Target, Parametric and Massive IP interception

Mattia Mazzola

Company highlights

- Company founded in 1996 for IT and Electronics design
- Based in Northern Italy, **100+ people, €35 mil. Turnover**
- First vendor to introduce Digital Multi-Channel Rec in Italy in 1999
- Company 100% owned by Italian founder and currently CEO
- **First Vendor In Italy, 100% dedicated to Law Enforcement Agencies**
- 100% in-house developed software
- Worldwide turn-key projects delivery

Market Share

- AREA is the largest italian provider of Lawful Interceptions Monitoring Centers, with over **300 installations**

- Italy has the highest penetration of Lawful Interception in Europe (72 every 100.000 inhabitants)

- Italy is a highly developed telecom market (i.e. cell phones)

- AREA currently works in many countries (Europe, Asia and Africa)

Our offering

AREA main activities are twofold:

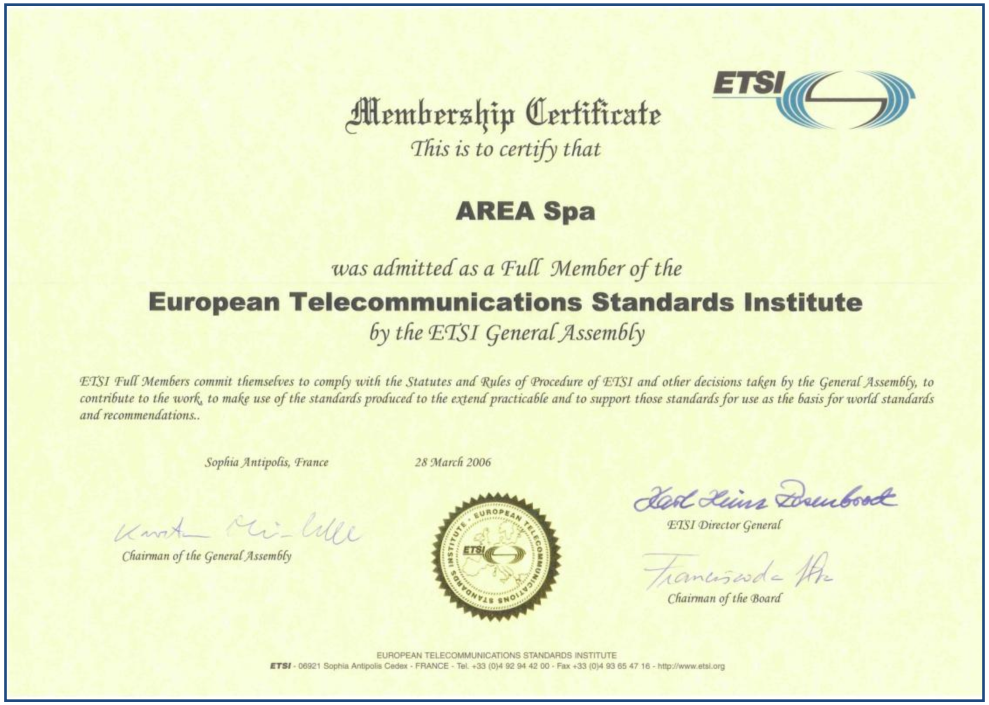
- **Lawful Interceptions Vendor**

  Monitoring Centers Applications (SW)
  Analysis Tools (SW)
  Tactical Devices (HW & SW)

- **LI Global Solution Provider**

  System Integrator
  Turn-Key provider

ETSI compliancy



ETSI

Membership Certificate

This is to certify that

AREA Spa

was admitted as a Full Member of the

European Telecommunications Standards Institute

by the ETSI General Assembly

ETSI Full Members commit themselves to comply with the Statutes and Rules of Procedure of ETSI and other decisions taken by the General Assembly, to contribute to the work, to make use of the standards produced to the extend practicable and to support those standards for use as the basis for world standards and recommendations..

