ORKASH

... ensuring Assurance in complexity and uncertainty

# Automating Intelligence Creation & Analysis

30 Jan 2020

*Ashish Sonal*
*CEO*
**Orkash Services Pvt Ltd**

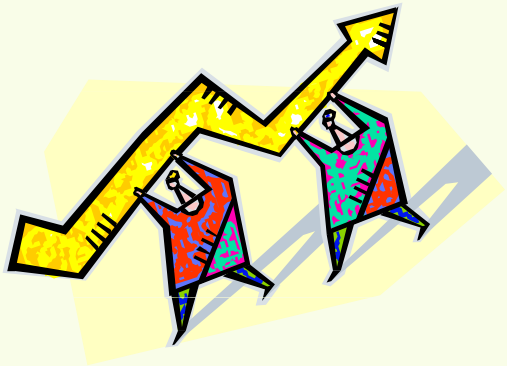
Orkash is an international management-consulting and high-technology services company operating in the following areas:

- Investment & Transaction Advisory Support
- Operational Risk and Security Risk Management
- Strategic Business & Market Intelligence
- SaaS-based Technology Solutions

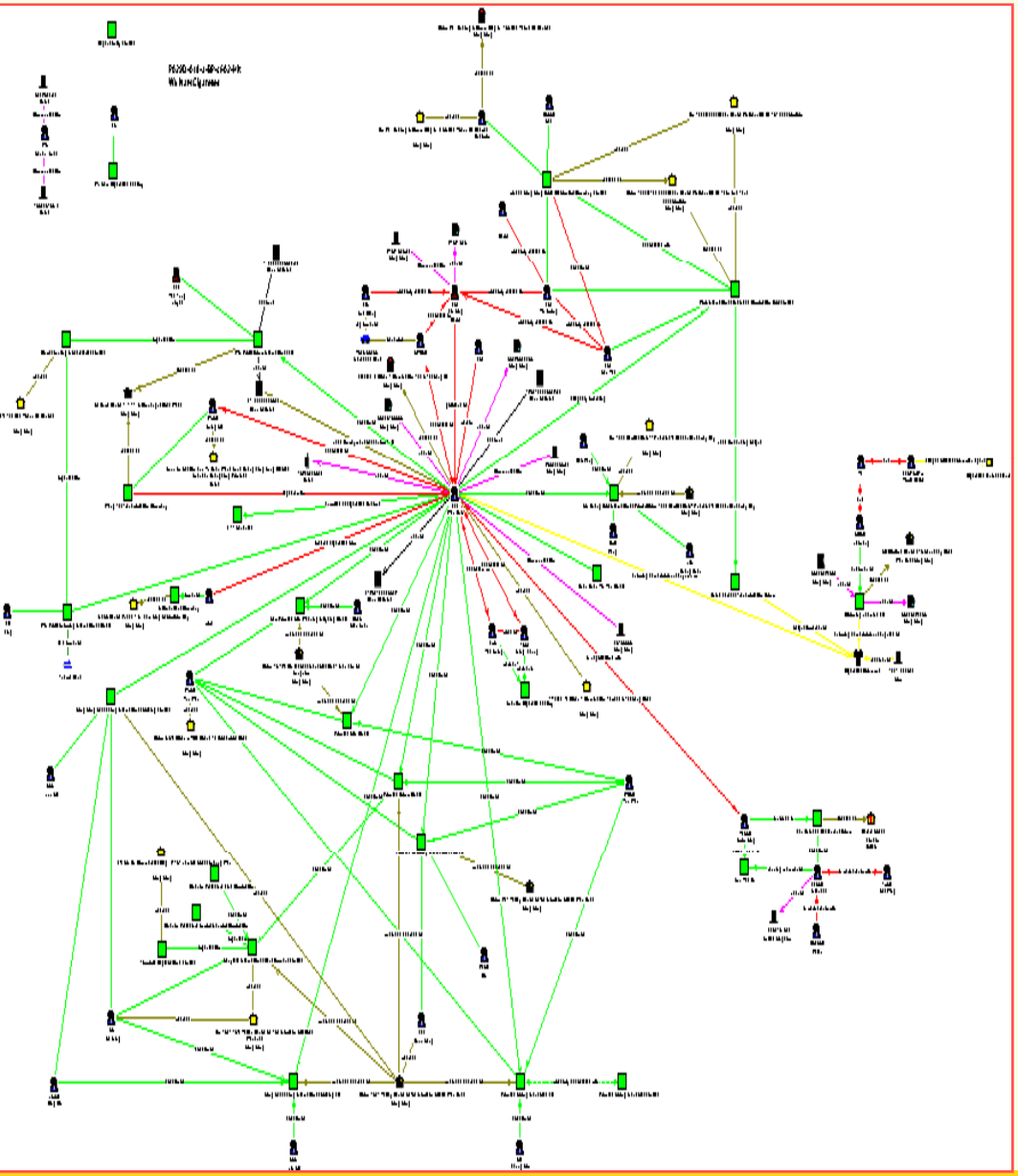
Cutting edge technology expertise across AI systems, very large data mining, BI, cyber forensics, and parallel computing clusters & cloud computing.

*Orkash is dedicated to turn knowledge and information into intelligence as a value driver for rapid response to new opportunities, competitive forces and risks. The greater the uncertainty, complexity and risk in an operating environment, the greater is the potential of the value that Orkash delivers.*

*The company prides itself in measuring the value that it creates for its clients on strategic business metrics such as efficiencies in execution, time-to-market, and returns.*



# Key Areas



**Automating Intelligence Creation**

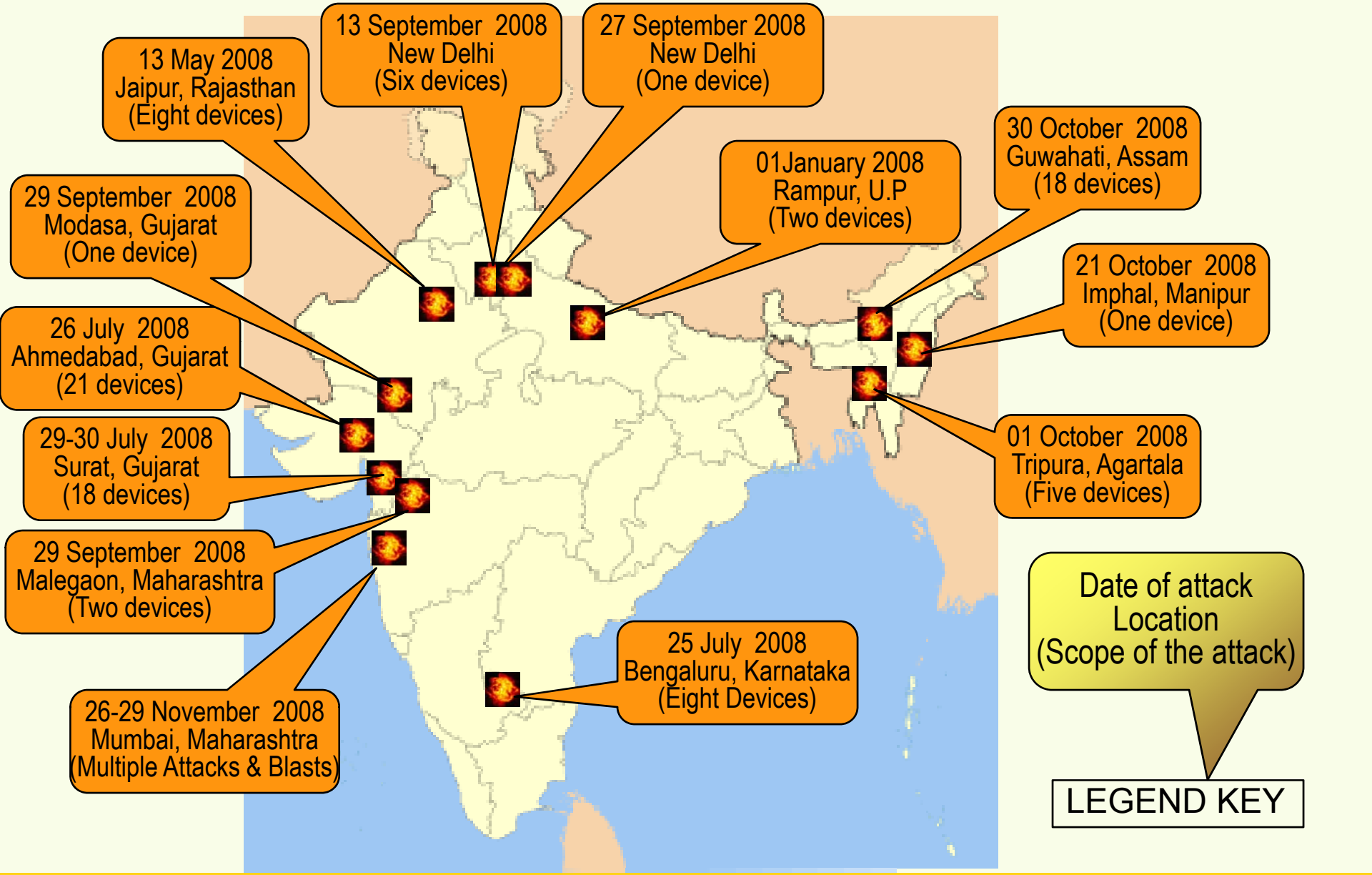
**Semantics & GIS Integration -** *Bridging Technical Intelligence & Human Intelligence*

