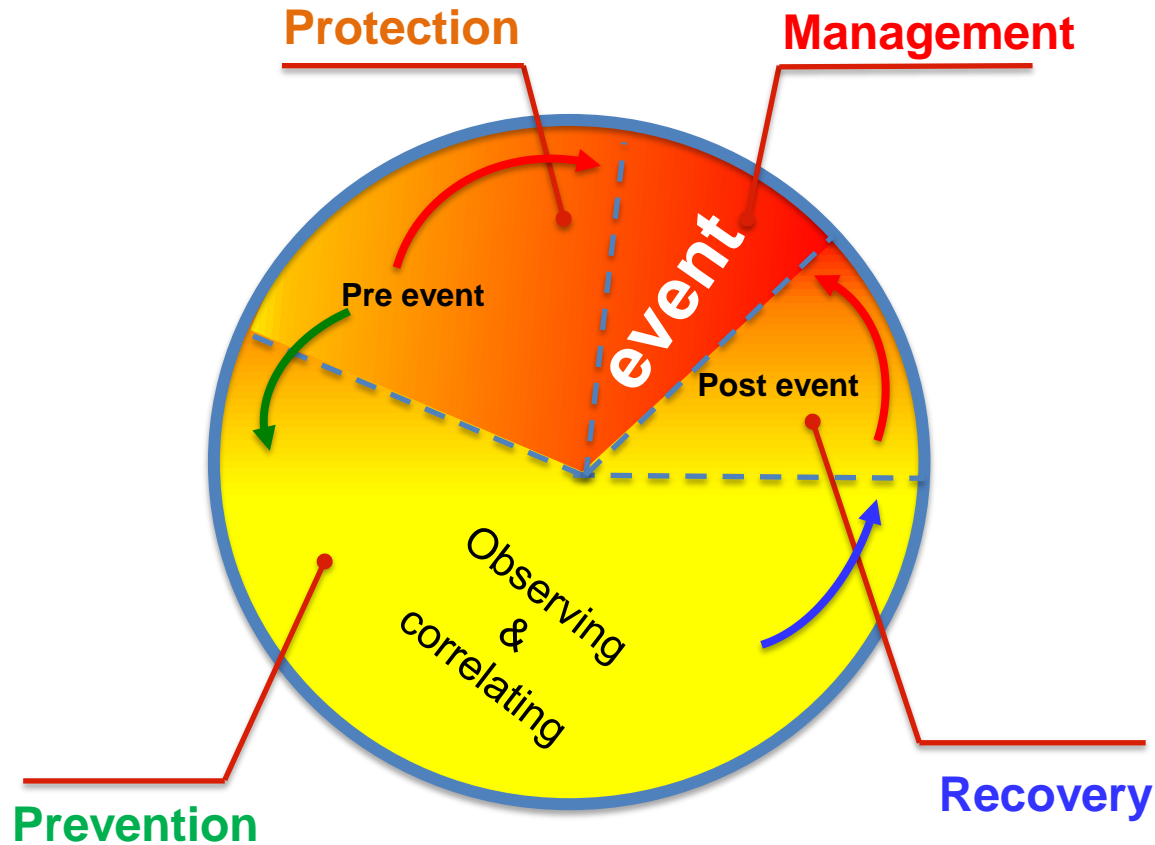# Leonardo @ Comunicazioni radio per la sicurezza
Il punto sulle reti mission critical

