



# EUROWAYS

## Outlining the future: Programmes and Research for Security of Institutional Communications

VI Forum Aerospaziale 2004, 15 Ottobre 2004 Centro Congressi Ville Ponti



# Information and communication networks for Critical Institutional Infrastructures are dynamic and evolvable

- Government (e- Government), Law enforcement
- Emergencies services (*Civil protection, Humanitarian Aid*)
- Energy and water distribution, Transportation (*land, sea and air*)
- Others (Health, banking, industrials, nuclear ...)

IT systems involved

- ✓ Public, private and government
- ✓ Terrestrial networks, satellite networks
- ✓ Wireless networks, fixed networks
- ✓ Civil networks, Public Safety networks

Utilities systems (electricity, water supply), Transportation facilities

Networks for (cyber) commerce & business

## Require Security, Resilience and Dependability

- Protecting the information infrastructure, and their use protecting the other infrastructures



# Information and communications Requirements

:

- Interoperability and integration of systems for information and communication
- Secure communication and information networks
- Development of concepts for meta information applied to Geographical Information Systems
- Advanced space technologies to support security operations (Galileo, Cosmo-Skymed...)
- To meet the dependability and security for unbounded information and communication networks



## Relevant issues for R&T project/programs on communication security

- Threat analysis, risk assessment and vulnerability of communication networks. *Should be considered also terroristic attack*
- Standardized methodologies and decision tools for assessing the nature of the potential threat (*both electronic or physical*) to critical networked infrastructures and to assess the respective vulnerabilities
- Assessment of space assets and infrastructure for security information systems
- Detection, prevention, response and alert capabilities to strengthen information and control systems



# Toward an European Critical Information Systems and Communications Services

## The Mission

- The Institutional critical activities must be immune to physical or cyber threats onto their ICT applications and depends on disaster-proof backup systems.
  - *to be able to adapt to negative and largely unexpected events and conditions*

## The Approach

- The survivability of networks supporting Institutional critical applications and communications services is financially and operationally accepted.
- Secure the underlying networks infrastructure at a reasonable cost, with acceptable constraints for the commercial, governmental and industrial organisations
- With focus on designing and realising backup services for disaster situation



## Overview of Security Research activities to enhance the level of security of information and communication networks

- Identify the mission-critical applications and associated networks and services
- Define the target level of dependability (reliability and security)
- Improve level of resilience achieved by federation of existing networks
  - *Share of assets by competing commercial networks to guarantee*
    - *Improved connectivity (cable, fiber, radio links...)*
    - *Guaranteed access, Resource Reservation, Integrity,*
    - *End to end propagation of privileged Class of Service*
- Improve level of security reached by optimised use of security IT technologies applied on existing networks
- Intrusion & Anomaly detection, Network cartography, counter-measures against attacks
- Improve standardised methodologies to assess vulnerabilities and threats



## Overview of Security Research activities to enhance the level of security of information and communication networks (Cont./2)

- Identify the additional European-wide services to be offered:
  - trusted broadcast, priority access, disaster-proof links
- Identify the appropriate actions to tackle the threats
  - detection, prevention, response, alert
  - Nature of attacks : IT Attacks, Physical Attacks, Electro Magnetic Pulse, Jamming ( Intrusion and data manipulation, Denial of services (overload of network), Virus, Trojan & Spy software, Non authorised access, "Human errors", electromagnetic radiation, physical destruction ...)
  - “Detection” requires the use of suitable sensors
  - “Response” improve the security level in presence of Physical Attack and EMP; allow operations in presence of jamming



## Overview of Security Research activities to enhance the level of security of information and communication networks (Cont./3)

- Grand public & administrations: Encourage a long-term security behaviour Initiatives, education, exercises
- National governments and EU: European-wide regulations
- Challenge and opportunity from GMES and Galileo, (the two major European Space Programs):

*“combining spatial and terrestrial data in a secure and integrated operational information system accessible to all networked Institutional User Communities in synergy with different kind of services provision (telecommunication, transportation, surveillance, observation etc.) “*