

The surveillance Olympics, Beijing 2008 – powered by European technology

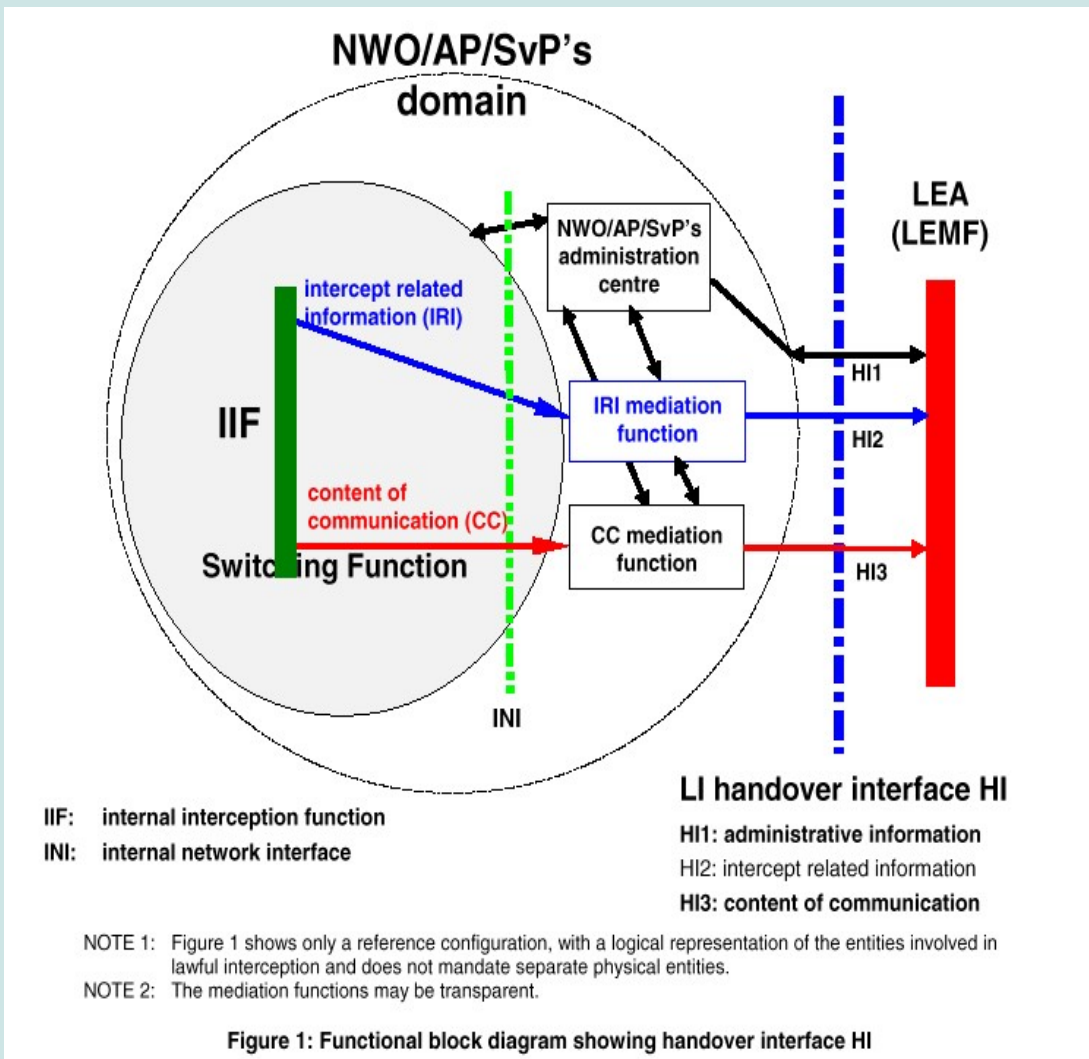
All telephone communications of European delegations, athletes and journalists will be under 24/7 surveillance during the Olympic Games. The equipment used by Chinese secret service was produced and deployed by European companies like Ericsson and Nokia Siemens. Surveillance methods and protocols are developed in the European Telecom Standards Institute.

