From
CyberSecurity to CyberIntelligence:
a new frame for
CIP-Critical Infrastructure Protection

Alessandro ZANASI
ESRIF
(European Security Research and Innovation Forum)

Bucharest
October 27, 2011

1. Background

The PPP Scenario

1. After 9/11, the new threats to *public* and *private security* appeared much more dangerous and pervasive, but also much easier to be delivered, than before.

2. It was understood that the unique way to try to protect ourselves was that *public* and *private partner* together, with private giving → its <u>practical know how</u> and its <u>innovation capability</u> and public → its <u>guidelines</u> and <u>funding power</u>.

The Target

1. Each system needs an infrastructure to live. The most delicate ones are the Critical Infrastructures, especially if regard the Information and Communication backbone, vulnerable to Cyber Attacks directed to obtain Intelligence or Disruption. Their Protection is central to our Security.

2.Cyber Security /Cyber Intelligence is the focus of the current CIP Research, to prevent problems as :

a. STUXNET → an IT virus, of unknown origin, which jeopardized Iran nuclear program

b. IRHABI 007 → a British resident who assured the Al Qaeda logistics from London suburbs, detected through the Net monitoring

c. HACKING, PHISHING, IDENTITY THEFTS, MONEY LAUNDERING...

d. WikiLeaks case...

The New Approach

Protection of Critical Infrastructures against

disruptive attacks

but also against

Intelligence hidden operations...

...which may create more, and unexpected, danger.

The Speaker

Zanasi & Partners

Description

Advisory research company, specialized in PPP for security and intelligence research.
Founder background: Nuclear Engineer, Scientific Investigations Carabinieri Officer, IBM Researcher in USA and Executive in Europe, ESRAB and ESRIF member.

Clients

Leading security and information technology private companies, national and Int'l public institutions.

Among them:

- EUROPEAN UNION → European Commission (DGs: Justice, Freedom and Security; Enterprise) EC OLAF- Office pour la Lutte Anti Fraudes, EUROPOL (European Police), FRONTEX (Agency for Border Security, based in Warsaw)

- GOVERNMENT AGENCIES and MINISTRIES → Italy , Belgium, Balkans and Middle East

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

- HI TECH→ Siemens AG, TEMIS SA, Bridge129, Booz&Co, EURISPES…

2. EU Vision and Actions

European Union "*vision*" on PPP and Security Research

→ *Research and technology* can play a supporting role as a force enabler

→ Our Security can be assured only through int'l cooperation among EU (and also extra-EU) public and private organizations, taking into account civil rights safeguard and social sensibility

(from ESRAB final report and ESRIF findings)