**Investigative Intelligence -** *Cyber Forensics*

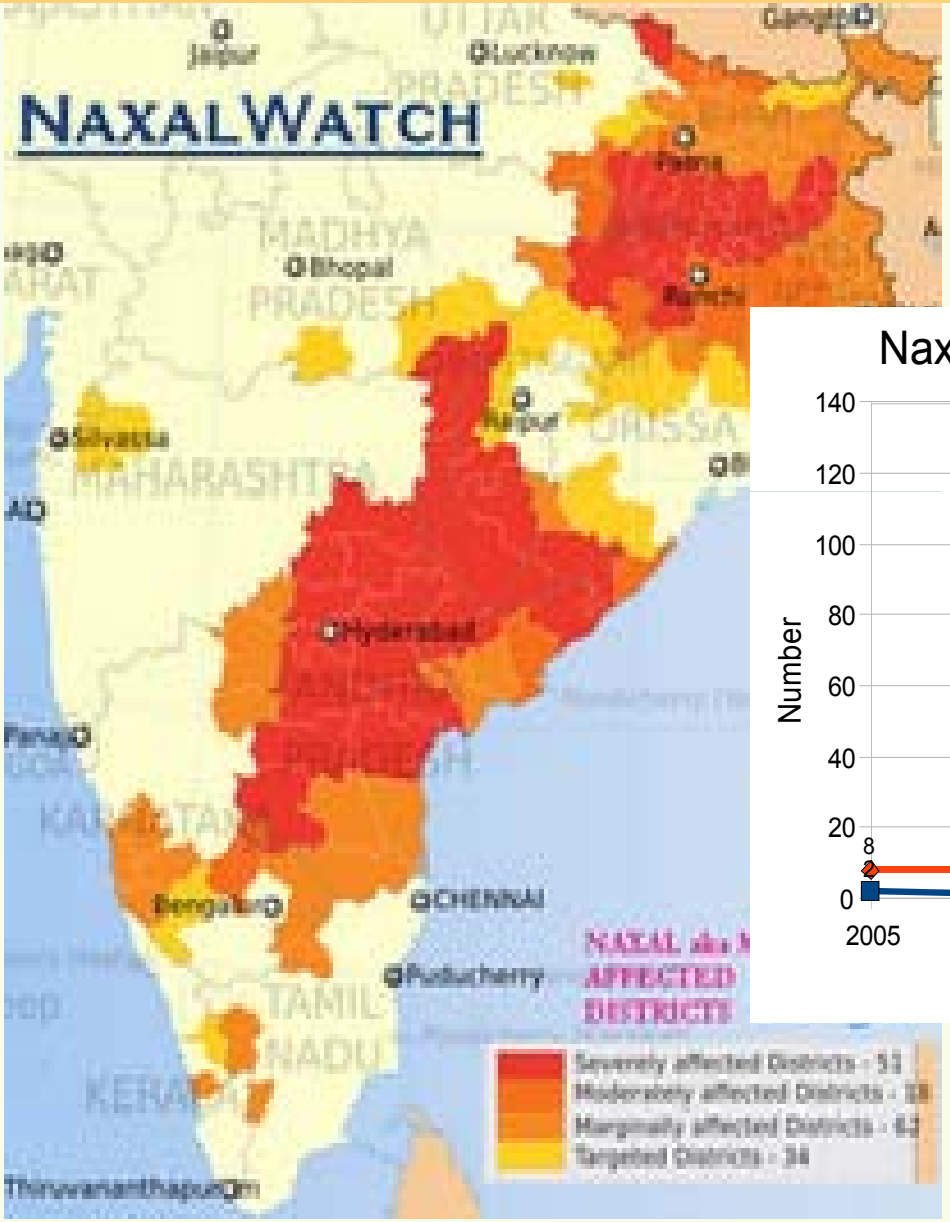
**Decision Support -** *Granularity & Visualization*

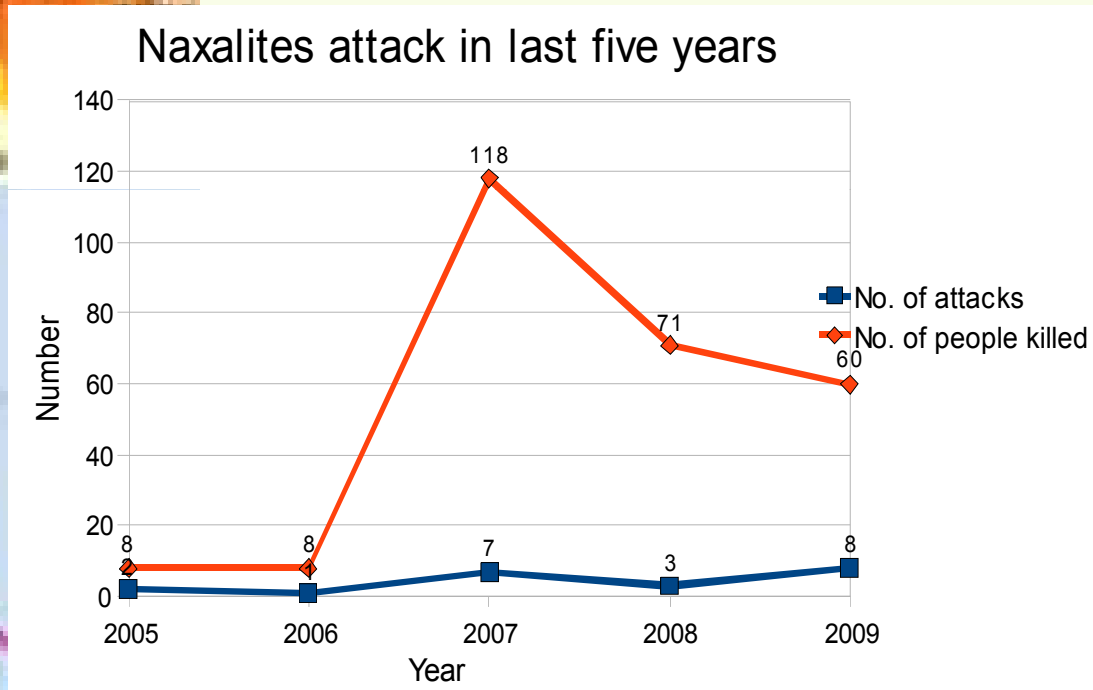
**Backend Technologies -** *HPC Clusters and Clouds, AI Expert Systems, Large Scale and Real Time Data Mining*

# Patterns ..



# Major Naxalites Areas



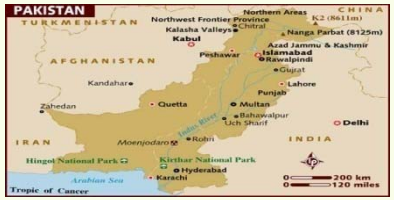



# Information Asymmetry

- From the organized 26/11 Mumbai attacks, it is clear that the attack was planned long ago
- Terrorist groups used the internet and the mobile networks, for communicating messages, collecting information, money transactions and other

**Banking and Card Usage**

**Internet account**
Account: Hazi Al
Password:
Hazi_123




**Location**

alarbi.alhindi@gmail.com

alarbi_gujarat@yahoo.com.uk

al_arbi_delhi@yahoo.com

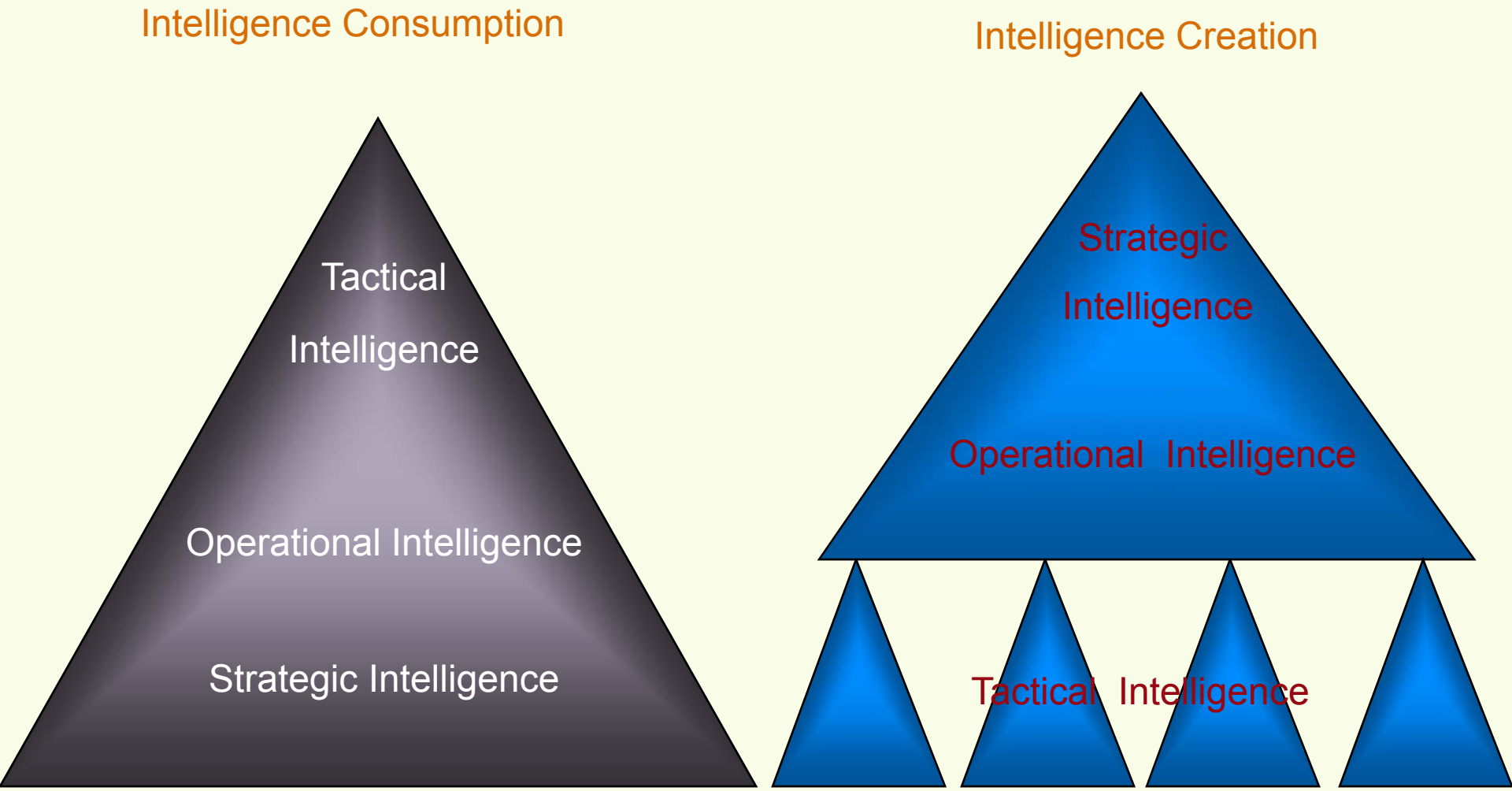

**Multiple Sims**

**Multiple Handsets**

Historical data analysis can train artificial intelligence expert-engines to raise triggers and red flags. Real time data mining of mobile traffic generate trends and patterns in the usage

**Telephone**

# The Intelligence Stack



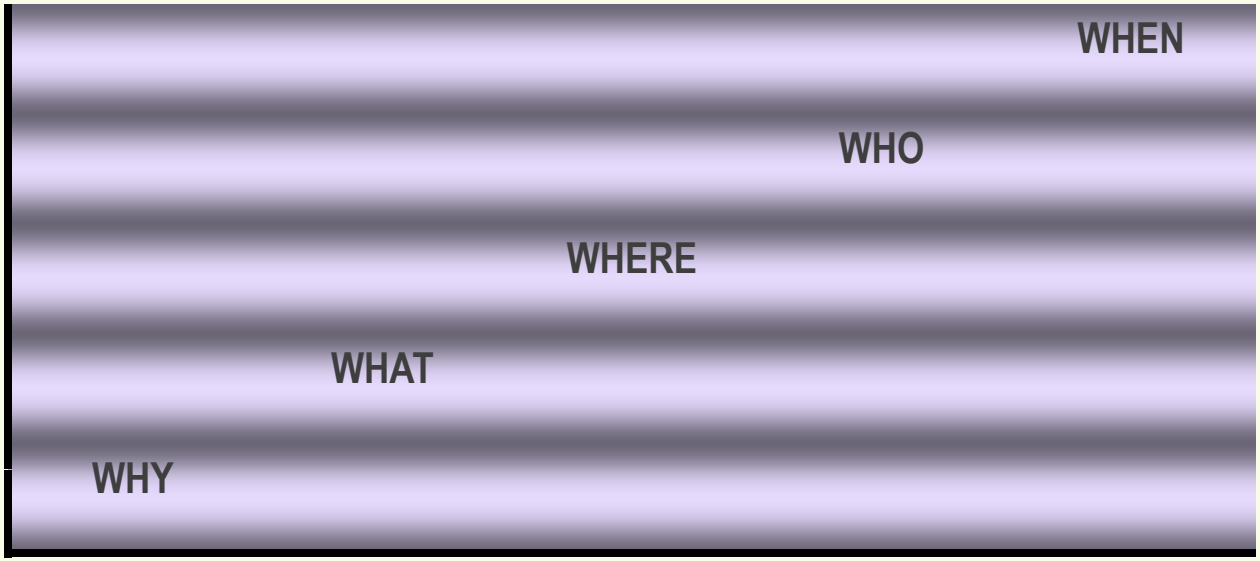
# Intelligence Needs

ORKASH

Technical Intelligence + Human Intelligence

Predictive and Investigative Intelligence

Granularity - Data Cubes



# The FOUR Pillars of Automated Intelligence Creation

ORKASH

## Information Extraction and Monitoring

- Extraction of data from various sources including websites, blogs, mobile phone, Emails and couriers
- Banking transactions, credit card usage, travel records
- Monitoring of web for any unusual communication and red flags

