SigDev Conference 2012

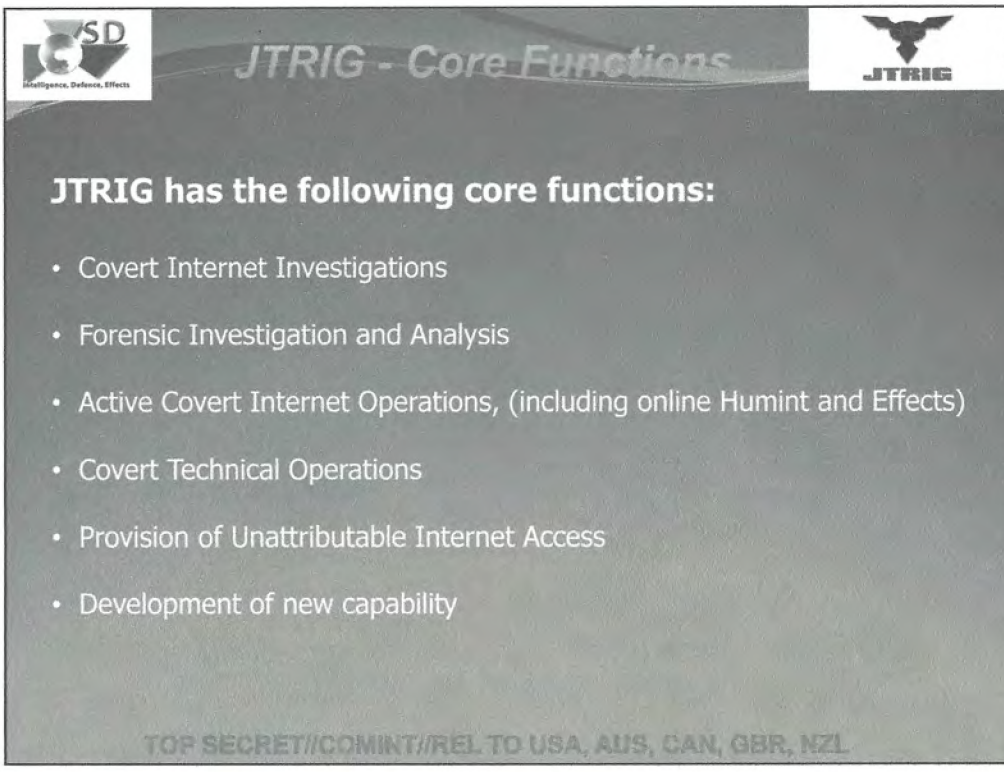
Cyber Integration
"The art of the possible"

[redacted] JTRIG / GCHQ

[redacted] CDO / GCHQ

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

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



[redacted]

Explanation of the "base-line" for JTRIG-related work and make-up:

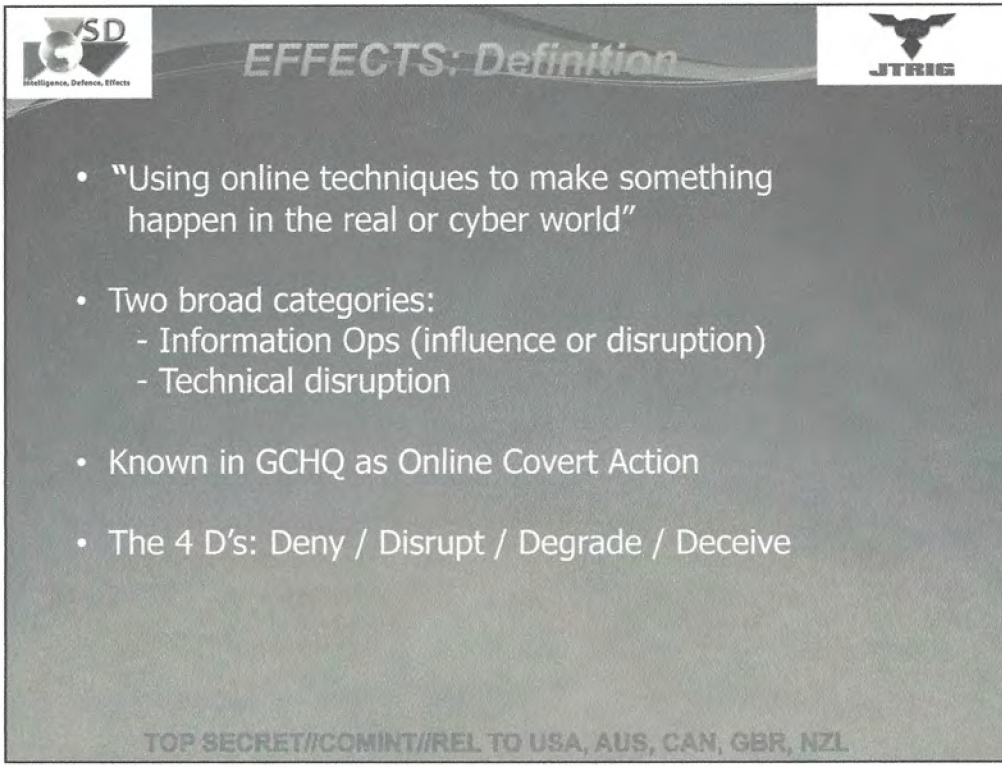
The structure of JTRIG:
- Ops / Technical (Cap Dev) / JBOS.

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 [redacted].

Development of new capability:

- Capabilities being developed to access data from various internet services
- How these data sources may help to mitigate the loss that passive access could suffer to encryption etc
- How to look further at integrating /fusing these data sources into our analytic stores and workflows

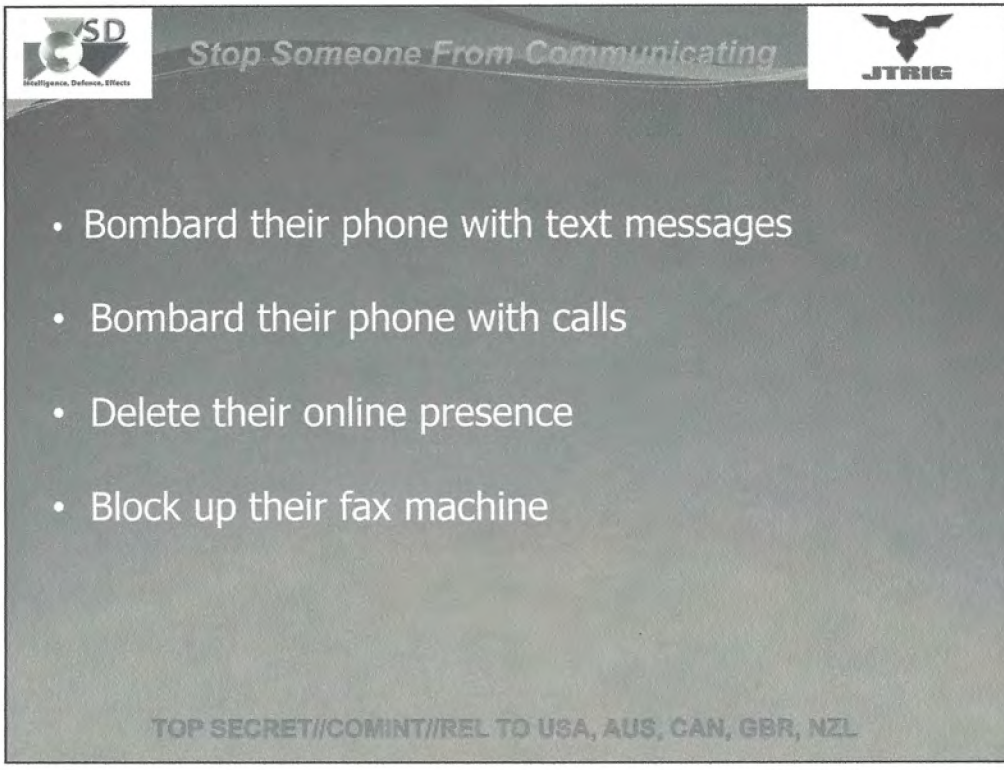


Key statement is the initial one.