ESRIF

European Security Research and Innovation Forum
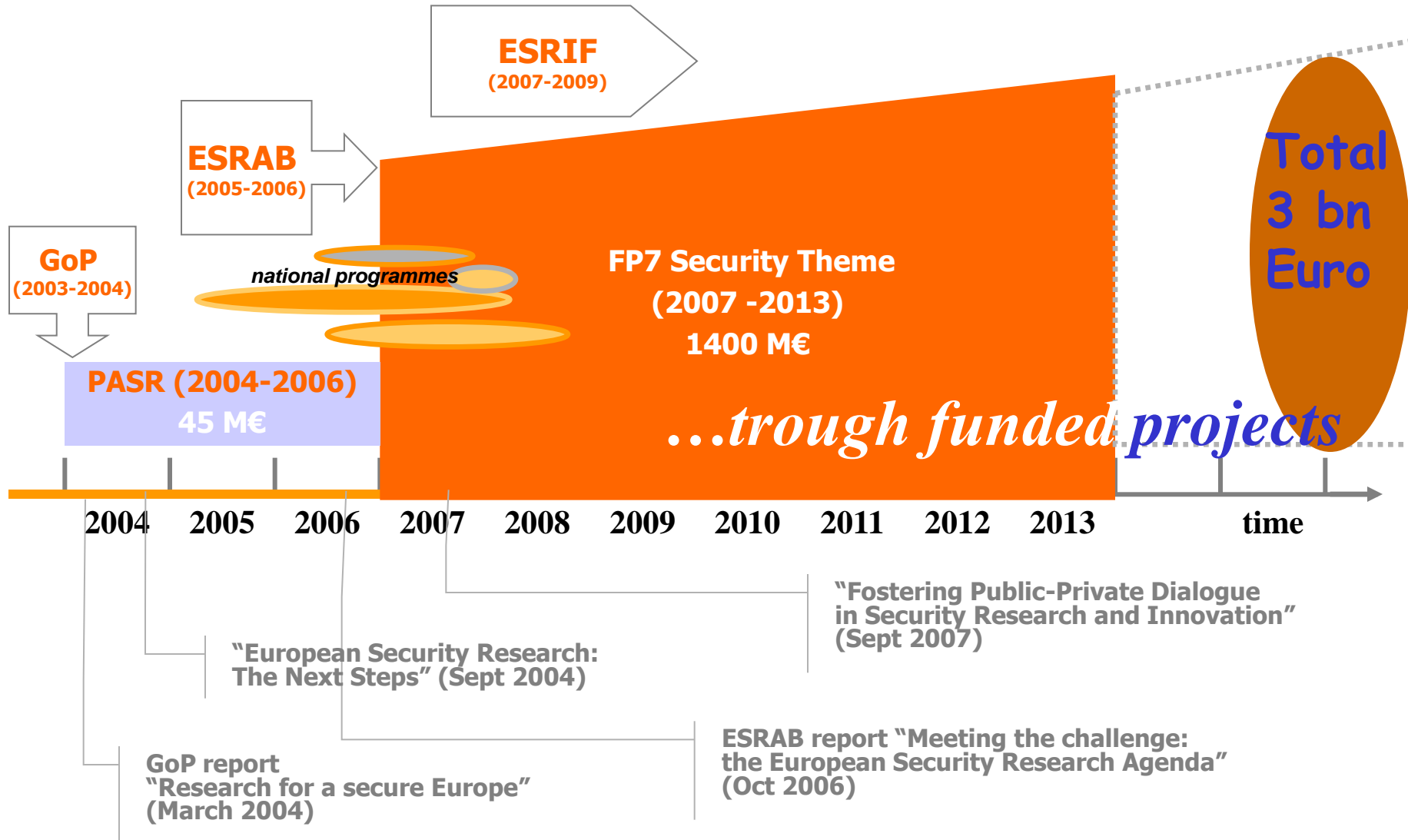### ...a PPP Committee !

- **64** members (27 EC Member States + Associates represented): strategists and experts from <u>European Security companies</u> (Eurisc, Thales, Finmeccanica, Eads, BAE, Sagem, Smiths ...and **Zanasi**), <u>government agencies</u> (Europol, BKA, EDA...) and <u>government ministeries</u> (Italian, French, UK Min. Interior; French, German, Italian Min. Defense, ...).

- <u>**Mission**</u>
  - **identify requirements for European Security Research**
  - **define** <u>security research funding lines</u> **and**
  - **advise on security research** *public private partnership*

President: Dragutin Mate (ex Minister of Interior of Slovenia)

European PPP actions in Security

PROTECTIA
INFRASTRUCTURILOR
CRITICE

ESRIF
(2007-2009)

ESRAB
(2005-2006)

GoP
(2003-2004)

national programmes

FP7 Security Theme
(2007 -2013)
1400 M€

PASR (2004-2006)
45 M€

Total 3 bn Euro

…trough funded projects

2004 2005 2006 2007 2008 2009 2010 2011 2012 2013   time

"Fostering Public-Private Dialogue
in Security Research and Innovation"
(Sept 2007)

"European Security Research:
The Next Steps" (Sept 2004)

ESRAB report "Meeting the challenge:
the European Security Research Agenda"
(Oct 2006)

GoP report
"Research for a secure Europe"
(March 2004)

3. EC Funded CIP Projects assure…

1

…Int'l PPP in EU but also outside EU…
(CH and NO but also USA, Israel but also Saudi Arabia)
*   to protect its CI…*

...in Financial Sector...

COMIFIN – Communication Middleware for Monitoring Financial Critical Infrastructure

Participant no. *	Participant organisation name	Part. short name	Country
1 (Coordinator)	ElsagDatamat S.p.A.	ED	Italy
2	Università di Roma	UoR	Italy
3	Technical Universitat of Darmstadt	TUD	Germany
4	IBM	IBM	Israel
5	Waterford Institute of Technology/TSSG	WIT	Ireland
6	Ministry of Economics and Finance	MEF	Italy
7	OptXware	OPT	Hungary
8	KreditTilsynet	KRD	Norway
9	University of Modena	UoM	Italy

Partners: 7 from EU...