## Semantic Analysis

Use of semantics to decipher the content

Using domain specific ontologies

Network analysis Tools and analytics

## Geospatial Analysis

Analysis in geospatial context to have better data visualization

Geospatial intelligence for effective decision making

Location intelligence for better interpretation of network

## Data Mining & Forensics

Data Mining on real time basis

Analysis of trends and patterns of activities

Internet & Cyber Forensics

Target Centric

Social Network Analysis

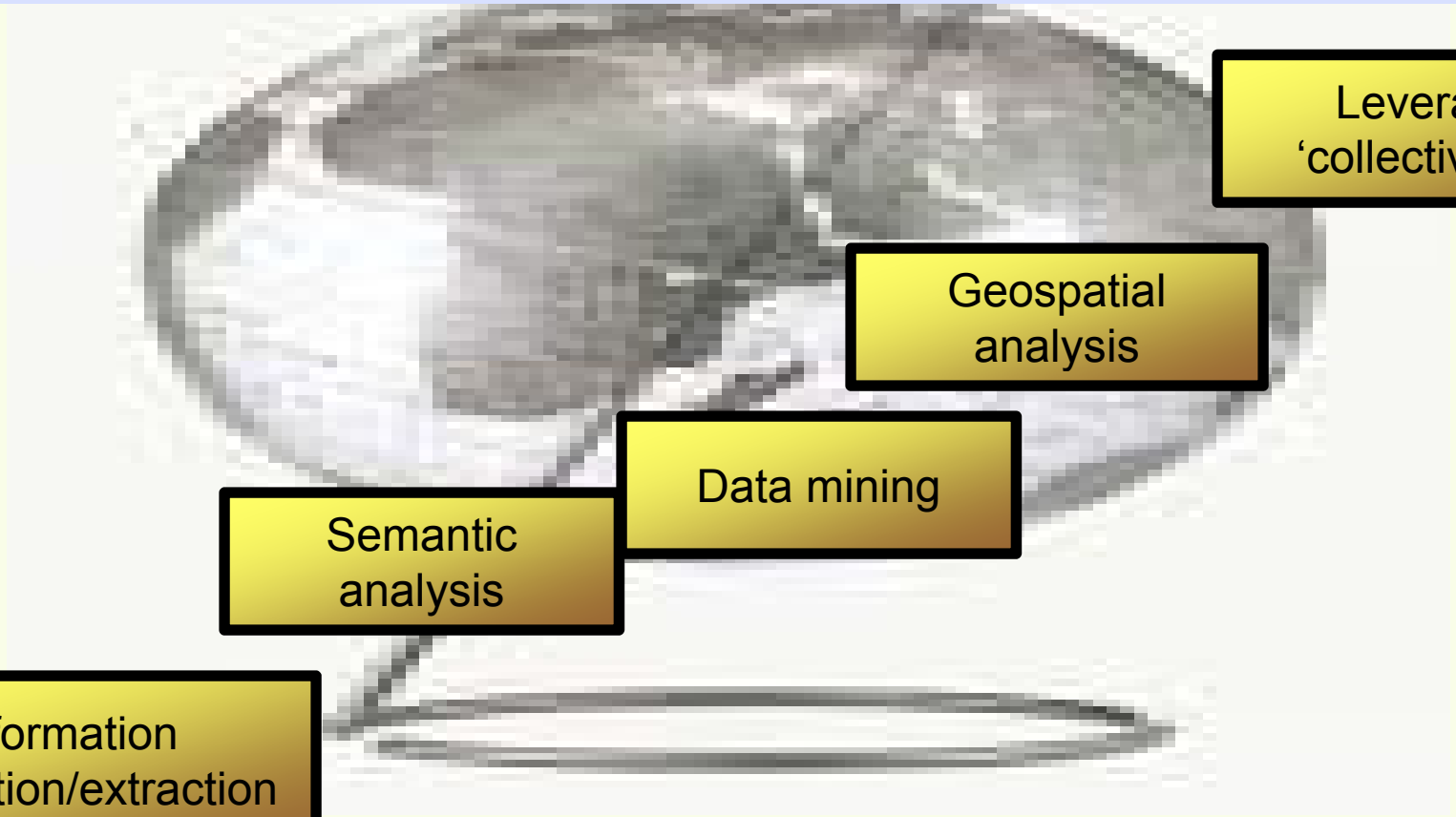
Pattern Tracing and Tracking

# Automating Intelligence Creation - The Process Layers

ORKASH

Where is the Intelligence Gap

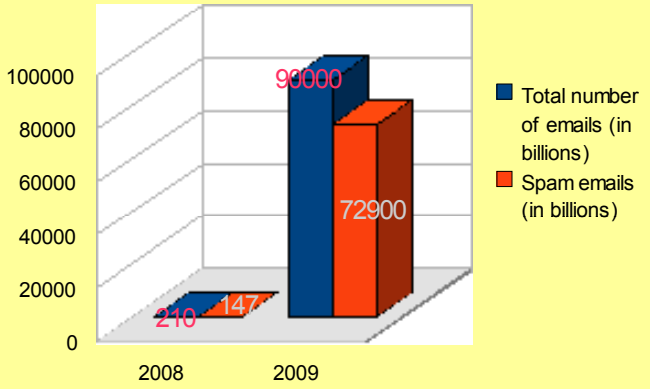
- *access and extraction of information*
- *language interpretation for the context, and removal of NOISE*
- *search vs scan .*
- *pattern tracking, granularity & visualization*



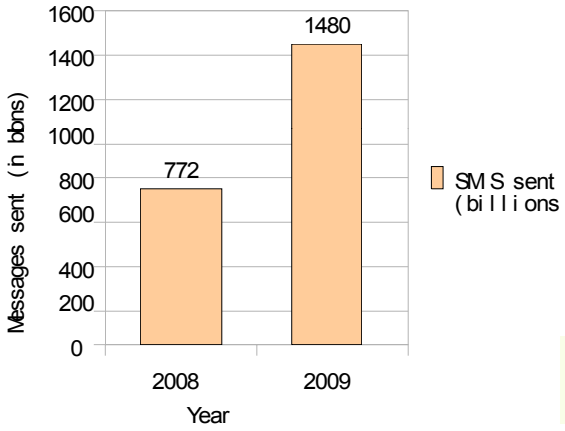
# Monitoring & Data Mining - Scale of the Problem

| Year | Number of email users | Total number of emails | Spam emails |
|---|---|---|---|
| 2008 | 1.3 billion | 210 billion | 70 percent |
| 2009 | 1.4 billion | 90 trillion | 81 percent |

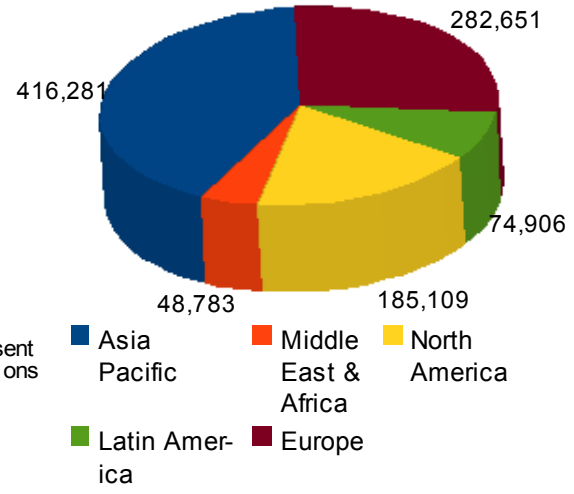
## Increased Email Communications




## Text Messages Sent




## Global Internet Audience (in ,000's)




## twitter

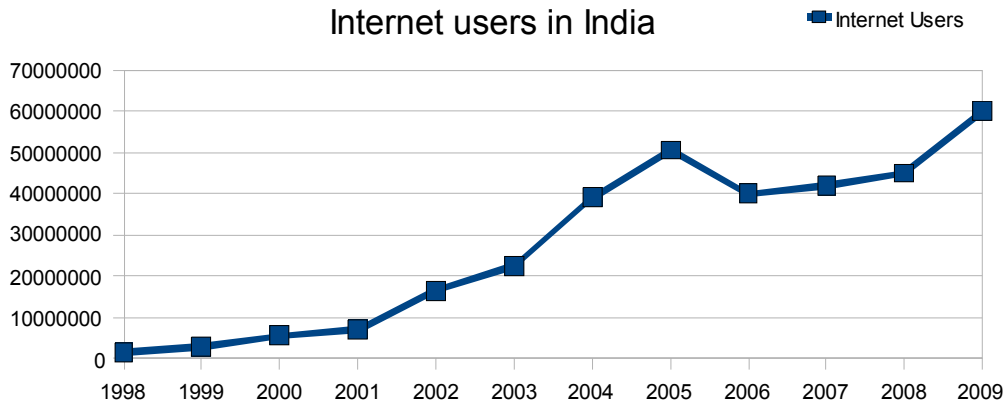
Active users: **1.3 mn**

Daily Tweets: **27.3 mn**

Tweets per hour: **1.8 mn**

"80 tweets per second were posted during 26/11 Mumbai attacks"

## Internet users in India



# Real Time Data Mining

- Requirement for massive high-performance parallel-processing clusters/cloud computing - consisting of hundreds of servers
- GPU processors - 1000 cores and above
- Massive data streams - very specialized database architecture

