Capitalizing the opportunity to learn about the latest advances in ESM

Daniela Pistoia, Company Chief Scientist
Head of Product Innovation & Advanced EW Systems

"FUTURE J-ISR" WORKSHOP - CASD - 10.10.2013

MIND IS THE FIRST DEFENCE

PROPRIETARY NOTICE
The information contained in this document is the property of ELETTRONICA S.p.A. Use of this information is limited to that for which it is supplied and may not be disclosed to any Third Party without the express written permission of ELETTRONICA S.p.A..

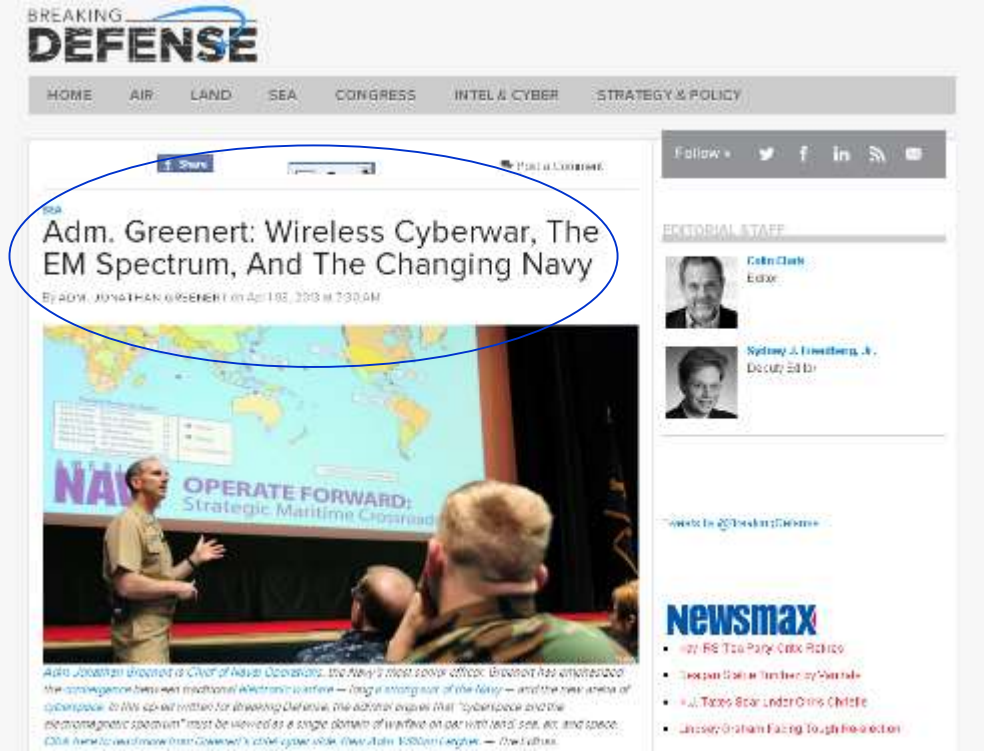
OUTLINE

- *The “21st century warfare” context*
- *Information Environment*
- *EM spectrum control in military operations*
- *ELT’s vision on future EW requirements*
- *New challenges for SIGINT & COMINT*
- *Integrated EM spectrum surveillance and cyber intelligence: the LOKI platform*
- *Conclusions*

The “21st century warfare” context

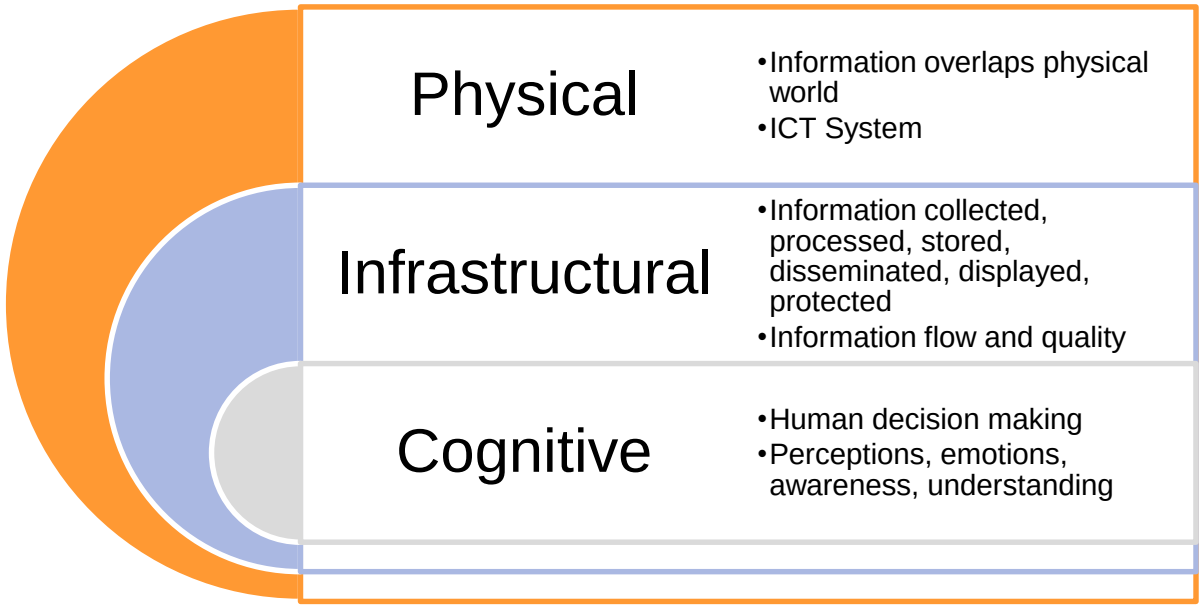
"In the next two decades, the [electromagnetic] environment may become our most critical warfighting arena.
Control of information -- much of it through the EM spectrum -- is already growing more important than control of territory in modern warfare.“

