

**(TS//SI//REL) Intelligently filtering your data:  
Brazil and Mexico case studies**

**SATC**

Antonio Veloz  
June 2012

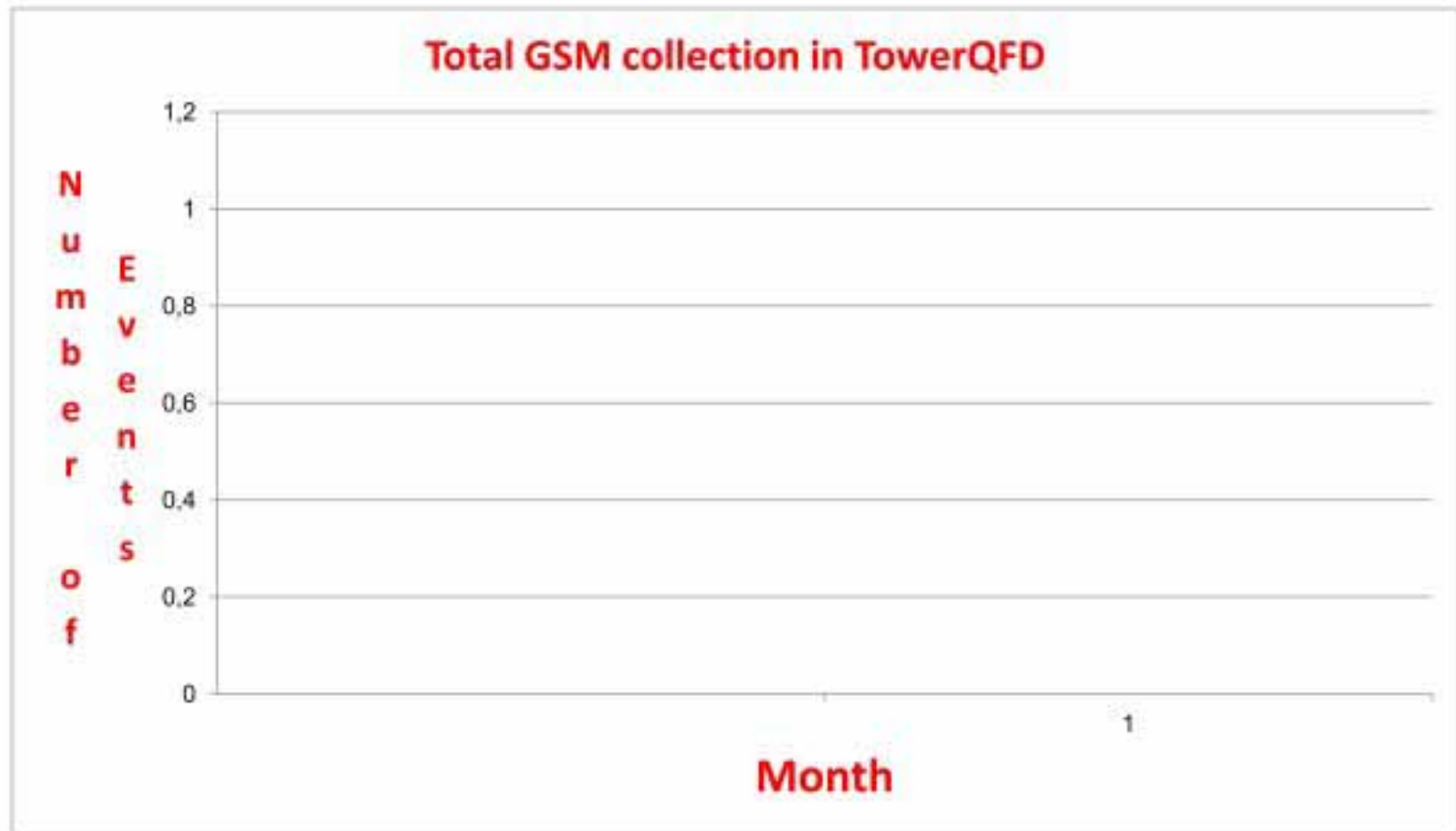
# (U) Classification

This presentation is classified  
TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL



# (U) The problem

- (S//SI//REL)Too much data ...



