Future Cybersecurity:
Threats and Countermeasures
A Research Opportunity

NATO AND THE FUTURE OF CYBER SECURITY
LA NATO E IL FUTURO DELLA CYBER SECURITY

Roma, 2 December 2013

Zanasi & Partners

EUROPEAN SECURITY RESEARCH & INNOVATION FORUM
ESRIF

Ing. Alessandro ZANASI
ESRIF Member
www.zanasi-alessandro.eu
alessandro.zanasi @ zanasi-alessandro.eu
Tel: +39 349 4131 718

1. Introduction

Speaker Background

- **Technical-Scientifical:**
  - *Degrees in*
    - *Nuclear Engineering – Università di Bologna*
    - *Economics – Università di Modena / Specialized in Financial Engineering – Paris University*
  - *16 years in IBM (Bologna, Parigi, San Josè-California)*
  - *Coordinator of KDD Center at CINECA (Italian Supercomputing Center)*
  - *META Group, Inc. Analyst (Business Intelligence)*
  - *Professor at University of Southampton – Data and Text Mining Courses*
  - *Reviewer and evaluator for EU funded projects*
  - *Founder of TEMIS SA, SW development company for automatic intelligence.*
- **Intelligence/Security:**
  - *Carabinieri Officer (retired)*
  - *Charged of phone calls interception at Centro Carabinieri Investigazioni Scientifiche (now RIS)*
  - *Builder of several Intelligence systems in all the world*
  - *Market Intelligence responsible for IBM in South Europe*
  - *Frequente speaker and chairman in int'l conferences dedicated to intelligence (eg: The New Forest, UK – Jun.2007)*
  - *ESRAB/ESRIF - European Security Research Advisory Board & Innovation Forum Member*
  - *Author of several articles and books on intelligence techniques.*
  - *Advisor in Intelligence and Security issues and fund raising*

Zanasi & Partners

Mission

Research and Advisory in security, intelligence, big data and European funding

Resources

Former LEAs high officers, IBM executives, Int'l Researchers…

Advisory *(here listed the ones not covered by NDA)*

Public Administration:

European Commission →DGs: Justice; Home; Enterprise; OLAF-AntiFraud Office; FRONTEX-European Border Security Agency; JRC-Joint Research Center…

Italian Government →Presidenza del Consiglio-CNIPA/DIGIT PA, Ministero Economia e Finanze,Ministero delle Comunicazioni,Consip…

Belgian Government →Federal Office for Technical Solutions, National Bank of Belgium, Federal Police

Romanian Government → Ministry of Justice…

Saudi Government

Turkish Government → MASAK…

Private Organizations:

Aerospace → ESA-European Space Agency, CIRA-Centro Italiano Ricerche Aerospaziali,...

Information Technology → Siemens AG, Politecnico di Milano, Università di Modena...

Consulting → EURISPES, Booz&Co...