Banking and Card Usage


Location

alarbi.alhindi@gmail.com

alarbi_gujarat@yahoo.com.uk

al_arbi_delhi@yahoo.com

**Internet account**
Account: Hazi Al
Password:
Hazi_123

**Multiple Sims**


**Multiple Handsets**

**Telephone**

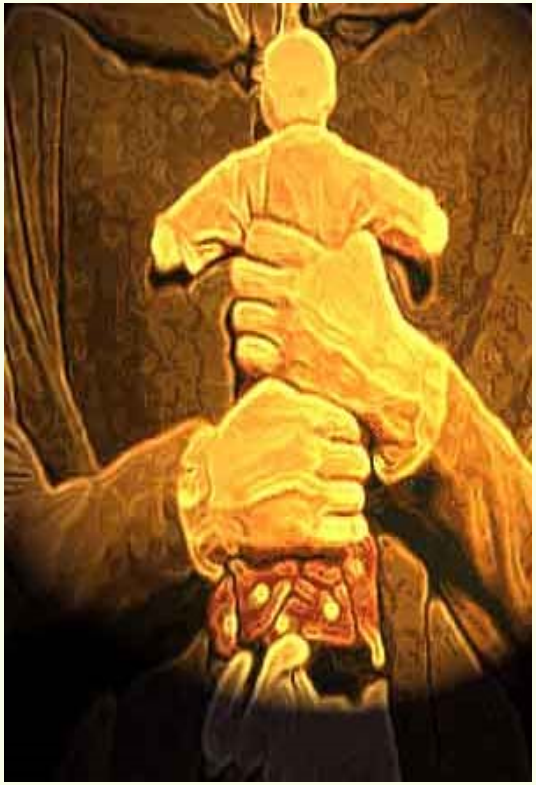
Historical data analysis would train expert engines to raise triggers and red flags. Real time data mining will generate trends and patterns in the usage

# A Key Intelligence Challenge

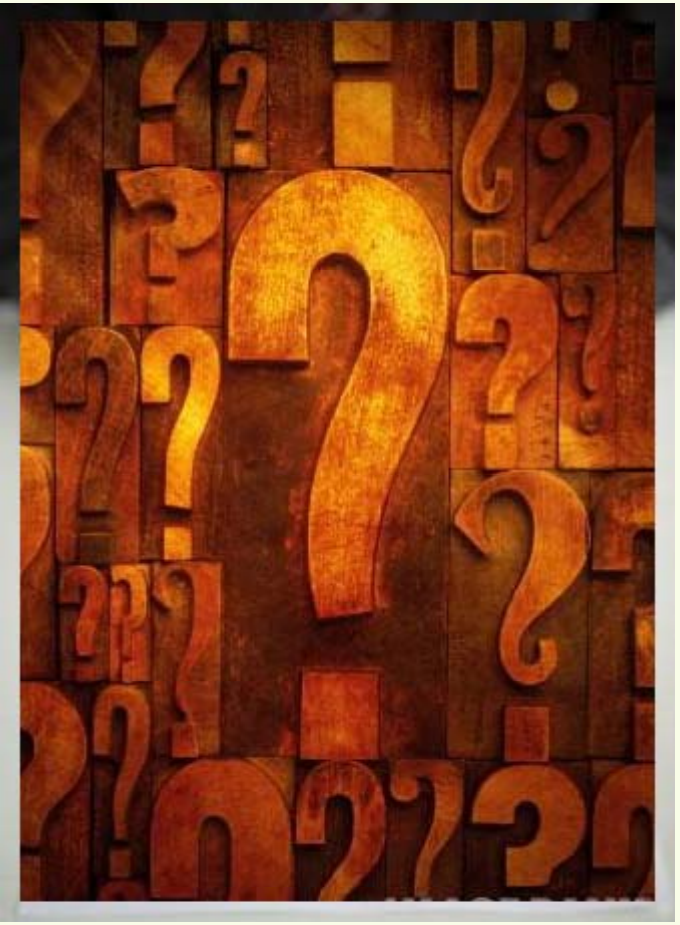
- A key challenge for intelligence purposes is

  ***Deciphering the Intent of a target individual***

- Behavior profiling
- Internet footprint - creation of filters over the internet traffic so that the keywords can be picked up and can be used as triggers
  - Search patterns and kind of websites visited
  - RSS feeds subscribed, social networking sites, search engine, alerts set, discussion board and blog postings
- Travel and movement of a person
- Email and communication patterns and linkages



# The Challenges



- The present platforms either do not tackle the issue of semantics fully or take into account a simple semantic structure. The burden of **'meaning construction'** is left entirely to the user

- Interpreting the geographical or the spatial context of text and technical metadata

- Conversion of unstructured to structured data

- Integration with geographic data.

# What is required??


***About 80% of all data and human decisions has a geographical component making the geo-spatial context more relevant in intelligence creation***

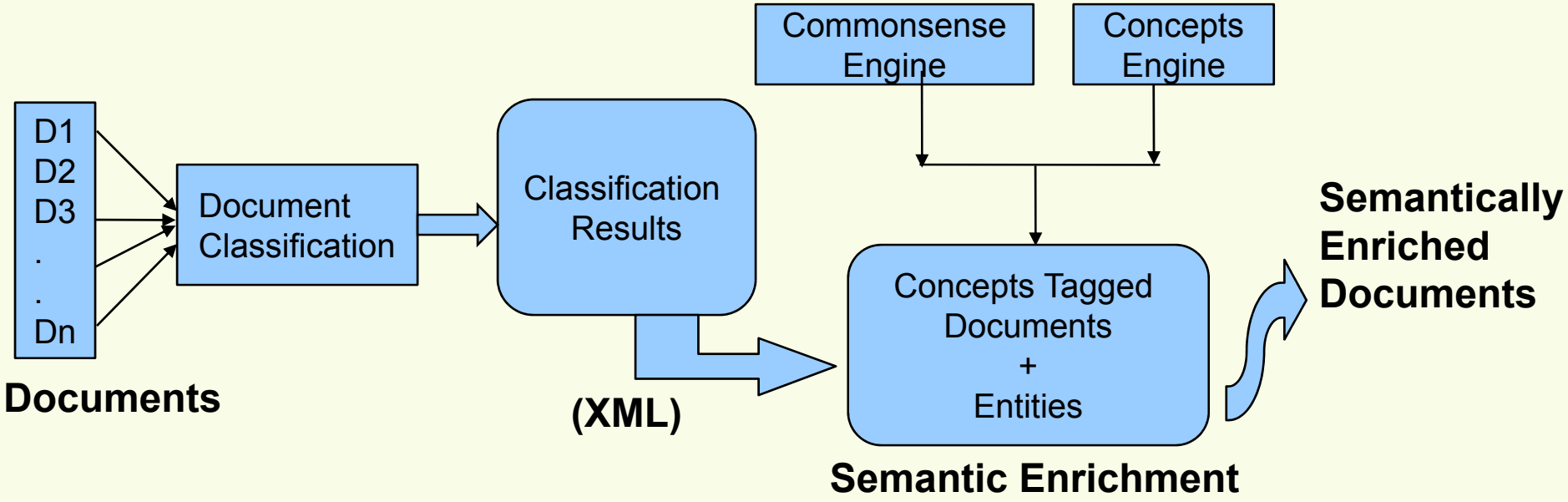
# Semantic Enrichment

**Semantic enrichment** is the process of creating or associating semantic tags in unstructured data or text, usually involving concepts, entities, relationships, events and properties described in an ontology or rule based

**Benefits :**

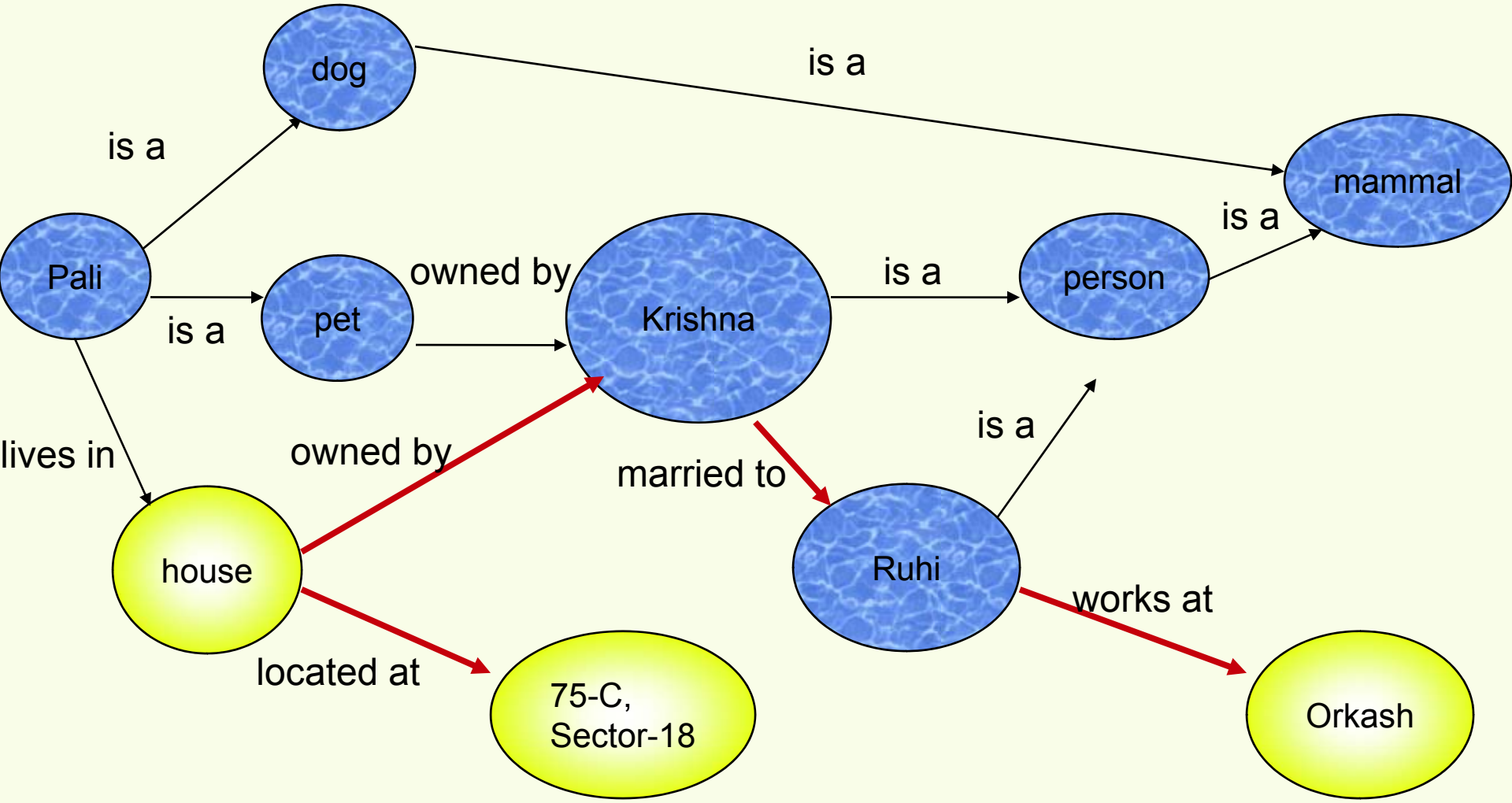
Adding semantic metadata tags to the original unstructured data enables advanced correlation and data fusion capabilities.

Enables concept , event and relationship extraction and automated metadata tagging.