Sophia Antipolis, France *28 March 2006*

Chairman of the General Assembly

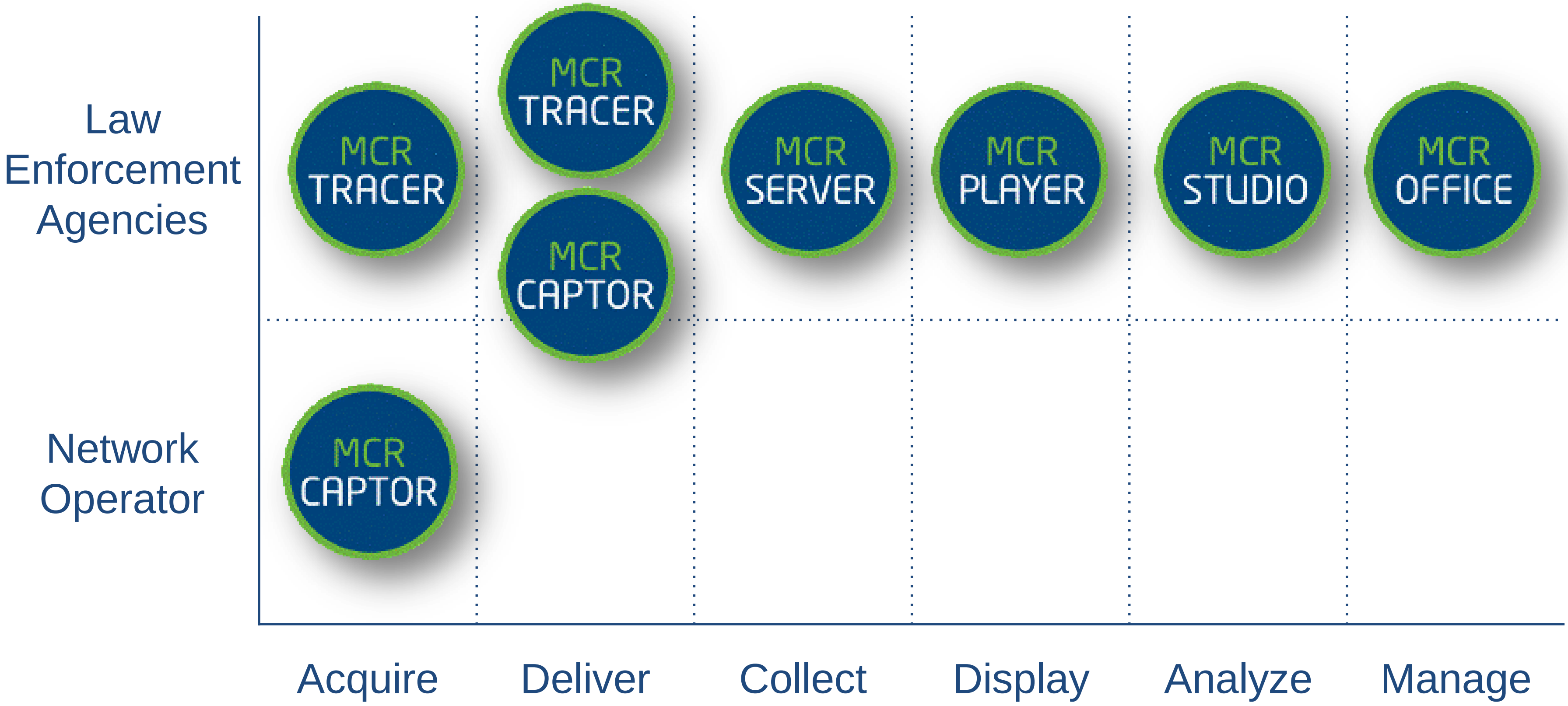
ETSI Director General

Chairman of the Board

EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
ETSI - 06921 Sophia Antipolis Cedex - FRANCE - Tel. +33 (0)4 92 94 42 00 - Fax +33 (0)4 93 65 47 16 - http://www.etsi.org