Research→ Cyber Intelligence

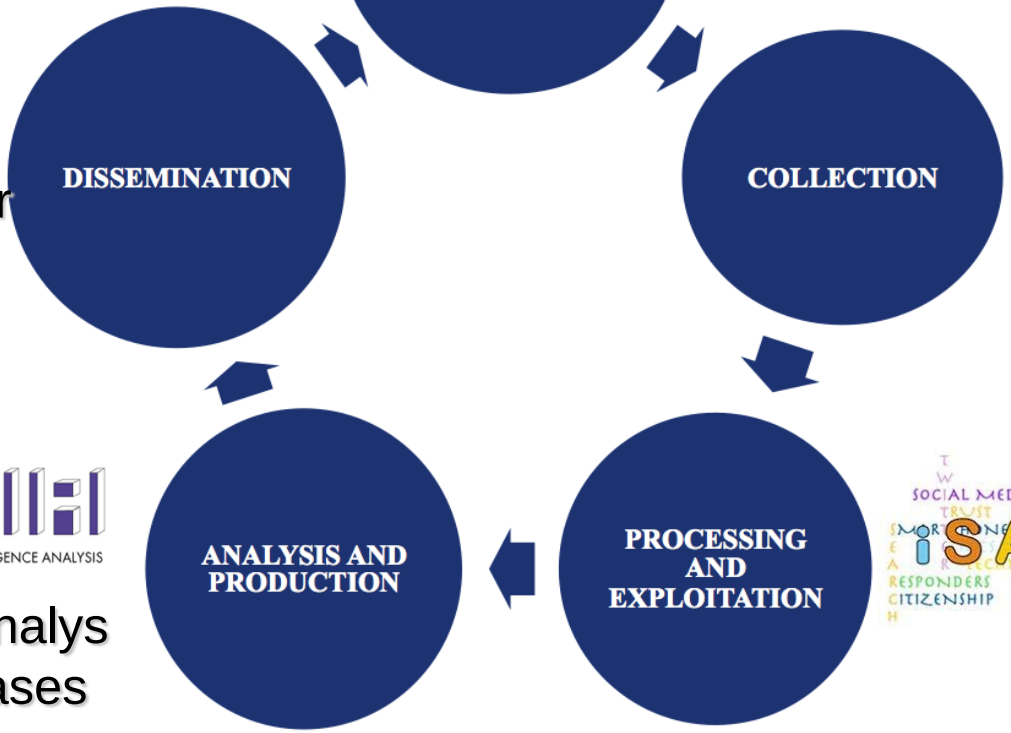
CRISYS

Countering WEEE Illegal Trade

Intelligence Planning

LEILA

Serious Gaming for Intelligence



THIS

Video Retrieval

REDUCTION OF COGNITIVE BIASES IN INTELLIGENCE ANALYSIS

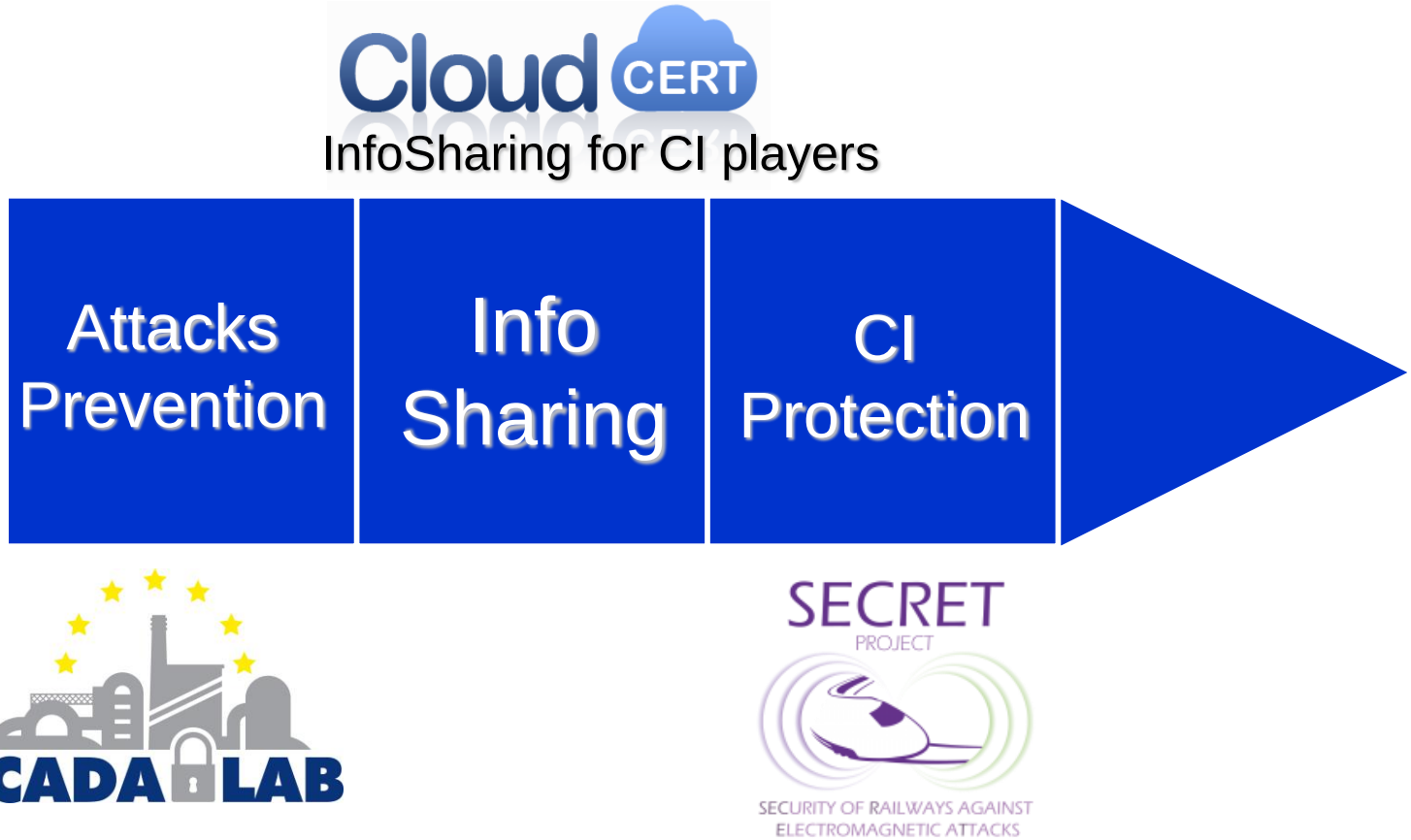
Intelligence Analys Cognitive Biases Reduction