ADM Jonathan Greenert, CNO US Navy, October 2011



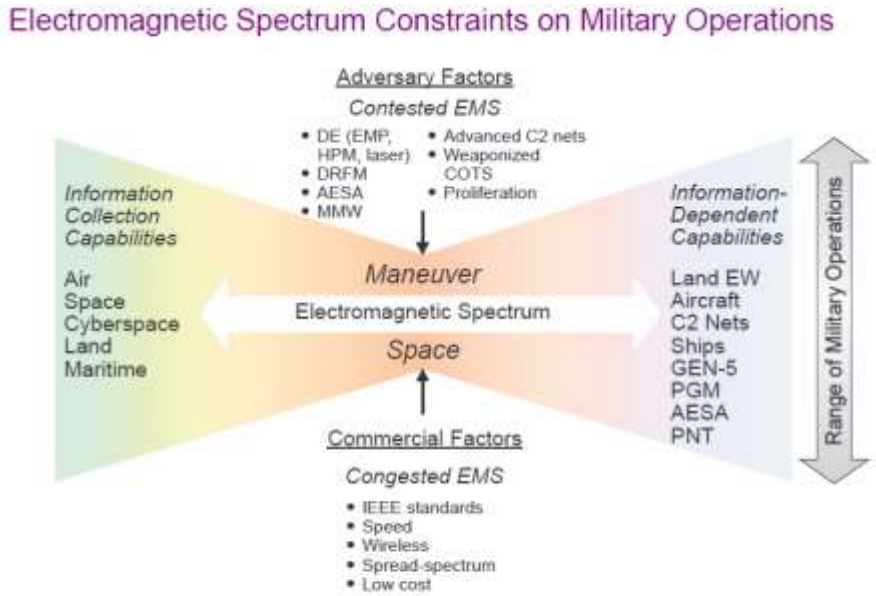
Information Environment

- **Information is consumed by the public, civil and military organizations**
- **Information systems are essential to ISR operations**
- **Information systems use the Electro Magnetic Spectrum (EMS) to communicate**
- **Information warfare evolution: cyberspace is the new battlefield for signal intelligence and psychological operations**



Electro-Magnetic spectrum control in military operations

- **EM spectrum control enables freedom of action in Military operations across all domains (land, sea, air, space and cyberspace) and throughout all phases of operations**
- **EMS control is essential to each of the warfighting functions: Intelligence, Fires, Command & Control, Manouver, Logistics, Force Protection**
- **The military's EMS maneuver space is more and more constrained by factors (weaponized COTS technologies fielded by adversaries, commercial standards, policies, and manufacturing decisions of a globalized industry)**



Legend

AESA	active electronically scanned array	GEN-5	generation-five
C2	command and control	HPM	high-power microwave
COTS	commercial off-the-shelf	IEEE	Institute of Electrical and Electronics Engineers
DE	directed energy	MMW	millimeter wave
DRFM	digital radio frequency memory	PGM	precision-guided munition
EMP	electromagnetic pulse	PNT	positioning, navigation, and timing
EMS	electromagnetic spectrum		
EW	electronic warfare		