Giorgio Mosca – SVP Strategy & Technology– Cyber Security Division
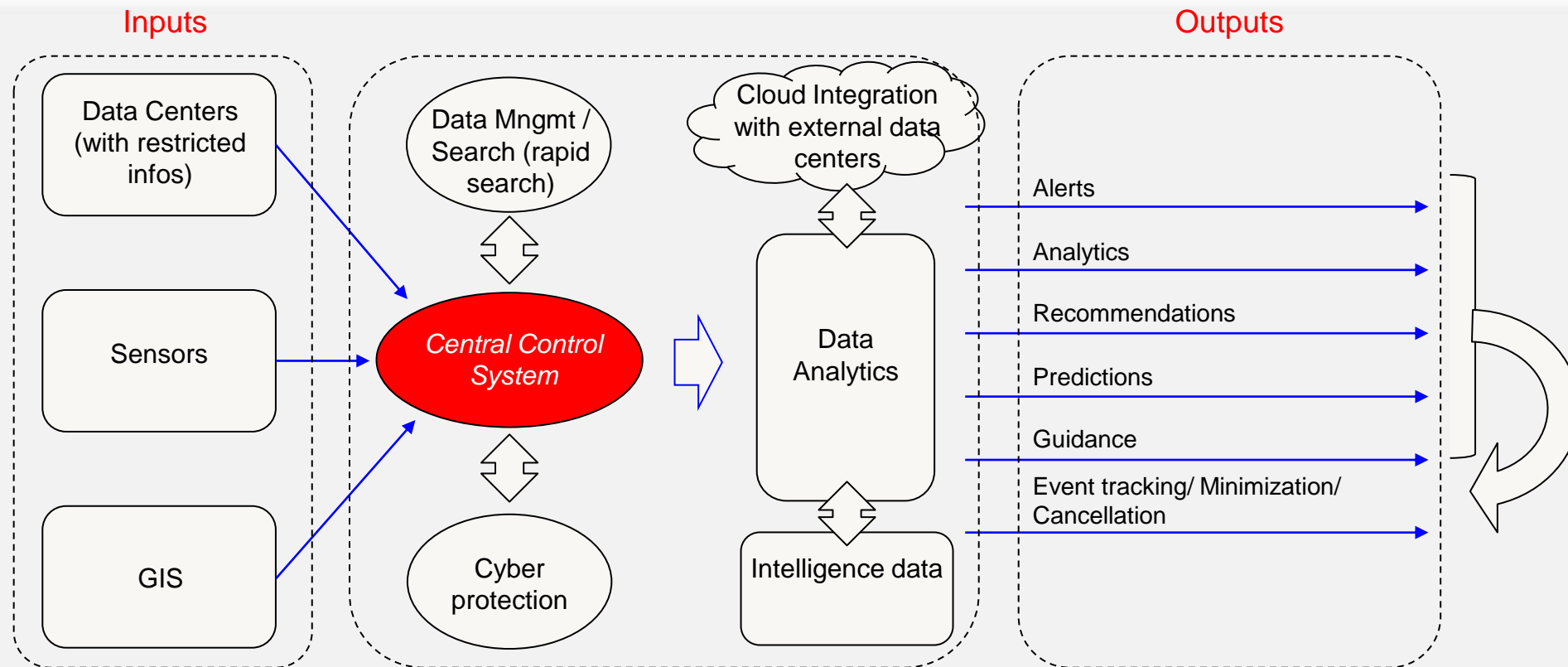
Milano, 08 aprile 2019

TECHNOLOGICAL SUPPORT

- **Prevention** – sensors, threat intelligence and advanced analytics allow better readiness

- **Protection** – integrated physical and logical security mitigate events' likelihood

- **Management** – impact and duration is reduced through better operations

- **Recovery** – support to resilience allows reduction of recovery time

Company General Use

TECHNOLOGICAL SUPPORT

Inputs

Outputs

Data Centers (with restricted infos)

Sensors

GIS

Data Mngmt / Search (rapid search)

Central Control System

Cyber protection

Cloud Integration with external data centers

Data Analytics

Intelligence data

Alerts

Analytics

Recommendations

Predictions

Guidance

Event tracking/ Minimization/ Cancellation

Integration and minimization - up to cancellation - of Critical Event

Source: consulting report on security market dynamics

MISSION CRITICAL TECHNOLOGICAL SUPPORT

- High Availability
- High Usability
- Coverage
- Priority & emergency calls
- Group call
- Coordination and field supervision
- Secure and protected operations
- Specialized terminals