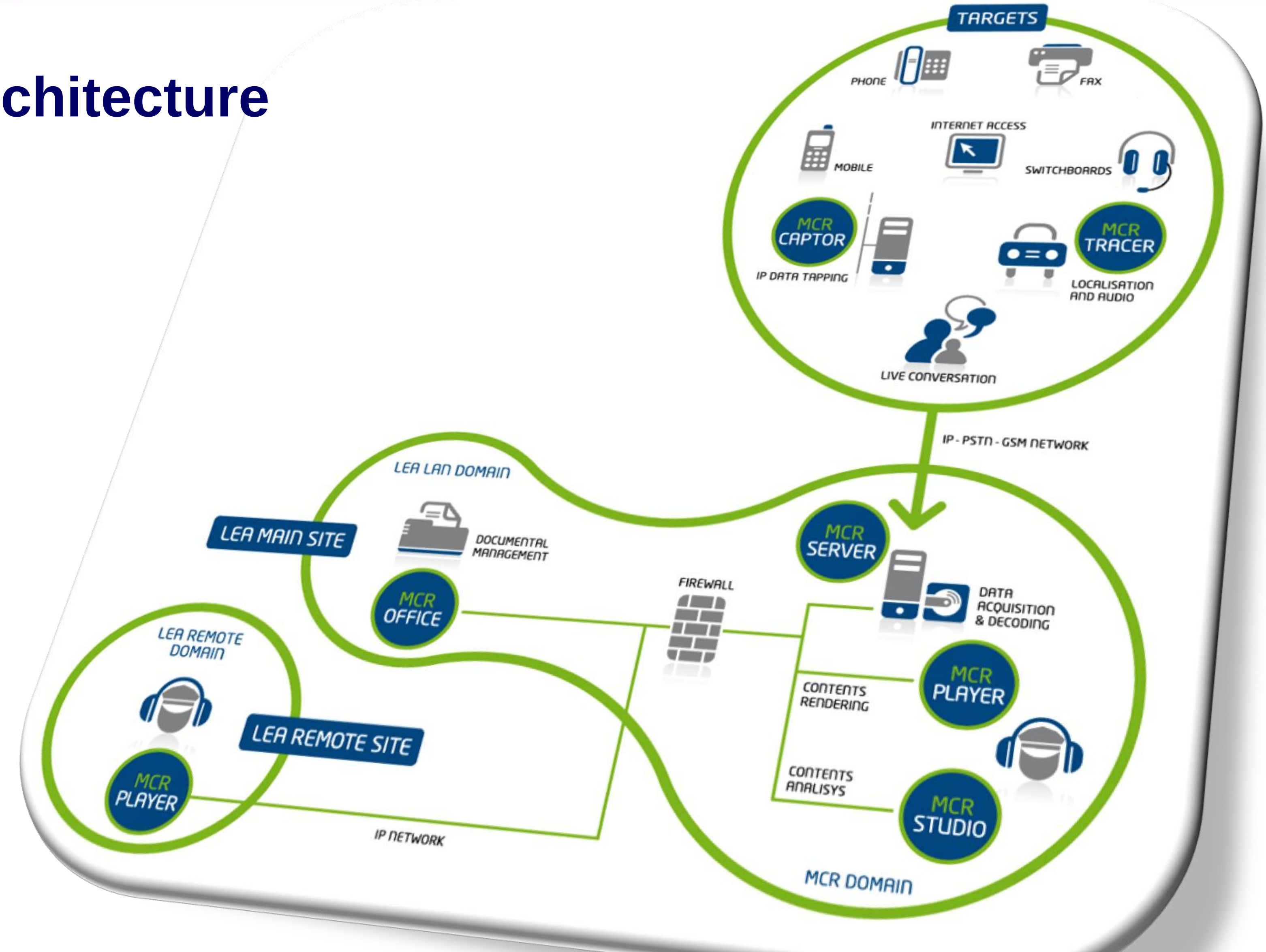
- Full Member of **ETSI**, the **European Telecommunication Standard Institute**
- AREA is an active component of the **Lawful Interception workgroup**

