When Cybersecurity meets intelligence

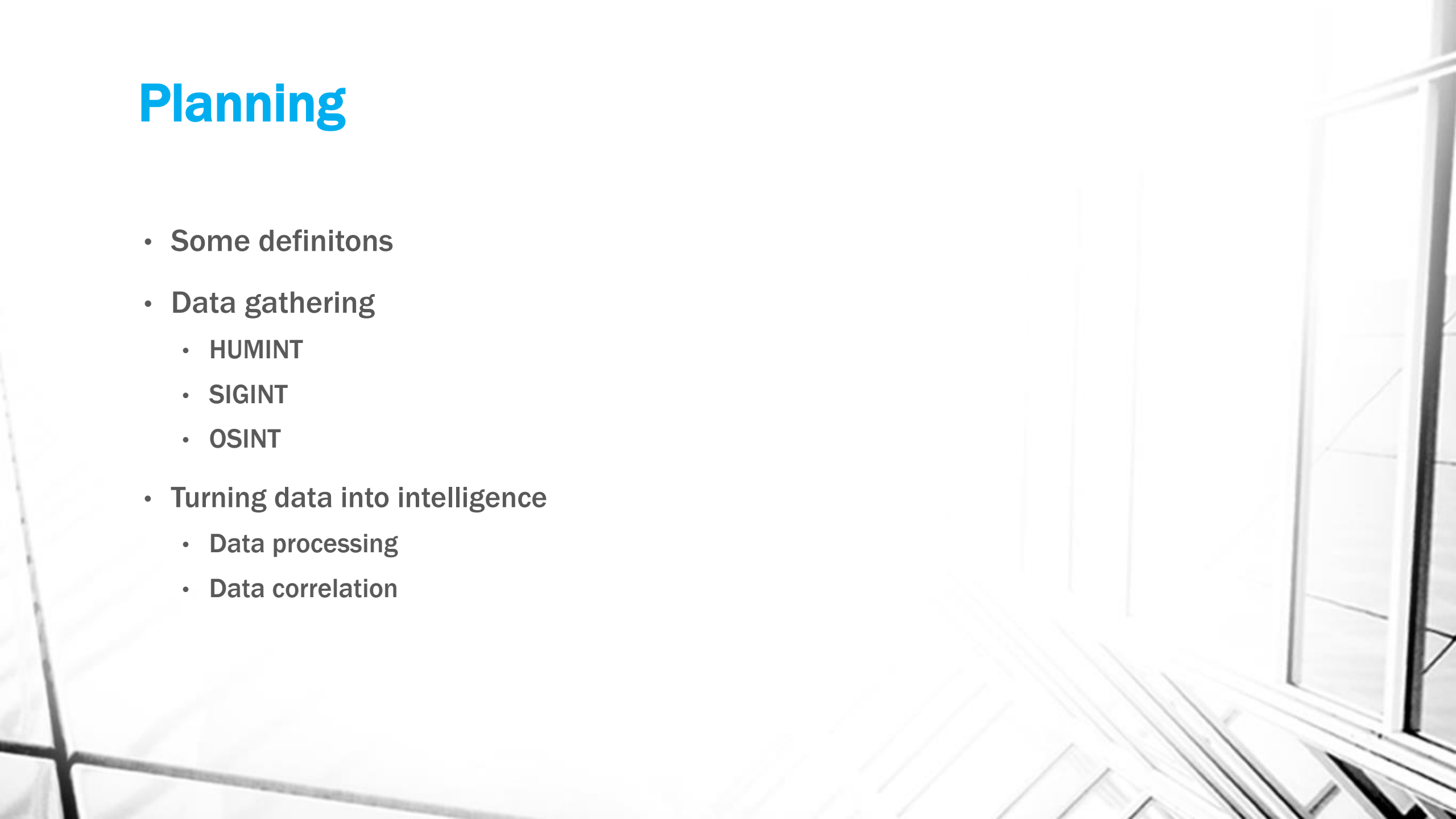
stephane.louis@l-a.lu

A short speak to show how cyber supports intelligence

01 december 2017 @ Paul Lambin

Planning

- Some definitons
- Data gathering
  - HUMINT
  - SIGINT
  - OSINT
- Turning data into intelligence
  - Data processing
  - Data correlation



Planning

- Some definitions
- Data gathering
  - HumInt
  - SigInt
  - OSINT
- Turning data into intelligence
  - Data processing
  - Data correlation

Intelligence : a few definitions

- Data → raw
  - Albert, de Belgique, rue Ducale 1, 1000, Brussels, Belgium,+322123456
- Information → human readable
  - Albert de Belgique
  - Rue Ducale 1
  - 1000 Bruxelles
  - Belgique
  - +32 2 123 456

Intelligence : a few definitions

- Intelligence → Contextualized information with help of analyst
  - Former king of Belgium
  - …
- Analyst
  - Someone in charge to turn information into actionable intelligence

Intelligence : for who and what for ?
State/Military

UK gathering secret intelligence via covert NSA operation

Lenovo caught yet again spying on Windows PC users

By Chris Smith on Sep 24, 2015 at 6:10 PM

COMPI

Meet Babar, a New Malware Almost Certainly Created by France

February 18, 2015 // 04:00 AM EST

Intelligence : for who and what for ?
Economic/Industry

Leaked Documents Reveal German Intelligence Spied on Airbus for U.S., Manufacturer Vows Legal Action

Leaked documents indicating that German intelligence spied on Airbus at the behest of U.S. officials have the European aircraft manufacturer vowing to seek legal redress.

