The role of Data Analytics and Social Networks in Cyber Security

Prof. Rodolfo Zunino
DITEN
Genoa University

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Overview

- Data Analytics, Social Networks
- Enabling Technologies
- DA and SN in CyberSecurity
- Sample Session
- Perspectives

EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Data Analytics, Social Networks

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Data Analytics

- Handling massive amounts of data
- Data → Information → Knowledge
- Data is not homogeneous
  - Structured data
  - Unstructured data
- Purpose is the leading key

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Social Networks

- Massive amounts of data → ok
- Data → Information → Knowledge
- Unstructured data
  - Natural (not so natural) language
- Purpose ?
  - Monitoring
  - Predicting
  - Profiling

EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Enabling Technologies For Data Analytics

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Technologies

- Purpose: understanding/grouping
  - Unsupervised learning
  - Clustering
- Purpose: recognition
  - Supervised learning
  - Classification (e.g. deep learning)
- Different scopes, different issues

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Clustering Ingredients

- Metric
  - Need to define similarity before clustering
- Algorithm
  - Complexity
  - Computational cost
  - Storage/timing requirements
- Experience!

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Issues in Clustering

- Computation time
  - Complexity can scale as O(2)
- Performance measurement
  - How do we measure it?
- Reporting results
  - Presentation is paramount

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Classification Ingredients

- Labeled Training Set
  - Can be partial, however accurate
- Algorithm
  - Predicted accuracy (complexity)
  - Implementation cost
- Experience!

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Issues in Classification

- **Confidence in Predicted Error**
  - Depends on many factors
  - Training set size
  - Classifier complexity
- MultiClass problems
- Cheating

EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Enabling Technologies for Social Network handling

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

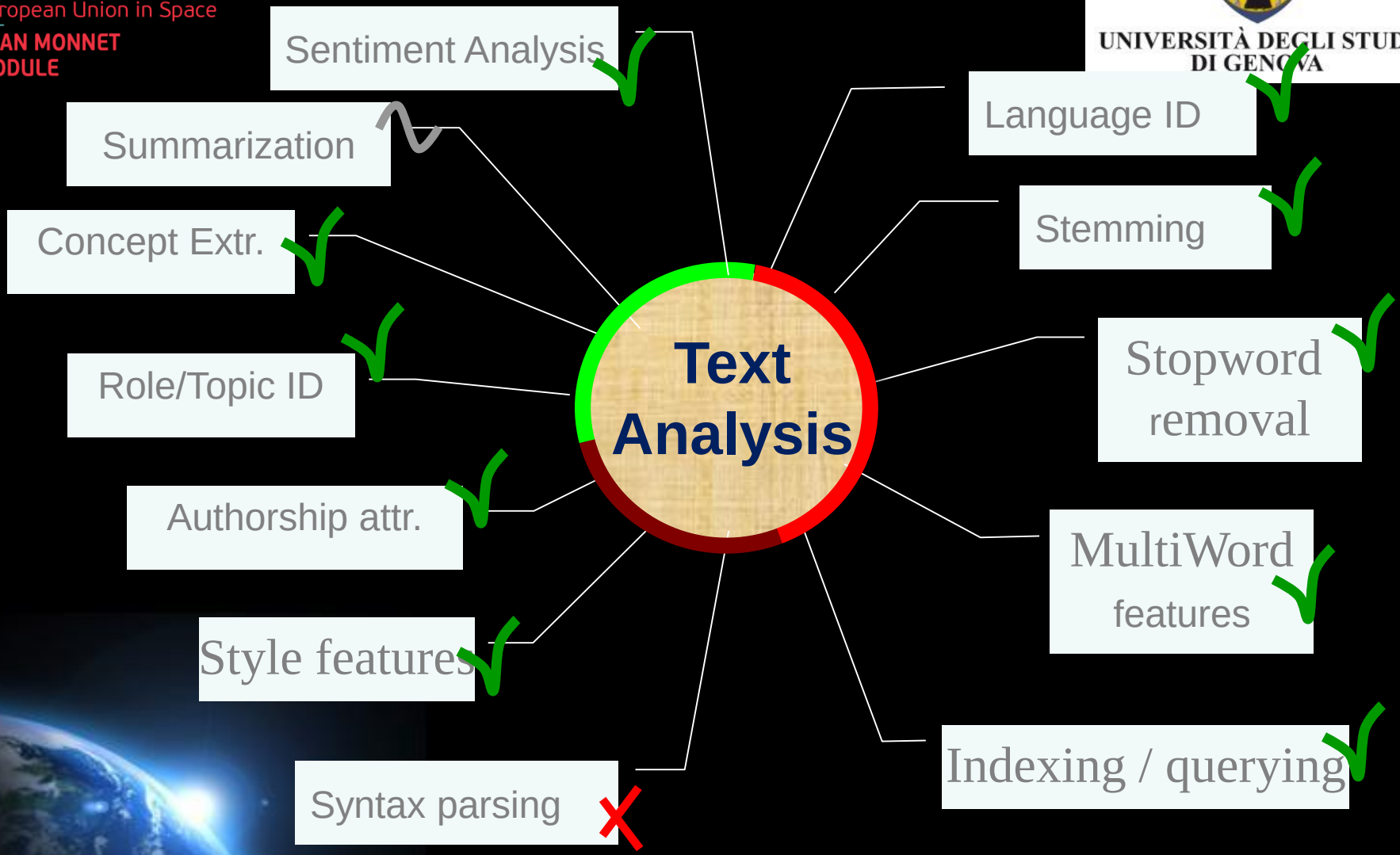
Text Mining

- Text processing
- Semantic characterization
- Text retrieval
- Text clustering
- Text classification