Market Positioning vs. Offering



	Acquire	Deliver	Collect	Display	Analyze	Manage
Law Enforcement Agencies	MCR TRACER	MCR TRACER MCR CAPTOR	MCR SERVER	MCR PLAYER	MCR STUDIO	MCR OFFICE
Network Operator	MCR CAPTOR					

Architecture



Speech focus

- Target, Parametric and Massive IP interception
- Three different approaches to face the same problem
- Patrol and control what happens in your country network
- When and how you should use them
- What a LEA really needs

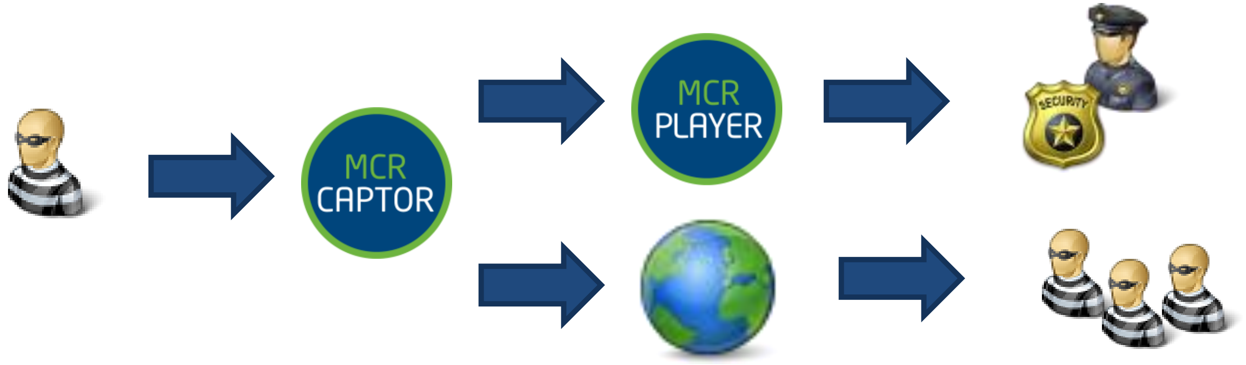
- Three simple examples showing the main differences…

1st Scenario

- There’s a “well known criminal” preparing a new crime
- Real-time monitoring of his activities
- Discover his possible accomplices and prevent the crime

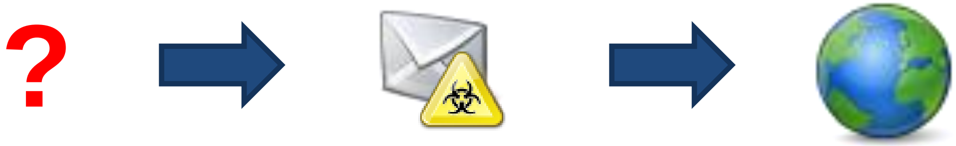
1st Approach: Target oriented interception

- Intercept and dump all his traffic (CC and IRI)
- Decode (and maybe post-process) intercepted data
- Collect the evidence and find accomplices
- Up-to-date decode engine and user-friendly interface



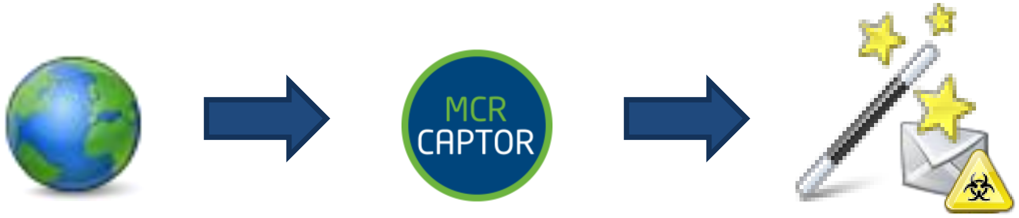
2nd Scenario

- There’s a “well known evil behavior” pattern
- Check the real existence of one or more “bad guys”
- Be immediately alerted when a behavior occurs