La France serait le plus grand espion industriel d'Europe

LES ECHOS (AVEC AGENCES) - LES ECHOS | LE 05/01/11 À 14H57

Intelligence : for who and what for ?
Marketing

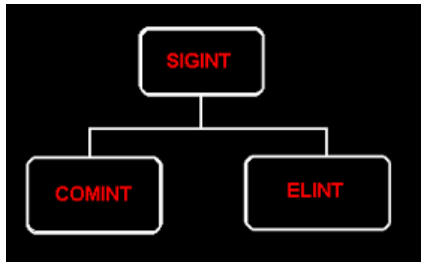
Planning

- Some definitions
- Data gathering
  - HUMINT
  - SIGINT
  - OSINT
- Turning data into intelligence
  - Data processing
  - Data correlation

Building intelligence : Data gathering ; HUMINT

- Human Intelligence
- Intelligence from field agents

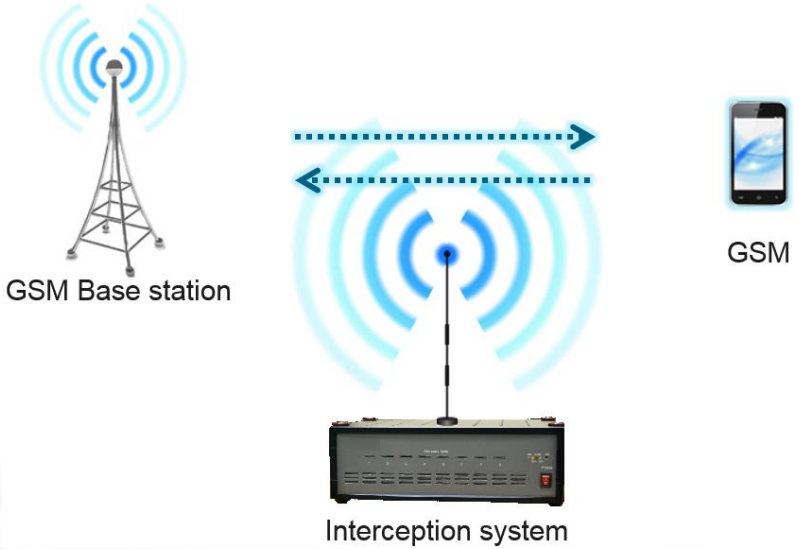
Building intelligence : Data gathering ; SIGINT - ELINT



- Signal Intelligence (SIGINT)
  - ELINT (Electronic Intel)
    - Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources.
    - Radar

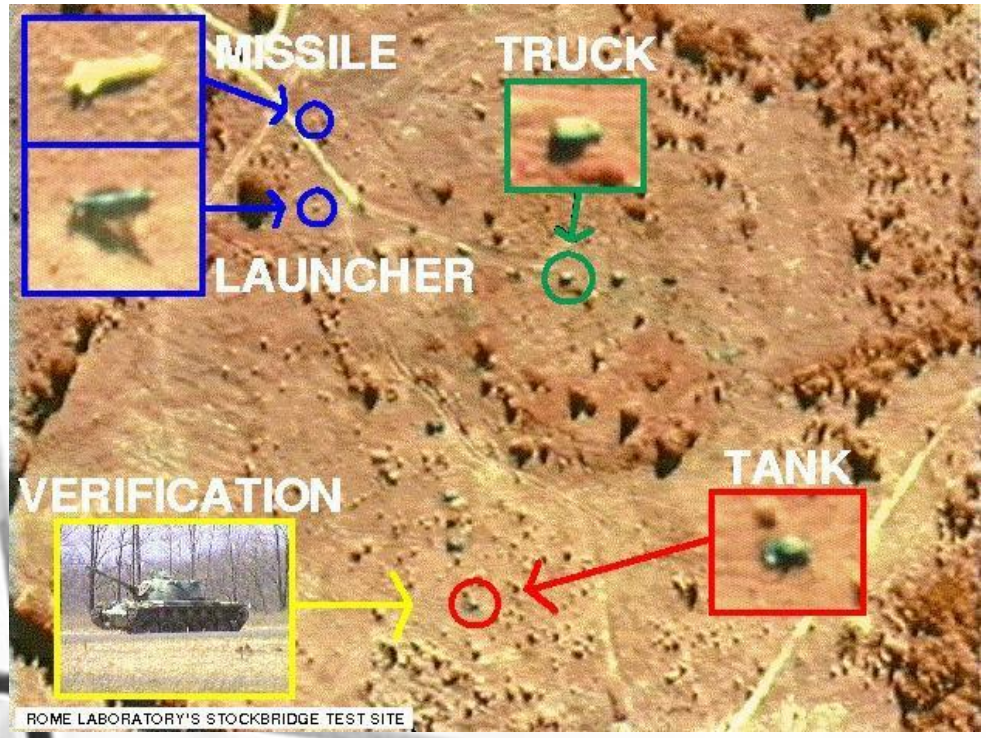
Building intelligence : Data gathering ; SIGINT - COMINT