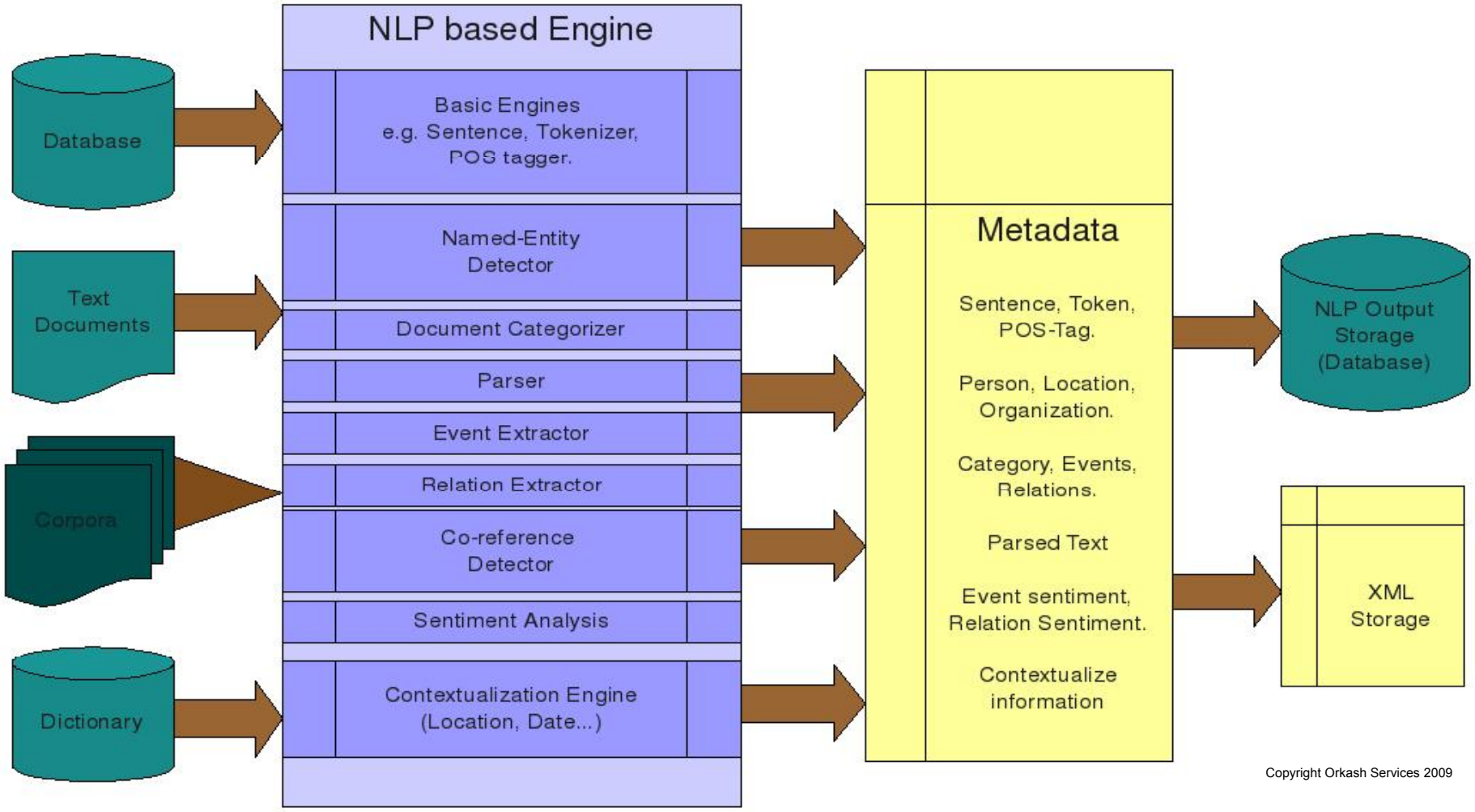


# Semantic graph to perform semantic search

**Query : Where does the woman who lives at 75-C, Sector 18 work??**

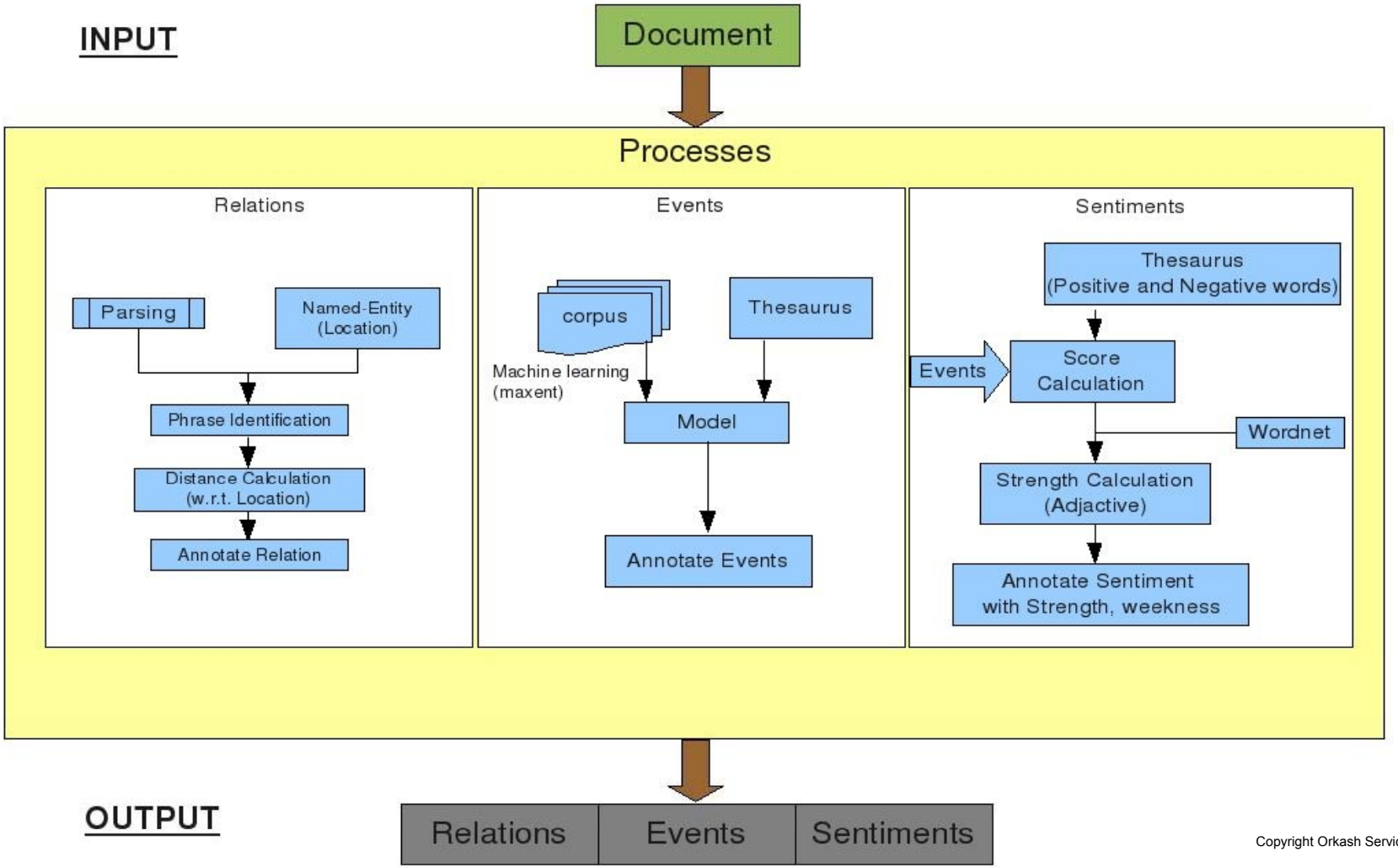


# Expert Engine based Contextualization




**Natural Language Processing Architecture**

# AI Expert Engine Analyzer



# Semantic query generation through NLP

ORKASH

## Query: What is the key reason behind the frequency of attacks and the transition of terrorism India?

"The Changing patterns of Terrorism in India": A study by Orkash

*The 'new breed' of terrorism in India is confident and increasingly sophisticated. In the study based on expert domain knowledge and proprietary research, Orkash identified prominent undercurrents of the changing patterns of terrorism in India.*

***In the wake of the Mumbai terror siege, the challenge today for India's security machinery is not only tackling terror attacks but also providing a tactical response to the changing operational and ideological undercurrents that terrorism in the country is presently going through."*** - Ashish Sonal, CEO, Orkash Services Pvt. Limited.

Terrorism is not new to India – but what is unique now is the evolved characteristics and the enhanced operational capabilities of the terrorist outfits and their operatives. Surprisingly, India is ranked second, right behind Iraq in the number of terrorist activities (excluding Jammu and Kashmir) despite the fact it is not a country in conflict. In the study titled **"The changing patterns of terrorism in India"**, Orkash has identified the bellwether currents that define the new breed of terrorism which is sending 'wake up' waves across the security machinery of the country. About 2-3 years ago – mo precisely before the 'defining' year of 2008 – terror attacks mostly included only sporadic blasts in the target cities. The frequency of major t attacks was also comparatively moderate – 4 terror attacks in 2007, 3 in 2006, and 1 attack in 2005. But 2008 was different – there were a 12 highly synchronized large terror attacks since the beginning of the year.

The 'new breed' of terrorism in India is confident, bold in actions and increasingly sophisticated. In the study leveraging upon the expert dom knowledge and proprietary research work, Orkash identified the prominent undercurrents of the changing patterns of terrorism in India:

Downloads

ORKASH

logo.jpg

## Contextualize through NLP

A +

> The frequency of major terror attacks was also comparatively moderate 4 terror attacks in 2007, 3 in 2006, and 1 attack in 2005. But 2008 was different – there were at least 12 highly synchronized large terror attacks since the beginning of the year.

B +

> The transition process, however, has been increasingly driven by the adoption of modern technology, better communication and information networks

C

> the terrorists in India are improving their technological sophistication in many areas of operational planning, communications, targeting, and propaganda.

### Transition of terrorism in India

16 January 2009

*Terrorism in India is undergoing an acute transition, both in the operational and the ideological aspects, says **Ashish Sonal**, CEO of marketing and business intelligence analyst firm, Orkash Services*

Terrorism in India has been acquiring a new degree of lethality characterised by meticulous planning, intelligence collection, sophisticated training, and exploiting local population for creating support networks. Most importantly, it is expanding beyond the 'cycle of anonymous' remotely detonated blasts towards exploitin (latest source inputs are indicative of these developments) and fiy assaults by well armed and trained terror cells), a trend that was India outside of Kashmir.

In this, the forces of polity, social dynamics, and international support networks continue to play a major role. The transition process, however, has been increasingly driven by the adoption of modern technology, better communication and information networks, and the unique phenomena of the globalization of terror. As a result, the terrorists in India are improving their technological sophistication in many areas of operational planning, communications, targeting, and propaganda.