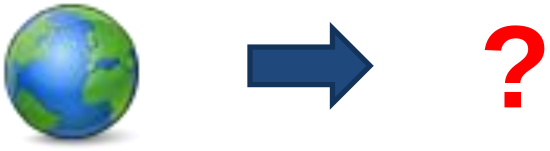
2nd Approach: Parametric interception

- Real-time network analysis (DPI)
- Figure out “optimal key parameters”
- Receive an alarm when a positive match occurs
- Easy-to-use and remotely configurable engine



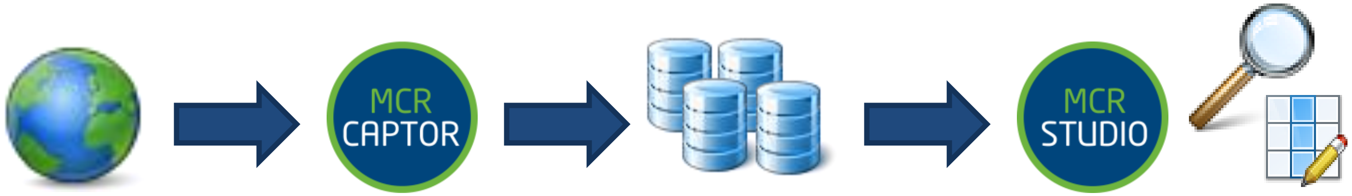
3rd Scenario

- Perform traffic analysis
- Obtain mass surveillance
- Data Retention

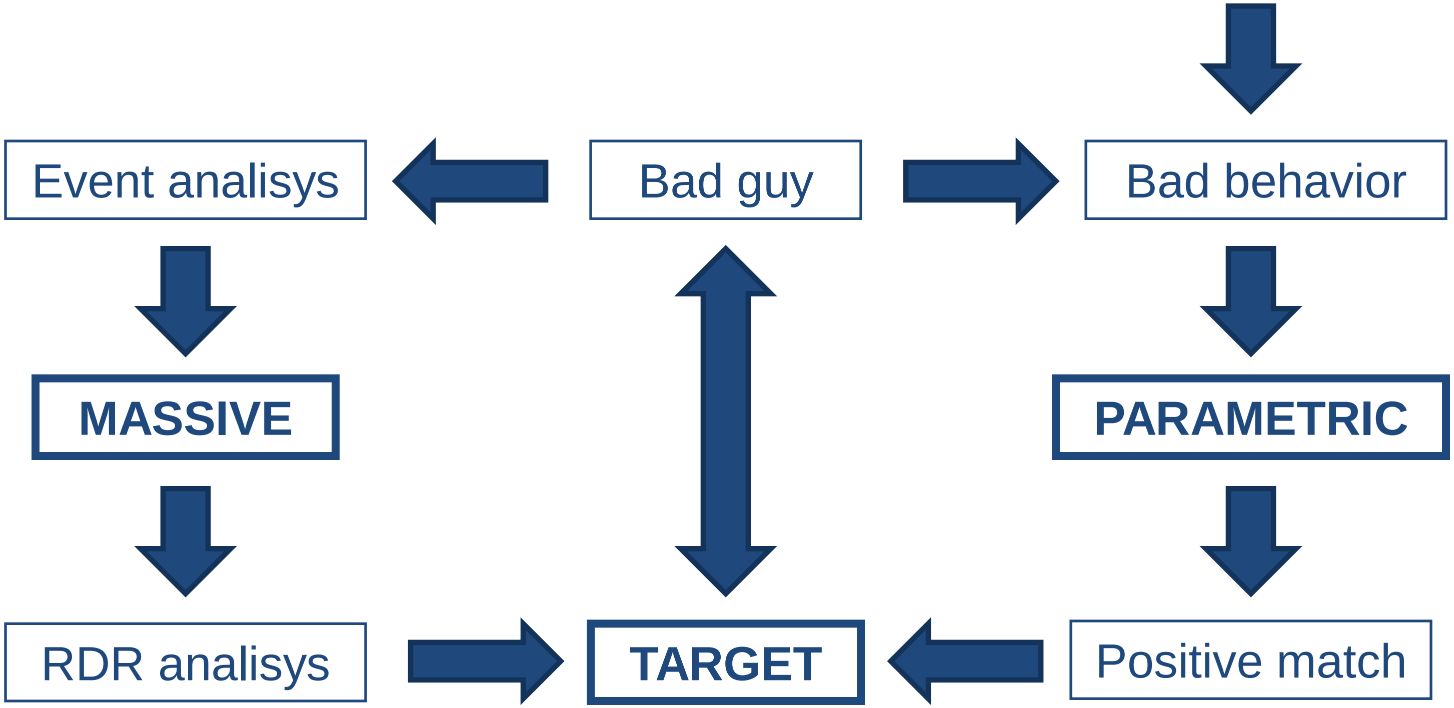


3rd Approach: Massive interception

- Dispose IPCDRs collectors on the net (huge and pervasive)
