RT^{10} Initiative Overview

Dr. James Heath

Program Management & Advisors: COL Bob Harms / COL Barb Trent / Michelle Gerhard [redacted]

Architects: [redacted] / Mark Ross

Presented by [redacted]

Why Innovate?

- Volume & convergence
  - Front-end filters data
  - Reaching limits on legacy systems
- Latency
  - Processing, storing, and query
  - Difficult to enable tactical operations
- Analyst Limitations
  - Non-integrated tools
  - Collaboration limited
  - Knowledge-bases are limited

RT^{10} Overview

- Real-time, distributed architecture for mobile (tactical) and fixed (national) operational environments
- Provides
  - Access to **more comprehensive** data in near real-time
  - Integrated analytical workflow with complementary tools
  - Real-time alerting, both national and tactical
  - **Integration** across national-to-tactical SIGINT capabilities
- Expected Results: Order of magnitude improvements in real-time SIGNIT architecture for the U.S. Cryptologic System, focused on national to tactical intelligence, enabling **better** decisions in **less** time.

Annex A Version 1.6

RT10 Iraq Analytics
SPIN-5 (1 Oct – 31 Dec 2006)

Remote Linguistic Support Elements
Voice Processing
Overflow

Gists Trnspts

Voice Queues

NSA-Georgia
Target Knowledge
Linguistic Support
Pre-deployment Training

A&P (NSA-W)
(Product Line TOPIs)
Target Knowledge
Tool Knowledge

Queries / Tasking Feedback

Alerts / Refined Data

"RT10 TTP Center"
TTP Testing
Evaluate New Algorithms
Respond to RFIs (realtime)
Conduct Field/Refresher Training
(Vans in Baghdad)
Open Positions: xxx

Queries and Tasking

Alerts / Refined Data

Sense Making
New Knowledge

CSTs
(TF-24)
(4ID)

CSG

MNC-I
(CASE)
(CORP)
(Marines)

Improved Products & Alerts

MNF-I Divisions Embassy

COBRA FOCUS
Target Knowledge
Linguistic Support

TTPs
RFIs
TNG

MOC & Dragon Tamers
Initial TTP Development
TTP Maturation as needed
Pre-deploy Training Base
Develop Best Practices
Host TTP & Best Practices Library

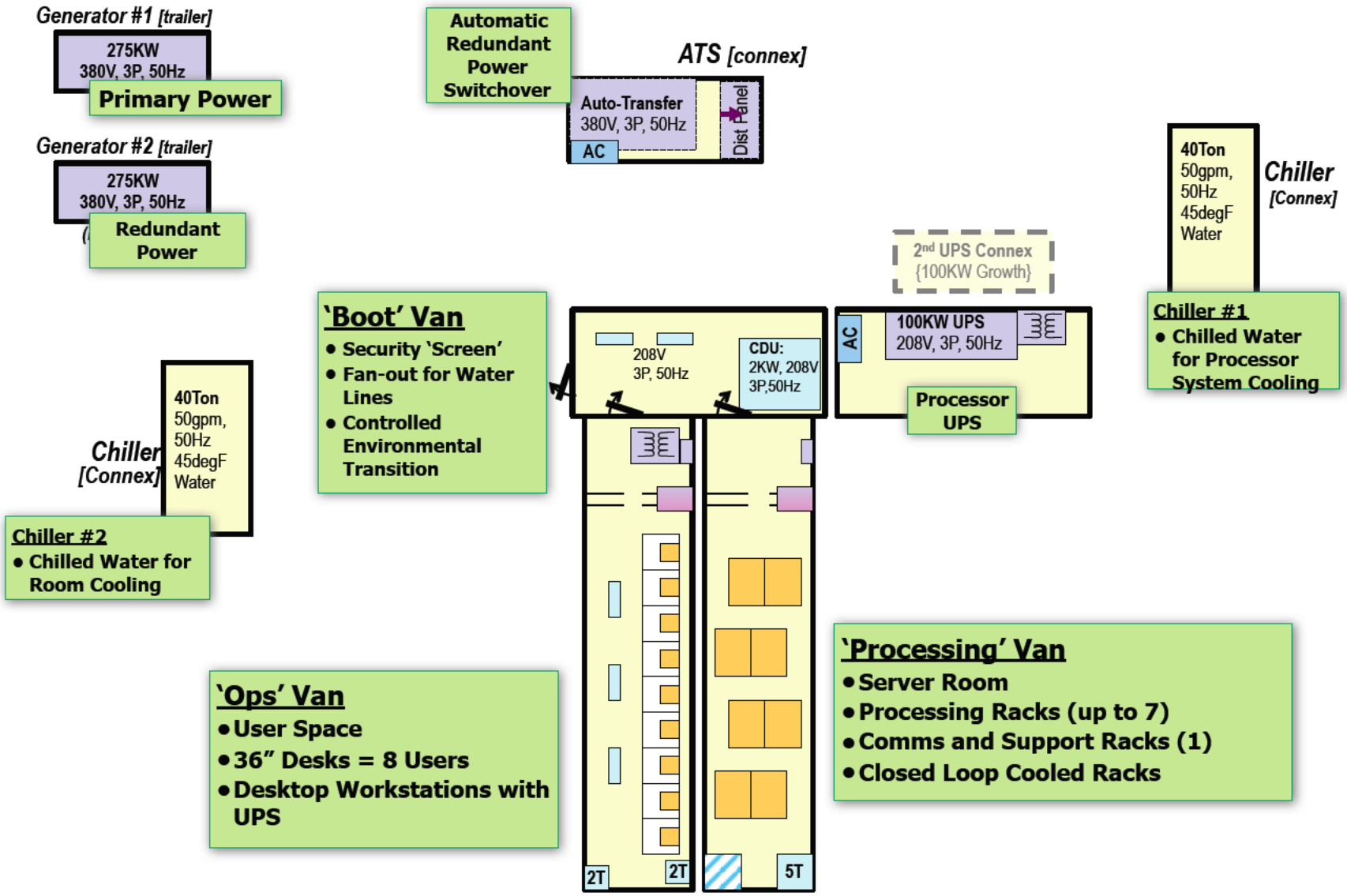
Tool Tradecraft Ideas
New Tool Recommendations

SIGINT Development GREEN DRAGON & RAD Elements
Tradecraft and Tool Recommendations
Analytic/Governance Advice
Algorithm (data-mining) development
Apply new TTPs at the National Level