*Query Result:* ***Operational sophistication and adoption of modern technologies has led to the transition of terrorism in India***

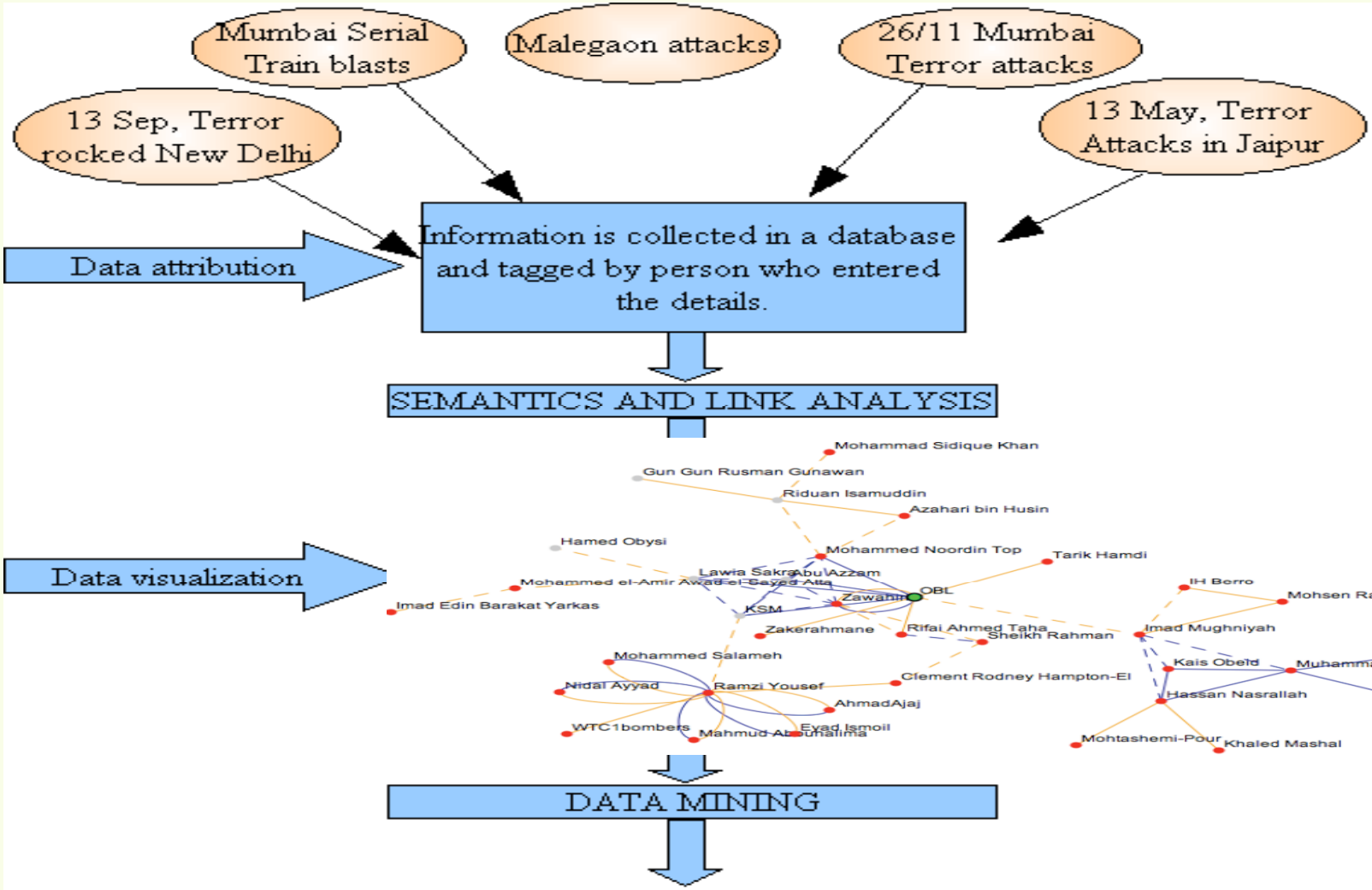
# Visualizing Semantic Data in GIS Context & Scan

- Visualization of the meta-data and the content – Creation of 'Visual' layers

- Role of contextual scan -semantic and geospatial

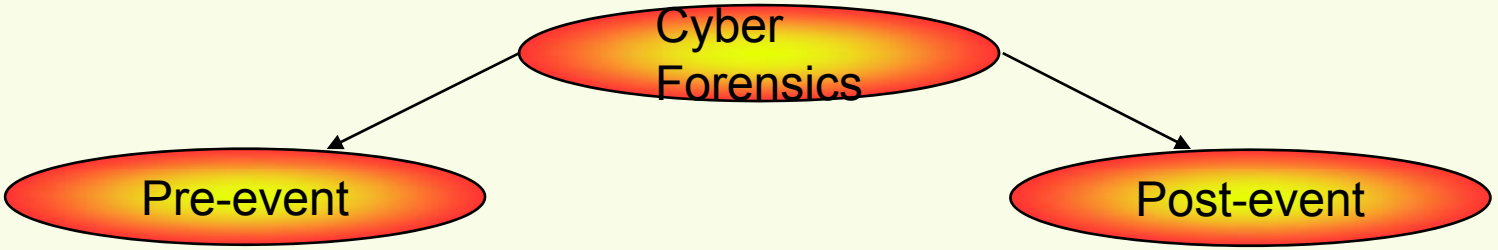
- User created content and collective intelligence

# Target Centric Intelligence Model




# Role of Cyber Forensics in Preemptive Intelligence

- *E-mail system of the Indian Prime Minister's Office (PMO) remained affected by a computer virus for 3 months during 2008. Spyware infection affected around 600 computers of the Ministry of External Affairs in February in 2009.*
- *There have been several serious attacks by international hacking communities on Indian government IT networks. Many Indian ministries, embassies, the NIC and other organizations have faced disruptions arising from such threats*
- *In 2006, investigations into the Mumbai train bombings highlighted that tech professionals in a leading technology firm in Bangalore were operating sleeper cells, using advanced techniques to mask identities of IP addresses and resorted to steganography for disguised communications and fund transfers*

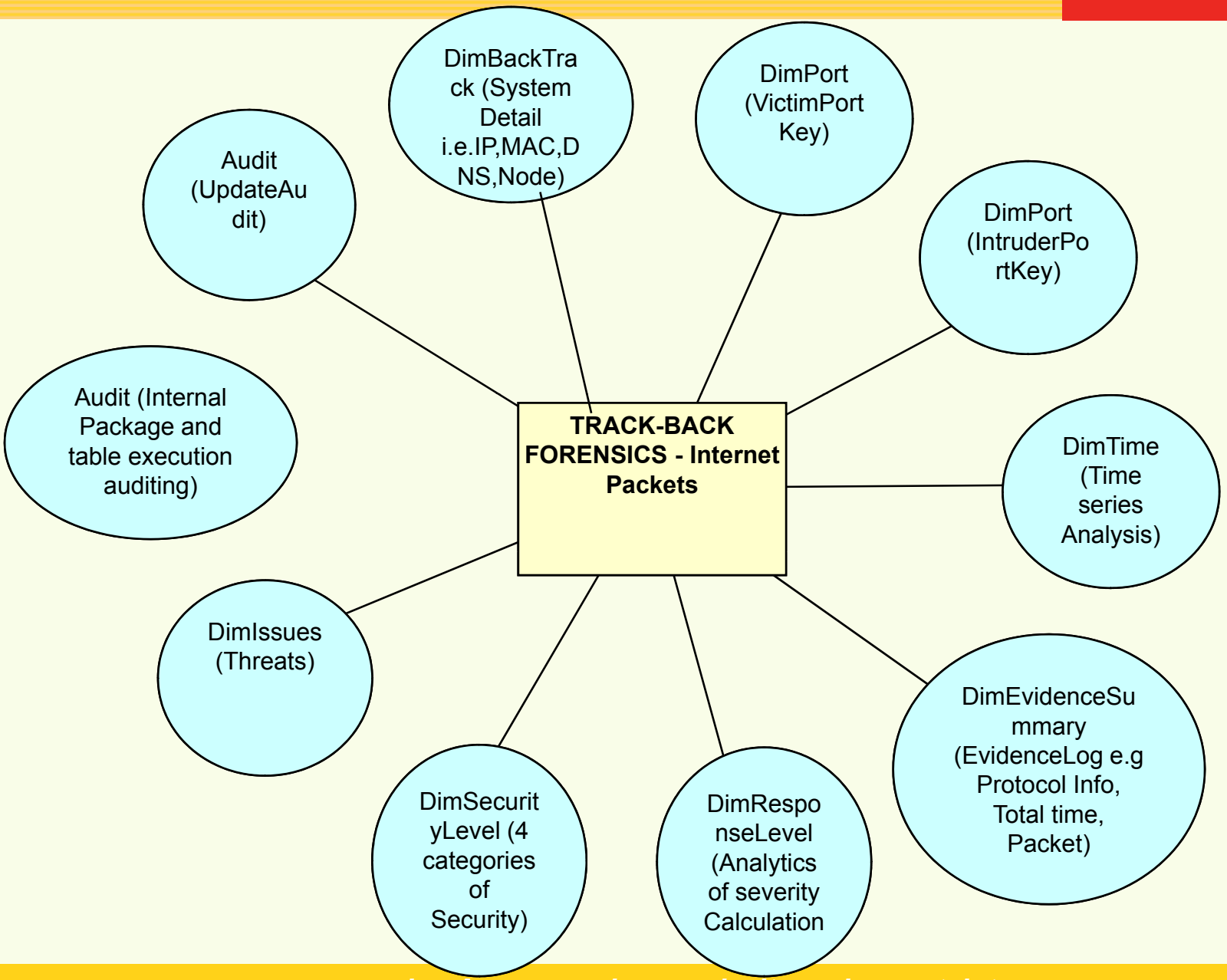



1. Driven by intelligence gathering
2. Is predictive in nature
3. Data Mining can produce trends and patterns
4. Track back analysis

