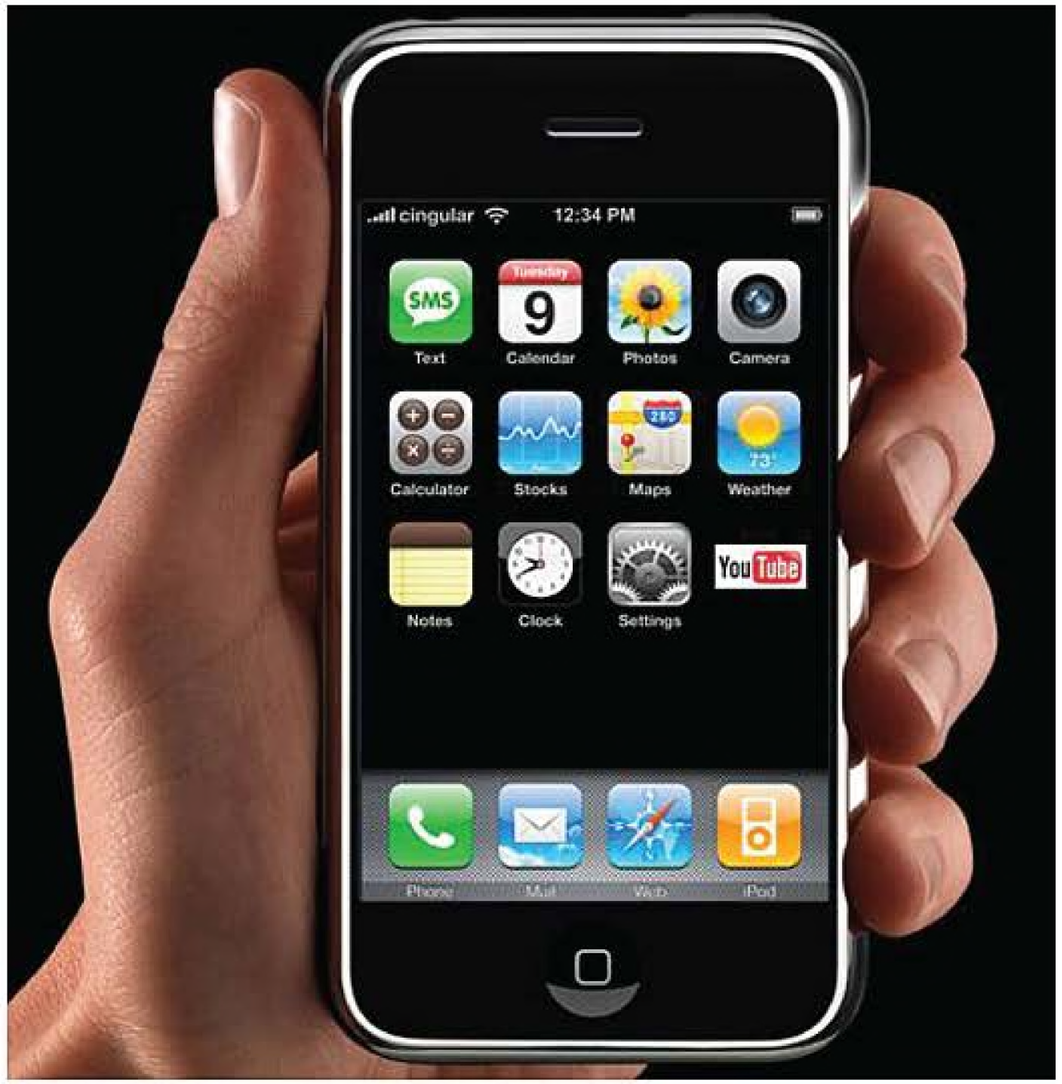
Information Ops

Spheres of Influence



This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Mobile Information Ops



50 new mobile TDIs being Developed by end of 2010

Also - Target Geographical Identifiers (TGI)

We can shape CNIO against specific locations, users with a high degree of cognition