Explain the categories more.

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

How to ...



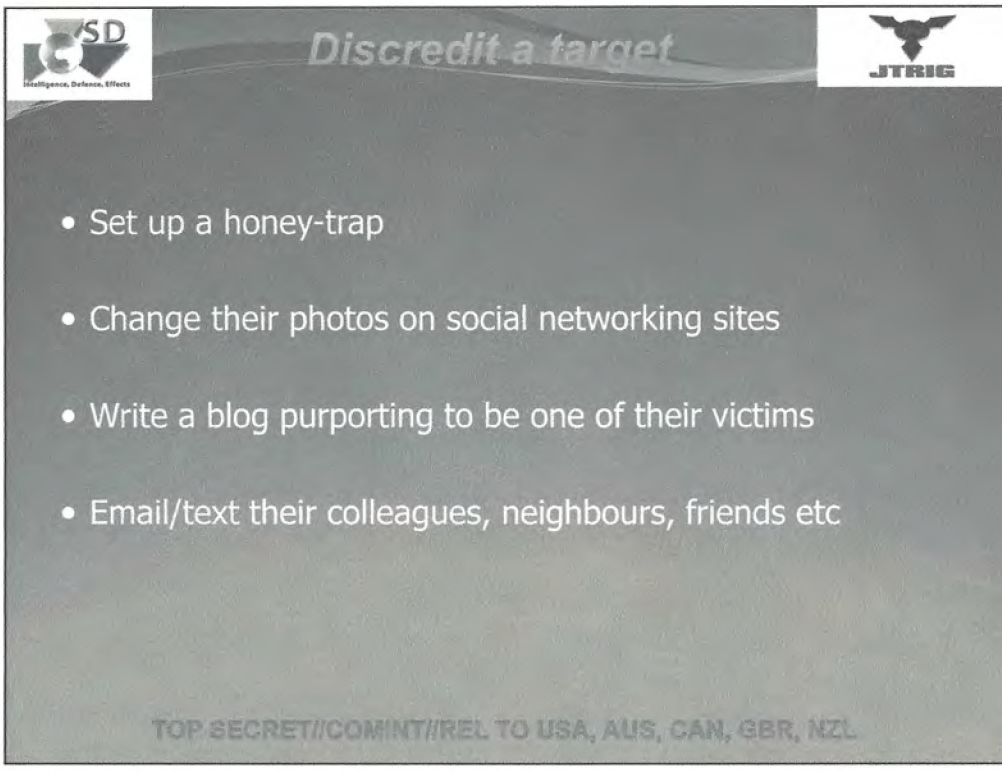
[redacted]

SMO examples from Afghanistan.

- 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.



[redacted]

Honey-trap; a great option. Very successful when it works.

- 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.