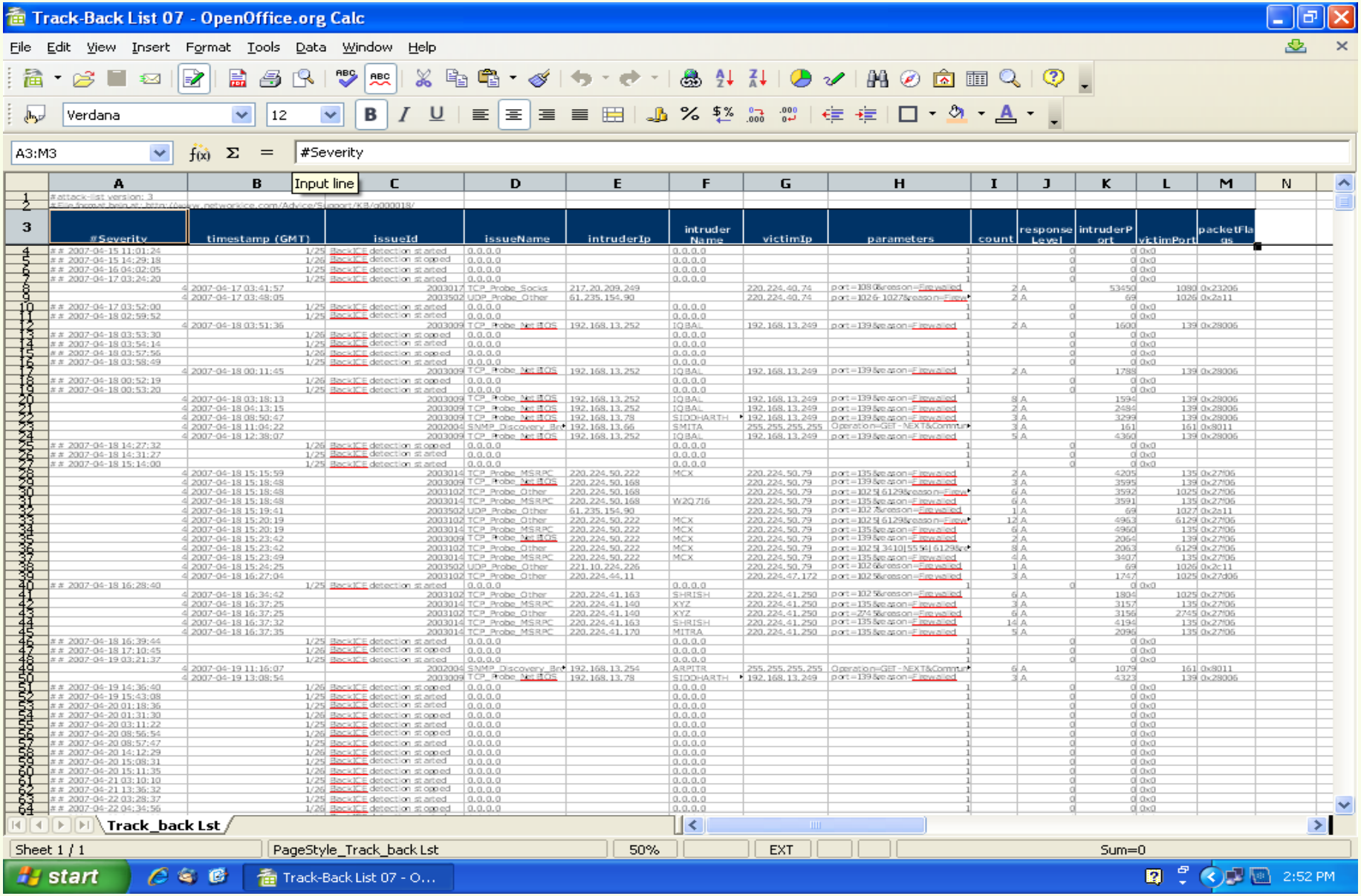
1. Driven by Evidence Chain Management System
2. Is investigative in nature
3. Evidence that can be produced in the court

# Packet Level Forensics

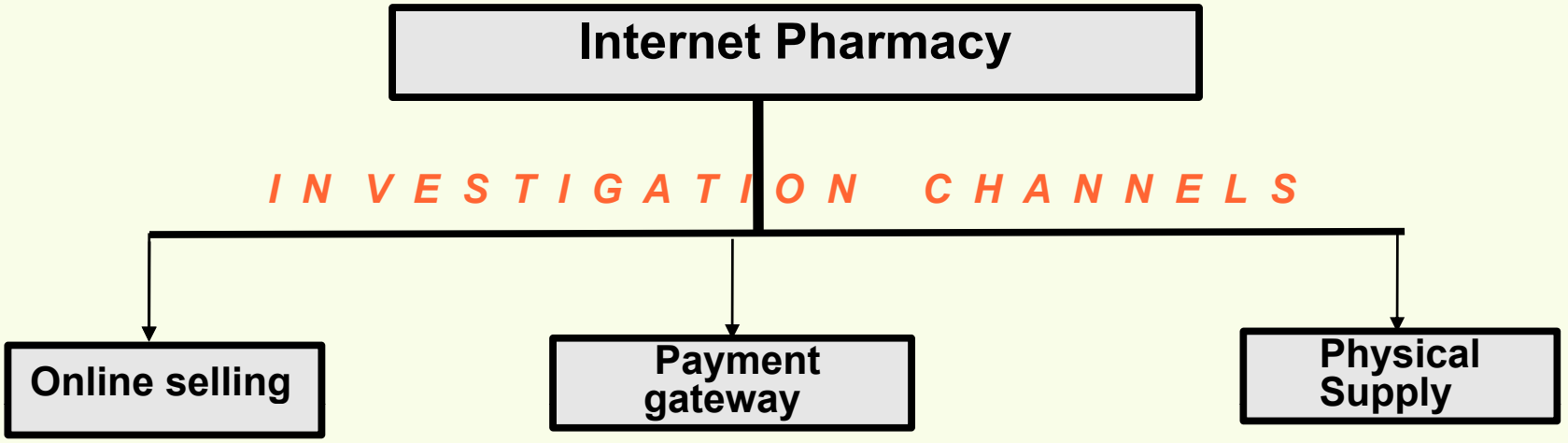
ORKASH



# Illustration : Track back analysis



# Internet-based pharmacy

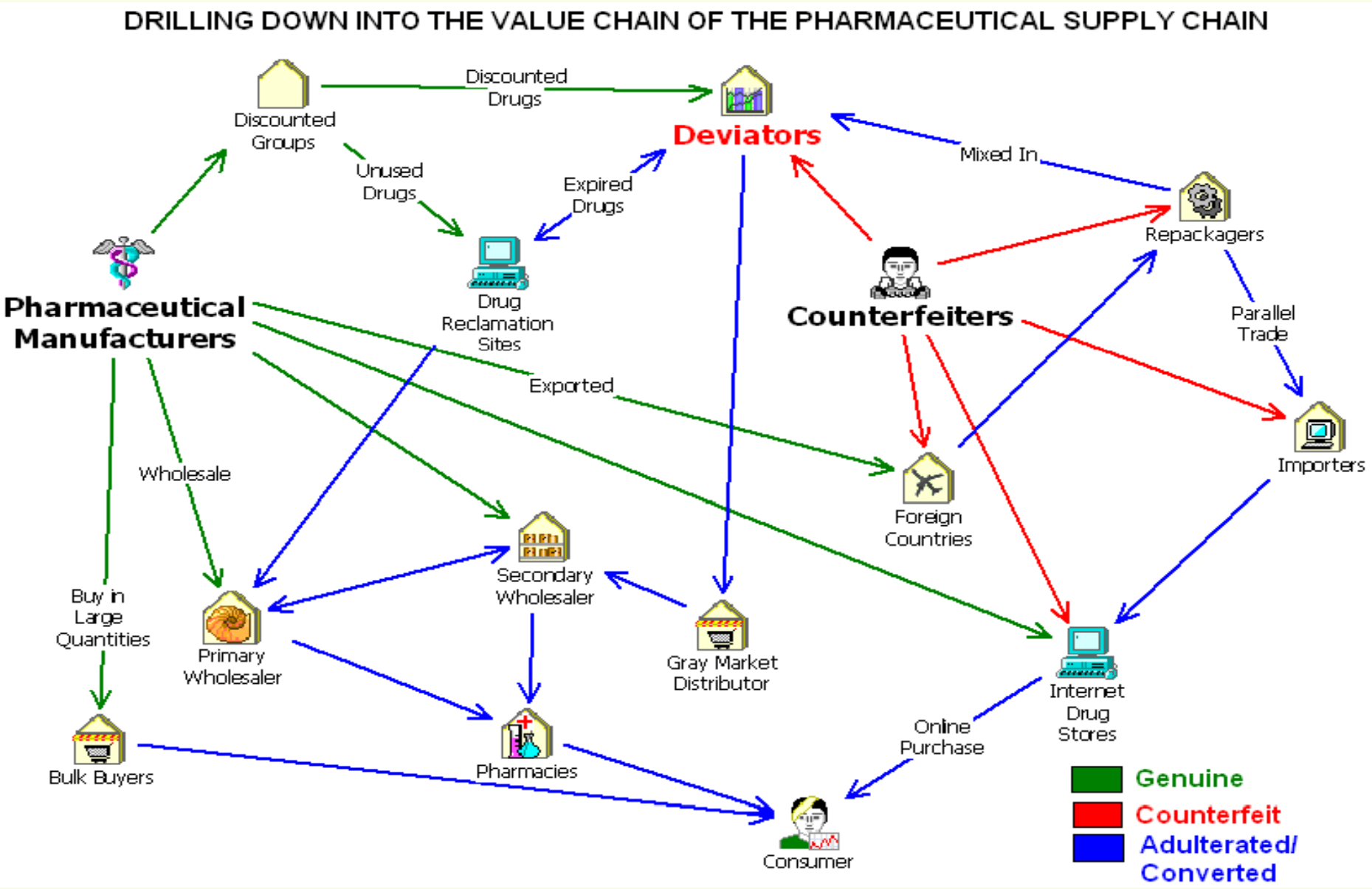



- Emails headers and firewall logs are critical in investigations through packet level forensics and track backs
- Employ data mining tools like clustering, classification and association
- Mining of data in a relationship database
- Narrow down on suspicious IP addresses through pattern detection

- Results from data mining can help in tracking payment transactions
- Derive the correlation between payment gateways and assess the business architecture of the sales channel