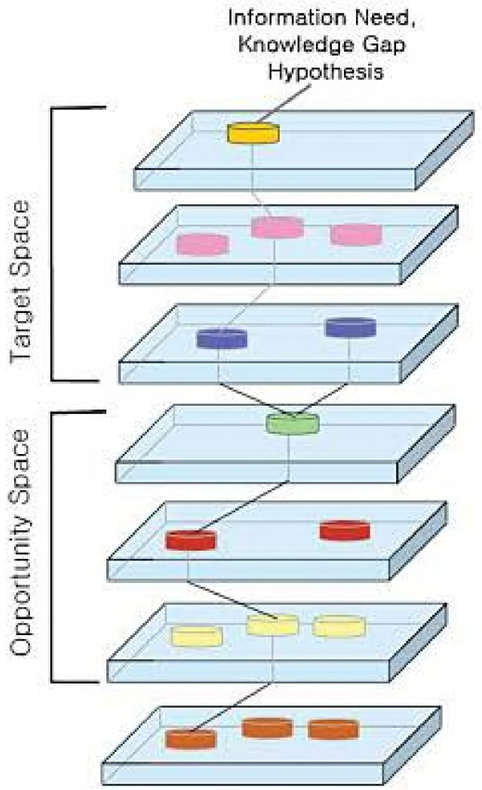
This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

CNA

Vulnerability Assessment Process Development

Enabling CNO For intelligence production teams, based on Target Templating methodology

Target Templating is a hypothesis-based, collaborative methodology for doing network analysis. By constructing a logical hypothesis from your knowledge gaps, a target thread is produced. The thread is based on the understanding of 6 "Layers" understanding the target domain and how it connects to the global network, and then understanding what opportunities can be exploited to gain access. Layer 7 captures the work flow, and what needs to be done to achieve the outcome. Target Templating provides that framework in order to break down a problem into the essential parts necessary to develop access and network knowledge. Visualisation of this knowledge at all layers is essential to spotting linkages both horizontally across the layers and vertically through them, so the use of a visualisation package during the NADP will be encouraged.



Layer 1: Target – An Entity such as a person or organisation.

Layer 2: Infrastructure - How the target connects to the global network

Layer 3: Technology - Understanding the technology the target uses to communicate

Layer 4: Vulnerabilities – Looking for vulnerabilities in the technologies

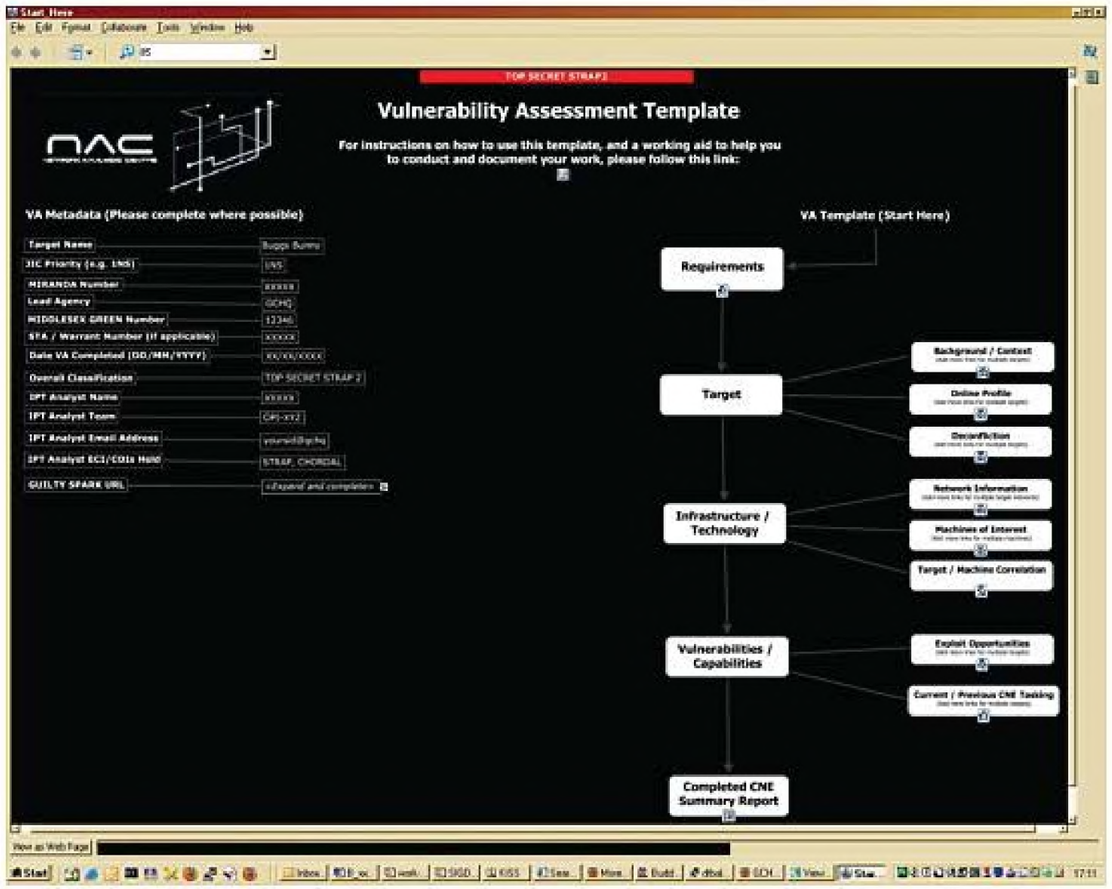
Layer 5: Capabilities - Can we exploit the vulnerabilities?

