INTERNATIONAL CONFERENCE

ARTIFICIAL INTELLIGENCE AND CYBER SECURITY IN CIVIL AND MILITARY AVIATION

Virtute Siderum tenus

FLIGHT SAFETY FOUNDATION MEDITERRANEAN
"Never take safety for granted"

Κυπριακή Δημοκρατία

EATEO
European Association of Aviation Training and Educational Organisations

ICT SERVICE PROVIDER

3ª DIVISIONE

AGENDA

Context

Information Security

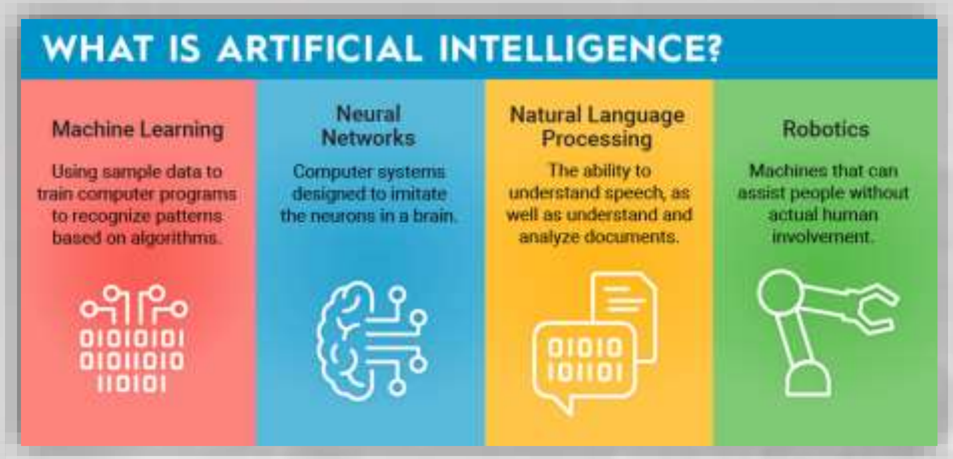
A.I. in Military World & CyberSec

Use case: UAV in cyber domain

Training

Context

Artificial Intelligence



WHAT IS ARTIFICIAL INTELLIGENCE?

Machine Learning
Using sample data to train computer programs to recognize patterns based on algorithms.

Neural Networks
Computer systems designed to imitate the neurons in a brain.

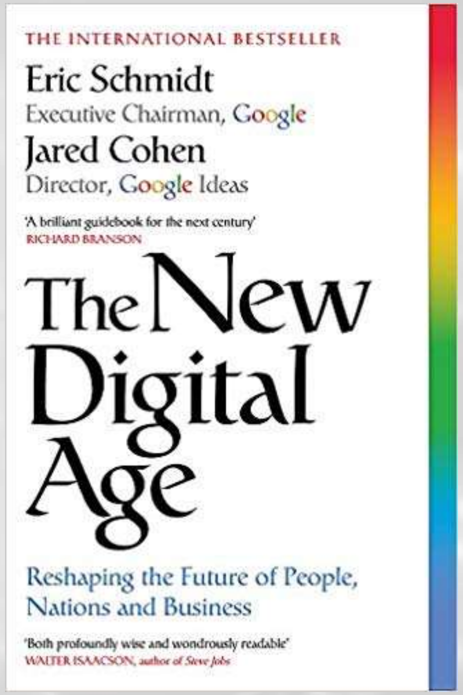
Natural Language Processing
The ability to understand speech, as well as understand and analyze documents.

Robotics
Machines that can assist people without actual human involvement.