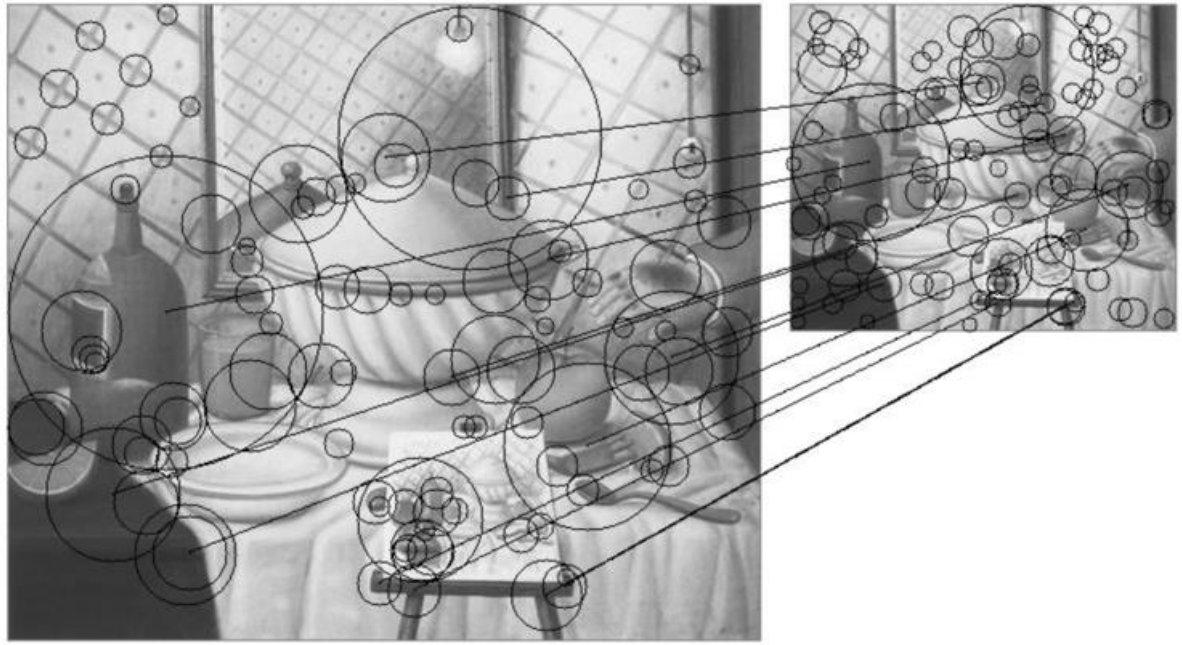
- Signal Intelligence (SIGNINT)
  - COMINT (Communication Intelligence)
    - Phone interception
    - GSM interception
    - Internet interception
    - ...