Layer 6: Access - What assets do we have to collect the traffic?

Layer 7: Expectation, Planning, Delivery - How are we going to achieve the desired outcome?

For further information on Target Templating visit the GUILTY SPARK portal on GCWiki [redacted]

guiltyspark



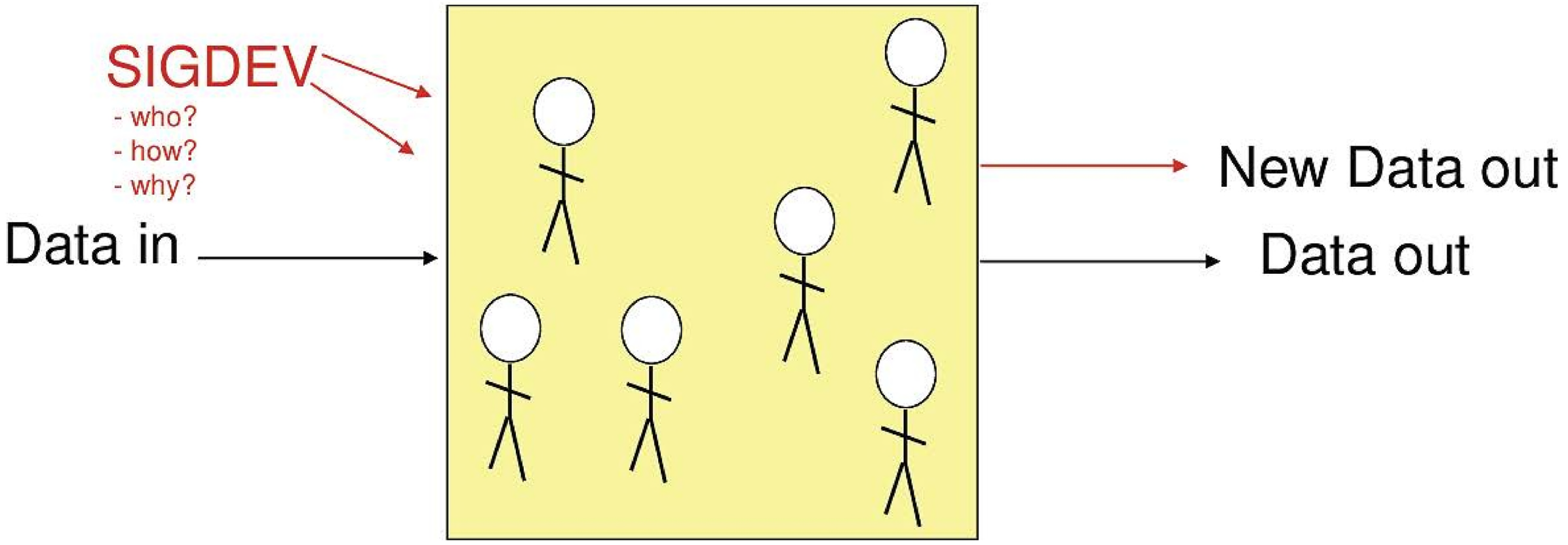
VA process delivered through NADP trained network analysts within each production team

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Human Systems Analysis

Foreign News Agencies:

- Credential Harvesting
- Employee Analysis



***Social* not technological solution**

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Future?

Formalising Tradecraft for Analysts:

"What SIGDEV needs to be done prior to starting an Effects operation?"



Joining up with 5 EYES where possible (cyber development)

BGP / MPLS network effects (HOTWIRE)

SIP and VoIP Effects – Denial of Service, Psychological Operations

Provide the defensive advice from the offensive perspective

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]

Questions?

[redacted]
Head of JTRIG
NSTS: [redacted]

[redacted]
SD Effects Lead
NSTS: [redacted]

Find me on TAPIOCA

names and phone numbers redacted

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on [redacted] or [redacted]