Cyber Security

Military Aviation

Context



THE INTERNATIONAL BESTSELLER

Eric Schmidt
Executive Chairman, Google
Jared Cohen
Director, Google Ideas

'A brilliant guidebook for the next century'
RICHARD BRANSON

The New Digital Age

Reshaping the Future of People, Nations and Business

'Both profoundly wise and wondrously readable'
WALTER ISAACSON, author of *Steve Jobs*

We are living in the so-called **information era**

- **knowledge economy**
- **sociological implications**

In 2013, Eric Shmidt and Jared Cohen (Google) published a book that provides an in-depth analysis of the **characteristics, opportunities and <u>risks of the digital age</u>.**

Information Security

Information Security is essential

Digital Information is an essential part of

- the daily business of any company
- the management of public administration tasks, economic and financial transactions
- the daily communication among persons

that is carried by

- Internet
- computers & smart devices

The ***cyber space*** is the new place where prevention, protection, and response to criminal activities has to be deployed

Information Security

Types of risk

In many sectors: events that affect **safety**

- Aerospace
- Process (e.g., nuclear, chemical) plants
- Energy
- Civil and environmental engineering
- The military

In information systems: events that affect **security**

- Confidentiality, integrity, availability of information
- Potential effects to the external environment (e.g., industrial automation)

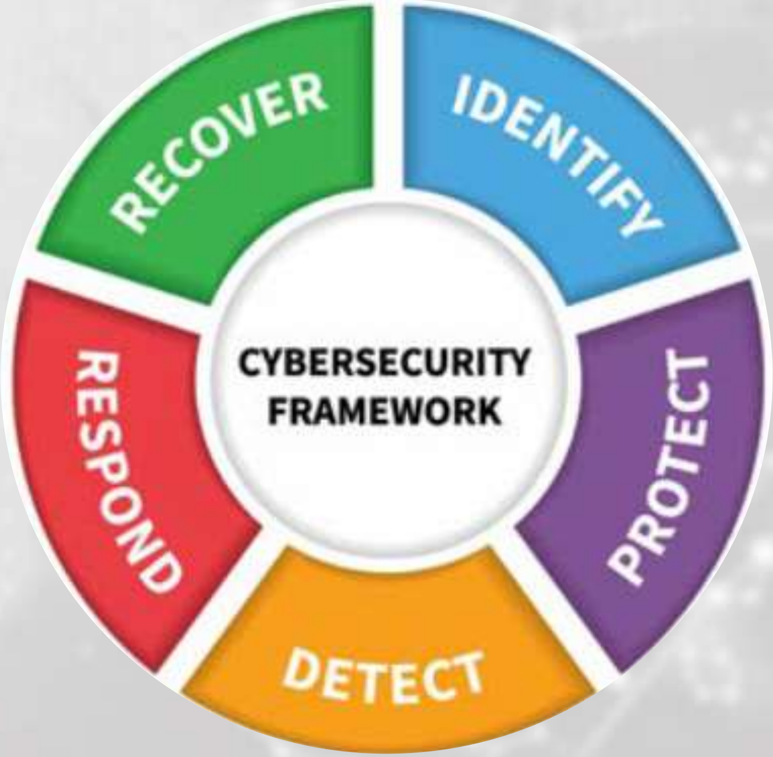
INFORMATION SECURITY

NIST CYBERSECURITY FRAMEWORK

A **RISK-BASED** APPROACH TO MANAGING CYBERSECURITY RISK

- **FLEXIBLE** APPROACH TO CYBERSECURITY, APPLICABLE TO ANY ORGANIZATION RELYING ON TECHNOLOGY INCLUDING IA.

- PROVIDES **A COMMON ORGANIZING STRUCTURE FOR MULTIPLE APPROACHES TO CYBER SECURITY** BY ASSEMBLING CURRENTLY EFFECTIVE STANDARDS, GUIDELINES, AND PRACTICES



A.I. in Military World

Artificial intelligence (AI) is revolutionizing the field of military aviation, offering advanced capabilities and enhancing operations in various ways.

- ✓ **C4ISR**

  facilitates the collection and analysis of data to provide timely and accurate decision support

- ✓ **Predictive Maintenance**

  predict when aircraft require maintenance before failures occur

- ✓ **Autonomous Weapon Systems**

  development of autonomous weapon systems, capable of operating without direct human intervention

- ✓ **Decision Support**

  AI assists pilots and ground personnel in making quick and informed decisions during missions

A.I. & Cyber Security

Significant impact in the field of cybersecurity.

- ✓ **Threat Detection and Prevention**

  AI-based systems can analyze large amounts of data to identify patterns and detect anomalies in real-time.

