



SKYNET: Applying Advanced Cloud-based Behavior Analytics

A Collaborative Project
by S2I, R6, T12, T14,
SSG, and S22

Presenters:

S2I51
R66F

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20370401





Outline

- What is SKYNET?
- DEMONSPIT Data Flow
- Automated Bulk Cloud Analytics
- Analytic Triage



What is SKYNET?

- Collaborative cloud research effort between 5 different organizations crossing 3 NSA Directorates:
 - Signals Intelligence: S2I, S22, SSG
 - Research: R6
 - Technology: T12, T14
- Partnerships
 - TMAC/FASTSCOPE
 - MIT Lincoln Labs & Harvard
- **SKYNET applies complex combinations of geospatial, geotemporal, pattern-of-life, and travel analytics to bulk DNR data to identify patterns of suspect activity**

SNOWFLAKE
PARTNER

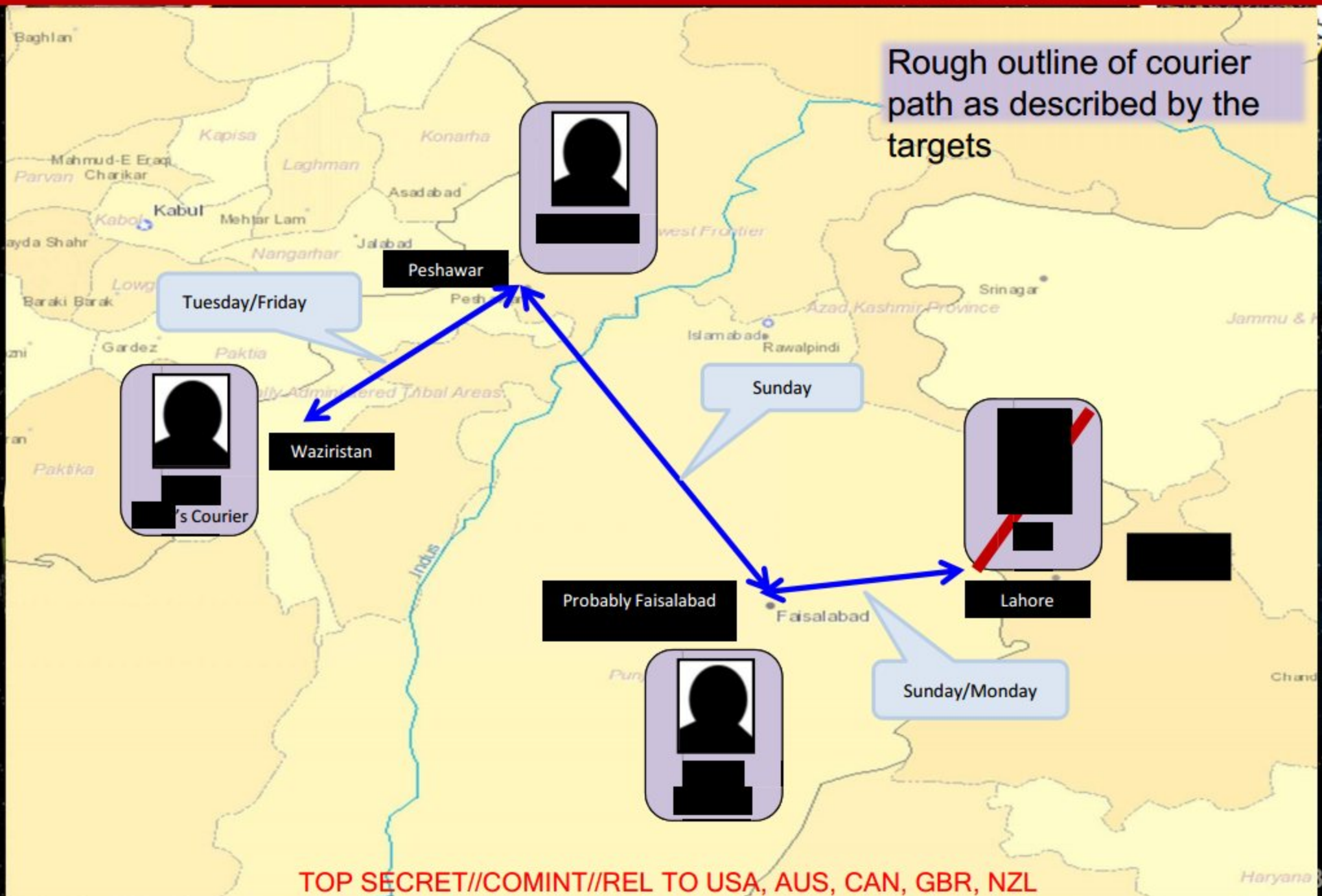


CTMMC

NSA/CSS Counterterrorism
Mission Management Center

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

Intelligence Update





SKYNET Analytic Questions

- Who has traveled from Peshawar to Faisalabad or Lahore (and back) in the past month?
 - Who does the traveler call when he arrives?
 - Who else is seen in the area when the traveler arrives, and who seen leaving the area shortly afterward?
- Who travels to/from Peshawar every other Sunday and "somewhere else" on a weekly basis?
- Who visits Akora Khattak periodically and also travels between Peshawar and Lahore?
- Who fits the above travel profiles and also possesses unusual behavior:
 - One or two hops from other suspects or known tasked selectors
 - Frequent handset swapping or powering down