Building intelligence : Data gathering ; IMINT

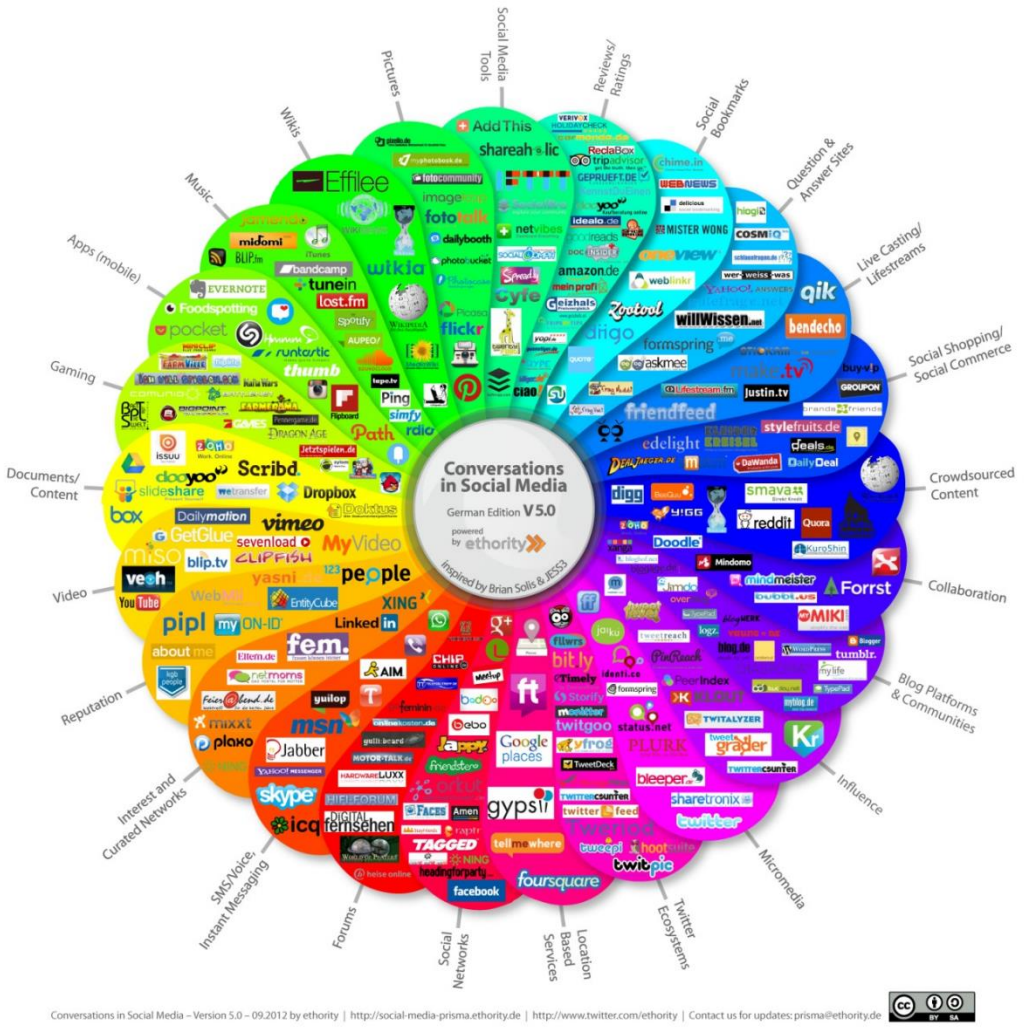
- Imagery Intelligence





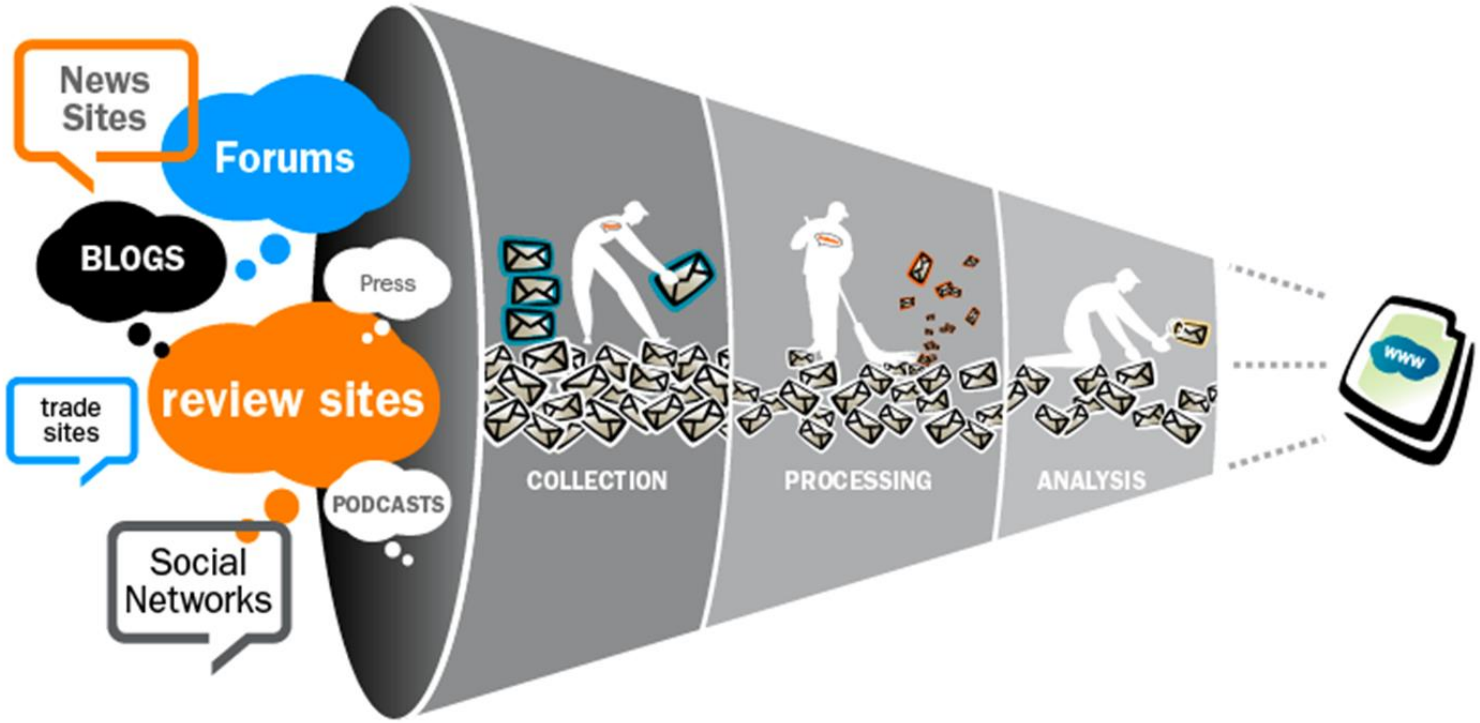
Building intelligence : Data gathering ; OSINT