Source: DoD JP06-01

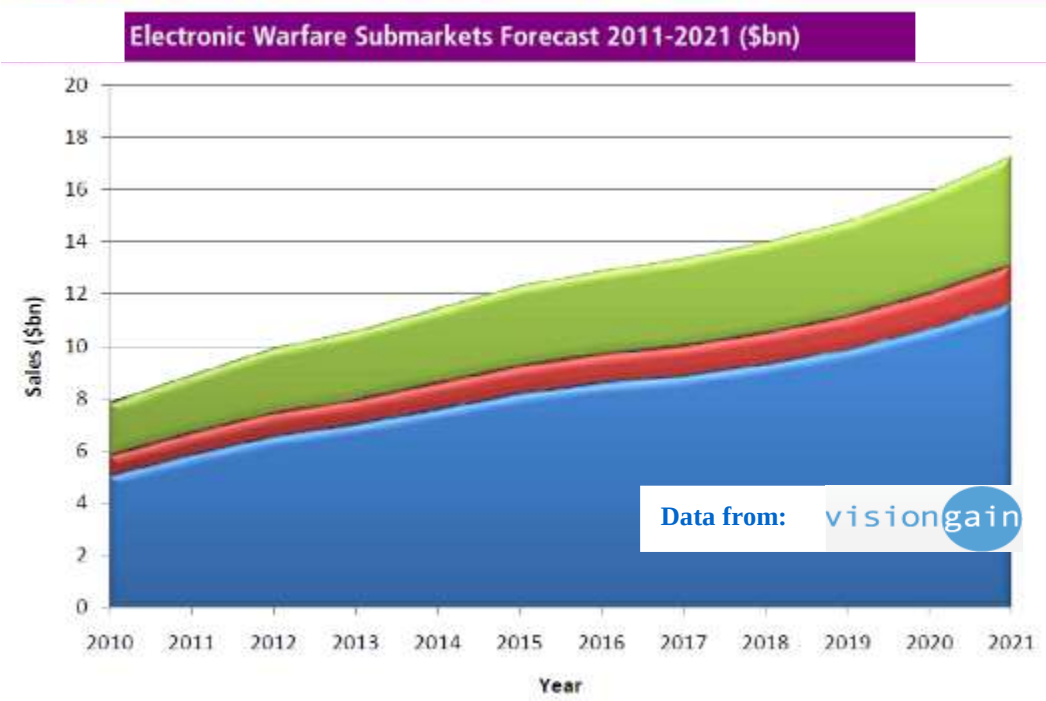
Operations in the EM Spectrum

- We need to defend military (coalition) and civil use of spectrum
  - Enabling defensive operations
  - Protecting beneficial economic activity
  - Protecting critical infrastructure
  - Reducing vulnerabilities
- We may need to generate EM effects
  - to intervene against adversaries
  - to reduce adversary capability
  - to deploy messages into cyber space
- We need integrated situational awareness in the cyber and human domains
  - Including EM spectrum

- In a world that is becoming both wholly connected and increasingly mobile, EMS is a primary enabler for future military, economic, and social development

ELT vision of EW trends

- Electronic Warfare (EW) is becoming important beyond the sphere of the Military Ops
- Network Centric Warfare (NCW) paradigm: it introduces new level of EW capability in terms of cooperation and synchronization of active (e.g. ECM) and passive EW systems (e.g. ESM, SIGINT), providing unprecedented C2 response and EW mission success
- EMS surveillance is also a vital aspect of the full national security issues. Therefore it will record positive growth rates for the next years



Electronic Attack (EA): radar jamming (ECM), flares and decoys, electromagnetic deception, directed energy (DE), anti-radiation missiles (ARMs), RC-IED.

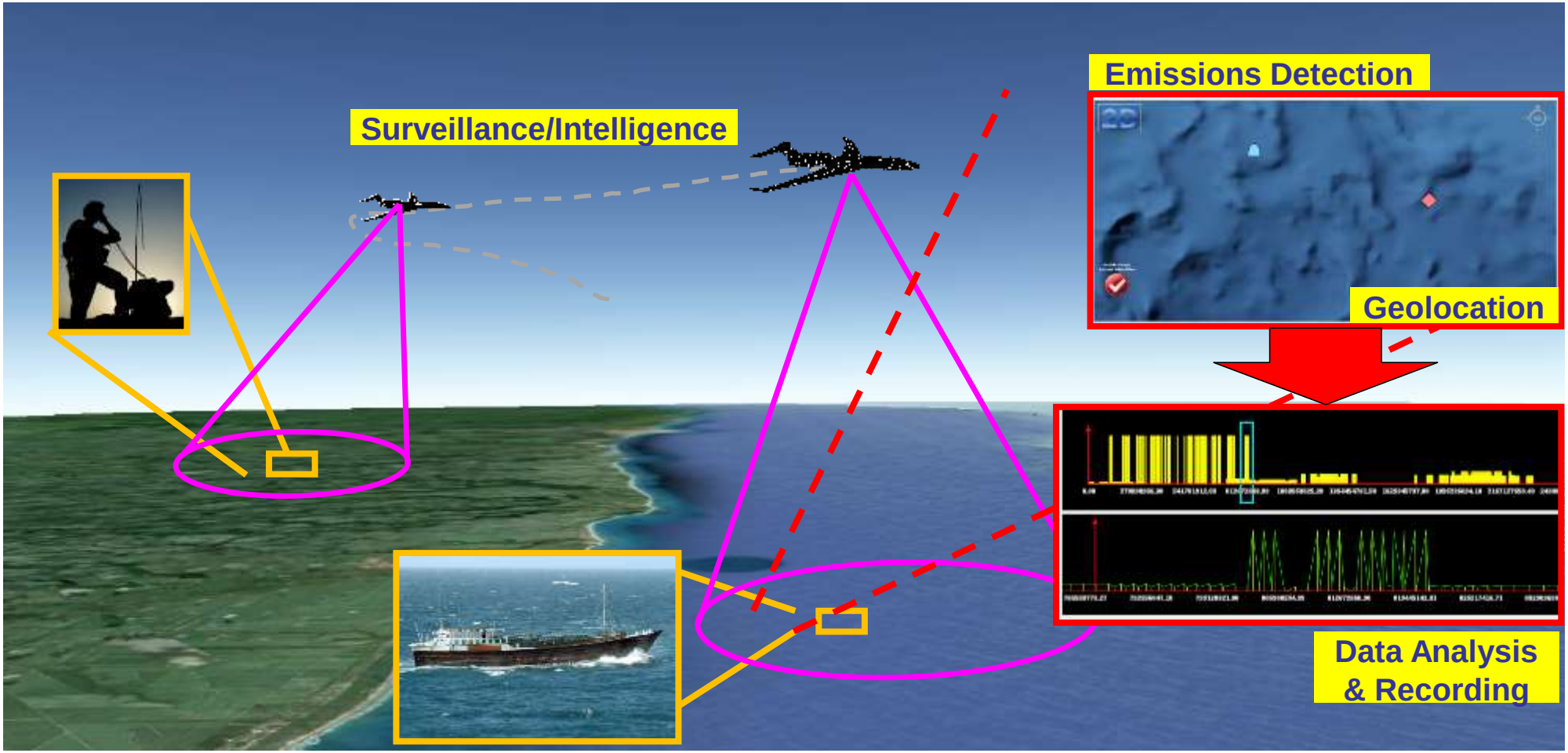
Electronic Protection (EP): spectrum management, electromagnetic hardening, emission control (EMCON)