- Normalize and store more than TBytes of IPCDRs
- Large structured historical archive of IPCDRs
- Powerful analysis tool to “find the needle in the haystack”



The big picture



A simple example

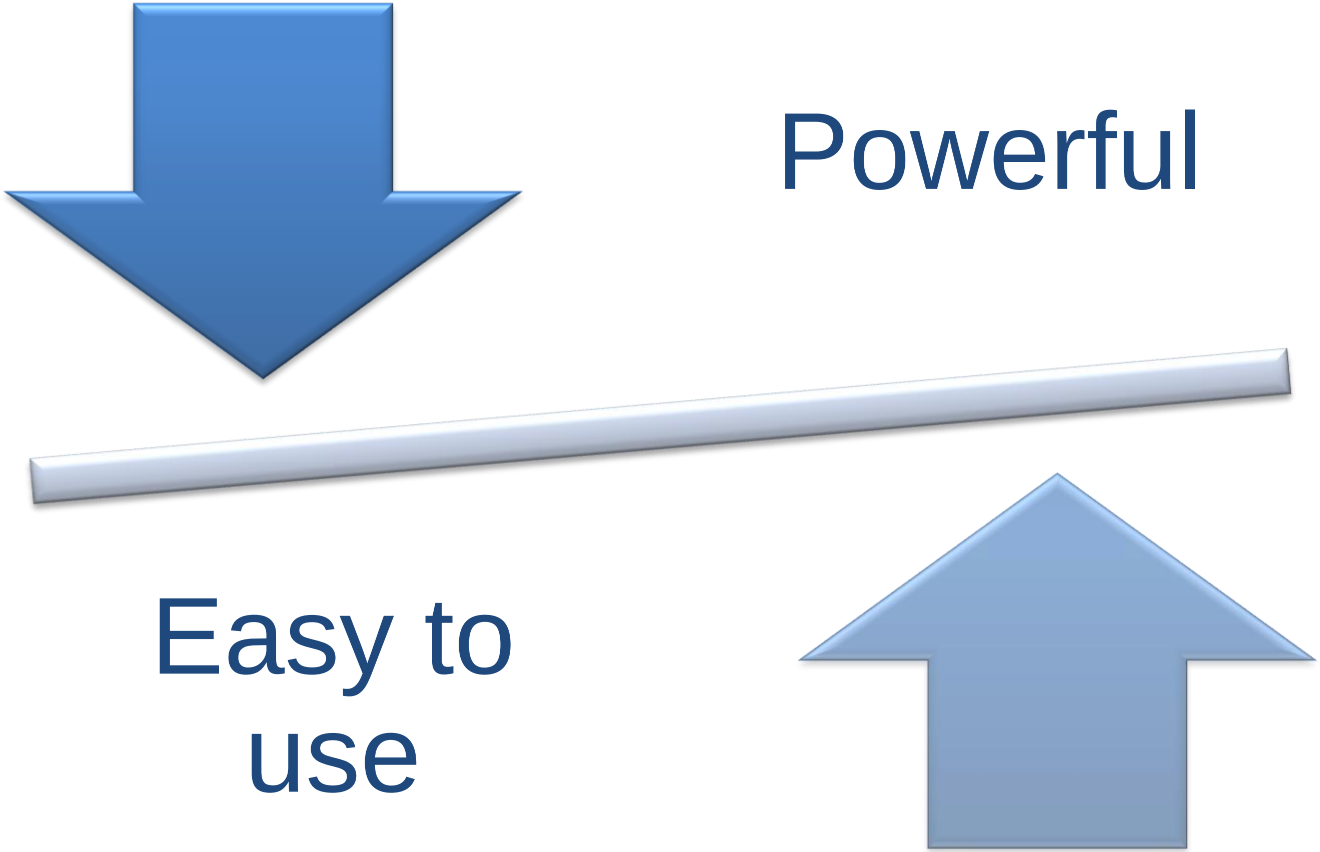
- You know that most of your “top secret” documents are being sent toward an hostile domain “.evil”
- Documents contain the special word “biohazard”
- You want to know who is committing this crime and how he is doing it