- Open Source intelligence



Building intelligence : Data gathering ; OSINT

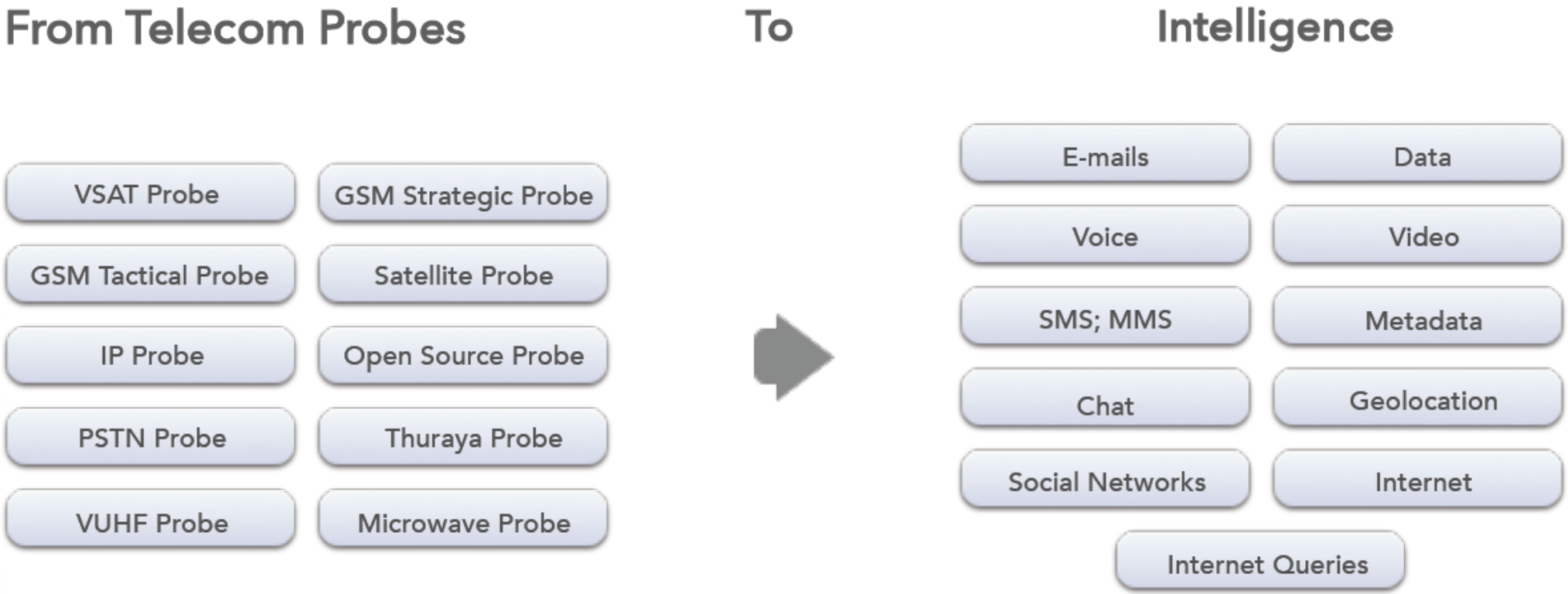
- Open Source intelligence



Planning

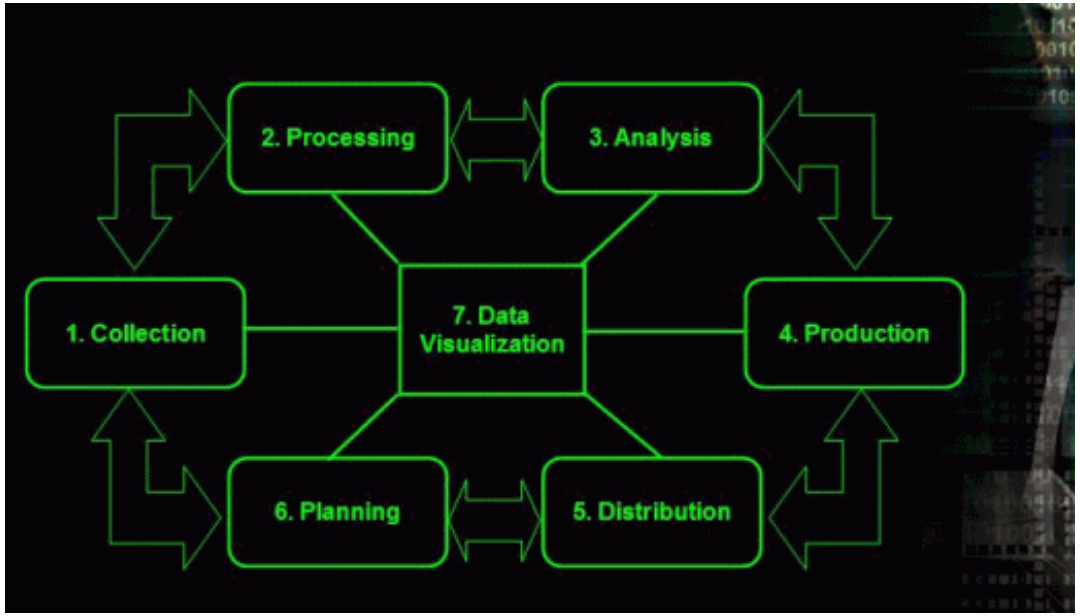
- Some definitions
- Data gathering
  - HUMINT
  - SIGINT
  - OSINT
- Turning data into intelligence
  - Data processing
  - Data correlation