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Text Processing



EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Data Analytics and Social Networks In Cyber Security

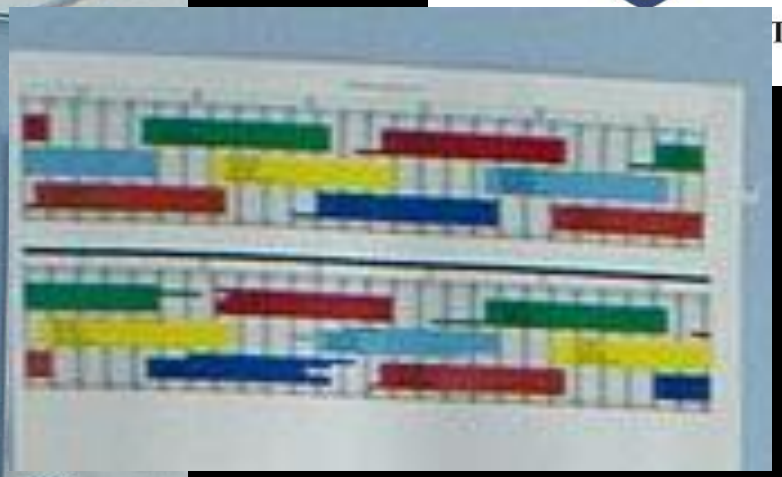
EUSPACE
European Union in Space
JEAN MONNET MODULE

Case Study I - The cute Prince

UNIVERSITÀ DEGLI STUDI DI GENOVA

EUS
European
JEAN MO
MODULE

TUDI



EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

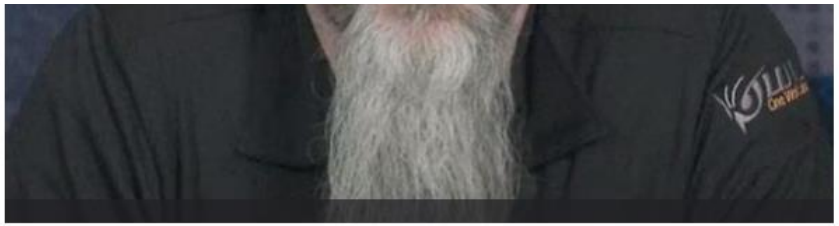
SICUREZZA INFORMATICA

Usa, hacker viola computer di un aereo in volo, l'Fbi indaga

Chris Roberts sarebbe riuscito a prendere il controllo di un aereo tra le 15 e le 20 volte in tre anni sfruttando le falle del Wi Fi a bordo e dei programmi di intrattenimento

di Marta Serafini

Find myself on a 737/800, lets see Box-IFE-ICE-SATCOM, ? Shall we start playing with EICAS messages? "PASS OXYGEN ON" Anyone ? :)
— Chris Roberts (@Sidragon1) 15 Aprile 2015



L'attenzione dell'Fbi si era concentrata su di lui lo scorso aprile dopo un tweet in cui Chris Roberts lasciava intendere di aver hackerato il sistema di un aereo di un volo della United Airlines in servizio da Chicago. Alla fine della scaletta, al suo arrivo a Syracyuse, Roberts aveva trovato l'Fbi. Dopo un'accurata perquisizione l'uomo era risultato in possesso di un computer e di una chiavetta Usb. Ma non solo, i sistemi di intrattenimento del posto da lui occupato risultavano manomessi.

EUSPACE
European Union in Space
JEAN MONNET MODULE

Case Study III guess what?

UNIVERSITÀ DEGLI STUDI DI GENOVA

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Purpose is the leading key

- Purpose: surveillance
  - Monitoring
  - Clustering
- Purpose: detection
  - Anomaly detection
  - Event recognition

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Purpose is the leading key

- Purpose: prevention (early warning)
  - Monitoring
  - Profiling
- Purpose: prediction
  - Semantic analysis
  - User categorization
    - Election outcome forecasting

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Purpose is the leading key

- Purpose: control
  - Information injection
  - User/Leader identification
- Purpose: attack
  - Information gathering
  - Preparation for APT

EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Sample Session

EUSPACE
European Union in Space
JEAN MONNET
MODULE

UNIVERSITÀ DEGLI STUDI
DI GENOVA

Perspectives

EUSPACE
European Union in Space
JEAN MONNET MODULE

UNIVERSITÀ DEGLI STUDI DI GENOVA

Now what?

- Text mining is mature technology
- Data Analytics is mature
- Social Networks are pervasive

→What do you expect as a result?

- Semantic analysis is improving
- Artificial Intelligence is consolidating

→ What do you expect as a result?

EUSPACE
European Union in Space
JEAN MONNET MODULE

Promised Land

UNIVERSITÀ DEGLI STUDI DI GENOVA