Electronic Warfare Support (ES): detect, identify and locate sources of electromagnetic signals. ES include: electronic reconnaissance, electronic intelligence (ELINT) and electronics security

Some fundamental elements of future ELT's EW systems

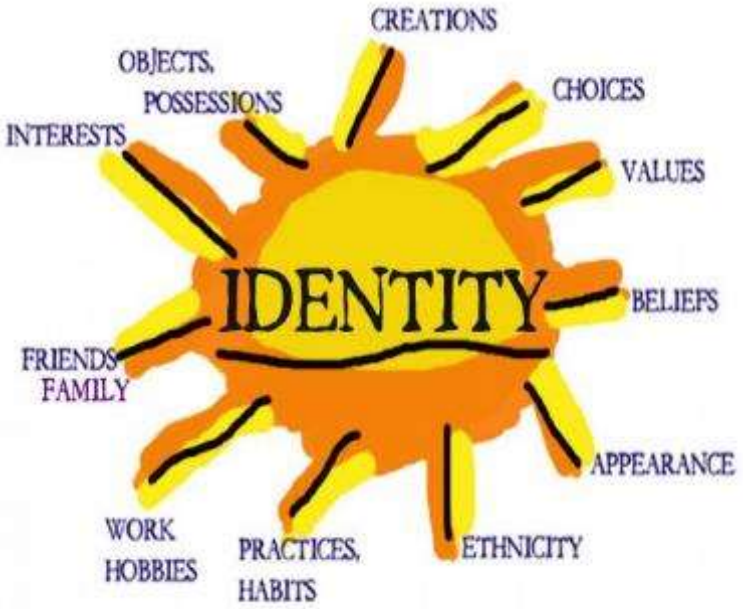
CAPABILITIES	OBJECTIVES
■ *MULTISPECTRAL*	Maximize EW spectrum coverage (EO-IR-RF-mmW) and minimize spectral gaps that can be exploited by the enemy
■ *DISTRIBUTED*	Maximize EW Spatial Coverage with a minimum of resources accepting single point failure
■ *COORDINATED*	Maximize effectiveness of EW across: on/off board systems, manned/unmanned platforms, avionic/ground/naval resources
■ *ADAPTIVE*	Maximize flexibility in responding to the new generation of emitters

SIGINT mission



COMINT mission (?)

Evolution of Communication Intelligence activities



A new “bad guy” in Information Environment: the cyber attack

- **Security becomes a crucial aspect in networked systems. Adversaries can exploit vulnerabilities of the network to blind systems, acquire information or insert fake information**

- **Any modern military platform will be a sensors’ network, interconnected to other networks; cyber security issues have to be taken into account since the early design phase of the distributed systems**

- **<u>EM Spectrum must be protected because it can be used to carry cyber attack</u>**