Building intelligence : Enabling intelligence - Telecom example

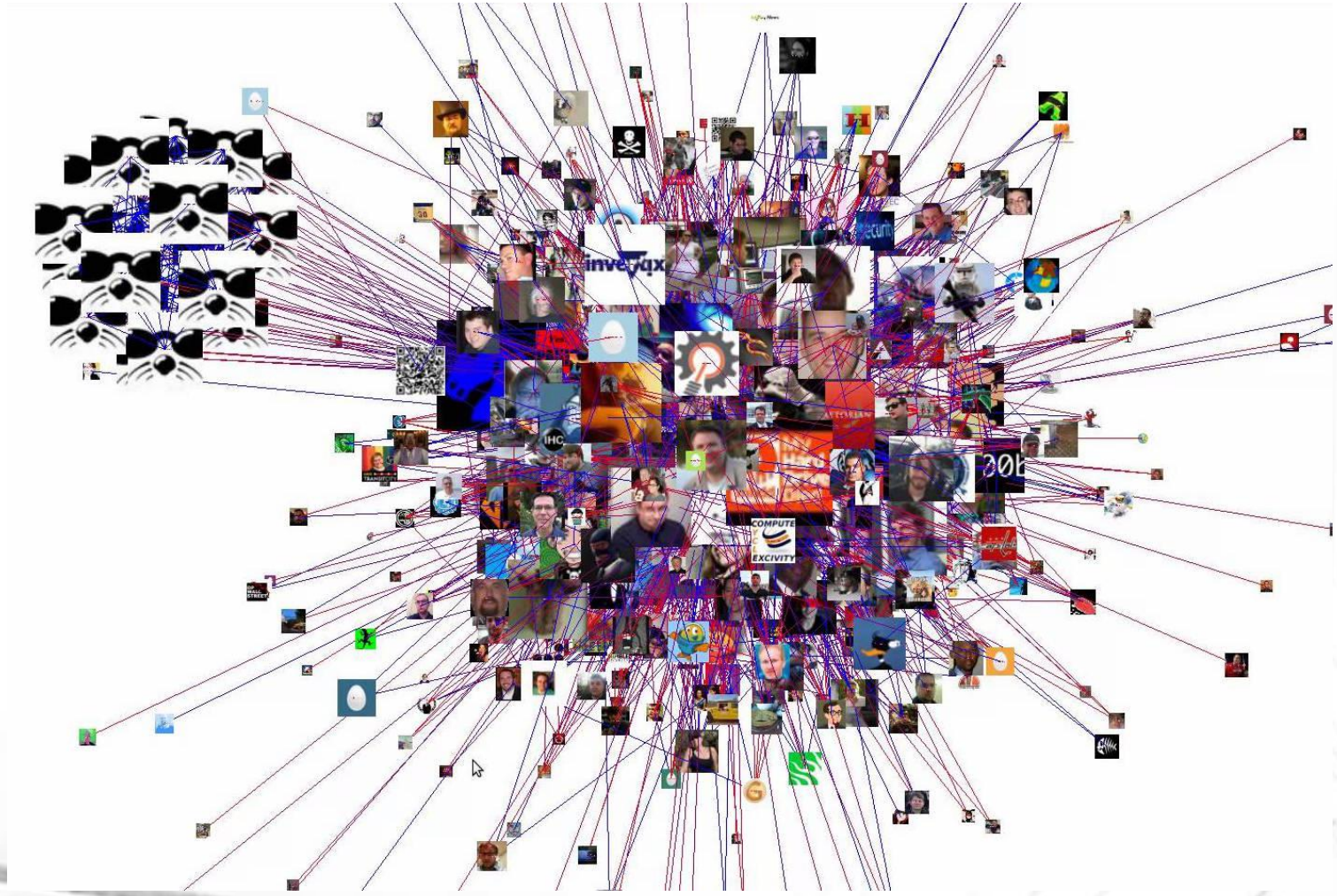


Building intelligence : Data Processing

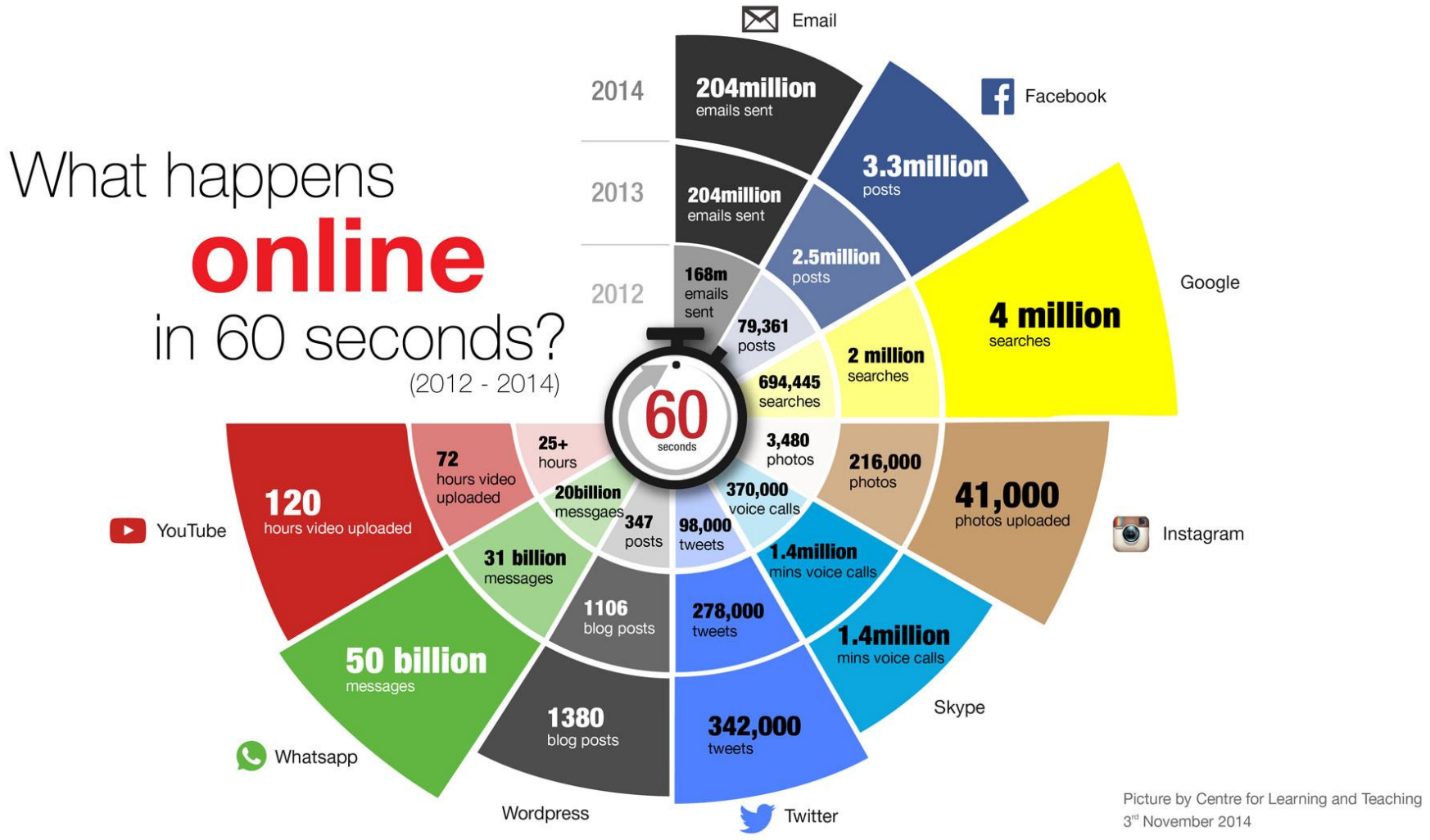
- Process



Building intelligence : Data Processing Challenge ; Big data !