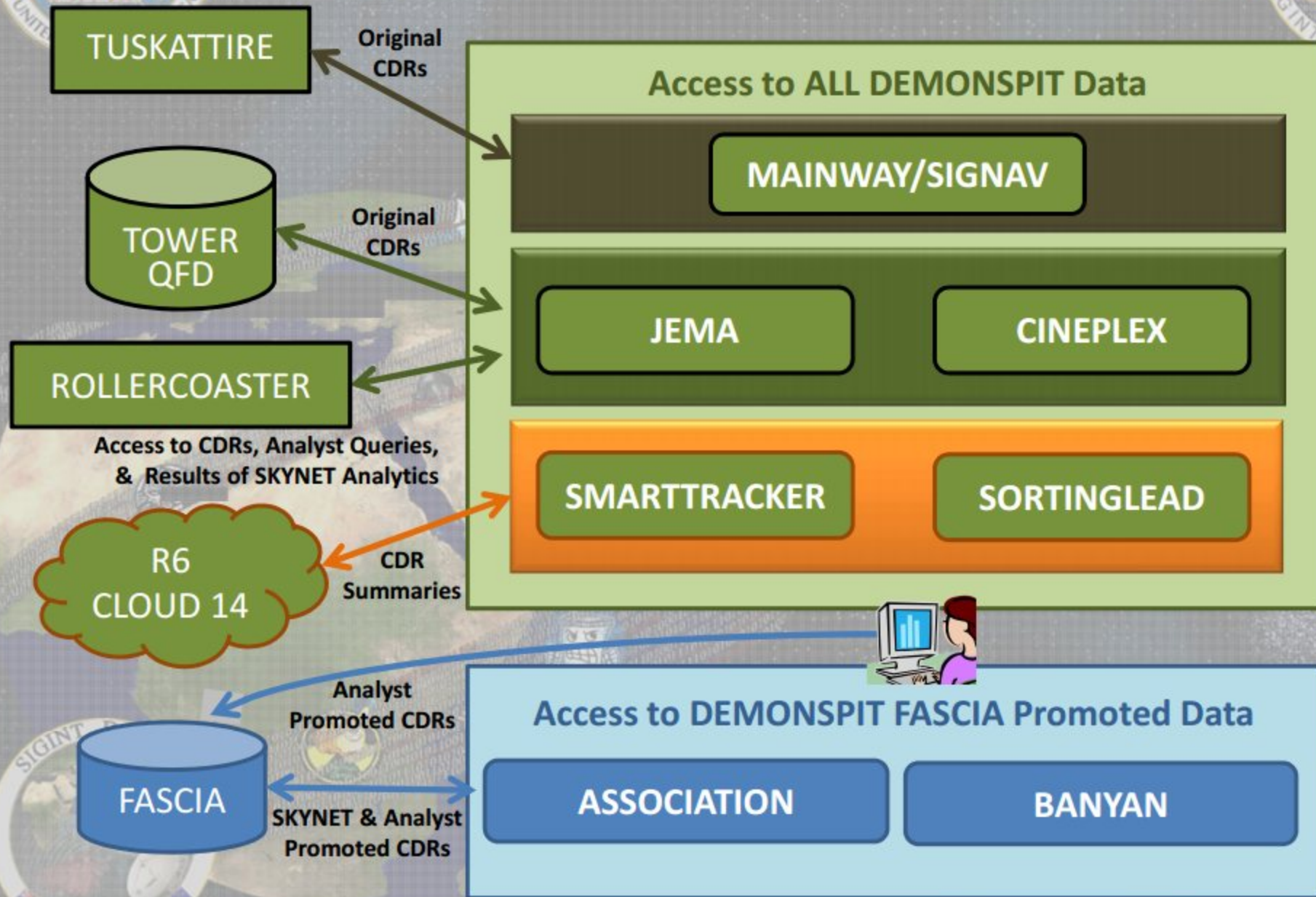
DEMONSPIT

- DEMONSPIT is a new dataflow for bulk Call Data Records (CDRs) from Pakistan
 - CDRs are being acquired from major PK Telecom providers
- Data is normalized through TUSKATTIRE, like all other Call Data Records
- DEMONSPIT data is forwarded by TUSKATTIRE to several Clouds:
 - GMHalo/DPS
 - Promotes records to FASCIA and feeds the SEDB Tower QFD
 - GMPlace & Cloud 14
 - Ingests DEMONSPIT into Sortinglead summaries to support SKYNET Analytics
 - Ingests DEMONSPIT into a Perishable QFD which will be available to analysts via JEMA and CINEPLEX
 - Bulldozer/MDR2

All of the clouds receiving DEMONSPIT data also receive all FASCIA data



Analysts' View of DEMONSPIT





Outline

- What is SKYNET?
- DEMONSPIT Data Flow
- Automated Bulk Cloud Analytics
- Analytic Triage



TOP SECRET//SI//REL TO USA, FVEY

Cloud Analytic Building Blocks



- Travel Patterns
 - Travel phrases (Locations visited in given timeframe)
 - Regular/repeated visits to locations of interest
- Behavior-Based Analytics
 - Low use, incoming calls only
 - Excessive SIM or Handset swapping
 - Frequent Detach/Power-down
 - Courier machine learning models
- Other Enrichments
 - Travel on particular days of the week
 - Co-travelers
 - Similar travel patterns
 - Common contacts
 - Visits to airports
 - Other countries
 - Overnight trips
 - Permanent move

TOP SECRET//SI//REL TO USA, FVEY



TOP SECRET//SI//REL TO USA, FVEY



Sample Travel Report: Haqqani Network

IMSI	seed-contacts	tasked- contact- count	selector_ swapping _num	associated_ selectors	visits_regularly	other_ countries	phrase
		3	3		lashkargah_city		helmand kandahar AF PK farah AF bala_bulk farah masow farah masow nowbahar masow
		14			nowbahar	IR	
		5	3			BA	ghazni AF sharan urgon AF
		1				AE	khost_airport kajir_kalay

TOP SECRET//SI//REL TO USA, FVEY



What Suspicious Selectors Were Seen Traveling Between Peshawar and Lahore?