Brussels, Olympic Rights for Human Games Conference
2008 05 15

How digital surveillance works

- Listening is out, traffic data analysis is in
- 99,9 percent of “lawful interception” = meanwhile “communications statistics”
- Who calls whom when where and from where
- Centrally managed telco networks are much easier to control than internet traffic.
- All GSM/UMTS networks have a standardized interface for voice and traffic data surveillance

The “lawful interception” interface [schematic]



- LEA = Law Enforcement agency
- HI1 request LEA
- HI2 traffic data
- HI3 call content
- dotted: borderline between democracy and police state. Interface supports multiple LEAs.

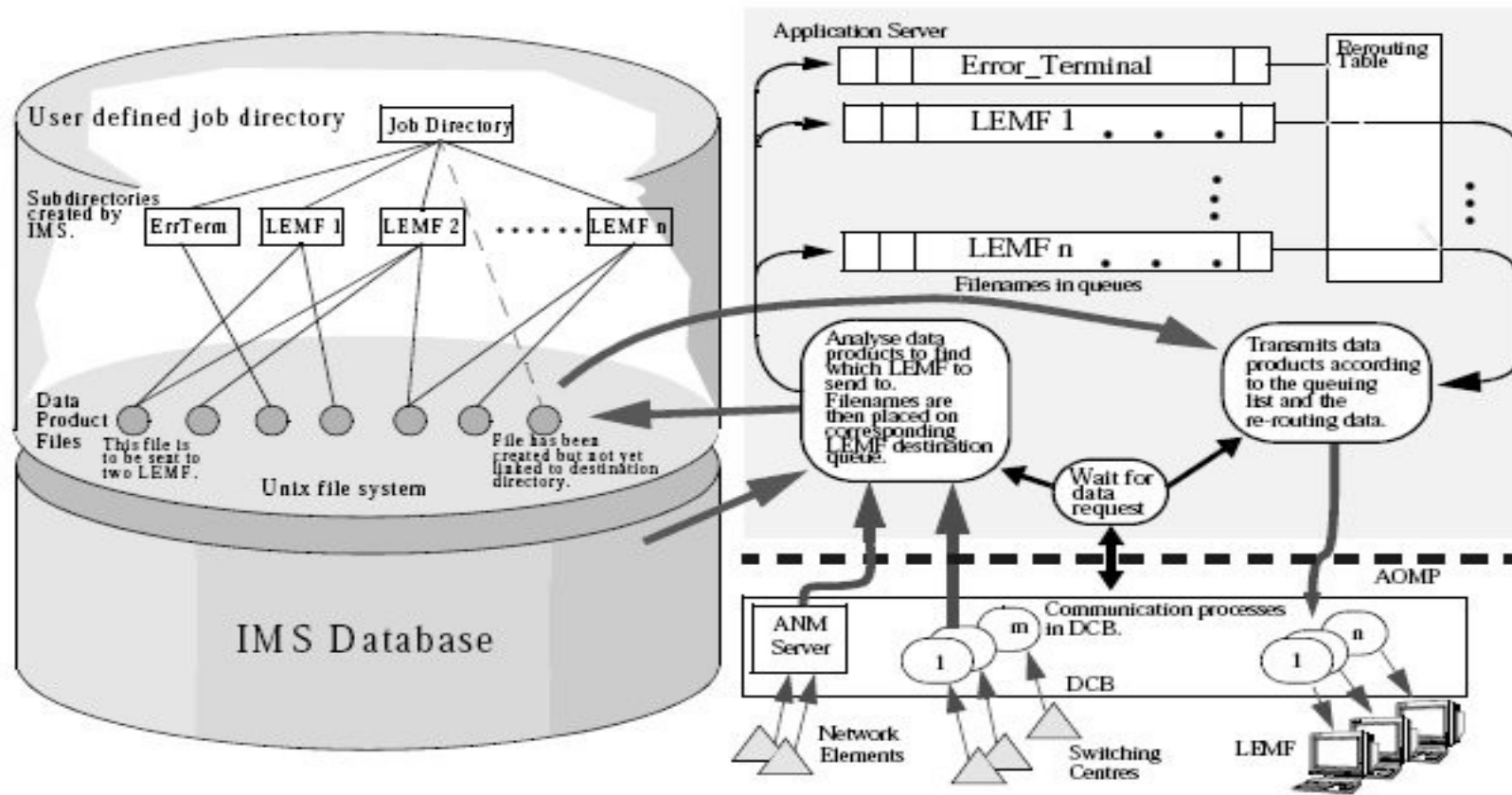
Equipment used to spy on reporters, athletes and delegates - Ericsson



- Intercept Management System [IMS] for fixed / mobile networks developed by Ericsson R&D Australia. Unit was moved to China.
- Two Ericsson R&D institutes, one academy, 5 dozen joint ventures, sub-companies and offices in china.