Operation “Orchard” - 2007

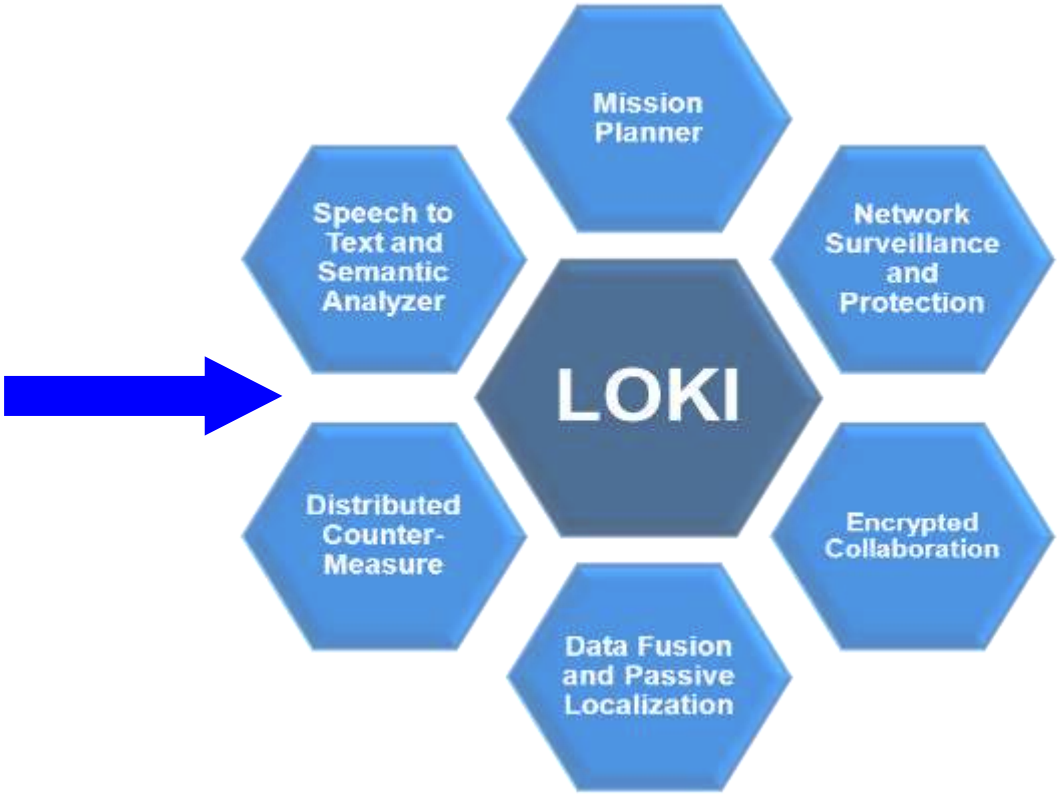
EM spectrum surveillance & Cyber intelligence integration

- The protection of information and ability to guarantee its transport though cyberspace are essential for military operations
- In the past, voice and data networks operated separately, but the convergence of these technologies has brought them together, enabling the delivery of multiple forms of media – text, audio, video – over the same wired, wireless, or fiber-optic infrastructures of the internet
- While providing great opportunity for increased effectiveness, technological convergence also introduces tremendous vulnerabilities
- In the cyber/electromagnetic contest, significant advantage will go to whom is able to gain, protect, and exploit advantages in the highly contested cyberspace domain and electromagnetic spectrum

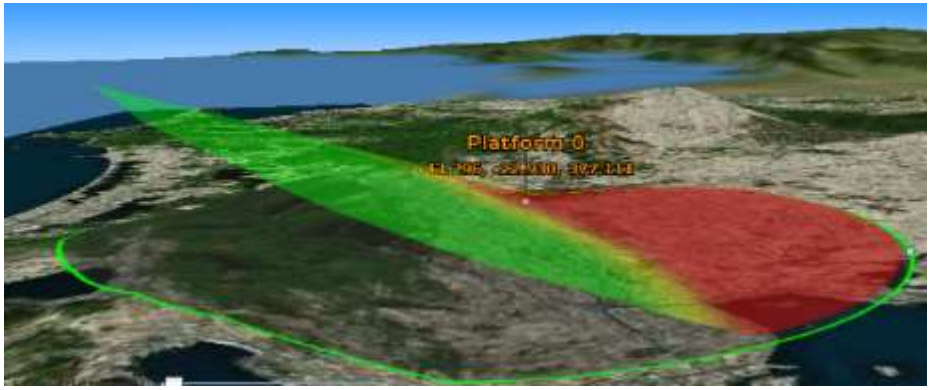
ELT "LOKI"

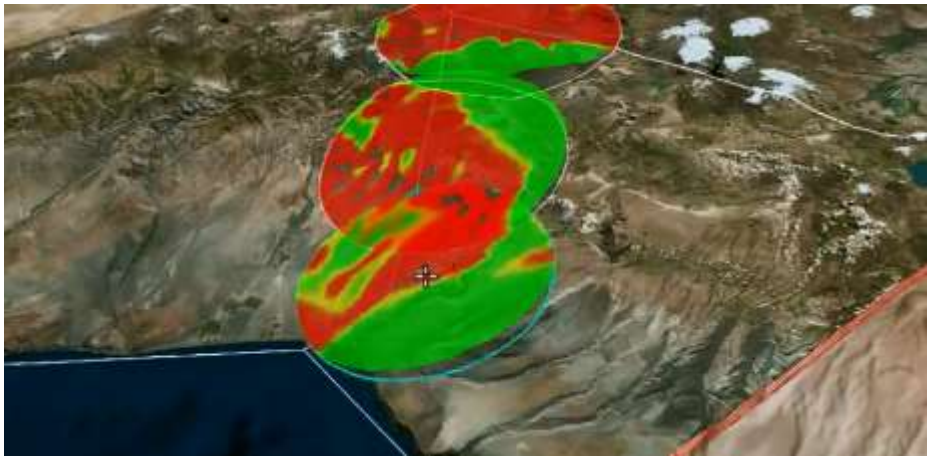
- Network Command & Control Integrated Situational Awareness Capability
  - Provide improved cyber situation awareness
  - Provide improved incident detection and prioritization
  - Provide improved network and computer sensor integration
  - Provide improved joint information sharing (interoperability) with Allies and Other Government Departments

