(U) Running Strategic Analytics Affecting Europe and Africa

Region: Europe, Middle East (Israel), and Africa: [redacted], ECC

The overall classification of this briefing is:
TOP SECRET//COMINT//REL USA, FVEYS//20291123
Outline

• (U) Background
• (U) Problem Definition & Challenge
• (U) Our AOR: Europe - Africa
• (U) Examples for Europe - Africa
• (U) Enrichment and Data Flow
• (U) Real-time, batch, XKEYSCORE
• (U) Conclusions
(U) Terrorists Transit via Europe

- (U) Communication
- Transit Points
- (U) Partners
  - Second Party
  - Third Party
- (U) Relationships
  - EUCOM
  - AFRICOM
  - CENTCOM

(U) US needs partners for data & to help capture, confine…. 
(U) Challenge: Integrating Tactical & National Collection

• (C//FVEY) Collection with HF/VHF/UHF
  - Digital packets
  - Analog comms
  - Noise issues, lack of experience with these types of signals

• (C//FVEY) Tactical versus National (Strategic) Collection
  - RTRG
  - DISTILLERY
(U) Analytics for Targets in Europe

- (C//FVEY) OPSEC Savvy Targets
  - “...most terrorists stop thru Europe”
- (TS//FVEY) Use advanced techniques
  - Steganography
    - Forensics or Analytics on front end
  - Encryption
    - Takes time and has “black hole” issue
- (TS//SI//FVEY) Reliance on “special” collection
  - GCHQ and FAA
  - Problems processing w/r to TS
## (U) Analytics for Identity Intelligence

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>Data Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>(U) Human Trafficking</td>
<td>(C//FVEY) Operations from Jordan to Syria in both directions; Sahel</td>
<td>Metadata for geolocation; content for confirmation</td>
</tr>
<tr>
<td>(U) Weapons Smuggling</td>
<td>(C//FVEY) From Libya to Sahel</td>
<td>Metadata for geolocation; content for confirmation</td>
</tr>
<tr>
<td>(U) Drug Smuggling</td>
<td>(C//FVEY) Sahel and financing of terrorism; Balkans into Europe</td>
<td>Metadata for geolocation; content for confirmation</td>
</tr>
<tr>
<td>(U) Biometrics &amp; Elections</td>
<td>(C//FVEY) Used in Africa</td>
<td>Need collection assets</td>
</tr>
</tbody>
</table>
(U) Enrichment Sources

- (U) Air Breather, HF & UHF/VHF
- (C//FVEY) Big Pipe & FORNSAT
- (U) Military SIGINT Services
- (U//FOUO) Forensics
- (U) Third Party Sources
- (C//FVEY) Second Party
  - GCHQ is critical for mission

(C//FVEY) Key Idea: Low Priority of AFRICA may cause loss of metadata and content; makes “Discovery” more uncertain
(U) Enrichment: SIGDEV & GCHQ QFDs

- (S//FVEY) 54% of current ECC DNI tasking based on QFD data
- (S//FVEY) QFDs provide better access to metadata for European & North African targets than any other access at ECC due to poor passive collection
- (C//FVEY) Flexibility provided by the use of TDIs and the first stage query allows for better target discovery and development

March 2012

Account Allocations by TOPI

Slide taken from ECC archives.

(C//FVEY) Much of ECC data comes from GCHQ QFDs

SECRET//REL USA, FVEYS
(U) Data Flow Integration is Constant Headache
(U) “Real Time” Analytics

- (U) Nascent Analytics with unclear definition of “real time”
  - How fast is alerting?
- (C//FVEY) DISTILLERY
  - Pulled from GHOSTMACHINE stack
- (U) NIAGARAFIILES
  - File based
  - Starting to gain experience
- (C//FVEY) RTRG
  - Tools not integrated into ECC
  - Data Sets are sparse
  - Tactically oriented
  - Unregulated alerts can quickly spam user
- (C//FVEY) ECC Current Effort:
  - Focused on NTOC and Distributed Denial of Service attack alerting
  - Uses DISTILLERY

(U) How fast is real time?
(U) Batch: MapReduce Analytics

- (U) Batch oriented versus streaming
  - Run every 15 min to once a day or so
  - Not streaming
- (U) Good Data Storage
  - Good access outward to MDR-1, MDR-2
  - Days to years of storage
  - Promotion (?)
- (U) Complex Analytics like “Pattern of Life”
  - Reasonable amount of processing cycles at the front end collection system (not yet tested)
- (U) Session can be quite long and still captured (not yet tested)
- (U) UUID’s (identifying sessions) are workable
- (U) No experience yet sharing with second and third party partners
- (U) Unknown level of entry training required
  - Menwith Hill has WHIZBANG

(C//FVEY) Batch gives you access to data 24 hours ago
(U) Xkeyscore Fingerprints

- (C//FVEY) Streaming
  - Data available one hour later?
  - Most do pulls up to yesterday
- (U) Good Data Storage
  - RAW content: 3 days to a couple of weeks
  - Metadata: 90+ days
- (U) Complex Analytics like “Pattern of Life”
  - Reasonable amount of processing cycles at the front end collection system
- (U) Session can be quite long and still captured
- (U) UUID’s are workable
- (U) Good for sharing with second and third party
- (U) Relatively low level of entry training required
(U) Key Take Aways

· (U//FOUO) Discovery in Africa is based on “we do not know what we do not see”
· (U) Europe has Opsec savvy CT targets
· (U) Analytics involve partners
  -- 3rd Party in future
· (U) Limited Resources: Processing Power & BW
NSA/CSS Europe & Africa

QUESTIONS?