# Cyber security e cyber privacy, la sfida dell'internet di ogni cosa

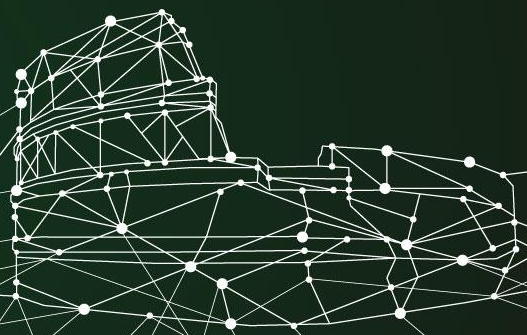
Gen. Umberto Maria Castelli, Comandante Comando C4 Difesa

Nautilus Mediterranean Exchange Point

NaMeX 20° Anniversario

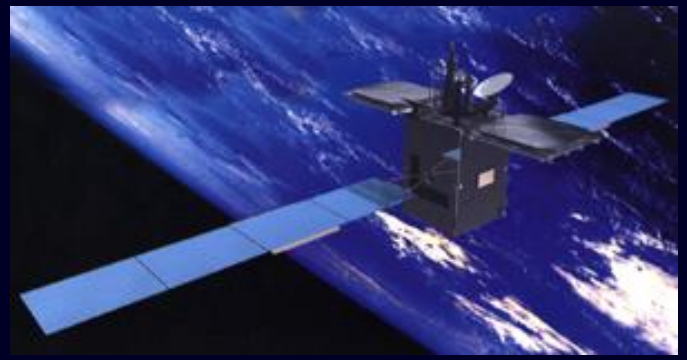
ANNUAL MEETING 2015

Roma, 17 giugno 2015 - Casa del Cinema



# COMANDO C4 DIFESA

Comando C4 Difesa



## NaMex Annual Meeting
## Casa del Cinema - Villa Borghese
## 17 giugno 2015


Comando C4
Difesa
LABOR OMNIA VINCIT

# Sommario

1. Componenti capacitive NOC - IOC - SOC
2. Cyber Defence Capability
3. Simulazioni di Cyber Defence

# COMPONENTI CAPACITIVE



SMD-6

## Comando C4 Difesa

NETWORKING

DATA CENTER MANAGEMENT SERVICES

SECURITY

CONTROL ROOM/CALL CENTER

Network Operation Center

NOC

Information Operation Center

IOC

Cyber Security

CERT

SOC

Centro di Gestione e controllo satellitare SICRAL

# COMPONENTI CAPACITIVE

## Call Center Unificato

Comando C4 Difesa

**Il Call Center è un Servizio del Comando C4 per offrire a tutti gli utenti Difesa (circa 20.000 utenti), sia Area Tecnico Operativa (T.O.), sia Area Tecnico Amministrativa (T.A.), un unico interlocutore di assistenza di primo livello per la gestione e la risoluzione di tutte le problematiche TLC ed Informatiche (HW e SW).**

**Il sistema utilizza il prodotto iET ITSM della iET Solutions© e comprende i seguenti moduli principali secondo standard ITIL:**

- **Change Management;**
- **Configuration Management;**
- **Incident Management;**
- **Problem Management.**