# (U) The problem

□(S//SI//REL)...so little time

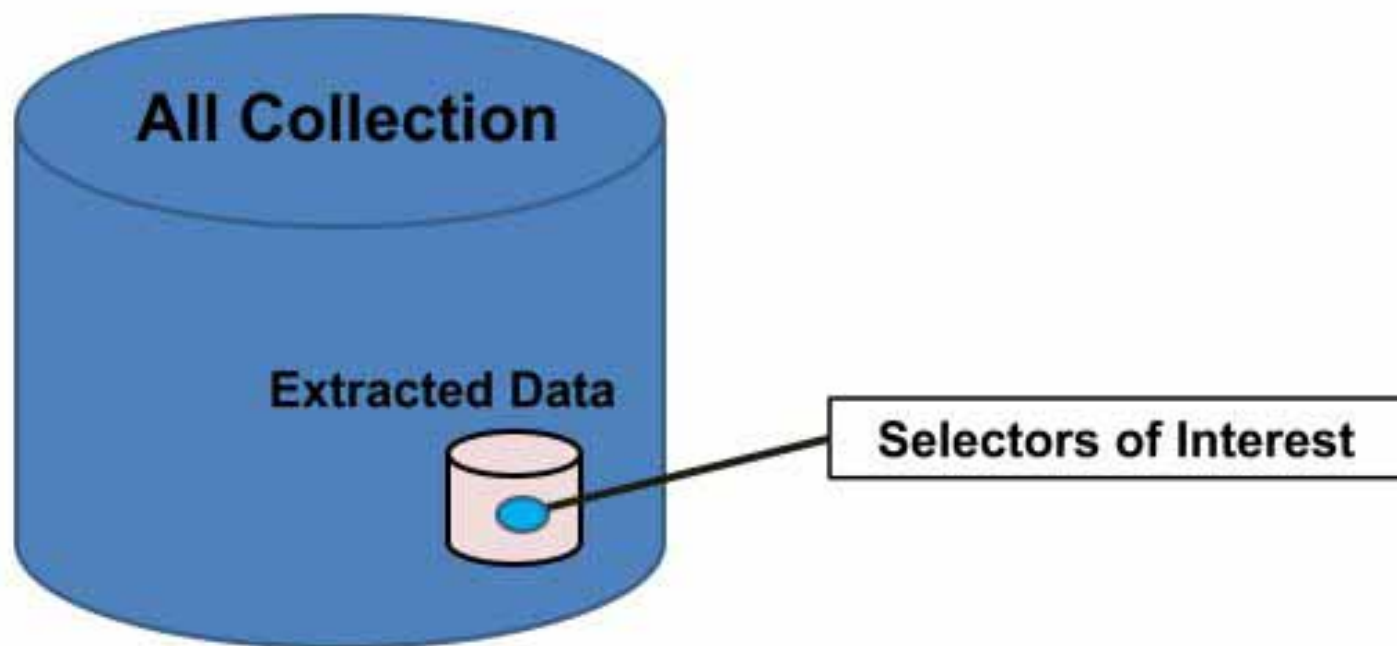


# (S//REL) CONTACT GRAPH-ENHANCED FILTERING



## (U) The benefits

- (S//REL) Extracts from the full collection of data the activity most relevant to the selectors of interest



## (U) The benefits

- (S//REL) Allows the analyst to implement analytics that
  - Are customized to their needs on a target-by-target basis
  - Could not or should not be run against all collection
  - Might find a needle in a haystack in an repeatable and efficient way