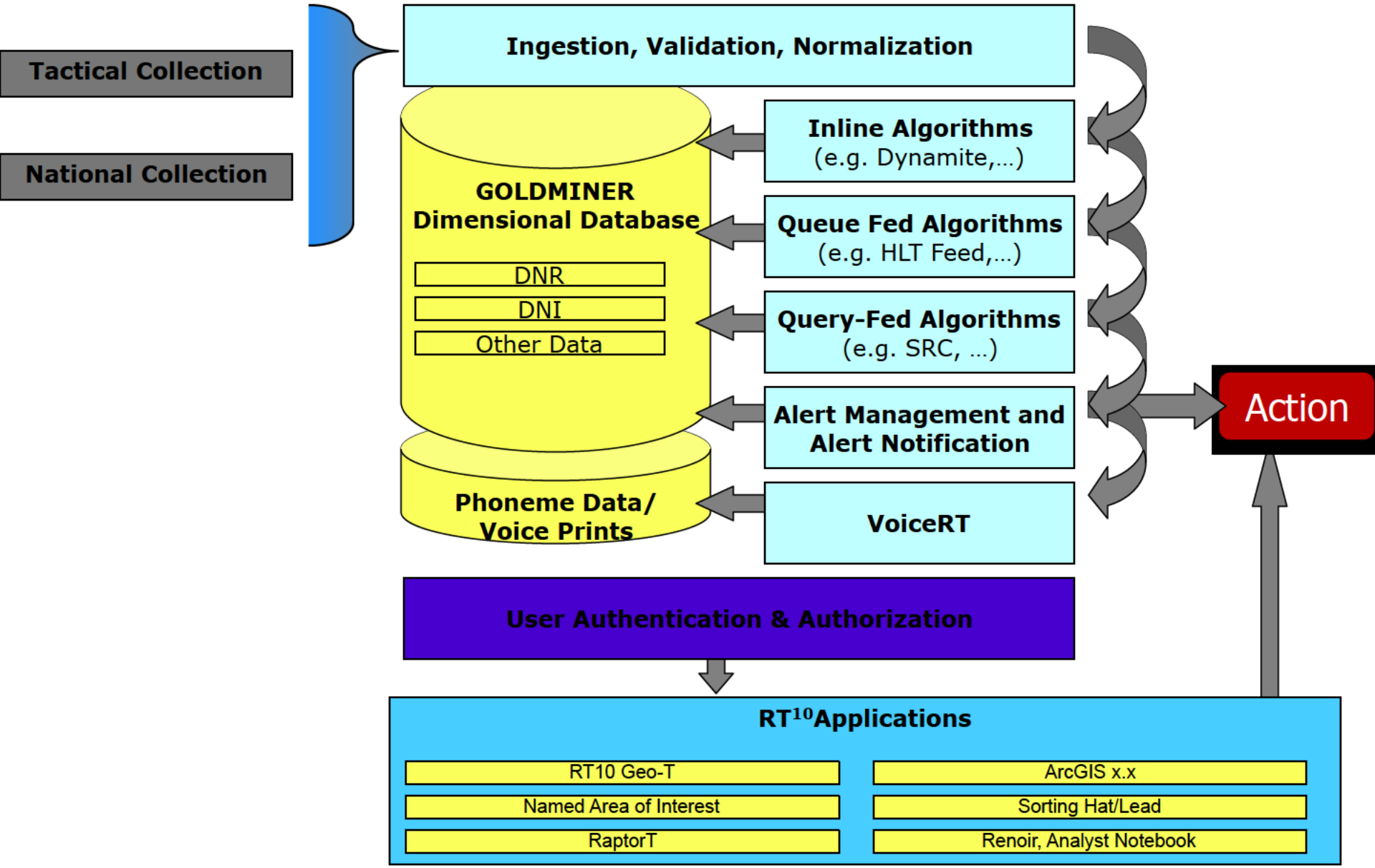
Respond to RFIs
(existing process)