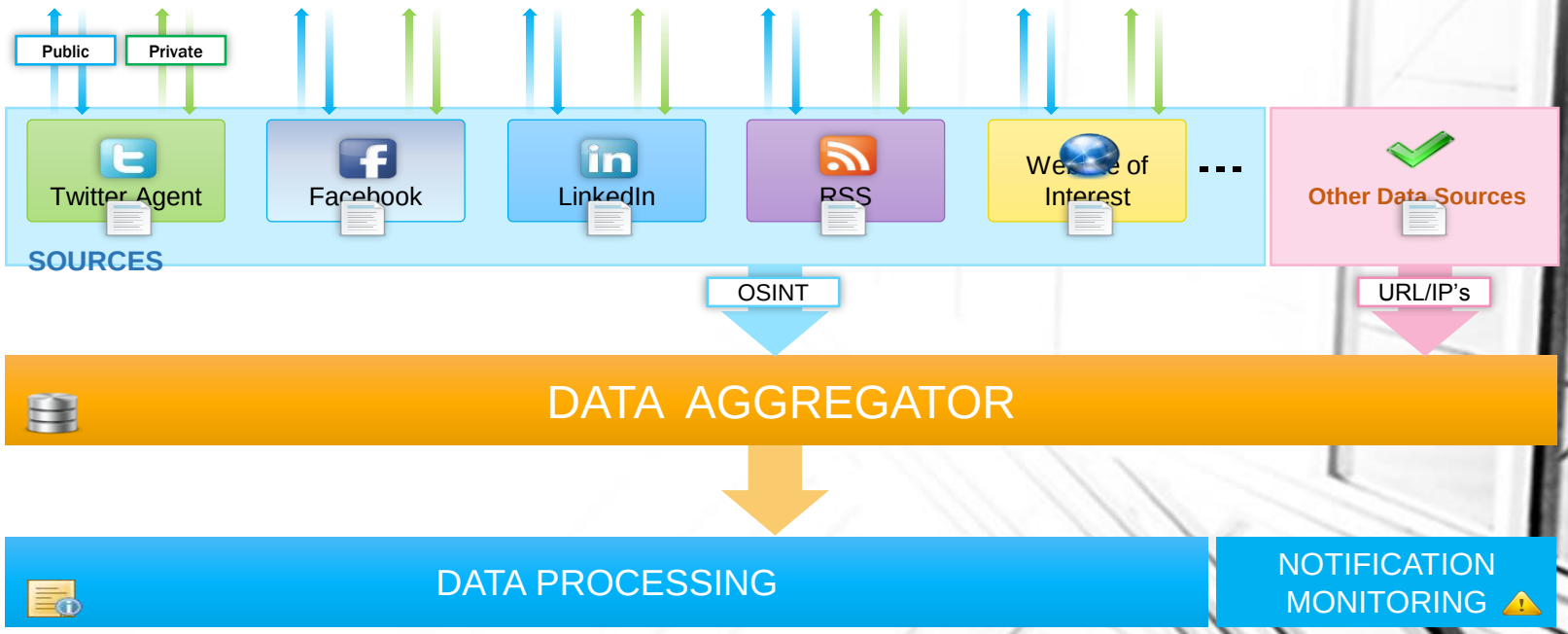
Building intelligence : Data Processing Challenge ; Big data !



Picture by Centre for Learning and Teaching
3rd November 2014

Building intelligence : Data Processing Challenge ; Big data !

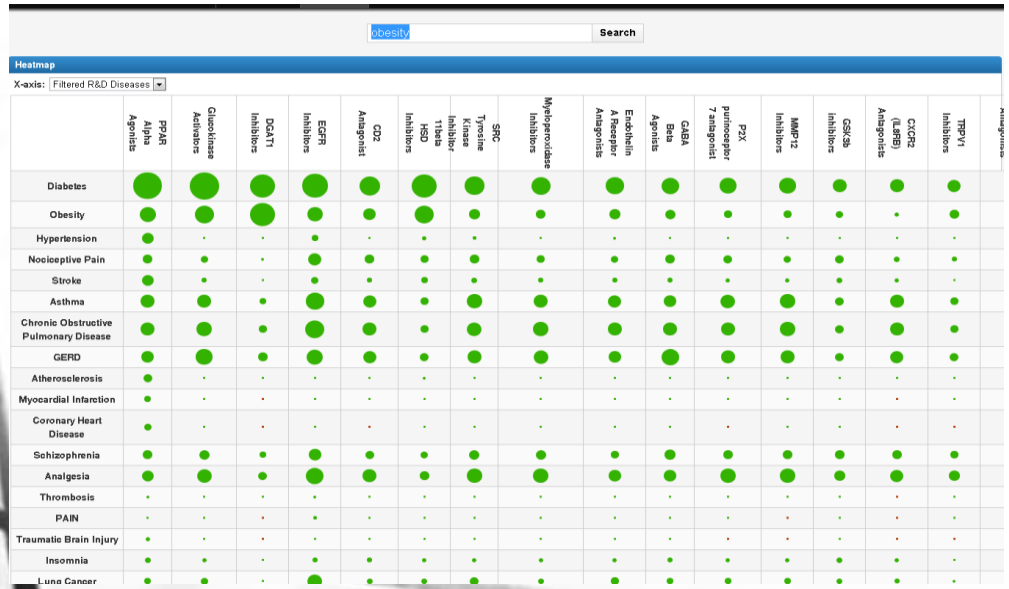
- OSINT Generate the most data among the other sources of data
- Good OSINT
  - Has good capability to crawl
  - Has good analysis capability