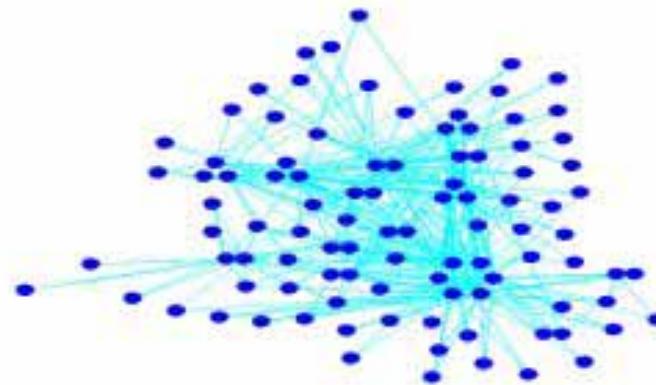
# **(U) BACKGROUND**





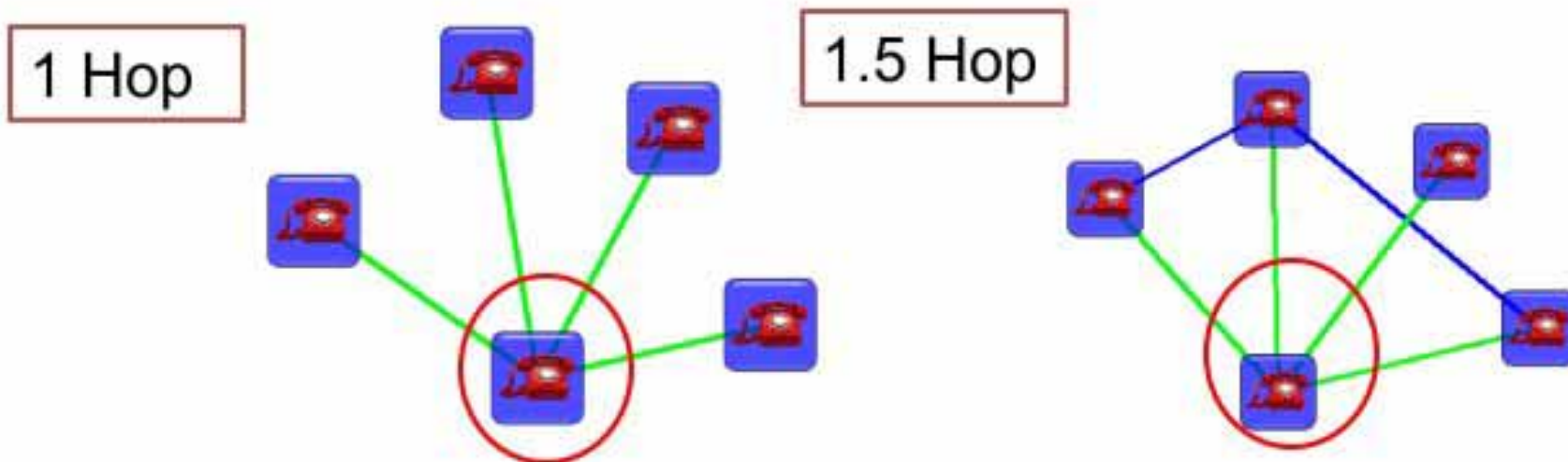
# (U) Contact Graphs

- (U) A **graph** is a set of objects (nodes, vertices) connected by links (edges).
- (U) Graphs are a useful way of visualizing and analyzing the structure of communication networks



# (U) Hops

- (U) We may build a 1-hop graph by selecting all vertices connected to a root node
- (U) A 1.5-hop graph contains all vertices connected to a root node and all connections between those vertices



# **(U) The General Procedure**



# (U) Two Phases



(U) One-time work



(U) Every-time work

## (U) One-Time work

- (U) The initial chunk of data extracted in this phase
  - Represents more data than what will be used in the next phase, but extracting this much data minimizes the risk of missing crucial data
- (U) Storage costs and computation time are highest in this phase