2 extra EU

SECRET: SECurity of Railways against Electromagnetic aTtacks

Participant Number	Participant organisation name	Country
1(Coordinator)	Europe Recherche Transport	France
2	Institut National de Recherche sur les Transports et leur Sécurité	France
3	ALSTOM TRANSPORT S.A.	France
4	Fraunhofer Institute IAIS	Germany
5	Politecnico di Torino	Italy
6	SNCF	France
7	TRIALOG	France
8	UIC	International
9	University of Liege, Institut Montefiore	Belgium
10	University of the Basque Country	Spain
11	ZANASI Alessandro Srl	Italy

...for ICT Security...

CLOUDCERT –Testbed Framework to Exercise critical Infrastructure Protection

The scope of Cloud-CERT tool consist on improving **international security** and **coordination**, implementing an ICT system, together with adequate processes, that supports the **complete cycle of infrastructure protection**. It integrates industry strategic plans in an efficient manner and reuse components, methodologies, and tools leveraging CERT capabilities.
To this end, the tool is built on a framework of cooperation among **large companies** (INDRA), SMEs (ZANASI, e4business), **think tank** (ICSA), **public organizations** (INTECO, CNPIC) EU member states.

	Name of the Organisation	Country (official ISO 2 code) 2	City / Postcode	Profit-oriented	Partnership declaration
0	Applicant organisation/Coordinator :INTECO	ES	León/240 05	☐	-
	Co-beneficiaries :				
1	National Centre for Critical Infrastructure protection (CNPIC)	ES	Madrid	☐	☒
2	INDRA sistemas (INDRA)	ES	Madrid	☒	☒
3	Zanasi Alessandro SrL (ZANASI)	IT	Modena	☒	☒
4	Intelligence Culture and Strategic Analysis (ICSA)	IT	Rome	☐	☒
5	Europe for Bussiness Ltd (e4business)	UK	London	☒	☒

CRISYS - *Critical Response in Security and Safety Emergencies*

Participant no.	Participant organisation name	Abbreviation	Country
1	European Organisation for Security	EOS	BE
2	EDISOFT–Empresa de Serviços e Desenvolvimento de Software, S.A.	EDI	PT
3	Center for Security Studies, KEMEA	KEMEA	GR
4	National Center for Scientific Research "Demokritos"	NCSR	GR
5	ALTRAN BV Netherlands	ALT	NL
6	International Association of Fire and Rescue Services, CTIF	CTIF	GE
7	Teletron Euroricerche	TLT	IT
8	Compania Nationale de Transport al Energiei Electrice ,TRANSELECTRICA	TRA	RO
9	Société Française de Medicine de Catastrophe- SFMC	SFMC	FR
10	THALES Security Solutions and Services	THA	FR
11	INDRA Sistemas	IND	ES
12	Istituto Affari Internazionali, IAI	IAI	IT
13	University Central of Lancanshire	UCLI	UK
14	Finnish Ministry of the Interior, Department of Rescue Services	FMOI	FI
15	Zanasi Alessandro SRL	ZAN	IT

...with a strong Civil Society presence...

USERS ADVISORY BOARD - UAB

UAB No.	User Name	Country
1	FIRE SAFETY & RESCUE DIRECTORATE GENERAL – MINISTRY OF INTERIOR & NATIONAL GOVERNMENT	BULGARIA
2	LANCANSHIRE FIRE & RESCUE SERVICES	UK
3	RED CROSS	EU
4	WORLD ASSOCIATION FOR DISASTER & EMERGENCY MEDICINE, WADEM	US – International Organisation
5	MANCHESTER FIRE AND RESCUE SERVICE	UK
6	LIGA DOS BOMBEIROS PORGUESES	PORTUGAL
7	CIVIL CONTINGENCIES STAFFORDSHIRE COUNTY COUNCIL	UK
8	LISBON MUNICIPALITY CIVIL PROTECTION	PORTUGAL
9	FIRE AND RESCUE REGION, THE HAGUE COUNTY	NEDERLANDS
10	FIRE DEPARTMENT, AMSTERDAM	NEDERLANDS
11	AMSTELLAND, SAFETY REGION OF AMSTERDAM	NEDERLANDS
12	ITALIAN CORPO FORESTALE DELLO STATO	ITALY
13	NATIONAL TECHNICAL CENTRE FOR FIRE PROTECTION & PUBLIC SECURITY	ALBANIA
14	EUROPEAN EMERGENCY NUMBER ASSOCIATION, EENA	BELGIUM
15	DOCUMENTATION AND CORPORATE CULTURE, FALCK HUSET	DENMARK
16	Haut Comité François pour la Défence Civile, HCFDC	FRANCE
17	CIVIL CONTINGECIES SCOTLAND	UK
18	EURISC/ European Institute for Risk, Security and Communication Management	ROMANIA
19	Asociación Empresas de Tecnologías de la Información y Comunicaciones de España, AETIC	SPAIN