iSAR+

SOTERIA

Social Media Monitoring

Research→ Cyber Security



SCADA Systems Defense

Protection of trains against EM attacks

ESRAB/ESRIF

European Security Research Advisory Board/Innovation Forum

- To avoid *mismatch* between technological development (*private*), security policies (*public*) and funding (*European Commission*) EC appointed ESRAB (before) and ESRIF (later) to define the policies of security research in general and of cybersecurity in particular (PPP).

- Composed by 50/64 members coming from private (*Eurisc,Thales, Finmeccanica, Eads, Saab, Sagem, Smiths …Zanasi*) and public security organizations (*Ministries of Interior, Defence…Europol, Frontex, BKA, EDA*…).

- **Italy represented by**
  - Ministero Interni → **Public**
  - Ministero Difesa → **Public**
  - Finmeccanica → **Large Industry**
  - Zanasi & Partners→ **CyberIntelligence/Security Expert**

It is essential for Italy...and NATO
to fight and win the

2. CyberSecurity Threats

2a. Cybersecurity Threats

The EU vision presented in its Cybersecurity strategy (*) is articulated in 5 strategic points, directed to fight 5 ***threats***:

- Achieving cyberesilience → ***Attacks to our CI***
- Reducing cybercrime → ***Cybercriminal actions***
- Developing Cyberdefence capabilities → ***Cyberwar***
- Develop the industrial and technological resources for Cybersecurity → ***Risk of becoming dependent on security ICT and services developed outside EU***
- Establish a coherent int'l cyberspace policy for the EU and promote core EU values → ***Attacks to open, free and secure cyberspace***

**(JOIN(2013)1 final)*

2b. Why Essential? For CP risks

It is ***essential*** because CP-Community Protection risks are dangerously approaching:

if 50 years ago we talked about ‘ iron curtain’ now the curtain is

an ‘***electronic***’ one (which must protect us from *cybercriminals* but also protect us against *the espionage of enemies/friends*).

It is a battle to win more through our intelligence (→ Research) than through our strength

2b.Why Essential?For its *accelerator* effect

Security is the strongest accelerator of research

→WWII started with horses and ended with V2. So what?

It is ***essential*** to develop our ***cyber*** skills, competences and intelligence because we are entering a new Age, as when we entered the Iron Age leaving the Stone Age and

who was not able to master the new technology ***died***.

EU Funding for CyberSecurity Research allows skill improvement and MUST be better exploited.

3. Countermeasures → Research

R&D, EU H2020 and Cybersecurity

R&D can support a strong **industrial policy**, promote a trustworthy **ICT industry**, boost the **EU internal market** and reduce **our dependence on foreign technologies**.

We should make the best of the Horizon 2020 Framework Programme for Research and Innovation, to be launched in 2014.

Horizon 2020 will support ***security research*** related to emerging ***ICT*** technologies.