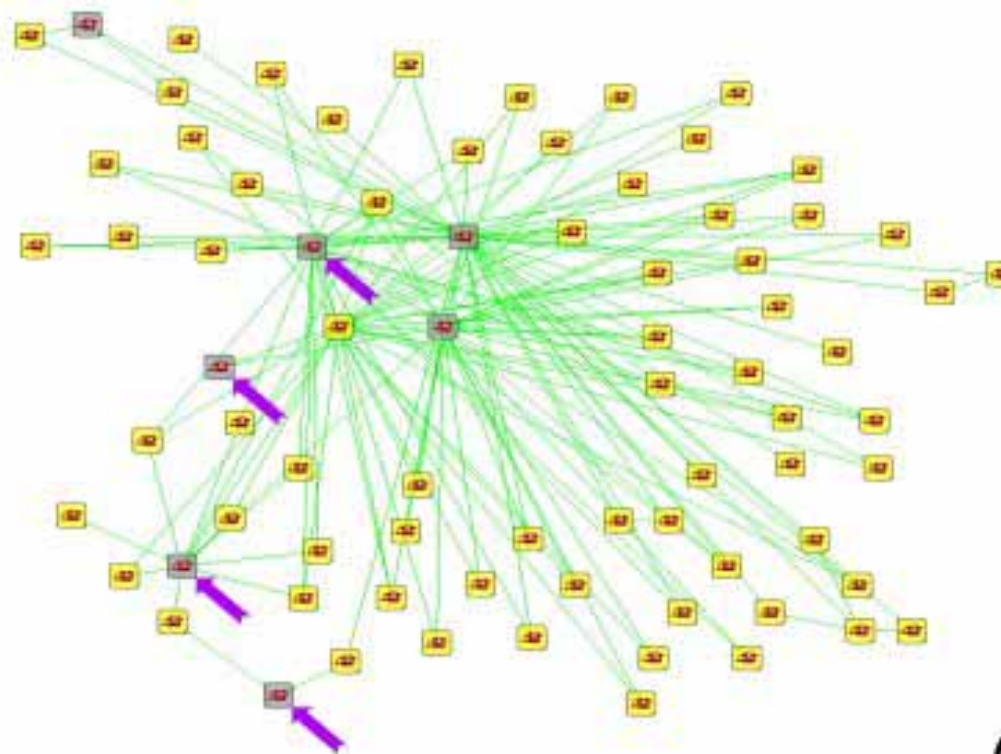
## (U) every-Time work

- (U) In this phase, the initial chunk of data is further sub-setted by more refined and targeted searches
- (U) The cost in both storage computation time are smaller than in the previous phase
- (U) Finally, possible results are validated



# (U) applications in target development

(C/REL)



(C/REL)