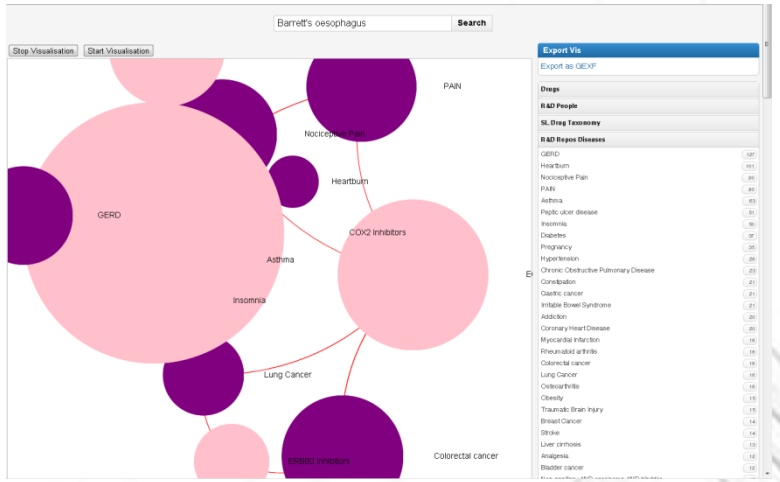


Building intelligence : Data Processing Challenge ; Big data !

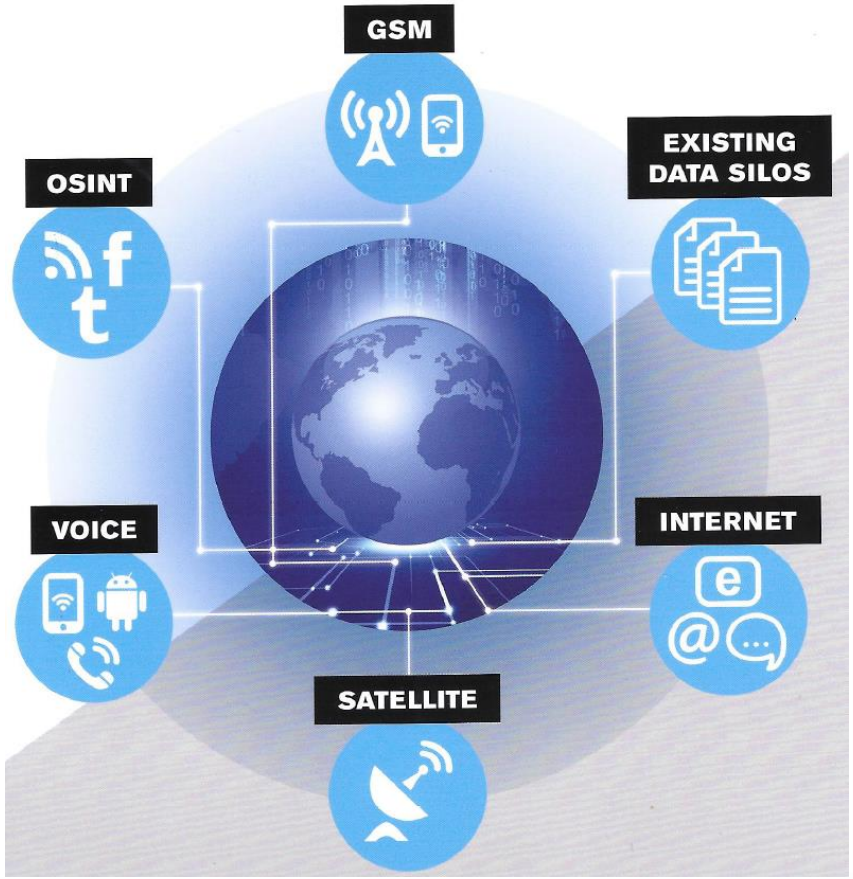
- 500 millions non structured documents have limited value

- Unless you can search, do semantics, linguistics, extract, link and detect …





Building intelligence : Correlation and intelligence exploitation



Building intelligence : Correlation and intelligence exploitation

- Emerging market (for civilian)
- Intelligence support decision maker
  - Need the ability to correlate different sources of intel
  - Need the ability to perform targeted search
  - Need a central view console

Take away

- Intel has been boosted with internet and big data
- Intel is build from data gathered by different kinds of sensors
- Intel needs to face big data issue due to the amount of unstructured data to process
- Intel needs user friendly GUI in order to facilitate the task of the decision makers
- Intel serves different kind of users/organizations


thank you
tenki
ขอขอบคุณคุณ
takk
спасибо
kam sah hamnida
je
hvala
הדות
dhanyavadagalu
tack
дзякуй
dziękuję
bedankt
blagodaram
mèsi
xièxie
tanemirt
dank
gracias
rahmet
enkosi
mochchakkeram
trugarez
djere dieuf
danke
kop khun krap
faafetai lava
arigatô
akun
shukriya
ありがとう
kia ora
dankon
děkuji
manana
diolch
ačiū
grazzi
gràçie
kiitos
spas
mamnun
barka
शुक्रिया
dhanyavad
gratias ago
tau
gràcies
sulpáy
tapadh leat
chnorakaloutioun
teşekkür ederim
bayarlalaa
σας ευχαριστώ
obrigada
sagolun
murakoze
taiku
mahalo
didi madloba
chokrane
rahmat
sukriya
obrigado
dakujem
misaotra
welalin
najis tuke
terima kasih
mercé
köszönöm
شكرا
asante
grazie
謝謝
mersi
sobodi
nandri
mauruuru
merci
nanni
vinaka
matondo
cảm ơn bạn
go raibh maith agat
paldies
ngiyabonga