- ✓ **Behavior Analysis**

  AI can monitor user behavior, network traffic, and system logs to identify suspicious or unusual activities.

- ✓ **Vulnerability Identification**

  AI can proactively identify vulnerabilities in networks and systems

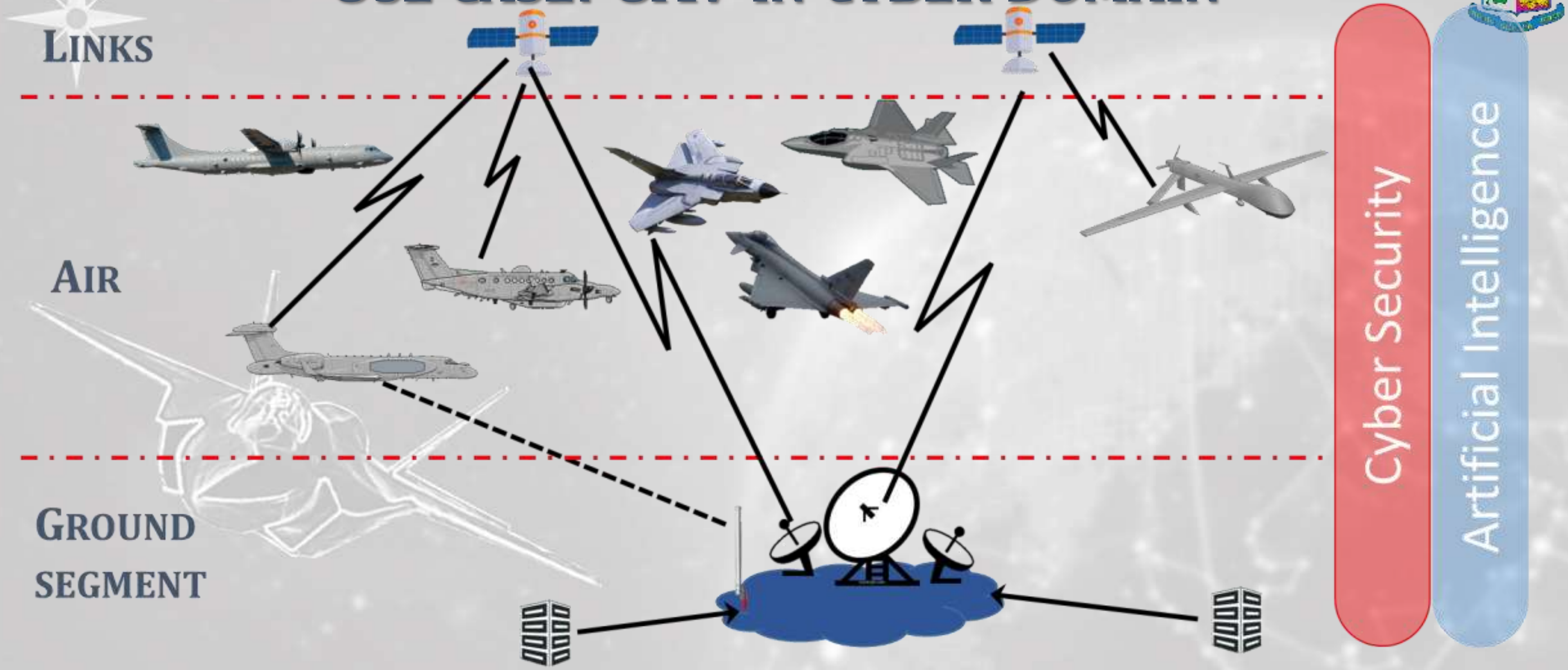
- ✓ **Reduction of Human Errors**

  Through automation and continuous learning

- ✓ **Enhancement of Network, IoT/OT, and Application Security**

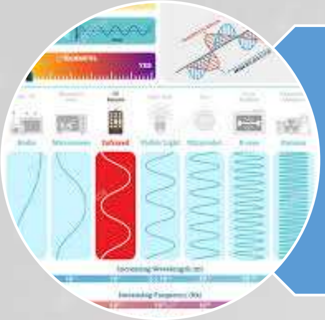
  AI can enhance security across various technological domains

USE CASE: UAV IN CYBER DOMAIN



Many assets to protect!!!