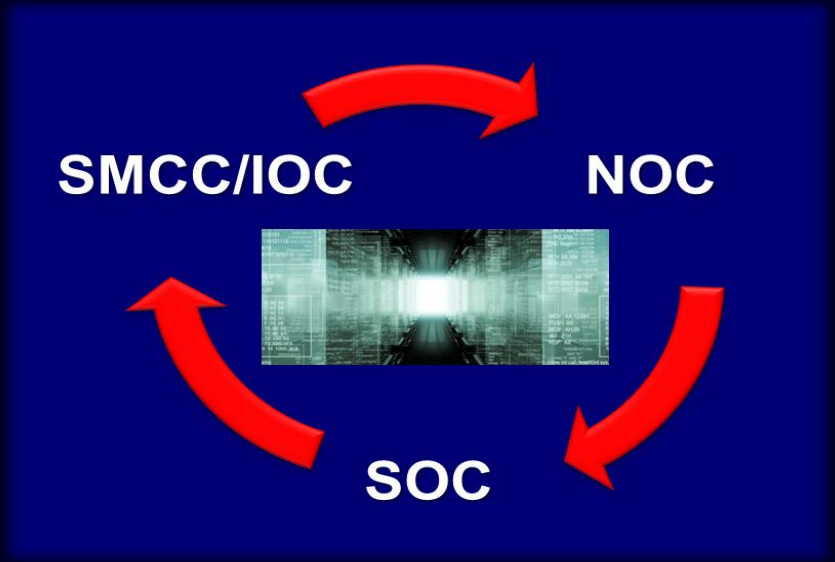
**TOTALE TICKET 2014:**

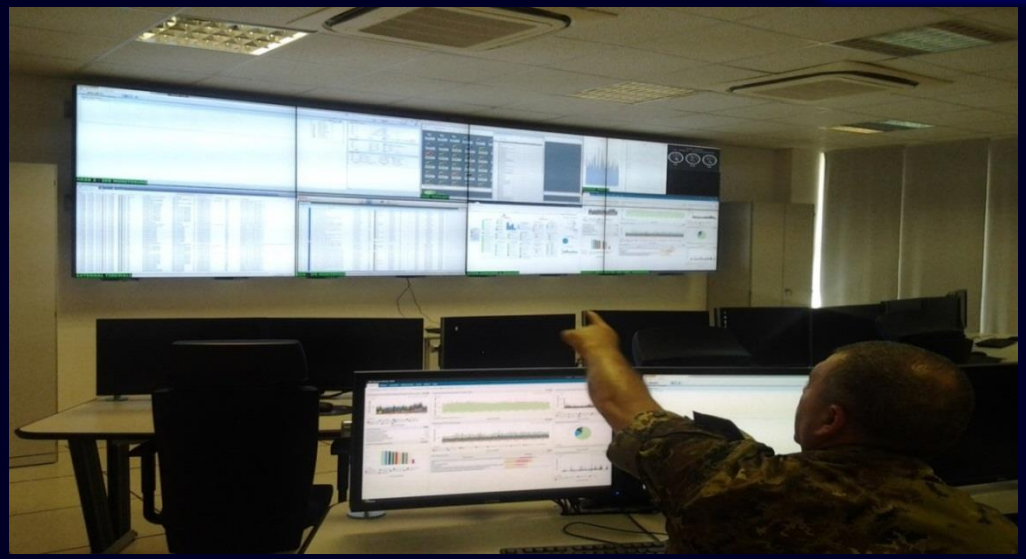
**20.000**

# COMPONENTI CAPACITIVE
## Control Room



Realizzazione di un sistema di *data fusion* per aggregare gli «stati di situazione» di SMCC/IOC, NOC e SOC in una CONTROL ROOM, finalizzato a conseguire una *Cyber Operational Picture* (CyOP) e consentire la gestione unitaria degli eventi da parte del CERT TC