The LOKI platform



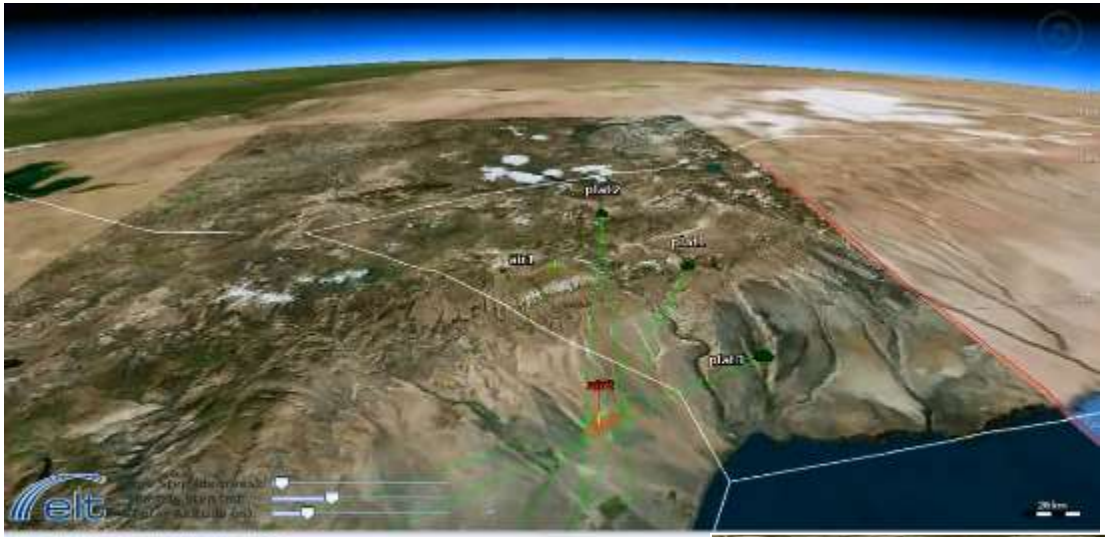
LOKI: mission planning

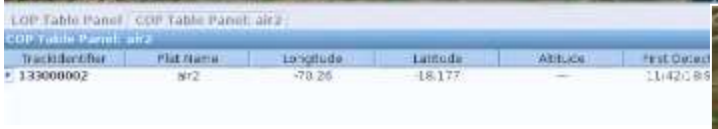


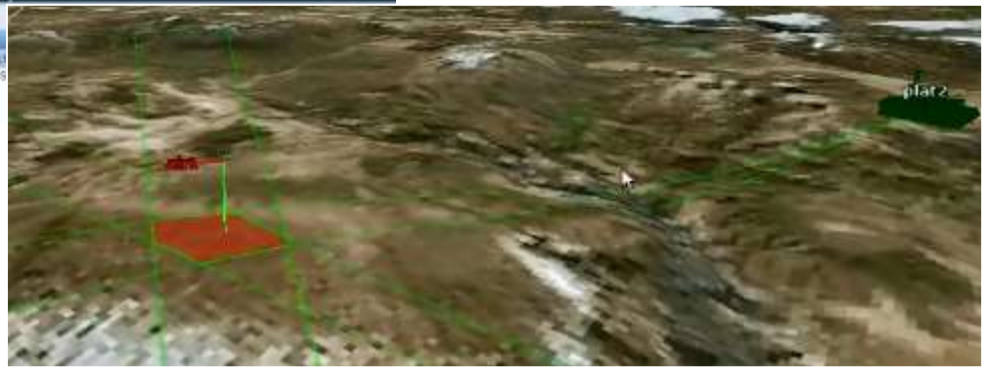


- ***What is the most effective arrangement in space and RF for the available sensors to properly cover a desired area and frequency range in order to:***
  - **Maximize Monitored Area**
  - **Maximize the probability of interception**
  - **Maximize the probability of triangulation**
  - **Reduce interference among sensors**
  - **Be close enough to achievable roads**
  - **Be connectable via radio links**

