Full-Spectrum Cyber Effects

SIGINT Development as an enabler for GCHQ’s “Effects” mission
Effects

Destroy | Deny | Degrade | Disrupt | Deceive | Protect

Computer Network Attack (CNA)
Computer Network Information Operations (CNIO)
Disruption
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
Propaganda
Deception
Mass messaging
Pushing stories
Alias development
Psychology
Disruption / CNA

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

INFINITE CURVATURE/MOUNTAIN SLOPE

Sending messages across the full spectrum of communications

Telephony  SMS  FAX  Email

SALAMANCA  Data Mining
Phone Code  Prefix

Open Source

RADIUS Data → TDIs
IP GEO → TDIs

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
Information Operations: The Social Web

Deliver messages and multimedia content across Web 2.0

Crafting messaging campaigns to go ‘viral’
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

Login Server

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;5MV
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 ************ or ************
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
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
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 layered 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 included to gain access. Layer 7 captures this workflow, and what needs to be done to achieve the outcomes. Target Templating provides that framework in order to break down a problem into the essential parts necessary to develop access and network knowledge. Visualization of this knowledge of all layers is essential to spotting linkages both horizontally across the layers and vertically through them, so the use of a visualization package during the NADP will be encouraged.

VA process delivered through NADP trained network analysts within each production team
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 [insert contact information] or [insert contact information].
Questions?

Find me on TAPIOCA

names and phone numbers redacted