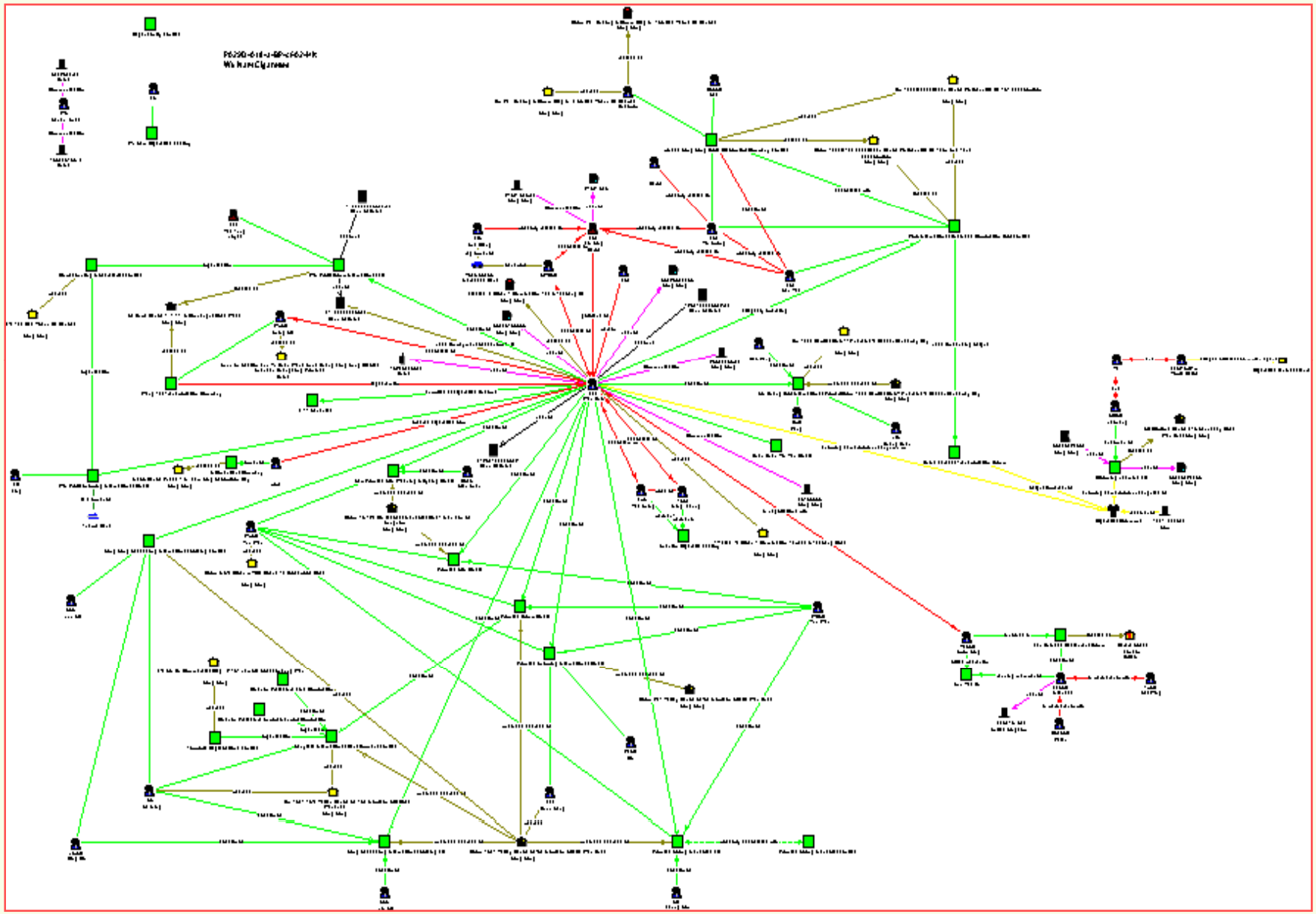
- Every physical packet of goods leaves a footprint during its transportation
- It is possible to track the international movement of goods and narrow-down on the source. Especially in case of medicines as these are classified as 'poisons'
- Track the network of courier services and/or other individuals involved in the transit

# Deviators – the critical juncture



# Combining Data Mining and Link Analysis

ORKASH



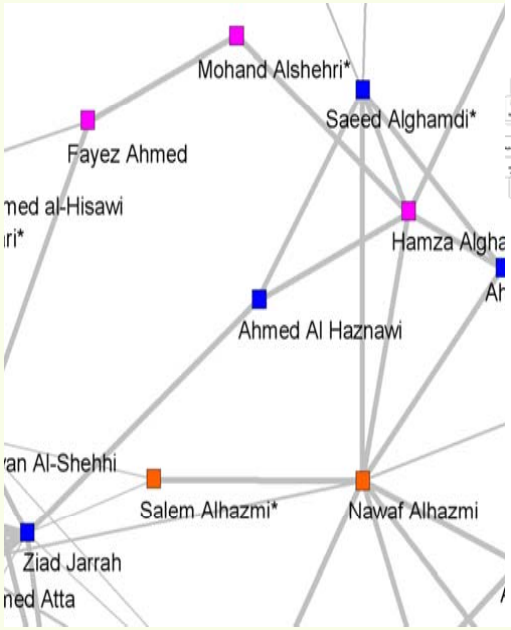
# Network Analysis and Data visualization

ORKASH

**Manual approach**

(1) Manually creation of association matrix by identifying the relations through raw data

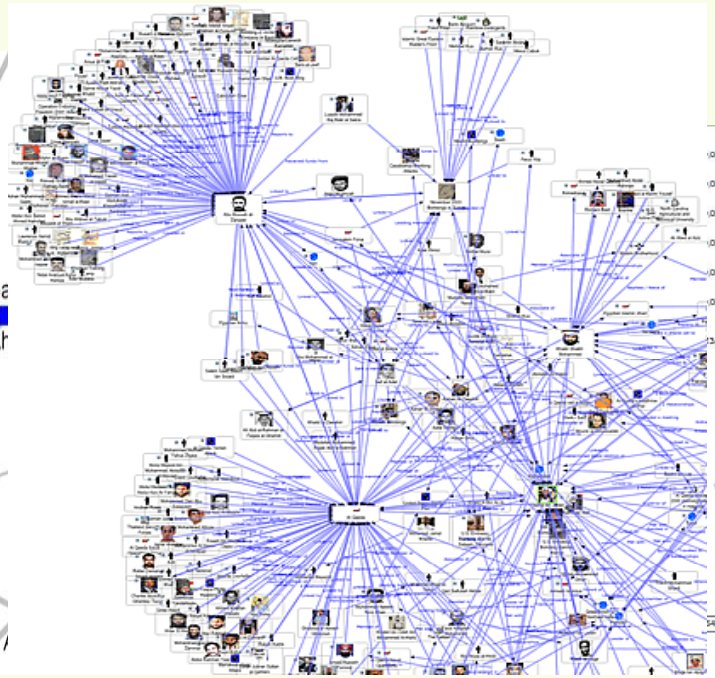
(2) Helpful in crime investigation, becomes ineffective where datasets are very large




**Graphic based approach**

(1) Graphically representation of terrorists networks using tools such as Analyst Notebook (i2)

(2) Helpful in visualization of large amount of relationship data but without analytical functionality.

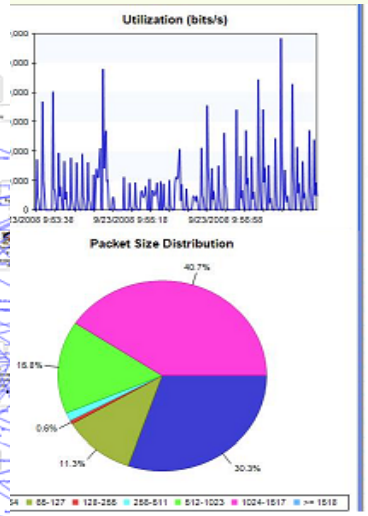


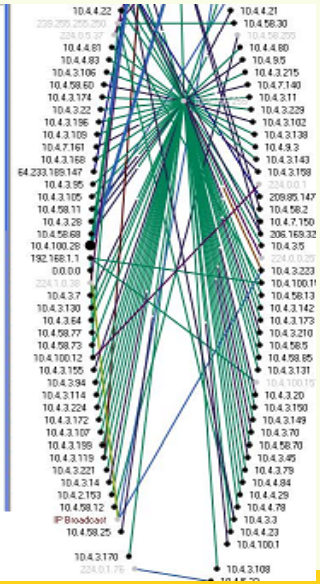
**Structured analysis approach4**

(1)Advanced analytical capabilities to assist investigation

(2) It can help in identifying networks to mining of large volumes of data to discover useful knowledge and create intelligence about the structure and organization of criminal networks

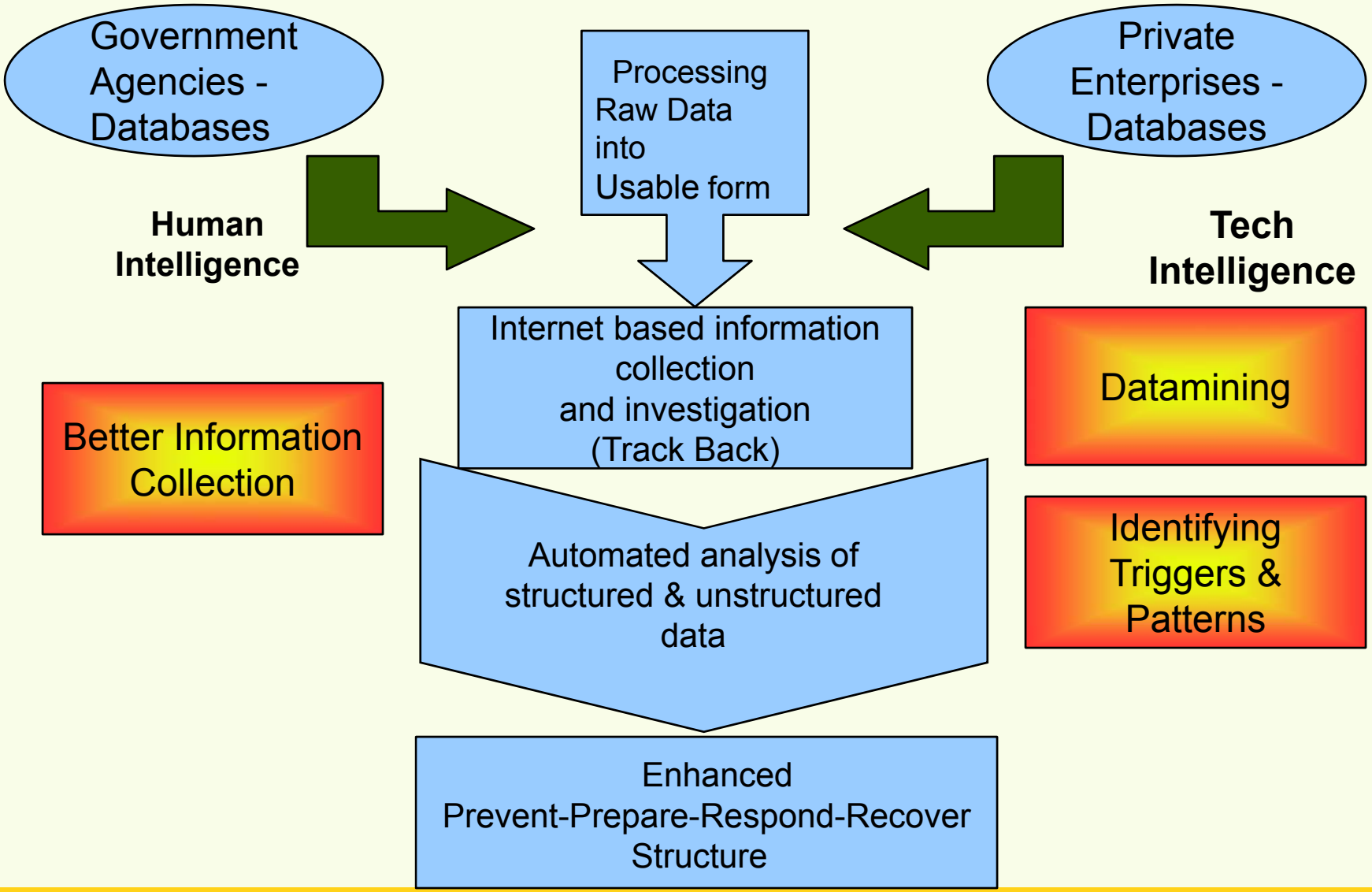
- Data Mining
- Social Network Analysis
- Pattern Tracing and interactions



ORKASH

## Convergence of Humint and Techint



# THANK YOU

Orkash Services Pvt Ltd
75 C, Sector 18
Gurgaon 122 015
Haryana, India

Phone: +91 124 4033773
+91 98102 36020

Contact@Orkash.com

www.orkash.com