Domain “.evil”

A simple example

- **Parametric** DPI (domain “.evil” and word “biohazard”)
- Discover a file sharing server from which documents are downloaded
- Analyze retained data records (**massive**)
- Identify the “bad guy” who uploads the documents
- **Target oriented** interception on this criminal
- Collect the evidence and find possible accomplices
- If needed start target oriented interceptions on accomplices

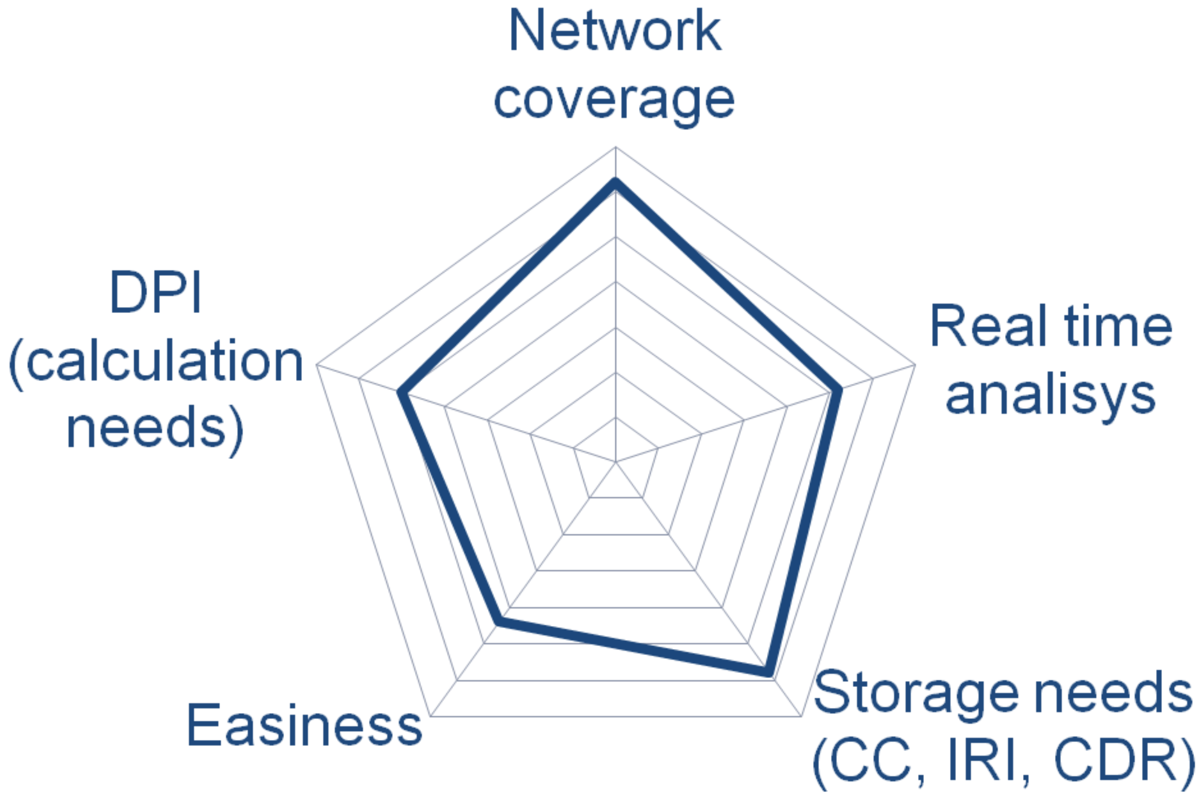
LEA needs: management interface



Powerful

Easy to use

LEA needs