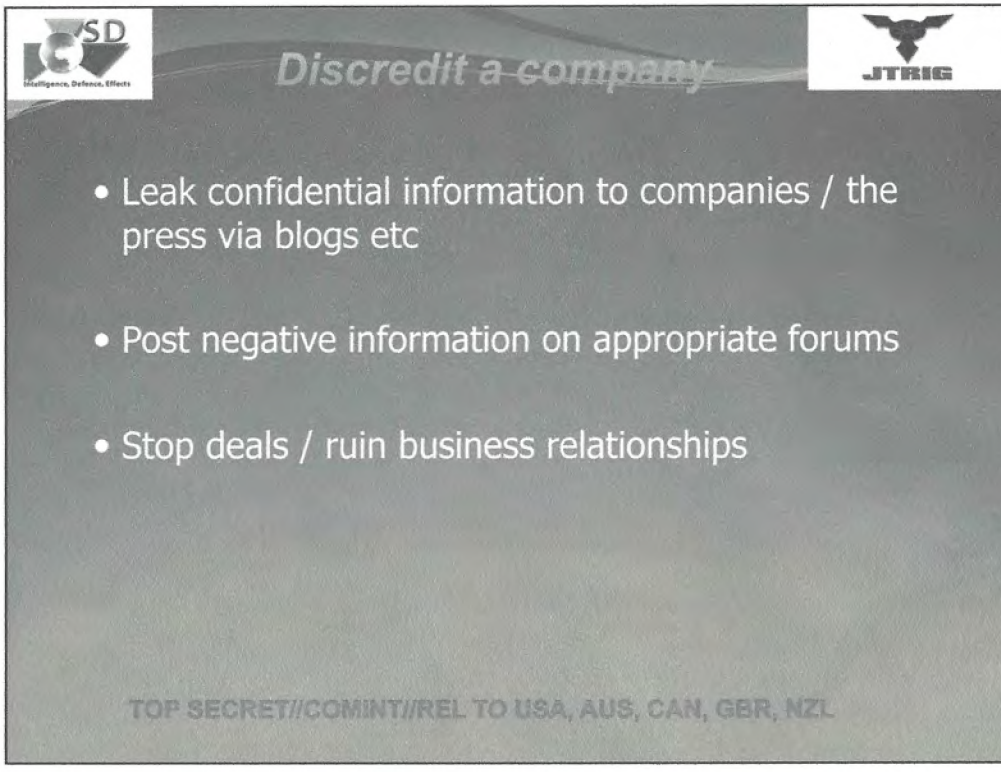
Blog writing:

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

Email/text:

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

- Helps with bringing SIGINT/Effects together.



[redacted]

Info Ops style work:

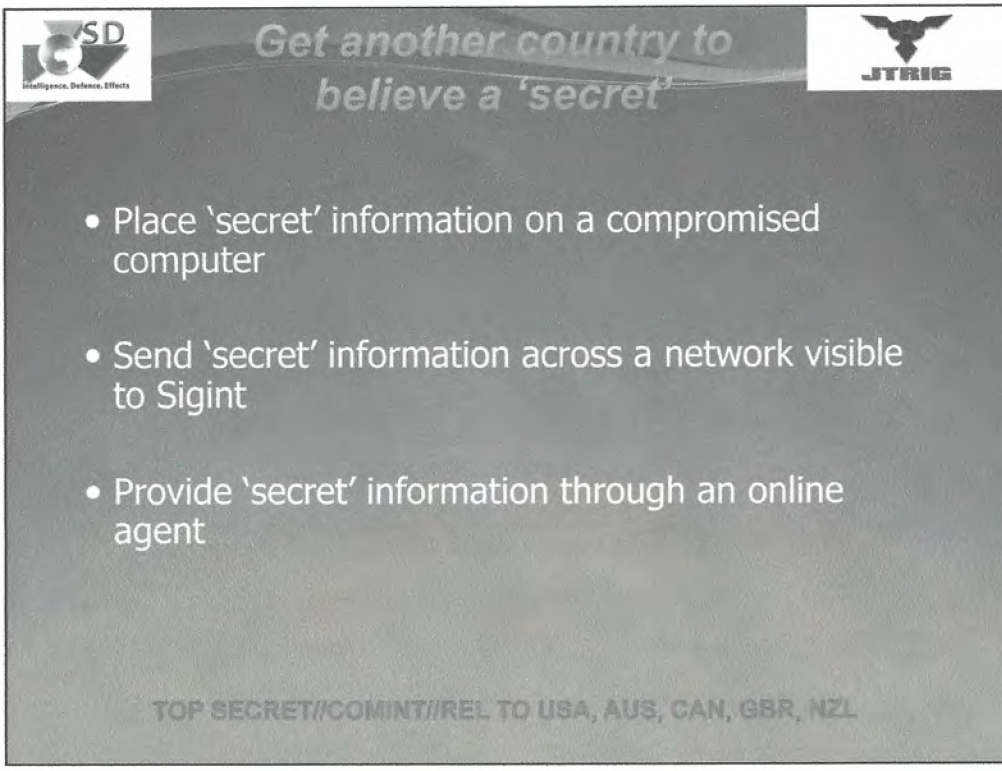
- Use of Open Source info and/or releasable Sigint items.