USE CASE: UAV IN CYBER DOMAIN



These aircraft interact with the surrounding environment through electronics and the electromagnetic spectrum

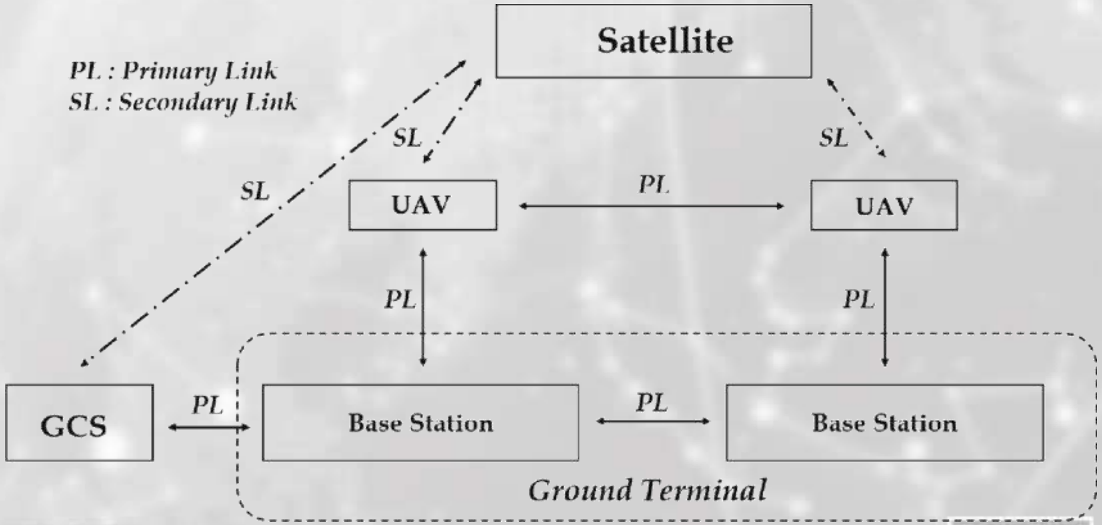
Collecting, processing and exchanging a large amount of data and information that travel in cyberspace and between the physical and network infrastructures dedicated to them

UAV and the cyber domain are two sides of the same aspect, an indissoluble union

Use case: UAV in Cyber Domain

To identify vulnerabilities in the cyber segment, including those of an electronic type, it is necessary to consider all the components of an UAV system, which is composed in its more complex configurations by the following elements:

- the **Aircraft**
- the Ground Control Station (**GCS**)
- **Links** of communication
- Exploitation Data Station (**EDS**)



USE CASE: UAV IN CYBER DOMAIN

IN THE CONTEXT OF CYBER VULNERABILITIES, AN UAV MAY BE ATTACKED TO PURSUE NUMEROUS PURPOSES, INCLUDING:

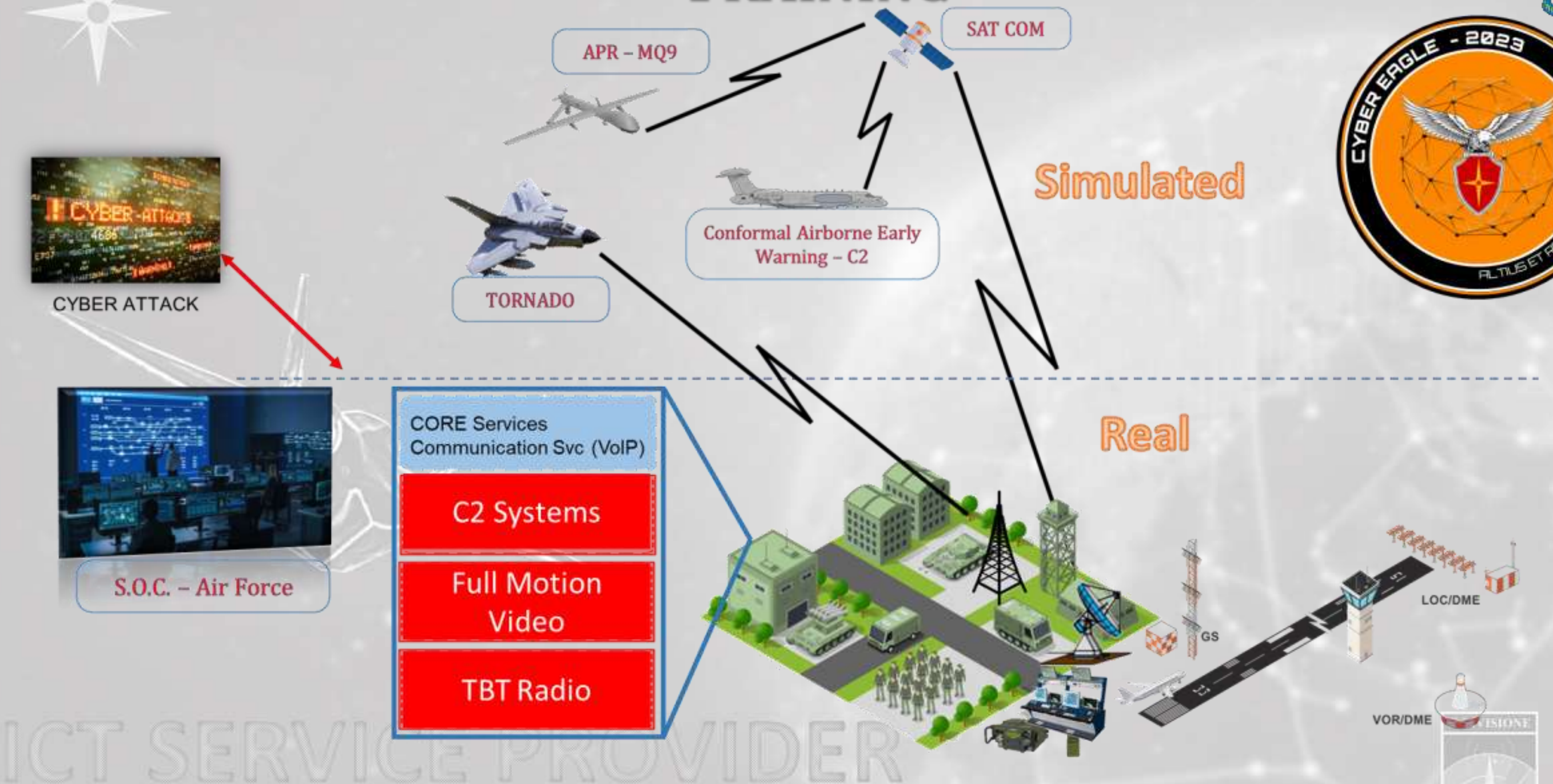
- ✓ PREVENT THE MISSION;
- ✓ CAUSE THE AIRCRAFT TO LOSE CONTROL;
- ✓ TAKE CONTROL OF THE AIRCRAFT;
- ✓ MODIFY THE AUTOPILOT SYSTEM INFORMATION BY ALTERING ITS FUNCTIONALITY;
- ✓ TRIGGERING EVENTS PREDETERMINED BY ON-BOARD SYSTEMS;
- ✓ PREVENT DATA COMMUNICATIONS AND C2;
- ✓ STEAL OR CORRUPT INFORMATION DETECTED;
- ✓ INFECT THE COMMUNICATION NETWORK AND WORKSTATIONS WITH VIRUSES, MALWARE, SPYWARE, ETC.

Use case: UAV in cyber domain

There is therefore a growing combined use ("blended") of different types of attack, i.e.:

- ✓ **Jamming:** it is possible to disturb / obfuscate the signal;
- ✓ **Man in the middle:** it is possible to take control of the aircraft or steal information;
- ✓ **Spoofing:** sending false information to obtain illegal access to the systems, indicating a false GPS location;
- ✓ **Typical cyber attack:** the classic attack carried to the network infrastructure on the ground, from outside or from inside, with viruses, malware, spyware, etc .;
- ✓ **Denial of Service** (DoS): to inhibit transmissions;
- ✓ **Supply chain:** it is possible to sabotage or add devices, sensors, hardware and software, during assembly and integration or during maintenance operations.