Network coverage
Real time analisys
Storage needs (CC, IRI, CDR)
Easiness
DPI (calculation needs)

Conclusion

- You may need to manage all the approaches
- Cover all the scenarios
- Importance of the ETSI compliancy systems
- Tailor your solution on your needs
- There’s no unique “best of breed” solution for everything

- AREA may help you build and deliver your “turn-key” solution

MCR TRACER

MCR CAPTOR

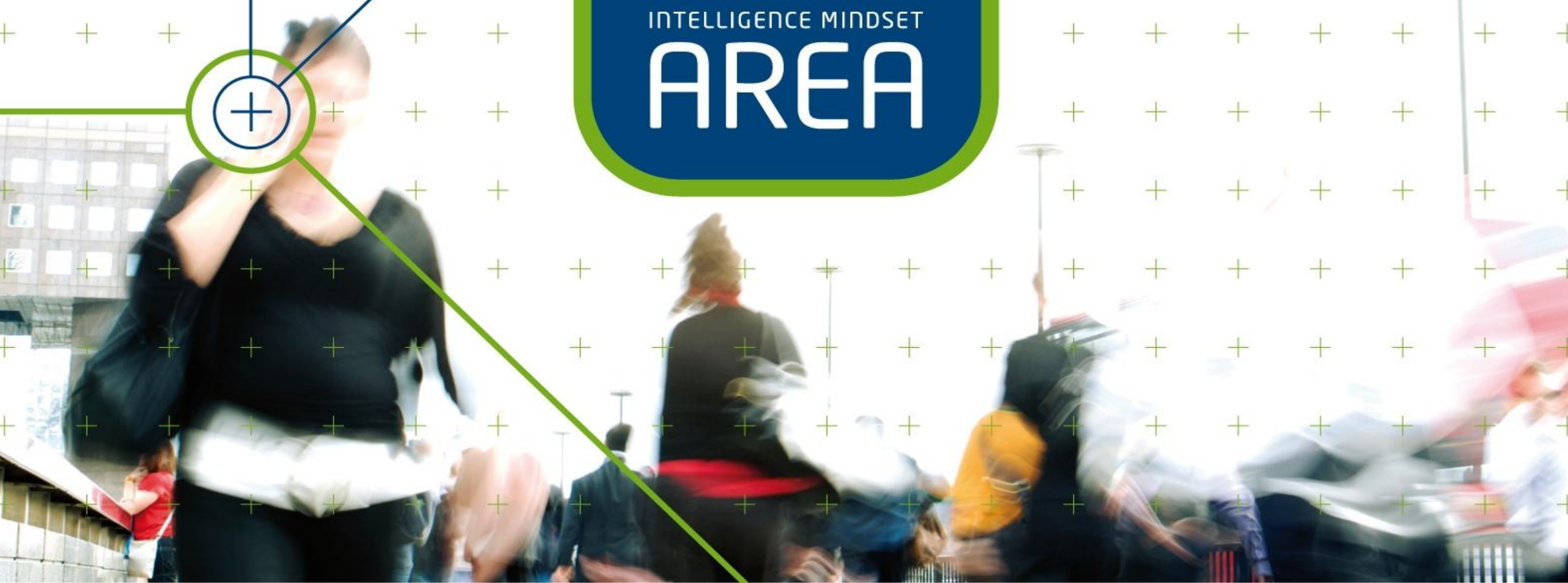
MCR SERVER

MCR PLAYER

MCR STUDIO

MCR OFFICE

Thank you



INTELLIGENCE MINDSET

AREA