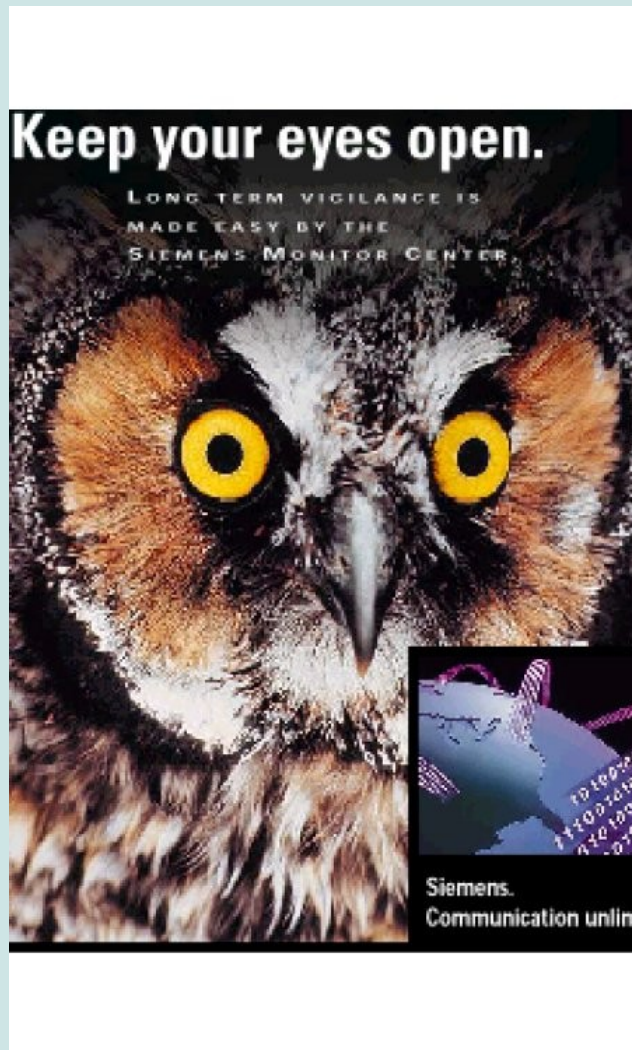
Ericsson IMS: 1 to n law enforcement monitoring facilities

Figure 1.3 Server functions implementation model



CHAPTER 1 Functional Specification of IMS
General functions
STRICTLY CONFIDENTIAL