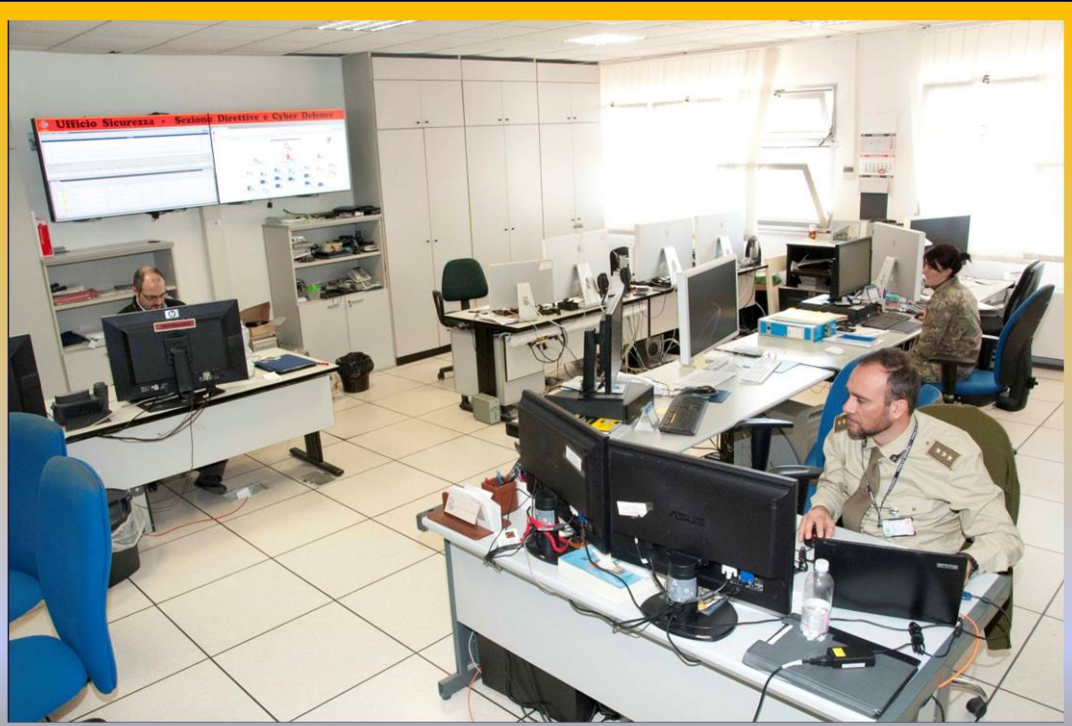


**Operatività h24/7gg**

# CYBER DEFENCE CAPABILITIES
## SOC






- ANTIVIRUS
- WEB DEFACEMENT MONITORING
- WEB CONTENT FILTERING
- WEB APPLICATION FIREWALLS
- USER POLICIES ENFORCING (GPO)
- FIREWALLS
- VPN MANAGEMENT
- INTRUSION DETECTION SYSTEMS
- INTRUSION PREVENTION SYSTEMS
- TRAFFIC SHAPERS