# (U//FOUO) S2C41 surge effort

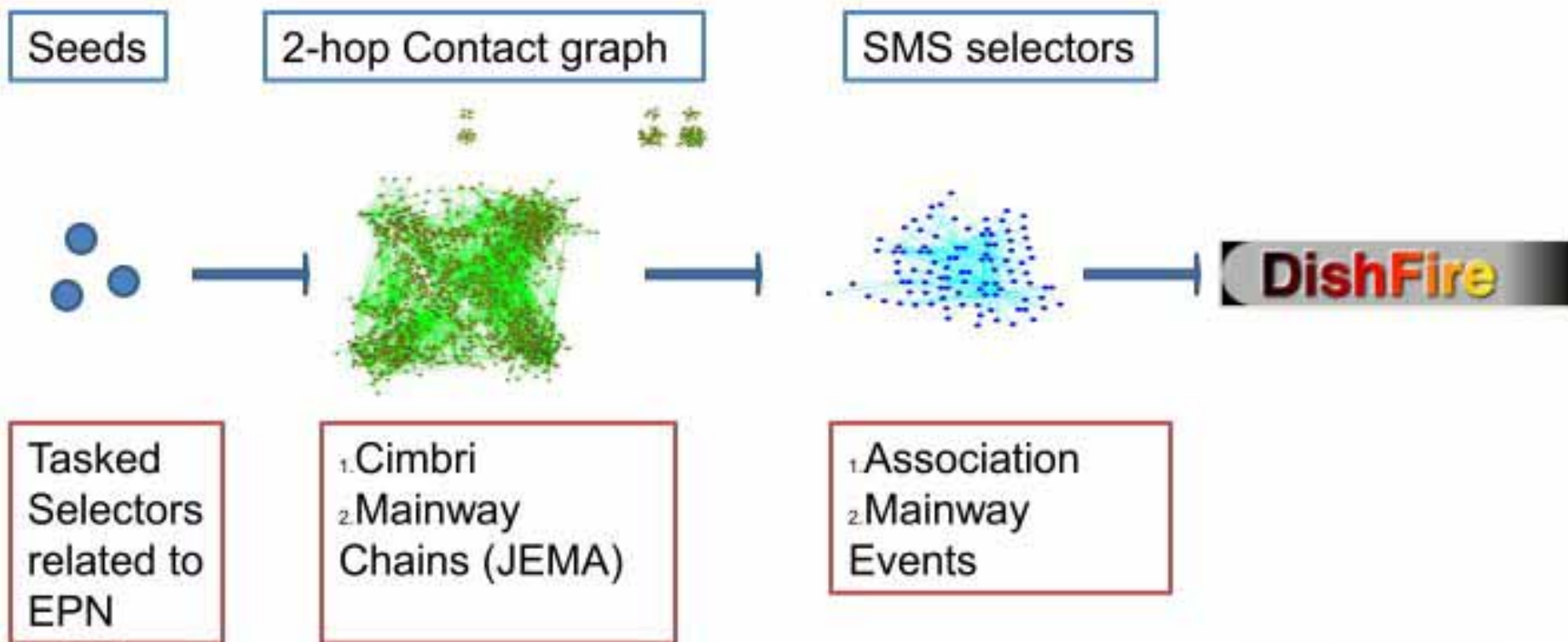
(TS//SI//REL) NSA's Mexico Leadership Team (S2C41) conducted a two-week target development surge effort against one of Mexico's leading presidential candidates, Enrique Pena Nieto, and nine of his close associates. Nieto is considered by most political pundits to be the likely winner of the 2012 Mexican presidential elections which are to be held in July 2012. SATC leveraged graph analysis in the development surge's target development effort.





# (U) One-Time Work

(TS//SI//REL)



(TS//SI//REL)





# (U) Results

□(S//SI//REL)85489 Text messages

## Interesting Messages

[REDACTED] Me dice Jorge Corona Srio de EPN que el escucho que BPR se iba a con Moreira no es asi? Y pues va soka salvo que le digas a alguien,, Assoc ID not requested,not requested,not requested,,, [REDACTED]

Nieto

[REDACTED], Mi Querido Alex el nuevo titular de Com. Social es Juan Ramon Flores su cel es [REDACTED] el ID [REDACTED] Nuevo Srio. Part. Es Lic. Miguel Angel Gonzalez Cel [REDACTED] el Nuevo ID de JORGE CORONA es [REDACTED] un abrazo y seguimos en contacto avisame si llego el msj. por favor....., [REDACTED]

# (U//FOUO) S2C42 surge effort

## (U) Goal

(TS//SI//REL) An increased understanding of the communication methods and associated selectors of Brazilian President Dilma Rousseff and her key advisers.



# (U) One-Time Work

(TS//SI//REL)

Seeds



2-hop Contact graph



DNI  
selectors

SCIMITAR

(TS//SI//REL)