TOP SECRET//COMINT//REL

System Block Diagram – Overview

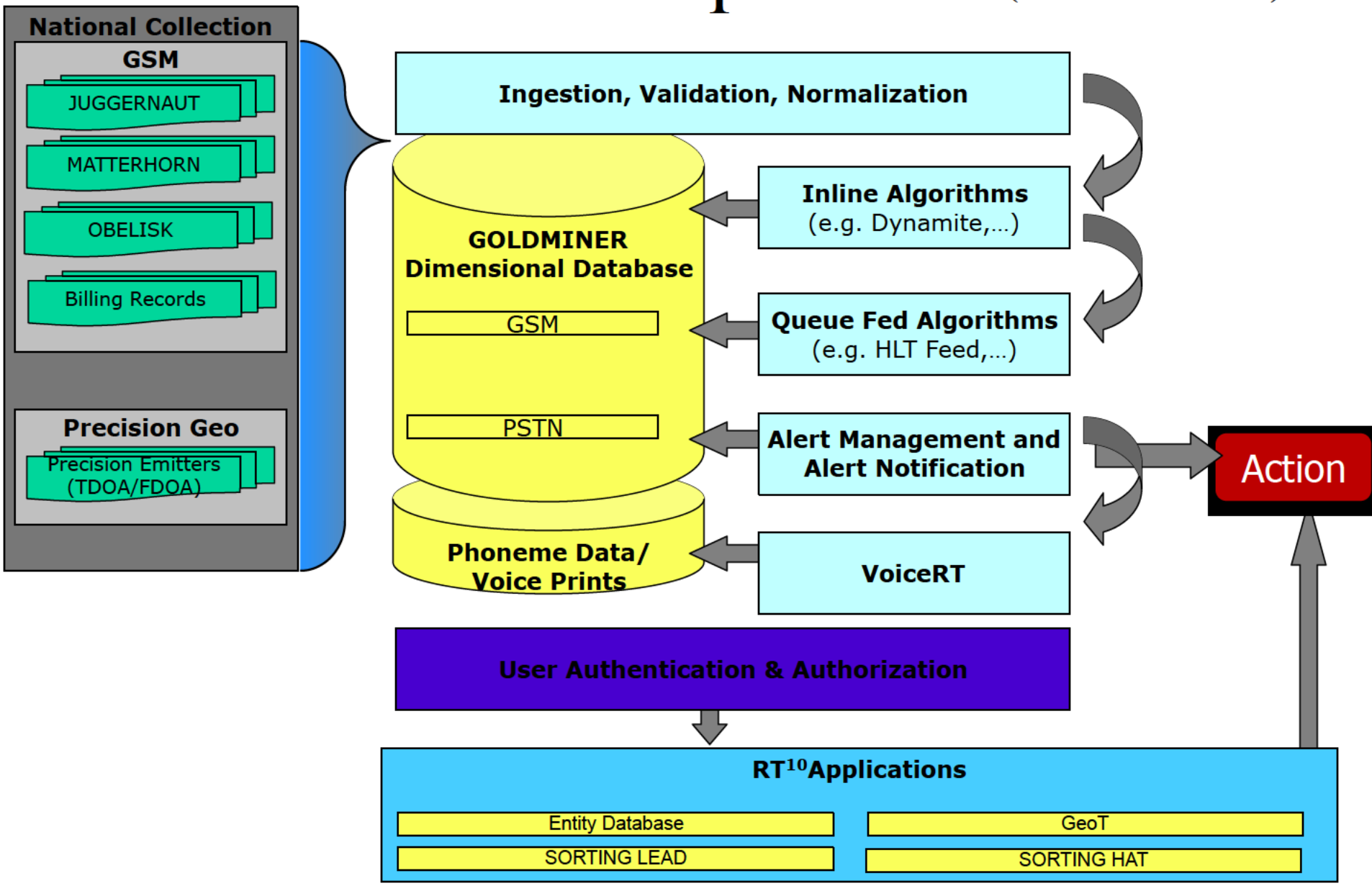


RT[10] Node Architecture

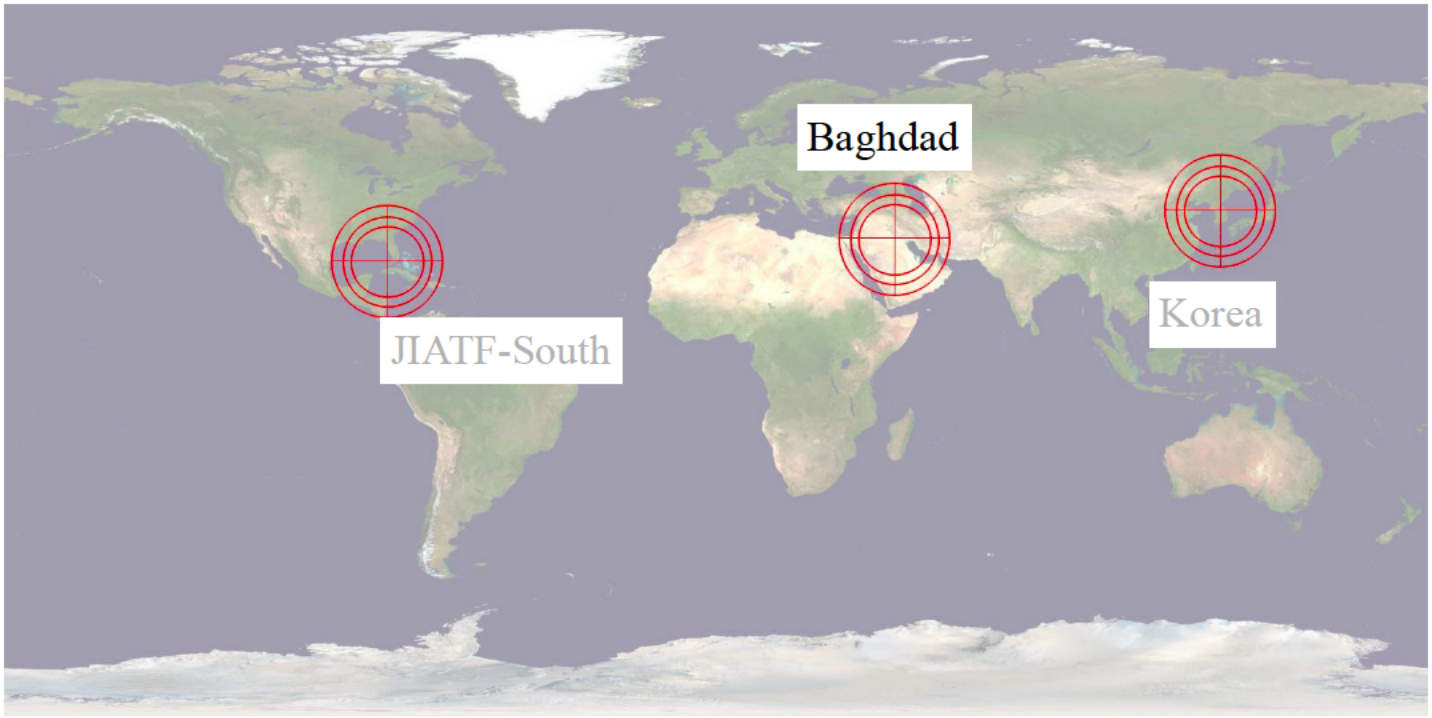


TOPSECRET//COMINT//20291123

RT[10] Iraq SPIN 5 (01 Oct – 31 Dec)