H2020 Funding & Cybersecurity Perspective

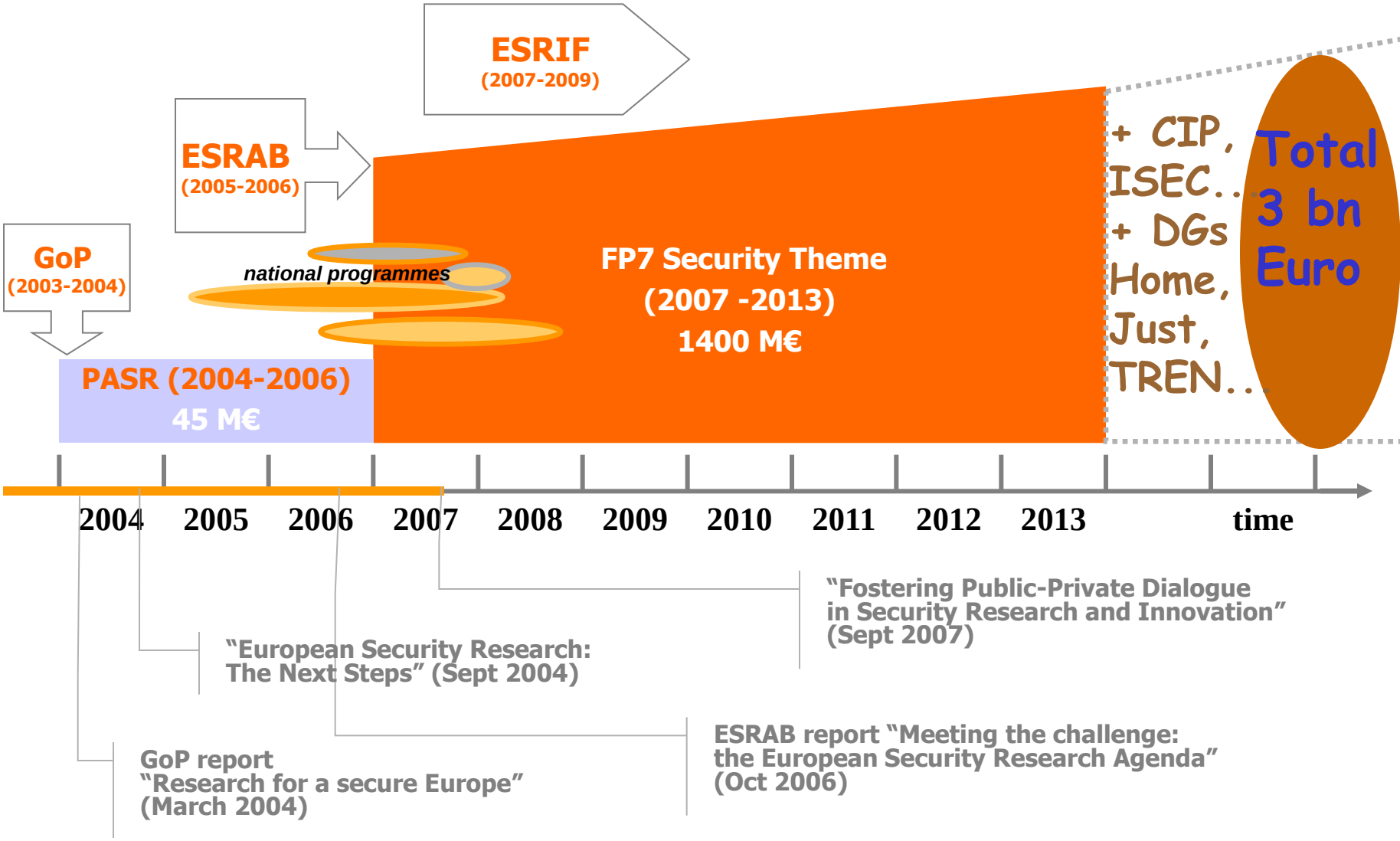
EU Research Funding passes from **€ 50 bn** in FP7 to almost € 80 bn in Horizon2020.

Security Research remains focused in Civil but not precludes cooperation with military, especially in Cybersercurity whose market reaches, globally, >$ 70 bn (2013 ASD Reports/ Markets & Markets).

Technology has no sex:
Research money will fund Prototypes & Demonstrators.

" It is not sufficient *to know*, you must also *apply*;
It is not sufficient *to want*, you must also *do* „
Goethe

EU Security Research Funding Evolution (→2013)



Expected funding in Cybersecurity Research 2014-2020

...→€ 3.8 bn

Protection of Cyber Space→ **€ 560 M**

- CyberSecurity
  - For CIP
    - Cip from insider threats
    - Secure SCADA, simulation test beds to assess SCADA/ICS
  - Smart/Intelligent CS
    - CS for Smart Cities
    - Smart control, smart agents
- Fight Cybercrime and Cyberterrorism
    - Cyber threats monitoring: data mining/big data analytics/intelligence
    - Social media analytics
    - Multinational information exchange

Critical Infrastructure Protection (Tr/En) → **€ 560 M**

4. An Example

Information Exchange/Sharing

Few activities are so central for national cybersecurity and PIC as the information exchange, their sharing and their protection, coordinated at tactical and operational level, strategic as political.

To guarantee it, not only best practices but also ***adequate platforms must be garanted,*** prepared and ***tested***.

This is the objective of ...

CloudCERT project

Testbed Framework to Exercise Critical Infrastructure Protection

- ***Objective*:** to develop a communication platform to allow information exchange and sharing among EU actors responsible of cybersecurity of EU CIP (CIs owners, national CERTs nazionali, ecc.).
- Funded by EC (***DG Home Affairs) ,lasting 2 years***.
- International Partners:
  - Spain (Ministry of Economics, Ministry of Interior, INDRA),
  - UK (E4B),
  - Italy (ICSA, Zanasi& Partners)

So….

in case of interest, read

http: // cloudcert.european-project.eu,

TIP: Visit project website

contact us

or leave your business card !

PIC SpA.

Dr.Mario ROSSI
AD

Roma
Bruxelles
NYC

Thanks!

Q&As?