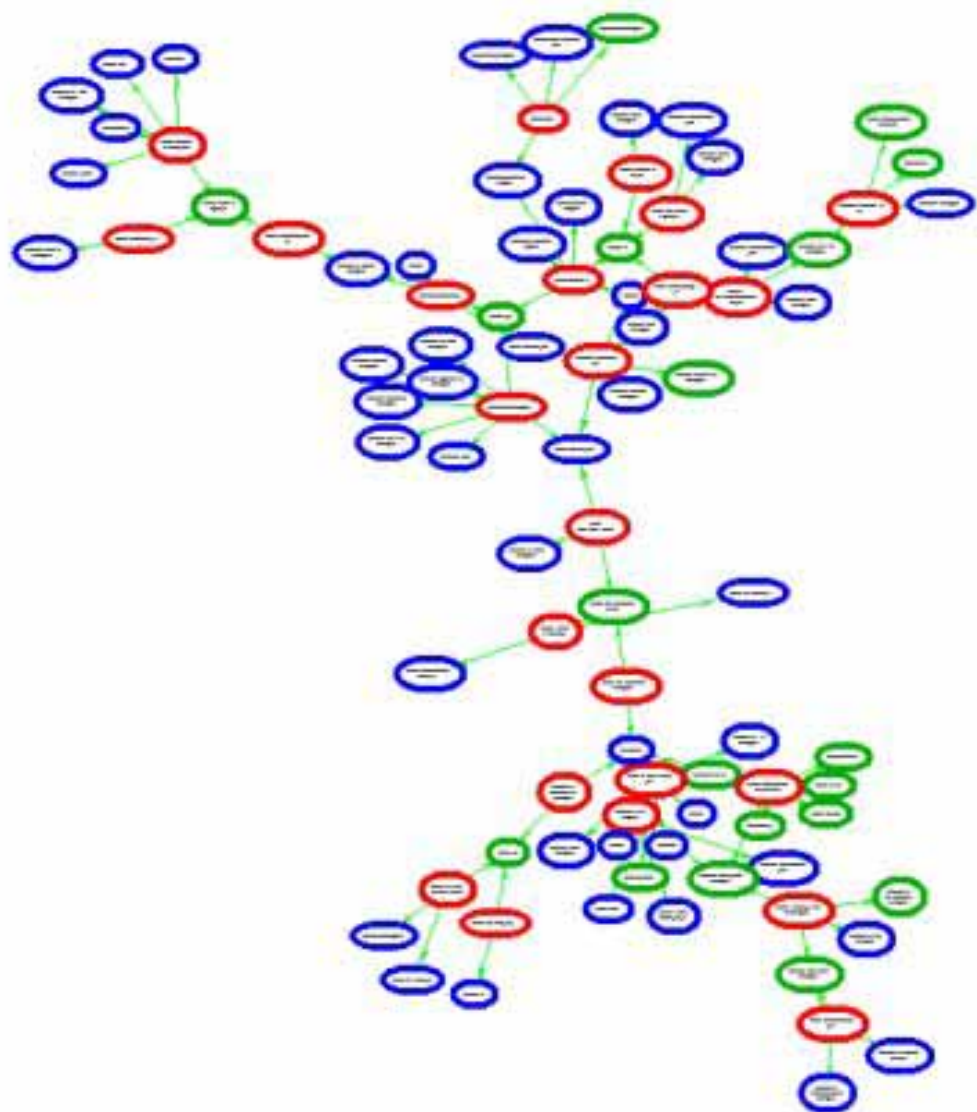






# (U//FOUO) S2C42 surge effort

(TS//SI//REL)



-Discovered new selectors associated with high-value targets

(TS//SI//REL)



## (U) Conclusion

- (S//REL) Contact graph-enhanced filtering is a simple yet effective technique, which may allow you to find previously unobtainable results and empower analytic discovery
- (TS//SI//REL) Teaming with S2C, SATC was able to successfully apply this technique against high-profile, OPSEC-savvy Brazilian and Mexican targets.



# Geopolitical Trends: Key Challenges

## (S//REL) Transnational Issues

- Extremism on AF/PAK Border.
- Economic prosperity/power, competition for natural resources, global problems.
- Arab Spring continues.
- Terrorist threats to the US and Allies.
- Cyber-threats to the US.
- Organized crime, Hacktivists, etc.
- Nuclear Proliferation.
- Non-State Organizations and Actors on the World Stage.
- The “Next” Internet – Governance and

## (S//REL) Nation-State Issues

- Destabilization of Korean Peninsula.
- Cyber-threats to the US.
  - Russia, China, and many others.
- Chinese Military Modernization.
- Russian Military Modernization.
- BRICS as new economic powers.
- Friends, Enemies, or Problems?
  - Brazil, Egypt, India, Iran, Mexico, Saudi Arabia, Somalia, Sudan, Turkey, Yemen, and others.
- Asymmetric warfare.