Case-Specific Behavioral Cloud Analytics

Peshawar-Lahore Travel 1 - 4 NOV 2011

TRAVEL PHRASE	DOW	MSISDN	IMSI	TASKED CONTACTS	NUM_SELECTOR _SWAPPING	ASSOCIATED_ SELECTORS	ACTIVITY_ CATEGORIES
torkham AF PK							
peshawar lahore	FRI	[REDACTED]		2			
PK peshawar lahore	THU	[REDACTED]					
behsud AF jalalabad						[REDACTED]	
jalal_abad jalalabad							
behsud rodat bati_kot							
mohmand_darah							
peshawar PK	WED		[REDACTED]	4	7		
gtrd PK nowshera							
gulbahar peshawar							
sanda_kalan lahore	THU	[REDACTED]					
jamrud PK peshawar							
lahore	TUE	[REDACTED]		10			
							5-or-fewer-contacts, sms-and-zero-duration-calls-only, low-use
PK peshawar lahore	THU		[REDACTED]				



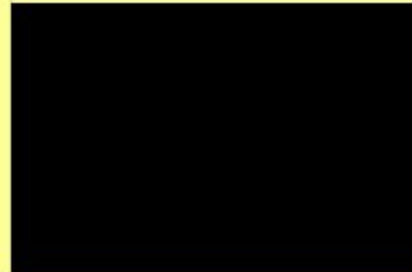
Outline

- What is SKYNET?
- DEMONSPIT Data Flow
- Automated Bulk Cloud Analytics
- Analytic triage
 - SMARTTRACKER
 - RT-RG
 - JEMA



TOP SECRET//SI//REL TO USA, FVEY

Selectors of Interest from Cloud Travel Analytic



(tasked)

IMSI:



Handsets:



TOP SECRET//SI//REL TO USA, FVEY

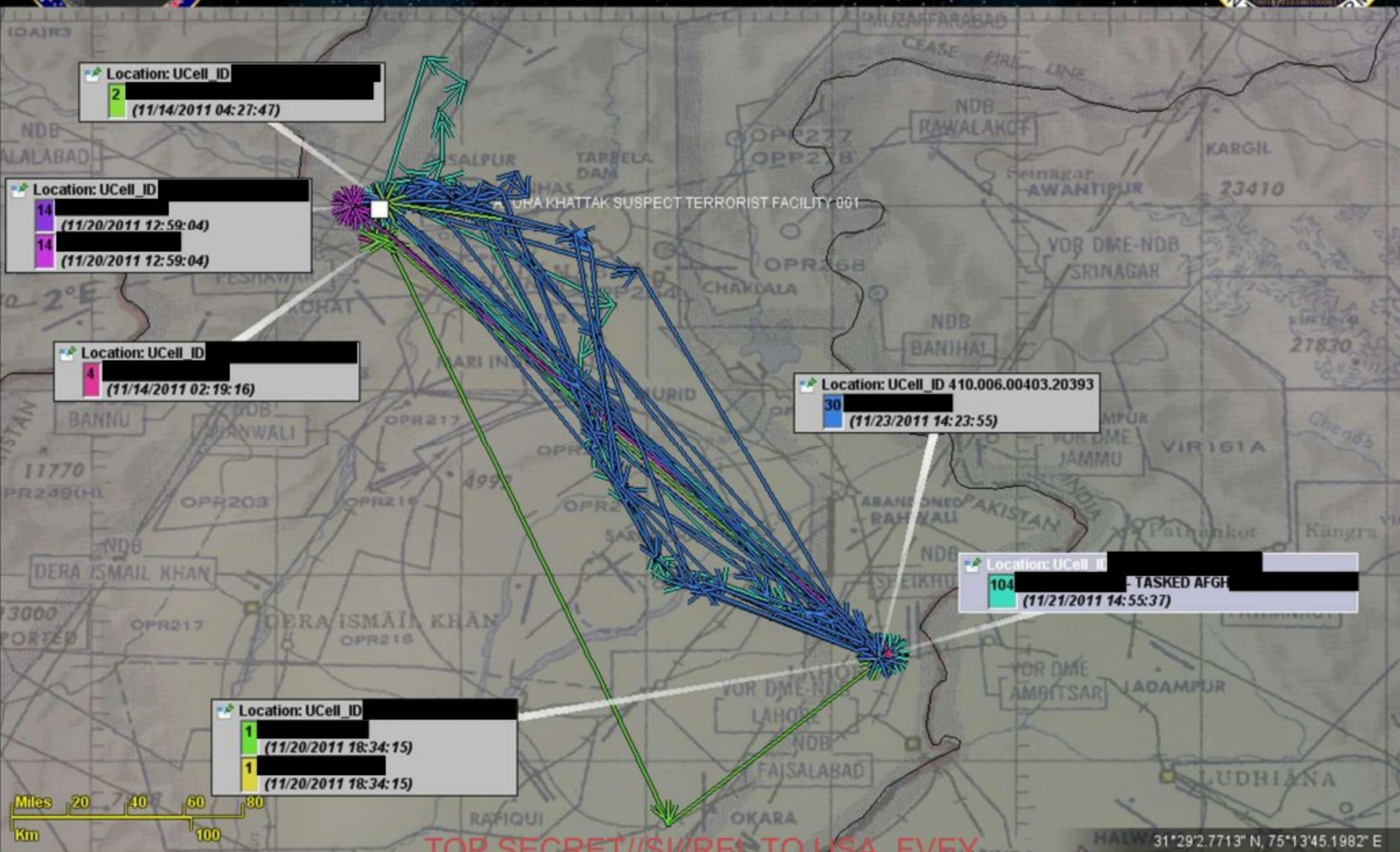


TOP SECRET//SI//REL TO USA, FVEY



SMARTTRACKER Travel View

31 October – 23 November





Analytic Tradecraft

- Examine travel patterns for common routes and meeting locations
 - Run cell soaks on all common meeting locations during meeting timeframe
- Analyze selectors for common contacts
- Analyze selectors for handset sharing behavior

Repeat procedure with resulting selectors
Correlate with other known and suspected selectors


























TOP SECRET//SI//REL TO USA, FVEY

SMARTTRACKER

Coincidence Report



		Who	Coincidence Count
Sets with 3 targets	Select	  	1 at 1 location
Sets with 2 targets	Select	 	101 at 16 locations
	Select	 	91 at 20 locations
	Select	 	39 at 24 locations
	Select	 	37 at 12 locations
	Select	 	33 at 12 locations
	Select	 	31 at 12 locations
	Select	 	24 at 11 locations
	Select	 	1 at 1 location
	Select	 	1 at 1 location
	Select	 	1 at 1 location