- Attempts to inform the public, where necessary (government protected environment)

- First stages of disruption and/or discrediting companies / organisations

[redacted]

- Stop /divert the flow of funding. Introduce panic etc.



[redacted]

Work alongside CNE:

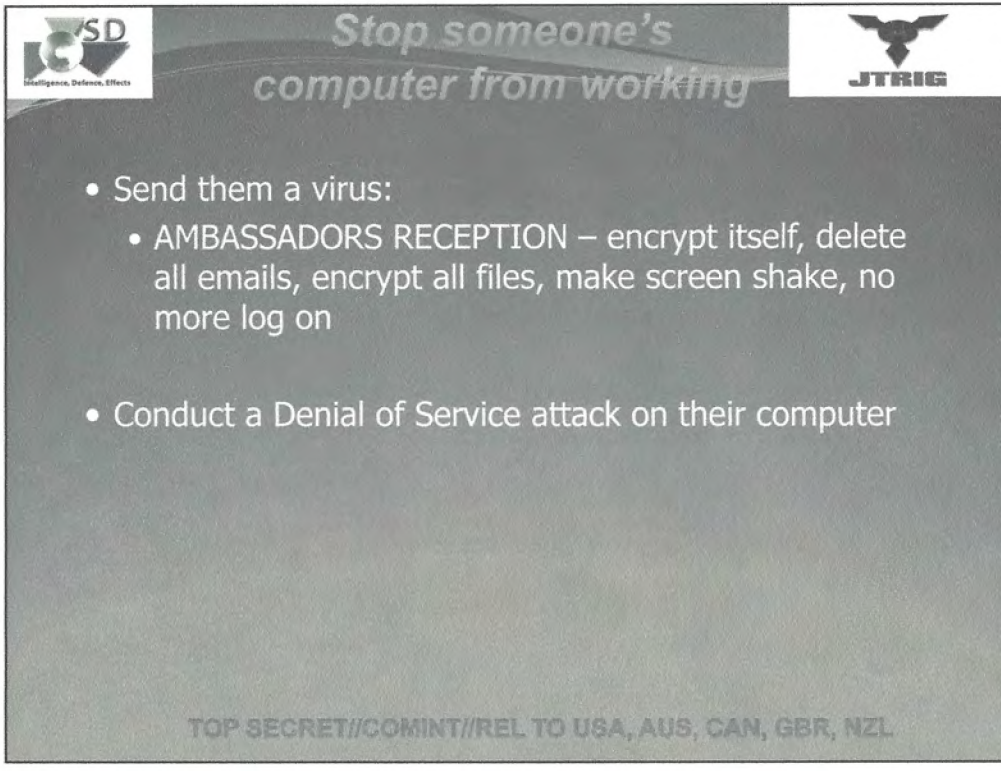
- Use of various masquerade type techniques.
- Placement of potential "damming" information, where appropriate.

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.