RT[10] Deployments



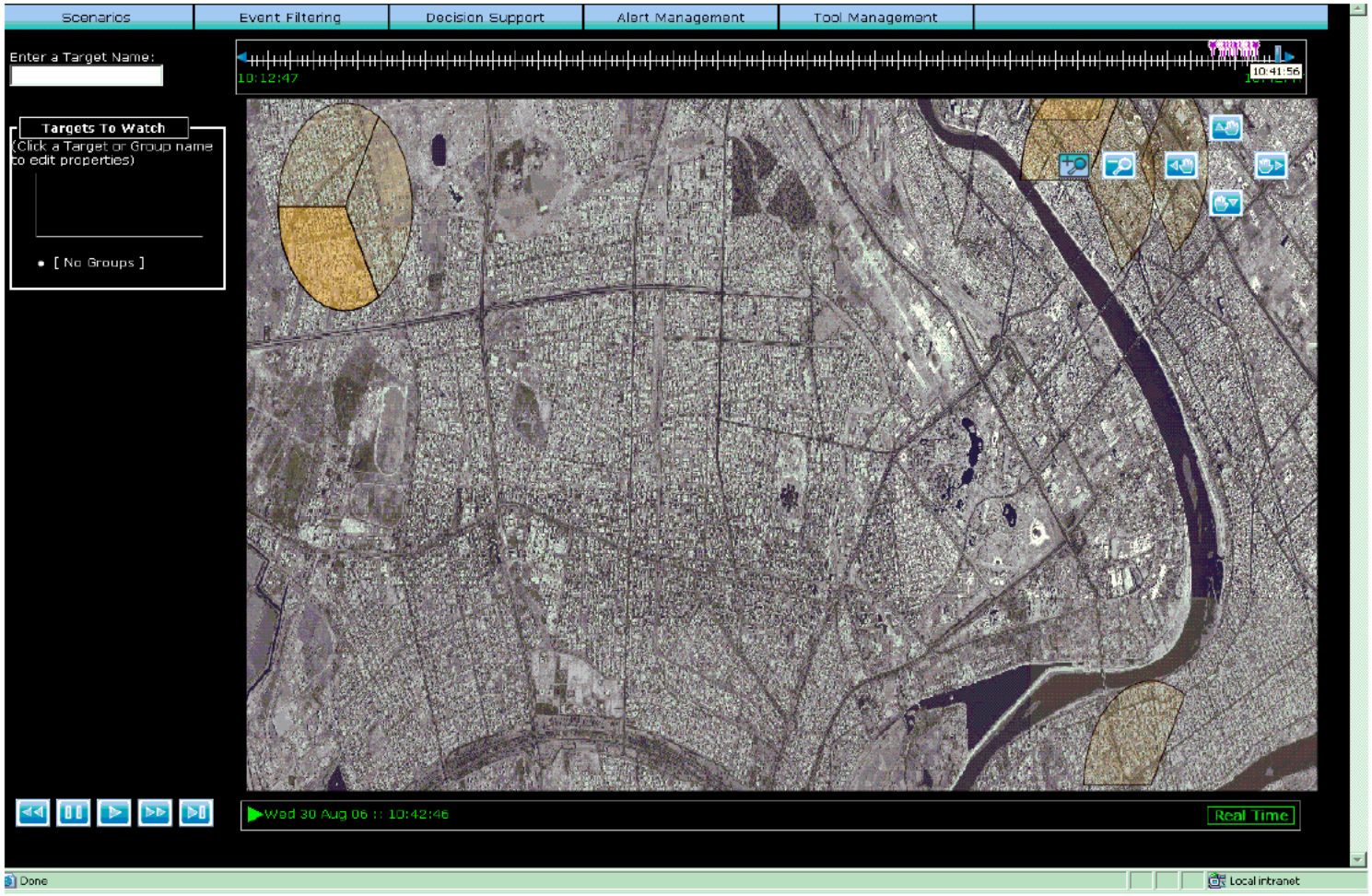
RT[10] in Baghdad, Iraq

- Baghdad, Iraq
  - Enable find-fix-finish operations
    - Provide immediate access to national / tactical collect
    - Integrate collection with geospatial alerting
    - Automatically correlate target behavior with collection, ie pattern-of-life
    - Prototype barrier monitoring systems
  - Expected results
    - Near-real-time data and advanced analytical tools provided to in-country units enable tactical decisions
    - VoiceRT provides alerting on spoken selectors, speaker identification, language identification, and content mining
    - Checkpoint data provides SIGINT tie to targets

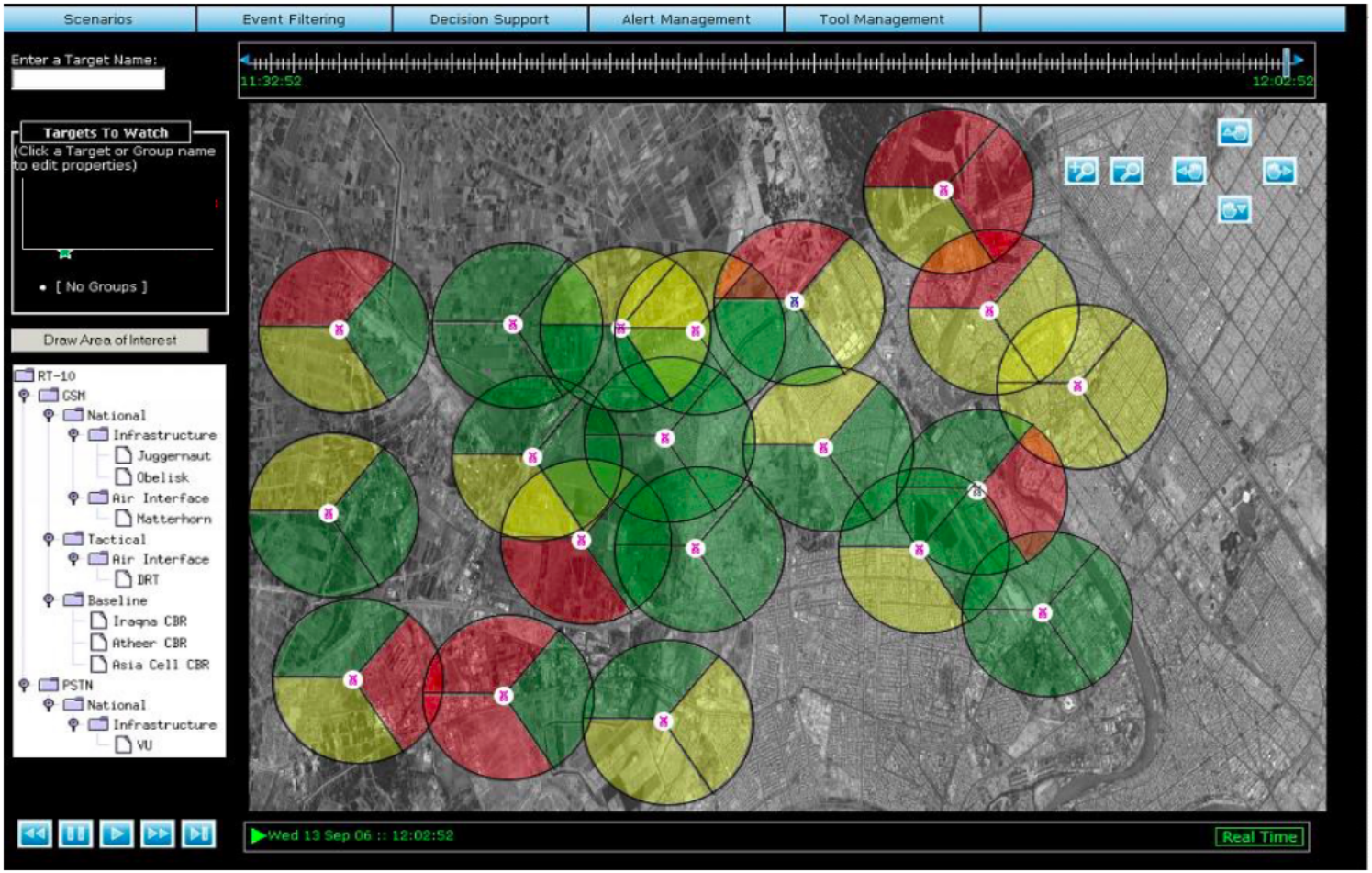
RT[10] Geospatial - GeoT

- Geospatial awareness
  - GeoT
    - Thin client similar to Google Maps and TIVO
      - Satellite imagery / other map layers
      - Overlay collection in real-time
    - Integrated with targeting database
      - Analyst defines named areas of interest
      - Can receive alerts when targets are detected in area
    - Display the health and coverage of SIGINT system
      - Where are our blind spots?