Nokia Siemens, Ericsson's main competitor in China

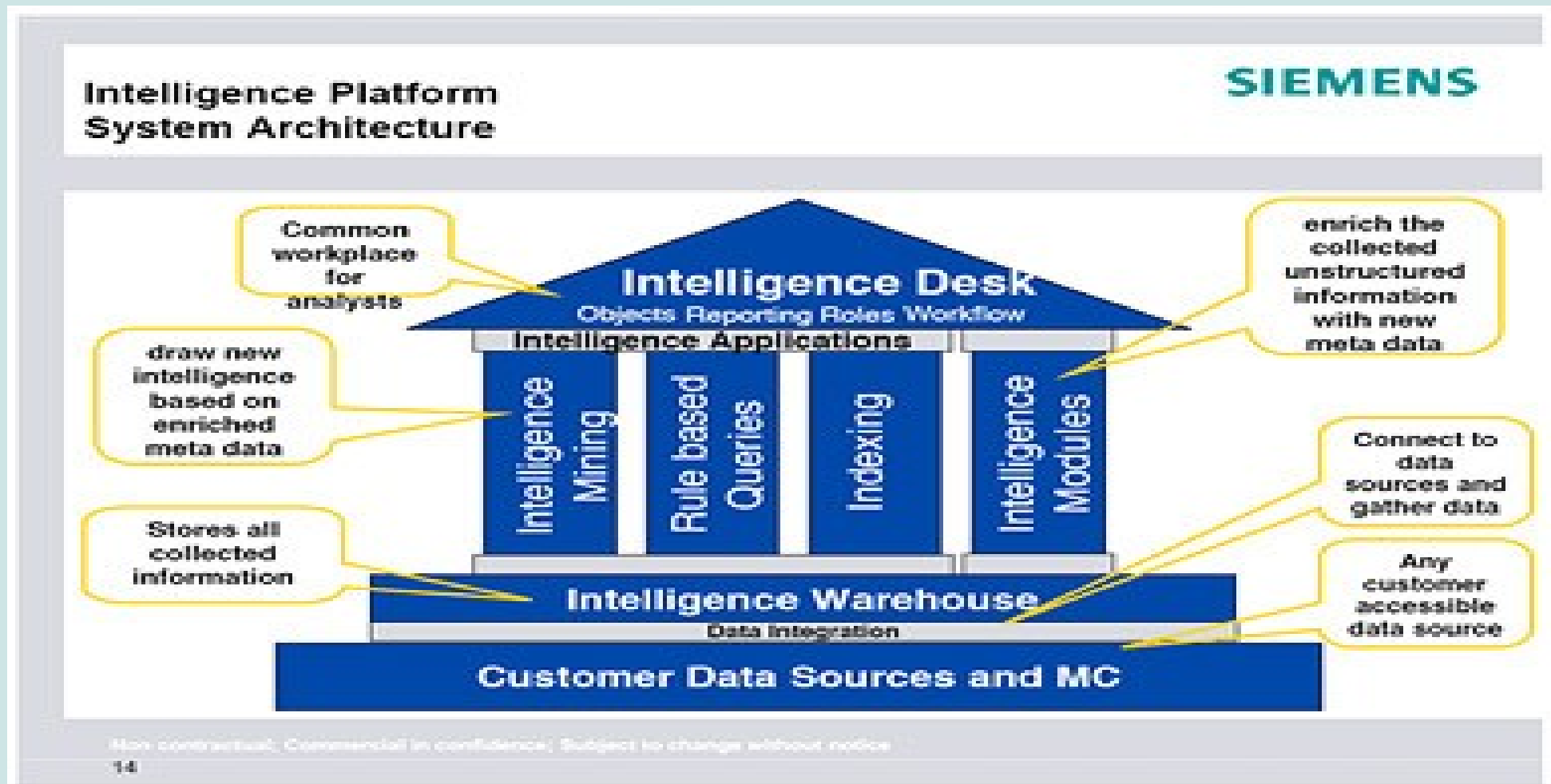


- The Siemens Monitor Center has been developed since the mid 90ies
- Even then: “10.000 calls can be monitored simultaneously per exchange.”

And what happened then?



This meta-machine ate the Siemens Moitor Center



“Data center dimensions processing mass data (TB)”

Intelligence Applications
Intelligence Mining: Pattern Recognition - Example


Example Task:

- Search for suspicious patterns in 21,237,645 call records

Criteria:

- Time frame: 1 hour
- Minimum count: 5

Results:



Additional Examples

- money transfers between bank accounts
- geographical movements of targets

- Communications pattern search in x million datasets
- Automated topic, word and speaker recognition and emotion detection
- Automated transcripts

The power of integration



SIEMENS

- Bank account transactions
- Insurance company data bases
- Border Control data base
- Passport data base
- Finger print data base
- DNA analysis data base

- “Data retention” datasets, traffic control systems, health data, geographical data merged with unstructured data, e.g. fone call transcripts, chat protocols & c.

Targeted markets

- Ericsson and Nokia Siemens main suppliers of Chinese telco market, by March 2008: 550 million mobile customers.
- Nokia Siemens says: 90 deployments of both systems in 60 countries. Target markets are Middle and Far East.
- Around the Athens Olympics 2004 Ericsson IMS was hacked by parties unknown and used to spy on the Greek government.

The Standardization of telco surveillance - made in Europe

- Surveillance methods and protocols for fixed/GSM/UMTS networks by the European Telecom Standards Institute from 1996.
- Regular participants in ETSI TC LI [“lawful interception”] and ETSI/3GPP SA 3: MI5/NTAC, Bundesamt für Verfassungsschutz, Platform Interceptie Decryptie en Signaalanalyse, FBI, Nokia Siemens, Ericsson, Huawei Telecom, BT, Deutsche Telekom and others.

Thanks for your patience – further communications

All documents

http://quintessenz.org/it_and_telco_surveillance_equipment/

related story: Olympische Disziplin Überwachung

<http://futurezone.orf.at/it/stories/277636/>

erich.moechel@orf.at

secure

me@quintessenz.org

pgp key

<http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x007DB429>