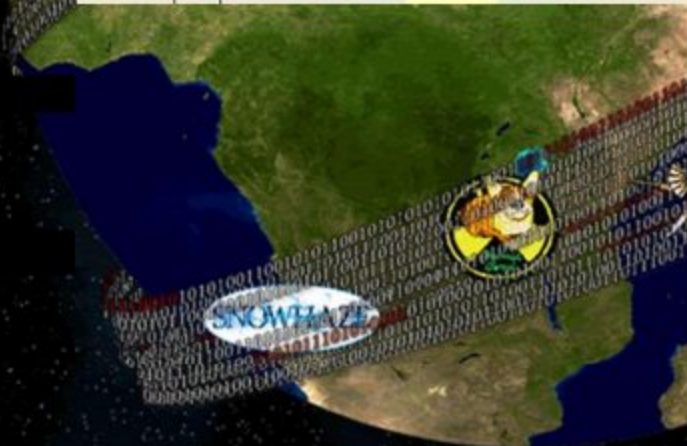
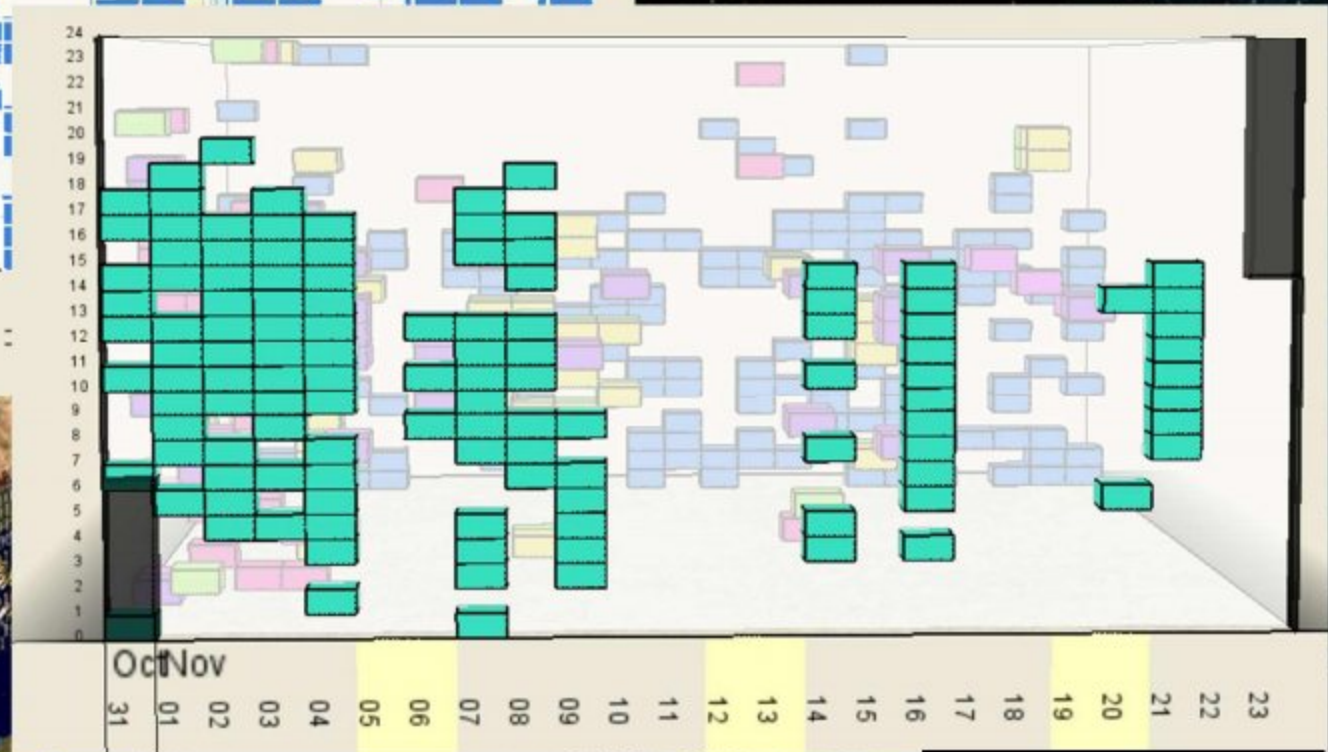
TOP SECRET//SI//REL TO USA, FVEY



TOP SECRET//SI//REL TO USA, FVEY

SMARTTRACKER

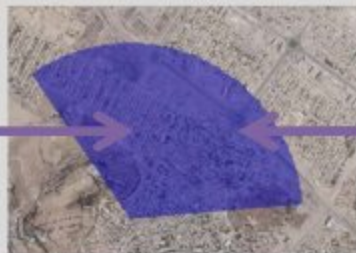
Smart Chart





TOP SECRET//SI//REL TO USA, FVEY

RT-RG Analytics



Meetings – who is at the same ucellid at the same time as the potential courier at the destination city?...Multiple times.