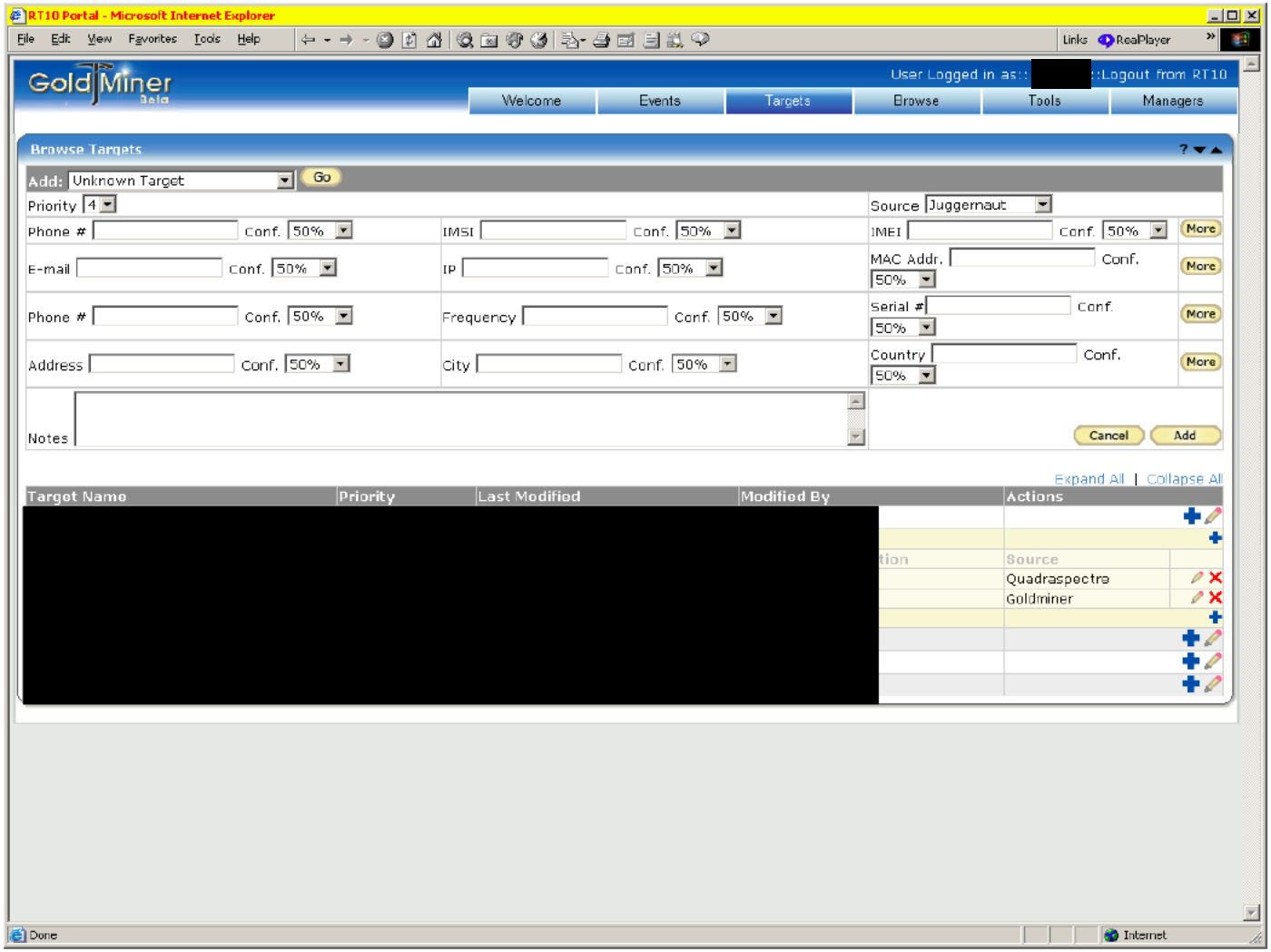
GeoT & Real-Time Collection



GeoT & Collection Status



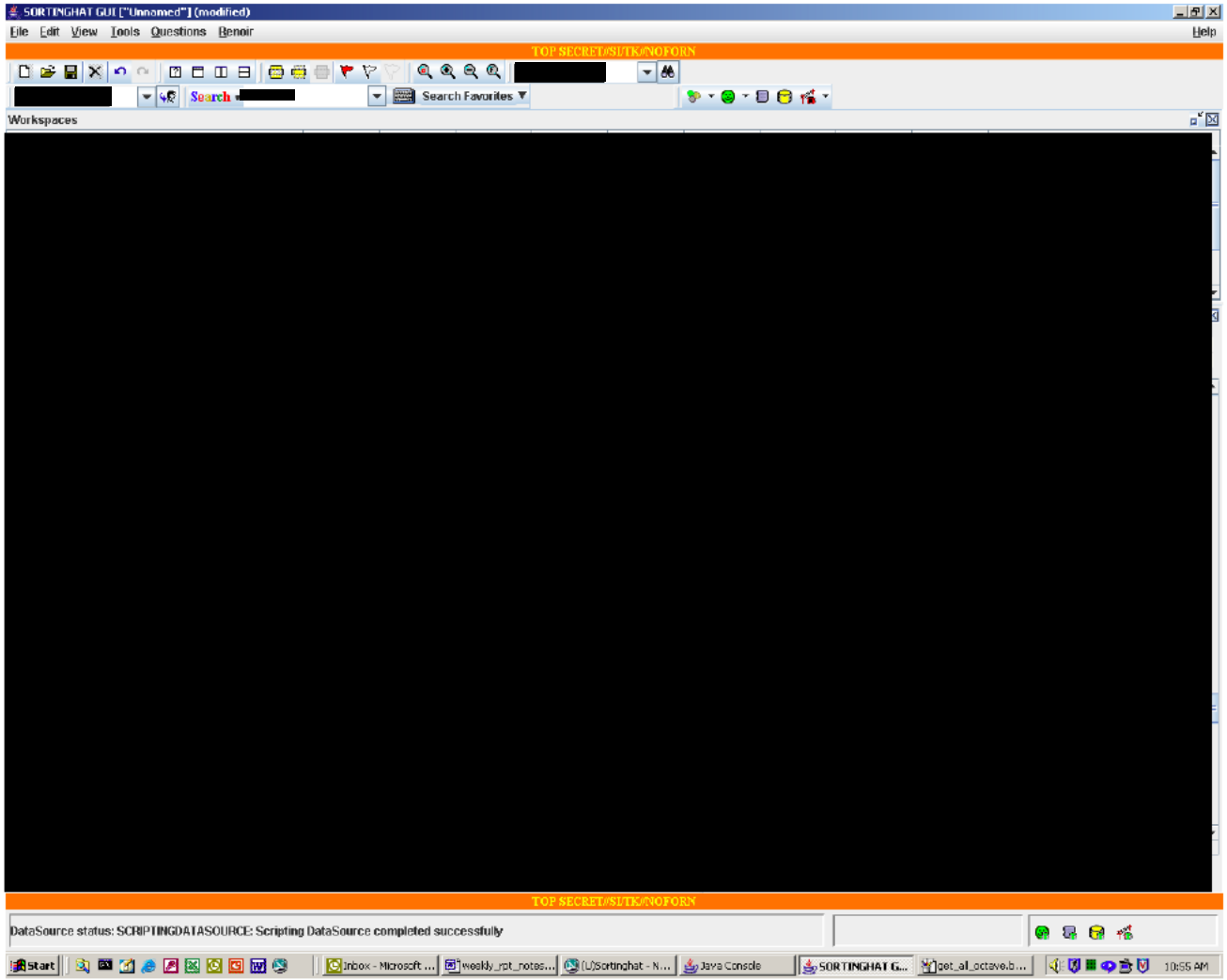
Integrated Target Database



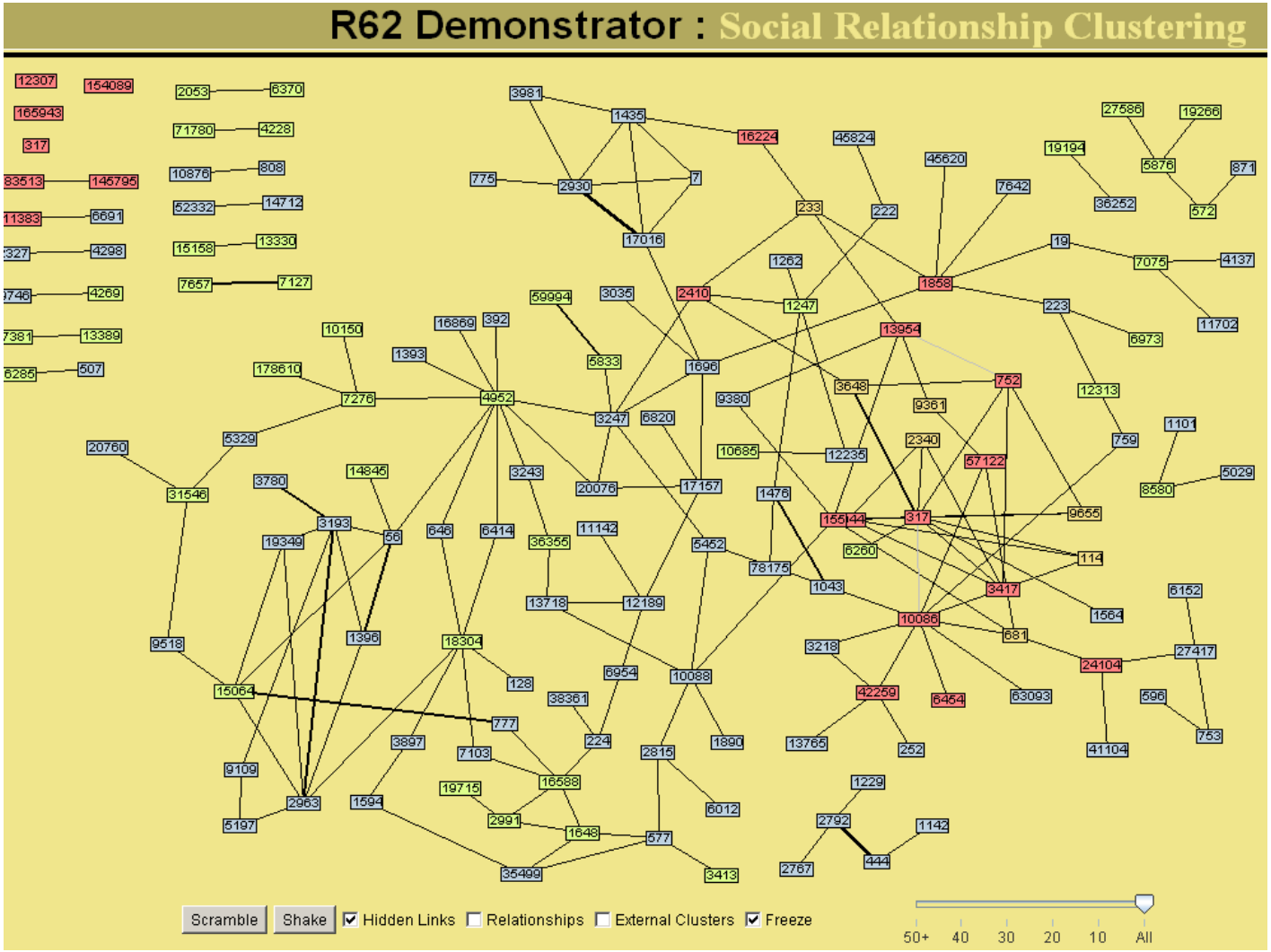
RT^{10} Geospatial Integration

- Logical views
  - SORTING HAT (R62)
    - Integrated SIGINT query
      - Historical SIGINT reports (Innovisions Testflight)
      - GLOBAL REACH
      - GOLDMINER / RT^{10}
  - Social Relationship Clustiner (GCHQ/R62)
    - Approximates social network analysis
    - Uses 11 algorithms to qualitatively connect targets
  - Analyst's Notebook and Renoir (InfoVis)

SORTING HAT (R62)