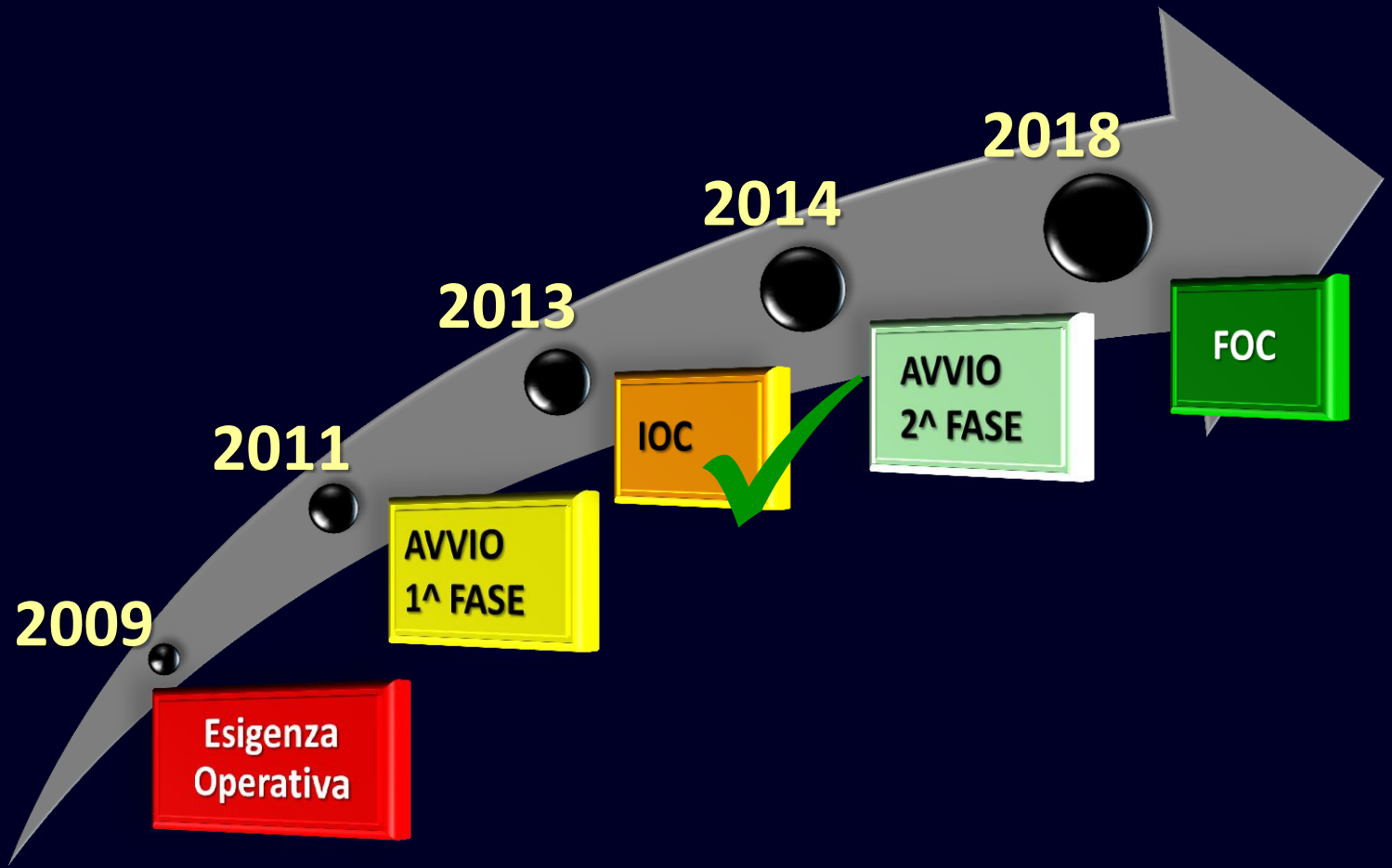
# CYBER DEFENCE CAPABILITIES
## CERT



- SIEM (EVENT CORRELATION)
- GESTIONE INCIDENTI

# CYBER DEFENCE CAPABILITIES ROADMAP

Comando C4 Difesa

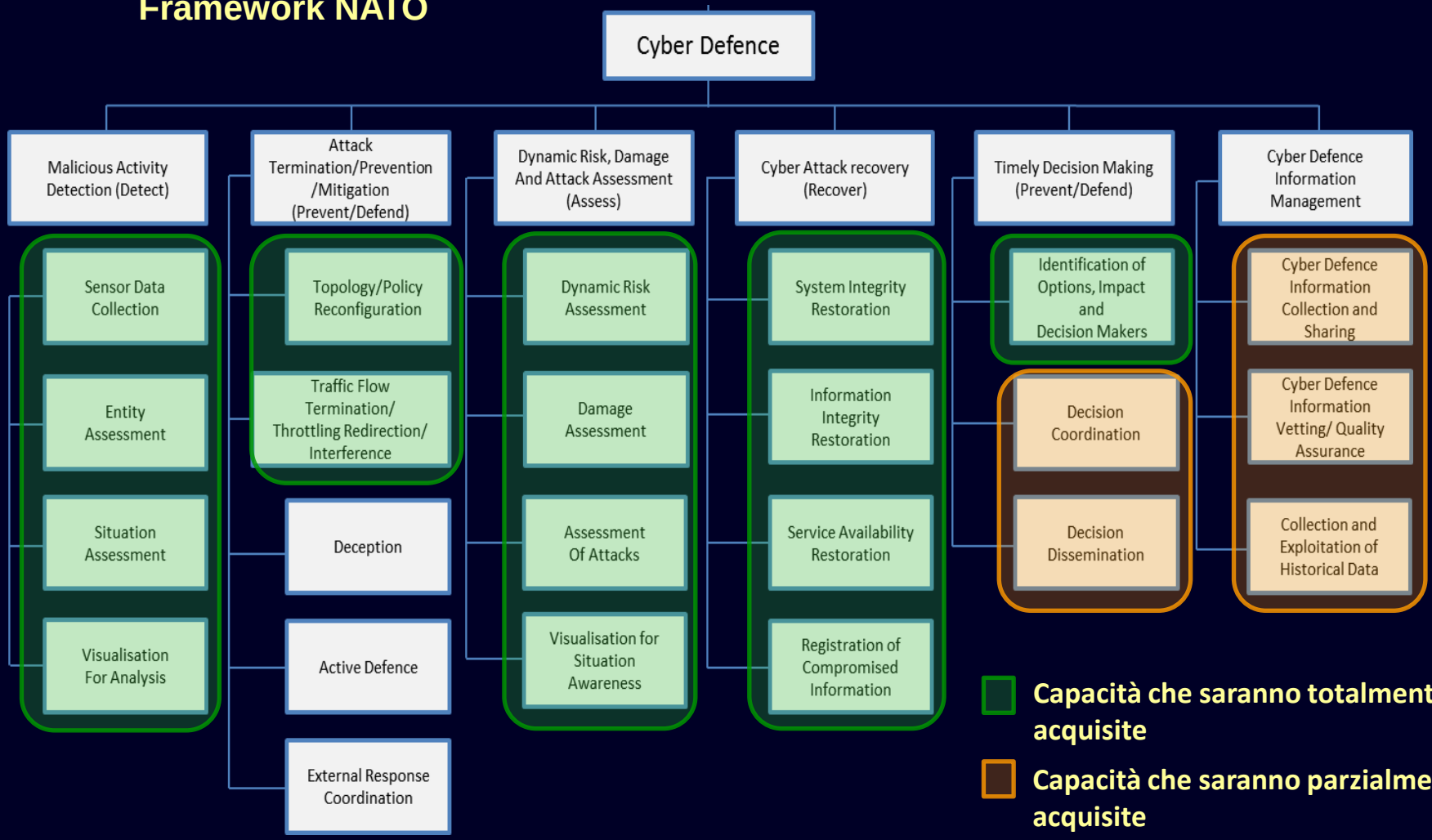


# CYBER DEFENCE CAPABILITIES

## Full Operation Capabilities

Comando C4 Difesa

### Framework NATO




**Capacità che saranno totalmente acquisite**

**Capacità che saranno parzialmente acquisite**

# SIMULAZIONI DI CYBER DEFENCE

## «Cyber Battle Lab»



- **Ambiente di simulazione** per:
  Attività di ***ricerca***, ***sperimentazione*** e ***test***, ***addestramento*** ed ***esercitazioni***

- **Strumento per conseguire sinergie** con:
  Forze Armate, Enti Istituzionali della P.A., Mondo Accademico, NATO/EU, Industrie, etc.


**CONVENZIONI CON:**

- **Università La Sapienza – Dipartimento Informatica;**
- **Istituto Superiore delle Comunicazioni e delle Tecnologie dell'informazione del Mi.S.E.**

# Esercitazioni di Cyber Defence (CDX) nazionali e NATO



| Tipologia | Caratteristiche | Esempi |
|---|---|---|
| **PROCEDURALE** | Esercitazione «a tavolino» di livello concettuale | CYBER EUROPE |
| **SEMI PROCEDURALE** | Esercitazione procedurale con alcuni *injects* di tipo reale | **CYBER COALITION** |
| **"LIVE-FIRE"** | Massimo livello di realismo, riproduzione fedele delle situazioni ed uso di strumenti reali | **LOCKED SHIELDS** |

# CYBER SECURITY

## Cyber Defence Exercise «Locked Shields»



LOCKED SHIELDS

**2014**

- **Esercitazione internazionale *live-fire* di tipo red/blue, estremamente tecnica**
- **1 red team aTallinn, 12 blue team in Europa, 14 nazioni + NCIRC participanti**
- **2 giorni di CNO continue "*near real life*"!**
- **Quest'anno il BT italiano si é classificato al 5° posto su 12, mentre il primo è andato alla Polonia**