Training



APR – MQ9

SAT COM

Conformal Airborne Early Warning – C2

TORNADO

CYBER ATTACK

Simulated

Real

S.O.C. – Air Force

CORE Services
Communication Svc (VoIP)

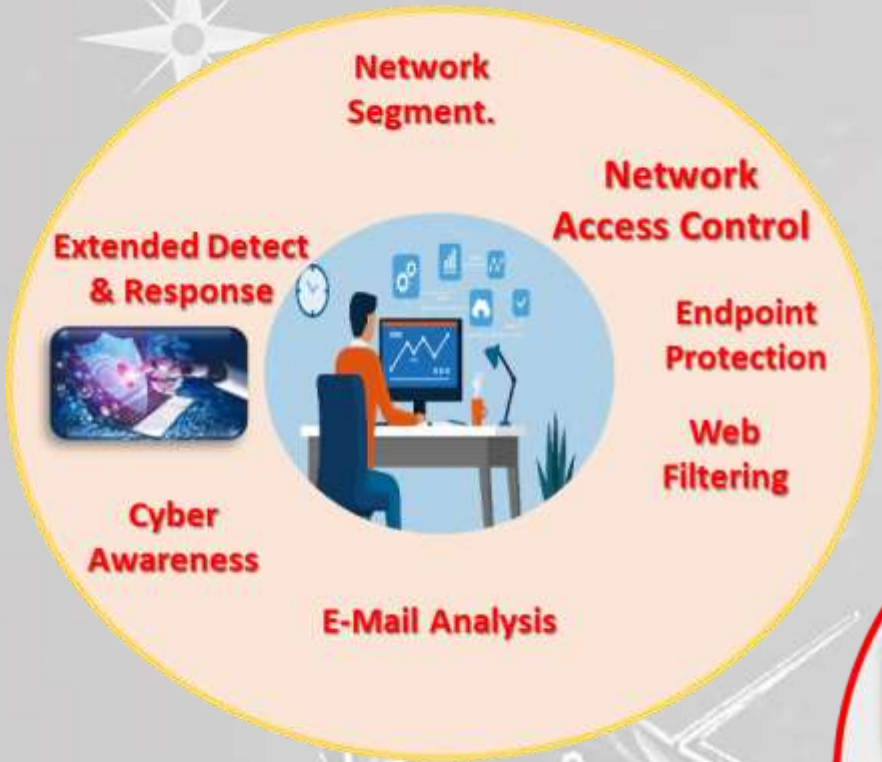
C2 Systems

Full Motion Video

TBT Radio

ICT SERVICE PROVIDER

TRAINING



Network Segment.

