



SigDev Conference 2012

Cyber Integration "The art of the possible"

JTRIG / GCHQ CDO / GCHQ Joint Threat Research Intelligence Group, a GCHQ unit focused on cyber forensics, espionage and covert operations

TOP SECRET/COMINT/IREL TO USA, AUS, CAN, GBR, NZL



JTRIG - Core Functions



JTRIG has the following core functions:

- · Covert Internet Investigations
- · Forensic Investigation and Analysis
- Active Covert Internet Operations, (including online Humint and Effects)
- · Covert Technical Operations
- Provision of Unattributable Internet Access
- Development of new capability

TOP SECRET/ICOMINT//REL TO USA, AUS, CAN, GBR, NZI



The structure of JTRIG:

- Ops / Technical (Cap Dev) / JBOS.

Mention the "Online Covert Action Accreditation" Programme.

- Commenced September 2011.
- Initially for JTRIG staff.
- A small number of ISD analysts now being accepted on courses.

Main skills covered:

- Information & Influence Operations.
- Online Humint.
- Disruption & CNA.
- Briefing to be provided by

Development of new capability:

- Capabilities being developed to access data from various internet services
- suffer to encryption etc

- How these data sources may help to mitigate the loss that passive access could

- How to look further at integrating /fusing these data sources into our analytic stores and workflows



EFFECTS: Definition



- "Using online techniques to make something happen in the real or cyber world"
- Two broad categories:
 - Information Ops (influence or disruption)
 - Technical disruption
- Known in GCHQ as Online Covert Action
- The 4 D's: Deny / Disrupt / Degrade / Deceive

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZI

Key statement is the initial one.

Explain the categories more.

The one thing to remember for JTRIG is the 4 "D's".



Online Covert Action



How to ...

TOP SECRETI/COMINT//REL TO USA, AUS, CAN, GBR, MZL

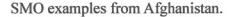


Stop Someone From Communicating



- Bombard their phone with text messages
- · Bombard their phone with calls
- Delete their online presence
- Block up their fax machine

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



- Significantly disrupting Taleban Operations.
- Sending targets a text message every 10 seconds or so.
- Calling targets consistently on a regular basis.

Ability to delete a target's online presence. Very annoying!!

Older type of Effects, but faxes are still used in some areas.



Discredit a target



- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

TOP SECRET/COMINT//REL TO USA, AUS. CAN, GBR, NZL



- Get someone to go somewhere on the internet, or a physical location to be met by a "friendly face".
- JTRIG has the ability to "shape" the environment on occasions.

Photo change; you have been warned, "JTRIG is about!!" Can take "paranoia" to a whole new level.

Blog writing:

- Has worked on a number of different Ops.
- One example is on a Serious Crime Op,
- Other examples on Iran work.

Email/text:

- Infiltration work.
- Helps JTRIG acquire credibility with online groups etc.

- Helps with bringing SIGINT/Effects together.



Discredit a company



- Leak confidential information to companies / the press via blogs etc
- Post negative information on appropriate forums
- Stop deals / ruin business relationships

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Info Ops style work:

- Use of Open Source info and/or releasable Sigint items.
- Attempts to inform the public, where necessary (government protected environment)
- First stages of disruption and/or discrediting companies / organisations
- Stop /divert the flow of funding. Introduce panic etc.

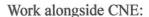


Get another country to believe a 'secret'



- Place 'secret' information on a compromised computer
- Send 'secret' information across a network visible to Sigint
- Provide 'secret' information through an online agent

TOP SECRET/COMINT//REL TO USA, AUS, CAN, GBR, NZL



- Use of various masquerade type techniques.
- Placement of potential "damming" information, where appropriate.

Visible networks:

- Shape the environment, so that Sigint can provide BDA for Operations.
- Use of releasable information, (support from SIA's etc).

Online agent:

- Use of online aliases to good effect.
- Visibly shaping the online environment.



Stop someone's computer from working



- Send them a virus:
 - AMBASSADORS RECEPTION encrypt itself, delete all emails, encrypt all files, make screen shake, no more log on
- Conduct a Denial of Service attack on their computer

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Virus sending:

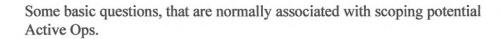
- Use of various JTRIG tools, including AMBASSADORS RECEPTION.
- Has been used in a variety of different areas, very effective.



Active Collection Techniques

- Use of active techniques to collect intelligence required to map out:
 - Who does what?
 - What institutions etc are being used?
 - What companies?
 - Who sets up the websites?
 - How do they communicate between ministeries and / or each other?
 - How do they communicate to investors?
 - How do they store information?

TOP SECRET//COMINT//REL TO USA, AUS. CAN. GBR. NZI.



In essence Intelligence Analysts use SIGINT to answer the "pattern of life" question.

But... do they know the "online – pattern of life" for their target set??

Do the analyst's know not just what their target is doing, but what is it thinking??



Impact of Effects

- How do we measure the impact of "effects"?
- "Blitz" style approach:
 - Creating as much disruption as possible within a short period of time
- More subtle approach:
 - Effects use less likely to be detected, therefore
 - More sustainable over a longer period of time

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZI,

Two main ways to measure the impact of "Effects" Operations.



Cyber Integration

Pros:

- Provide an opportunity for JTRIG analysts to be more actively involved with ISD counterparts
- · Enable further upskilling (e.g. C2C etc)
- Provide JTRIG analysts with the opportunity to identify CNA-type options a lot earlier in Operations
- Provides ISD analysts a greater baseline and understanding of JTRIG work
- An Opportunity for analysts to learn new ACNO skills, (e.g. On-line HUMINT etc)

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



Cyber Integration

Cons:

- Current lack of JTRIG IT infrastructure on the general floor-plate
- · Lack of wider resource investment
- Lack of overall training and support resources
- · Integration process will be resource intensive for CDO