Company General Use
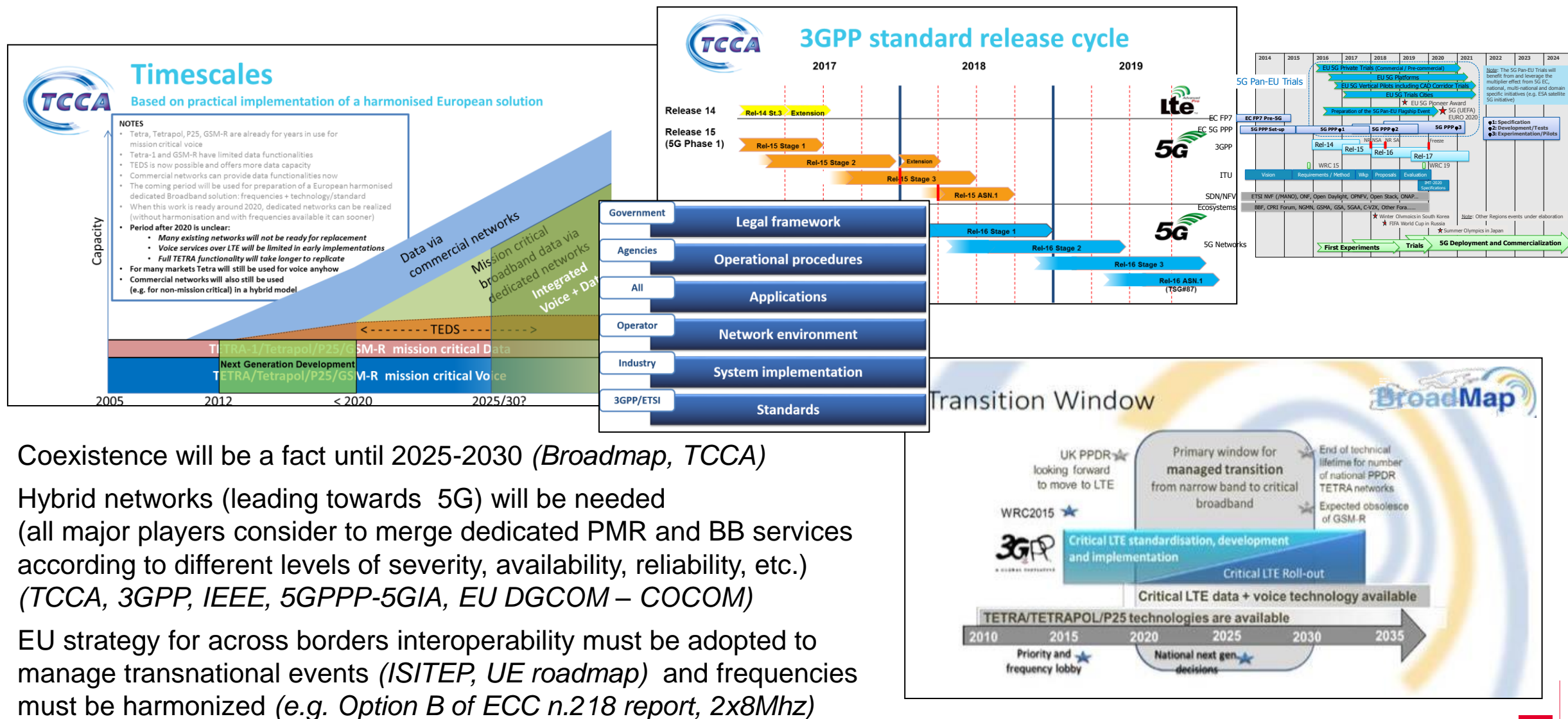
MISSION CRITICAL TECHNOLOGICAL SUPPORT

- High Availability → Particularly in disaster events
- High Usability → Voice quality / best effort data
- Coverage → Also in areas with low commercial value
- Priority & emergency calls → Available bandwidth & Preemption
- Group call → Allow heterogenous distribution of users
- Coordination and field supervision → Analytics / Control Rooms
- Secure and protected operations → Cyber protection / resilience
- Specialized terminals → vs. General purpose Devices

MISSION CRITICAL PARTNER

- High Availability → Service Partner (full service on Tetra network)
- High Usability → Hybrid Network with MC Core
- Coverage → Hybrid Network + Deployable
- Priority & emergency calls → QoS, PTT + MCPTT
- Group call → Interworking, MC services
- Coordination and field supervision → Integrated Control Rooms
- Secure and protected operations → Users DB, SIMs, Cyber & NW protection
- Specialized terminals → BoB + Specialized applications

The COMMS SCENARIO: a Public & Private effort…

- Coexistence will be a fact until 2025-2030 *(Broadmap, TCCA)*

- Hybrid networks (leading towards 5G) will be needed
  (all major players consider to merge dedicated PMR and BB services
  according to different levels of severity, availability, reliability, etc.)
  (TCCA, 3GPP, IEEE, 5GPPP-5GIA, EU DGCOM – COCOM)

- EU strategy for across borders interoperability must be adopted to
  manage transnational events *(ISITEP, UE roadmap)* and frequencies
  must be harmonized *(e.g. Option B of ECC n.218 report, 2x8Mhz)*

Giorgio Mosca

Sr. Vice President Strategy & Technologies

Cyber Security Division, Leonardo

THANK **YOU** FOR YOUR ATTENTION