2

…but also research in Intelligence for Critical Infrastructure…. realizing…

Theme 10: Security
Topic FP7-SEC-2009-1

Proposal full title: Versatile InfoRmation Toolkit for end-Users oriented Open-Sources explOitation

Proposal acronym: **VIRTUOSO**

VIRTUOSO – Versatile Information Toolkit for End Users Oriented Open Sources Explotation

Partners:

9 EU...

...1 extraEU

Participant no.	Participant organization name	Participant organization name	Country
	Members of the project team		
1 (Coordinator)	Commissariat à l'Energie Atomique	CEA	FR
2	EADS Defence and Security Systems	EADS	FR
3	ATOS ORIGIN SAE	ATOS	SP
4	MONDECA	MON	FR
5	Newstin a.s.	NWT	CZ
6	SAIL LABS TechnologyAG	SAILLABS	AU
7	Aalborg Universitet	AAU	DN
8	THALES Communications S.A.	THALES	FR
9	Bertin Technologies	BERTIN	FR
10	Stichting Katholieke Universiteit Brabant	TILT	NL
11	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek	TNO	NL
12	Ingeniera de Sistemas para la defensa de Espana	ISDEFE	SP
13	EUROSINT Forum ASBL	EUROSINT	BE
14	Hawk Associates Limited	HAWK	UK
15	ETH Zurich	ETHZ	CH
16	Compagnie Européenne d'Intelligence Stratégique	CEIS	FR
17	Università di Modena e Reggio Emilia	CRIS/UOM	IT
18	Columba Global Systems Ltd	COLUMBA	IE

...intelligent video monitoring...

THIS-**Transport** Hub Intelligent video System

The project addresses **automatic behavioral analysis** through video processing, focused on crowded scenarios, for transportation hubs. New **video surveillance** systems provide moving object detection and people tracking (e.g. for abandoned pack detection) but the monitoring task is all in charge of human inspectors. A system performing human behavioral analysis, detaching what is usual from what is not, would fill the gap and provide a reactive, and hopefully pro-active control task, **preventing terroristic attacks** or crime situations in public pla...

	Name of the Partner Organisation	Country (official ISO 2 code) 2	City
0	Applicant/Co-ordinator: CRIS	IT	Modena
	Partners/Co-beneficiaries of the grant:		
1	Hungarian Academy of Sciences (MTA-SZTAKI)	HU	Budapest
2	Technical University of Catalunya (UPC)	ES	Barcelona
3	Bridge 129 (BRIDGE)	IT	Reggio Emilia
4	Vitrociset (VITROCISET)	IT	Roma
5	Zanasi s.r.l. (ZANASI)	IT	Modena
6	Research and Education Laboratory in Information Tech. (AIT)	GR	Athens

RECOBIA: REduction of COgnitive BIAses

Participant Number	Participant Organisation Name	Short Name	Country
1 (Coordinator)	COMPAGNIE EUROPEENNE D'INTELLIGENCE STRATEGIQUE	CEIS	FR
2	HAWK ASSOCIATES LIMITED	HAWK	UK
3	THALES	THALES	FR
4	ATOSORIGIN	ATOS	ES
5	COMMISSARIAT A L' ENERGIE ATOMIQUE	CEA	FR
6	ISEA PSY	ISEA	FR
7	EUROSINT FORUM ASBL	EUROSINT	BE
8	ZANASI ALESSANDRO SRL	ZANASI	IT
9	UNIVERSITAT KONSTANZ	UKON	DE
10	GRAZ UNIVERSITY OF TECHNOLOGY	TUG	AT

Thanks for your attention

Alessandro.Zanasi@zanasi-alessandro.eu