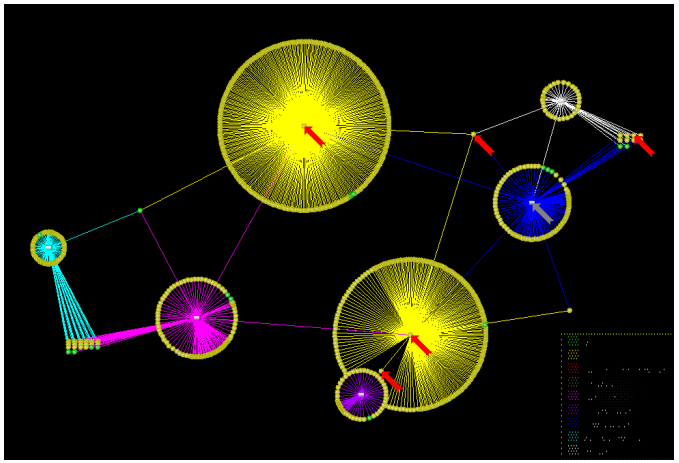
Social Relationship Clustering (GCHQ/R62)

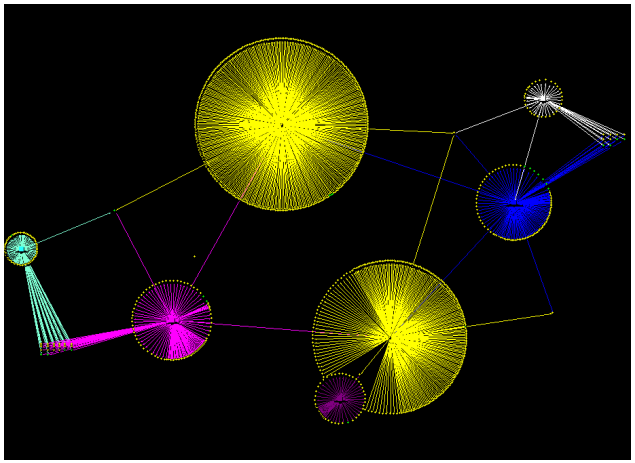


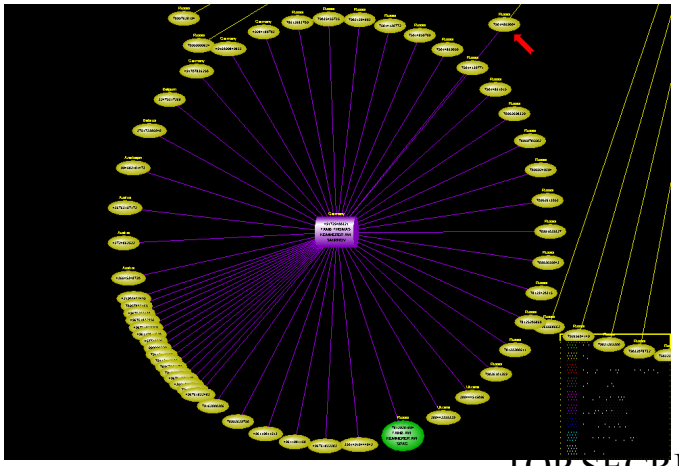
ANB Integration (InfoVis)