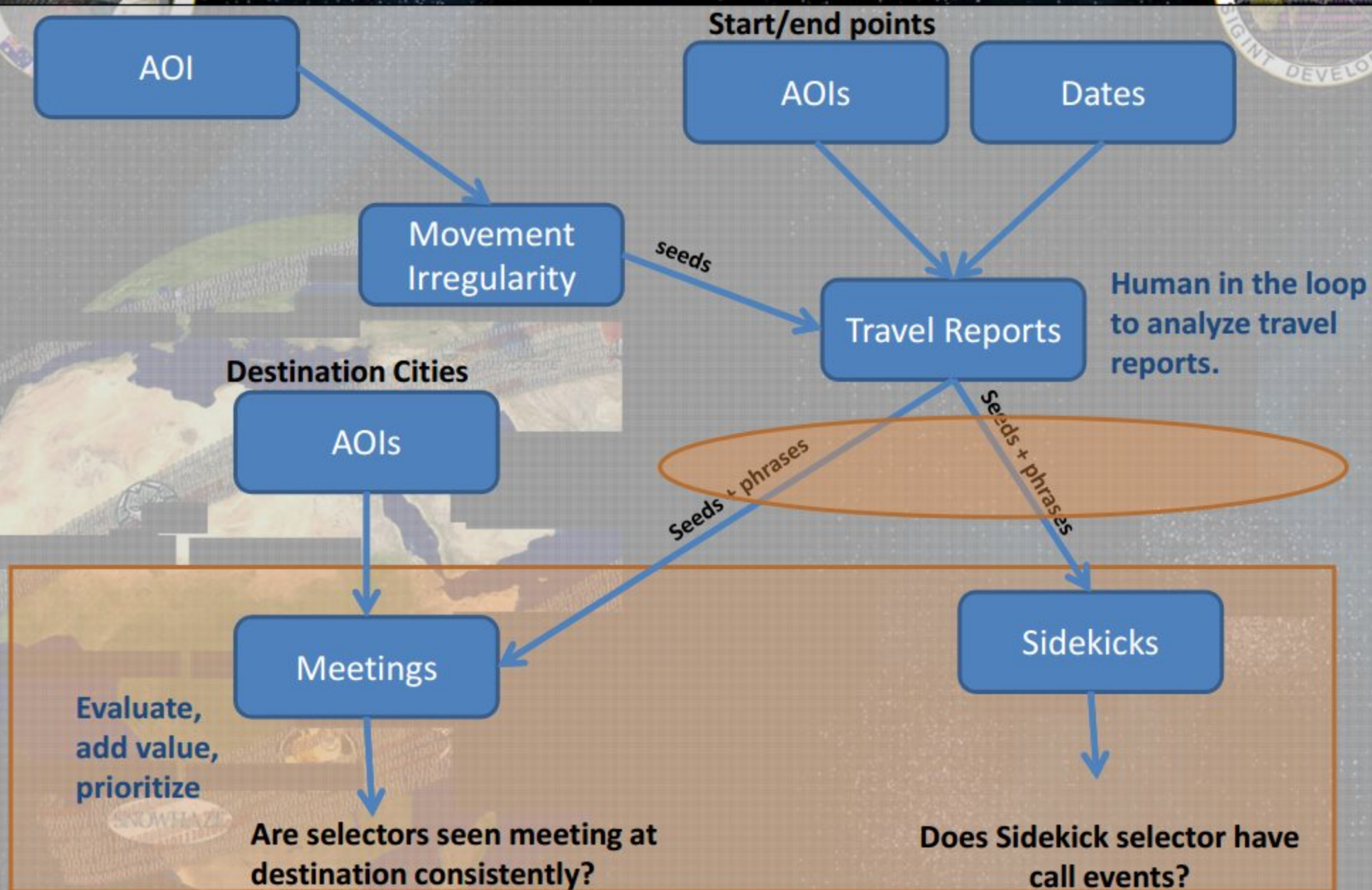
Sidekicks – is there a pair traveling together to the destination city?

TOP SECRET//SI//REL TO USA, FVEY





JEMA: Pulling It All Together





THANK YOU!

SKYNET WIKI:

[https://\[REDACTED\]/wiki/SKYNET](https://[REDACTED]/wiki/SKYNET)

, S2I51, [REDACTED] @nsa.ic.gov
, R66F, [REDACTED] @nsa.ic.gov