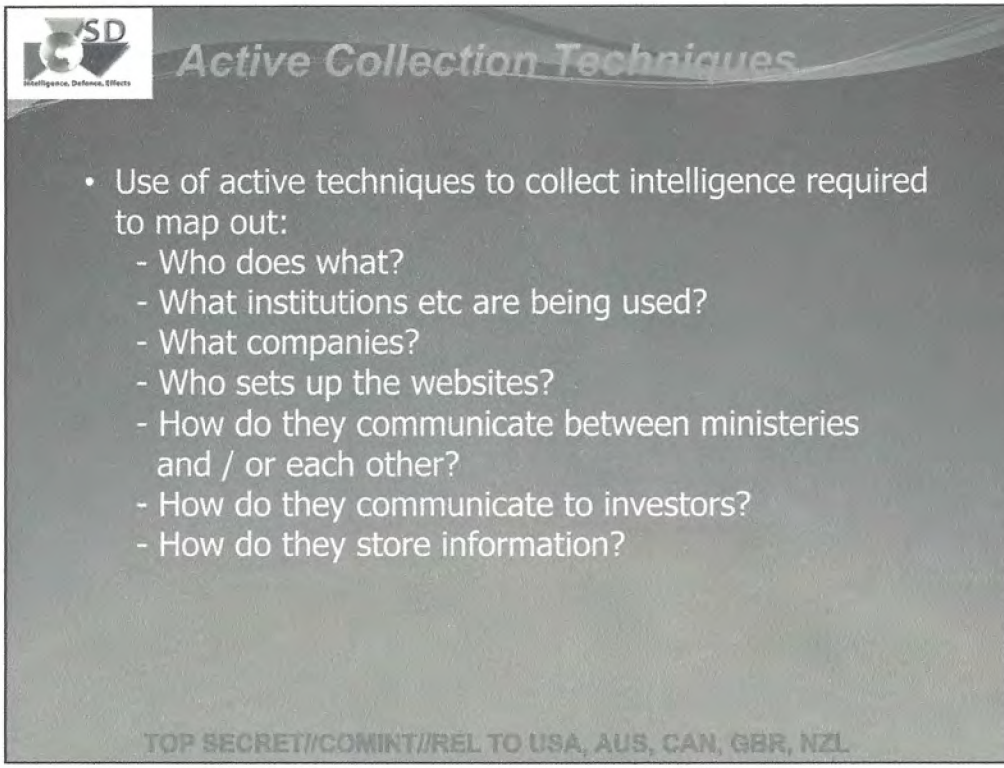


[redacted]

Virus sending:

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

[redacted]

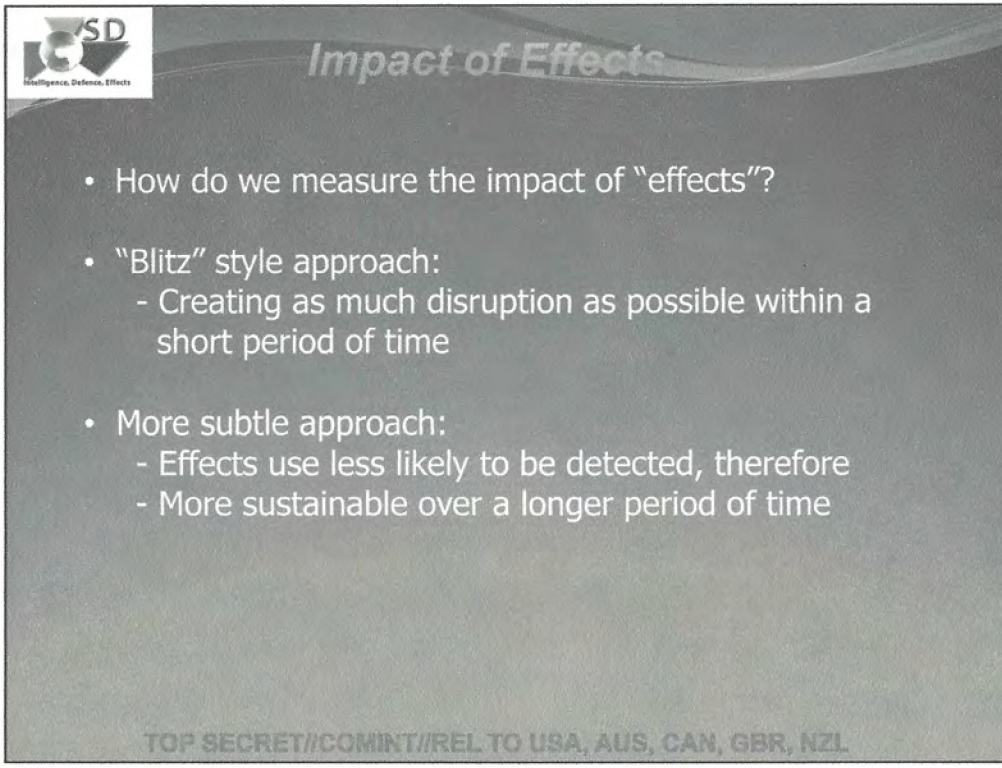


Some basic questions, that are normally associated with scoping potential Active Ops.

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??



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)

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