LOKI: passive localization

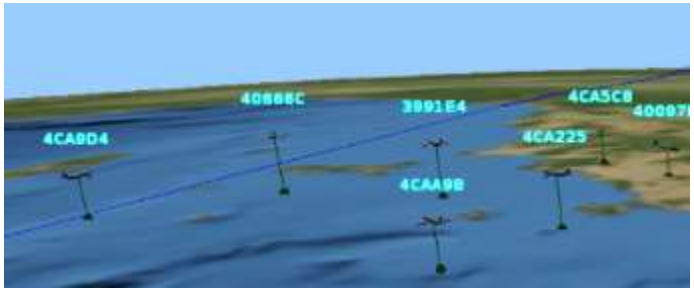


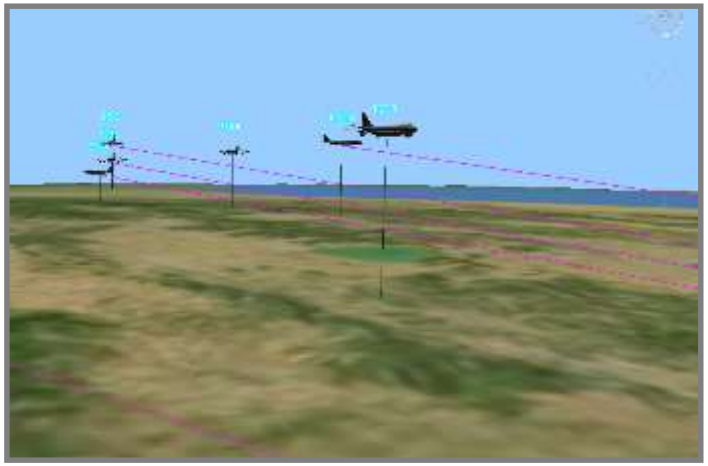


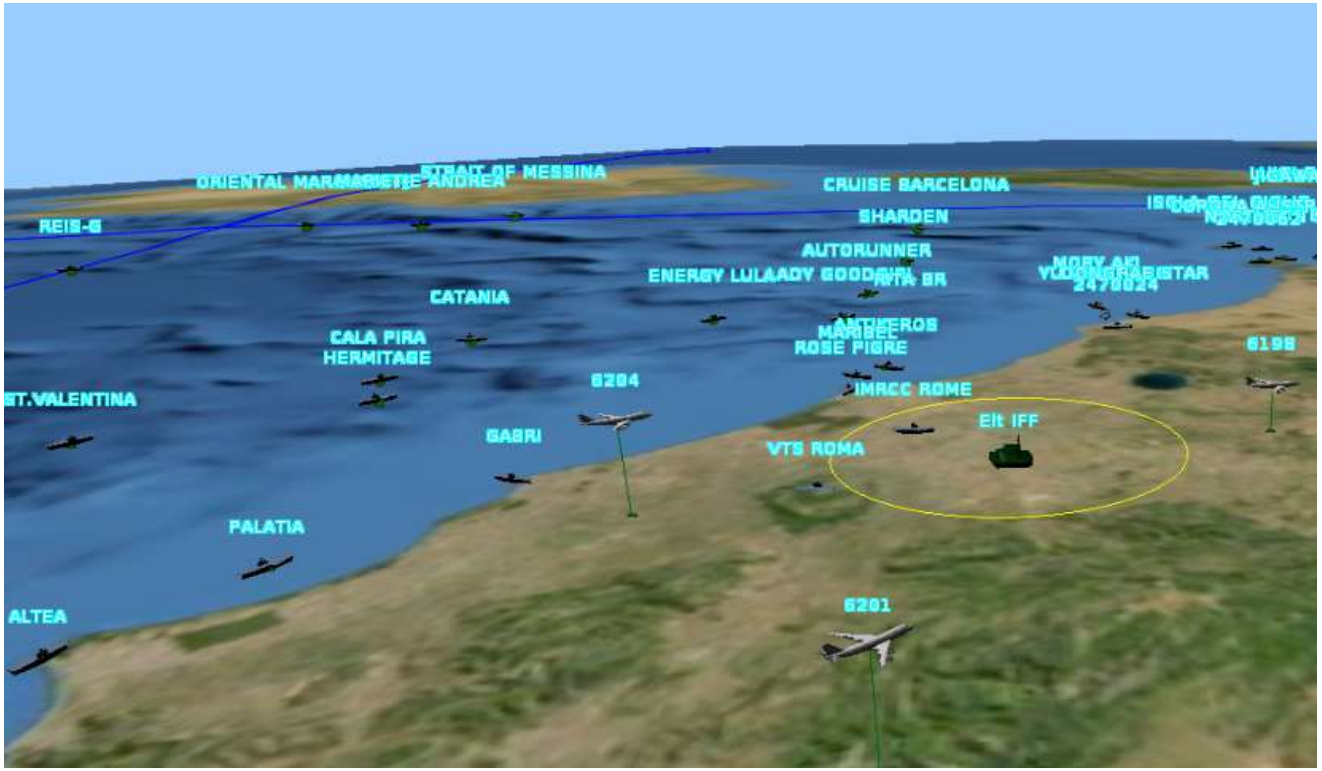


Passive localization, enabled by the continuous sharing of information among the cooperating platforms, can be continuously performed by means of triangulation and periodically improved via multilateration

LOKI: AIS, IFF and CESM integration







LOKI: decision support functions/1

- In a information warfare scenario, operators will probably be overwhelmed by an enormous amount of information
- Taking decisions based only on raw data would be probably infeasible
- Moreover, stressful situation can affect decision taken by operators and worst scenarios may appear
- Decision support functions have the task to help operator in understanding data and taking decision in a more easy way
- They are based mainly on Artificial Intelligence techniques and on the use of knowledge ontology, built from previous missions/experiences