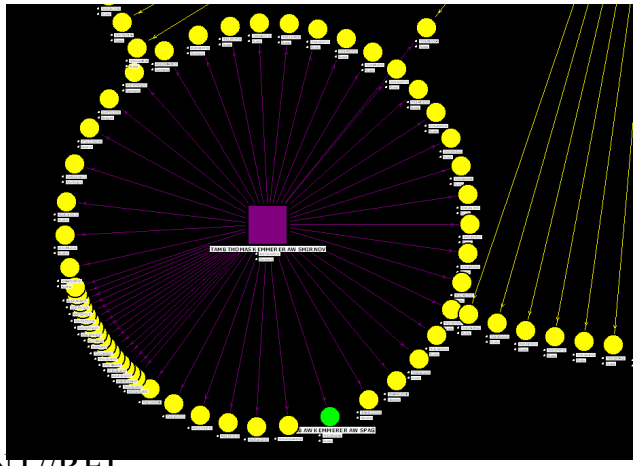
Renoir w/in SORTING HAT

Analyst's Notebook









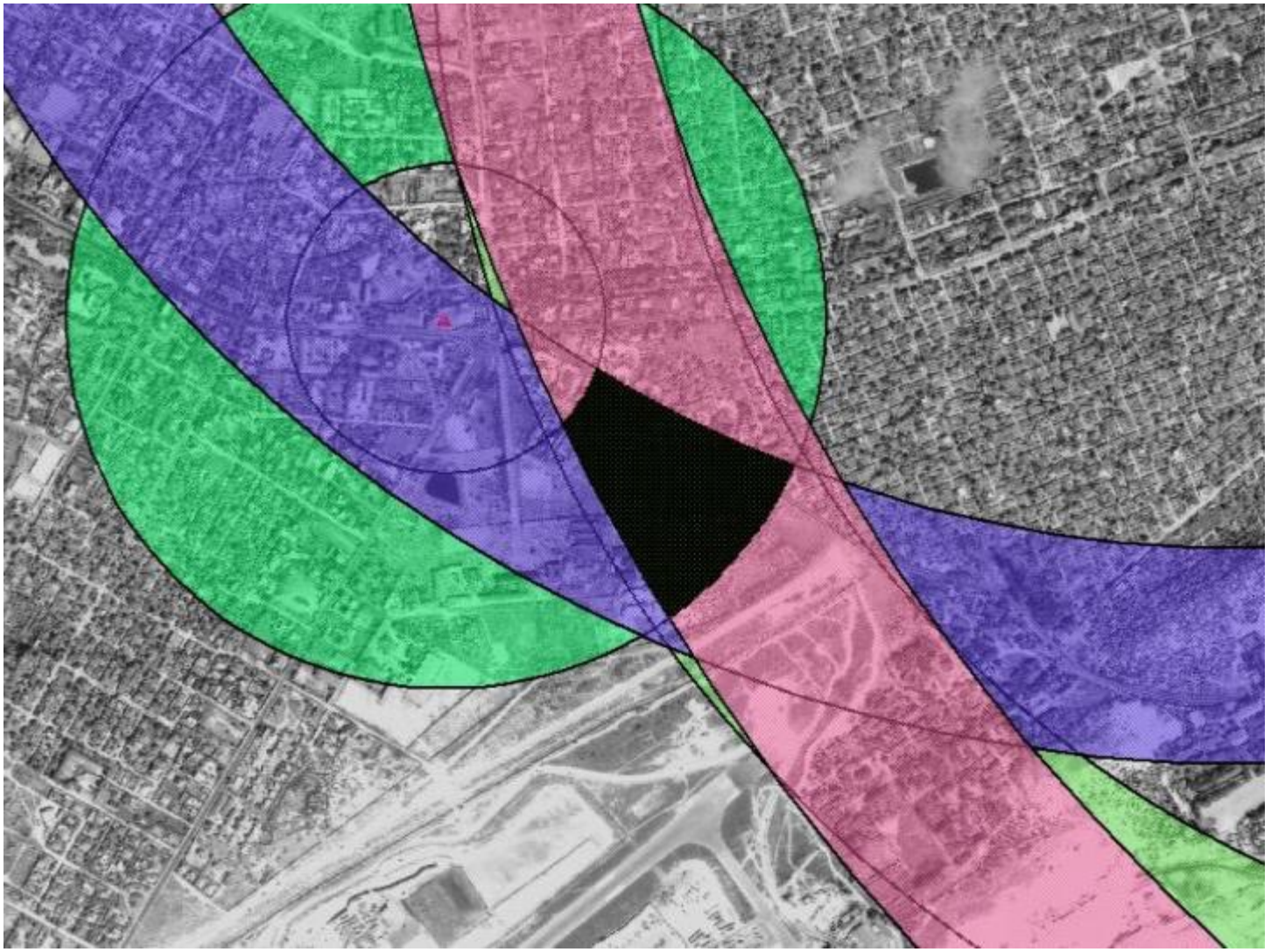
RT[10] Geospatial Integration

- Geospatial transform for a logical view?
  - Single selector
    - Last detected activity (or that within area of interest)
    - All activity (or that within area of interest)
    - Others: timeline view, color coded based on activity, area of interest, etc.
  - Graph
    - Some variation of single selector with graph overlaid
    - Every instance of activity between two callers
  - What transformation does the analyst expect?

Precise Geolocation of Handset

- Increasing precision with GSM geolocation
  - RT^{10} is situated at front-end
    - More access to timing advance data
  - Several RT^{10} and agency efforts
    - Manipulate GSM infrastructure to have data from multiple cell towers
    - SHARPFOCUS-2 (S327)
    - TOGA (RT^{10} - NRO/Penn State)

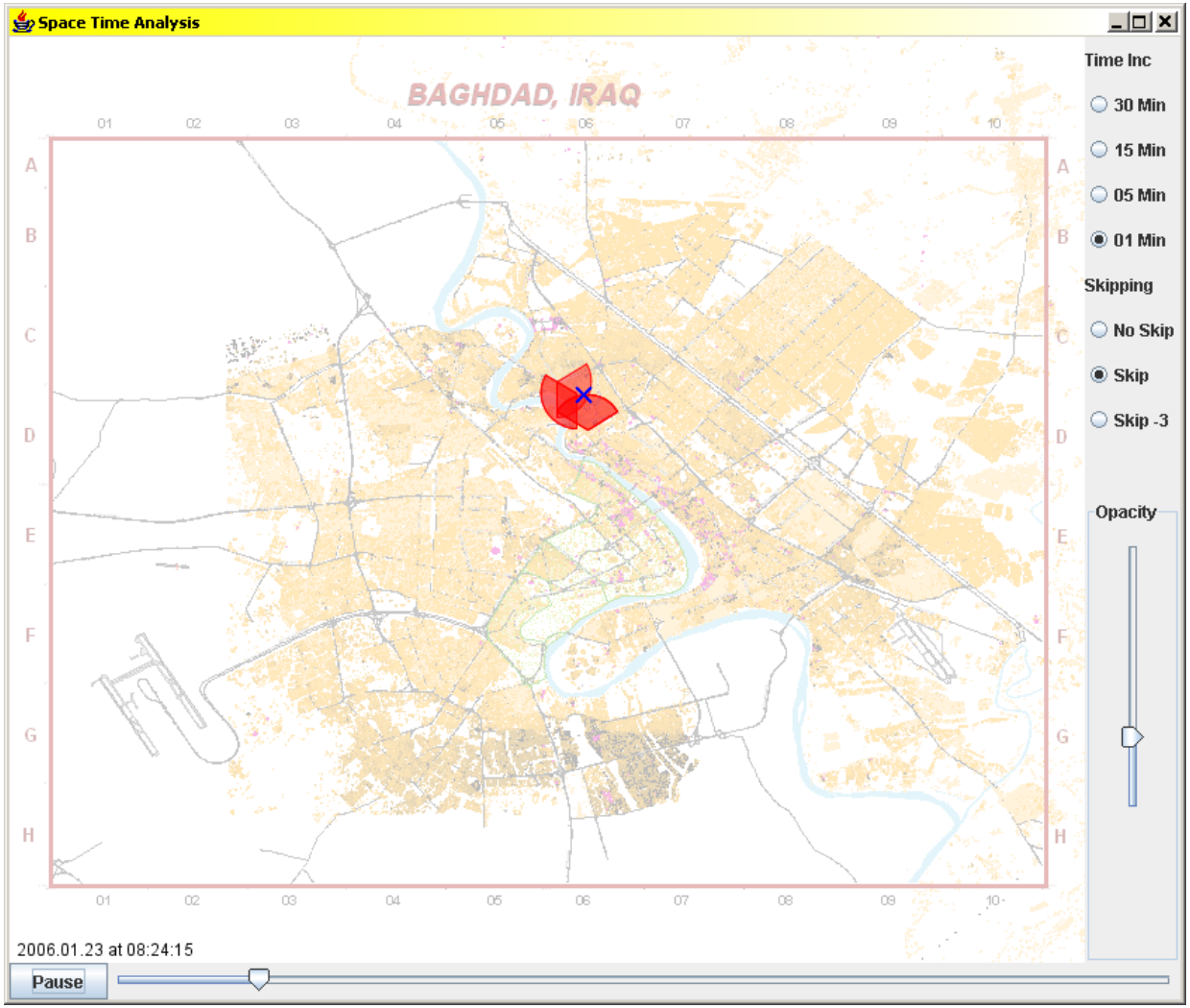
SHARPFOCUS-2 (S327)



Automated Analysis

- SORTING LEAD (R62)
  - Characterizes GSM behavior
    - Based on location, time-of-day, callee, etc.
    - Identifies
      - When target has multiple phones
      - When target has swapped phones
      - When target deviates in behavior
  - Correlate DNI persona to GSM handset
    - Enable tactical operations, tracking of DNI targets
    - Help with internet café geolocation problem

DNI Correlation Example



Questions?