Network Access Control

Extended Detect & Response

Endpoint Protection

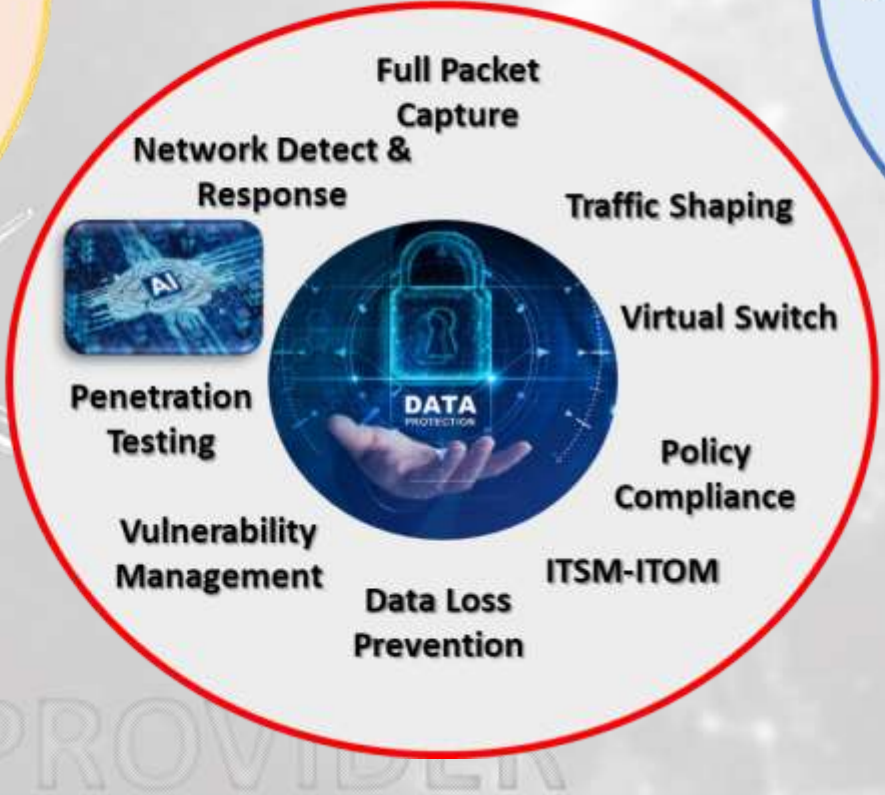
Web Filtering

Cyber Awareness

E-Mail Analysis

END POINT & USER PROTECTION

DATA PROTECTION



Full Packet Capture

Network Detect & Response

Traffic Shaping

Virtual Switch

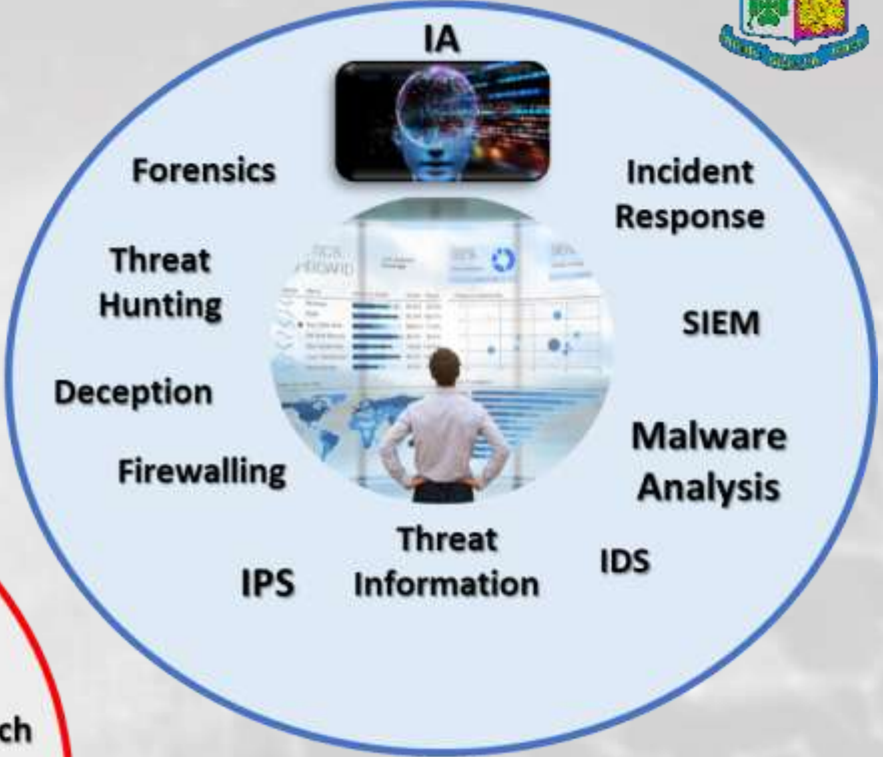
Penetration Testing

Policy Compliance

Vulnerability Management

ITSM-ITOM

Data Loss Prevention



IA

Forensics

Incident Response

Threat Hunting

SIEM

Deception

Malware Analysis

Firewalling

Threat Information

IPS

IDS

REAL TIME SECURITY MONITORING EARLY WARNING & CYBER THREAT ANALYSIS

Thank you for your attention!

Maj. Carmine MARRESE
Automated Information Systems Department (Re.S.I.A.)
Network and Security Group Commander