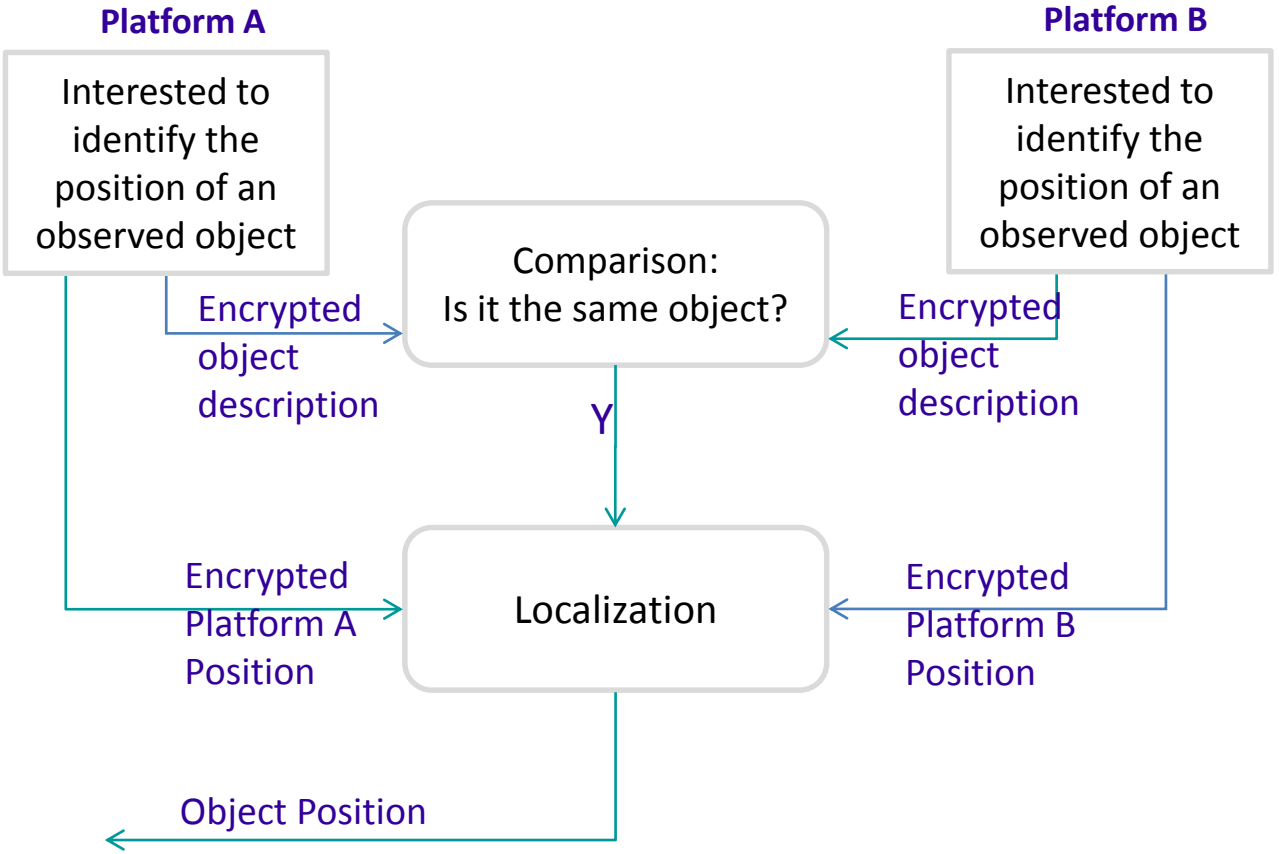
LOKI: decision support functions/2

- For example, in this case we have a chaotic scenario with a lot of platforms on the screen (different types)
- Our system, having at disposal different features for each platform (e.g., type, speed, trajectory) has decided to issue a warning for the circled platform: this platform, a foreign fishing boat, is too close the Italian coast
- The system warns the operator to have a closer look: it could be a clumsy fisher or maybe some real threat

LOKI: encrypted collaboration in joint military operations

- Nowadays Joint Operations involve many Armies from different countries
- These forces are often asked to share their data in order to mazimize the effectiveness of military operations
- Secure Information Sharing:
  - perceived threats
  - objects positions and characteristics
- Secure Threat Identification:
  - Identify threats exploiting partners libraries without accessing them
- Secure Threat Localization:
  - Comparing partners threat data to improve localization

Encrypted collaboration: example



Cyber & Network Centric Operations Lab @ ELT

Conclusions

- ***Control of information, much of it through the EM spectrum, is already more important than control of territory in modern warfare***
- ***We assist to the Information Warfare evolution: cyberspace is the new battlefield for signal intelligence and psychological operations***
- ***EW is becoming a vital asset for Military Operations***
- ***Information Warfare, Cyber Warfare and Electronic Warfare are intermingled: some events have confirmed this concept***
- ***In the cyber/electromagnetic contest, significant advantage will go to whom is able to gain, protect, and exploit advantages in the highly contested cyberspace domain and electromagnetic spectrum***
- ***ELT provides state-of-the-art ESM sensors and EW-C2 platform, integrating EM spectrum surveillance and Cyber intelligence: LOKI***

Thank You for Your Attention!

Q&A