- **L'Italia si è distinta per la migliore difesa e la migliore strategia di protezione del routing**

# CYBER SECURITY

## Cyber Defence Exercise «Locked Shields»



LOCKED SHIELDS

**2015**

- **Esercitazione internazionale *live-fire* di tipo red/blue, estremamente tecnica**
- **1 red team aTallinn, 15 blue team in Europa, 14 nazioni + NCIRC participanti**
- **2 giorni di CNO continue "*near real life*"!**
- **Quest'anno il BT italiano si é classificato al 8° posto su 15, mentre il primo è andato a NCIRC**
- **L'Italia si è distinta per il miglior report di forensic** (2° posto) **e per la migliore strategia di protezione del routing**

# LOCKED SHIELDS 2015 CONCEPT



- **Esercitazione tecnica di cyber defence (CDX) *live fire* di tipo *Blue* - *Red* :**
  - I **Blue Teams** (x15) devono mettere in sicurezza e difendere una propria rete virtuale precostituita da circa 70 macchine, nelle quali sono presenti diverse vulnerabilità non dichiarate
  - Il **Red Team** (x1, Tallinn) conduce attacchi informatici reali contro tutti i Blue Teams secondo un approccio "***white-box***"

- **Organizzatori:**

  **CCDCOE** (Cooperative Cyber Defence Center of Excellence), **Forze Armate estoni**, **Cyber Defence League estone**, **Forze Armate finlandesi**.

# LOCKED SHIELDS 2015 CONCEPT



- **Oltre ai teams blue e red, sono presenti anche altri tipi di squadre:**
  - **Legal Teams** (1 x ogni Blue Team), sono un «sottoinsieme» dei blue teams, e forniscono consulenza legale al blue team di appartenenza
  - **White Team** (x1, Tallinn), responsabile del controllo dei partecipanti, della corretta applicazione delle regole e dello scoring
  - **Green Team** (x1, Tallinn), responsabile del setup e della manutenzione tecnica dell'infrastruttura esercitativa. Supporto tecnico fornito da Cisco, Clarified Networks, Clarified Security e Codenomicon.

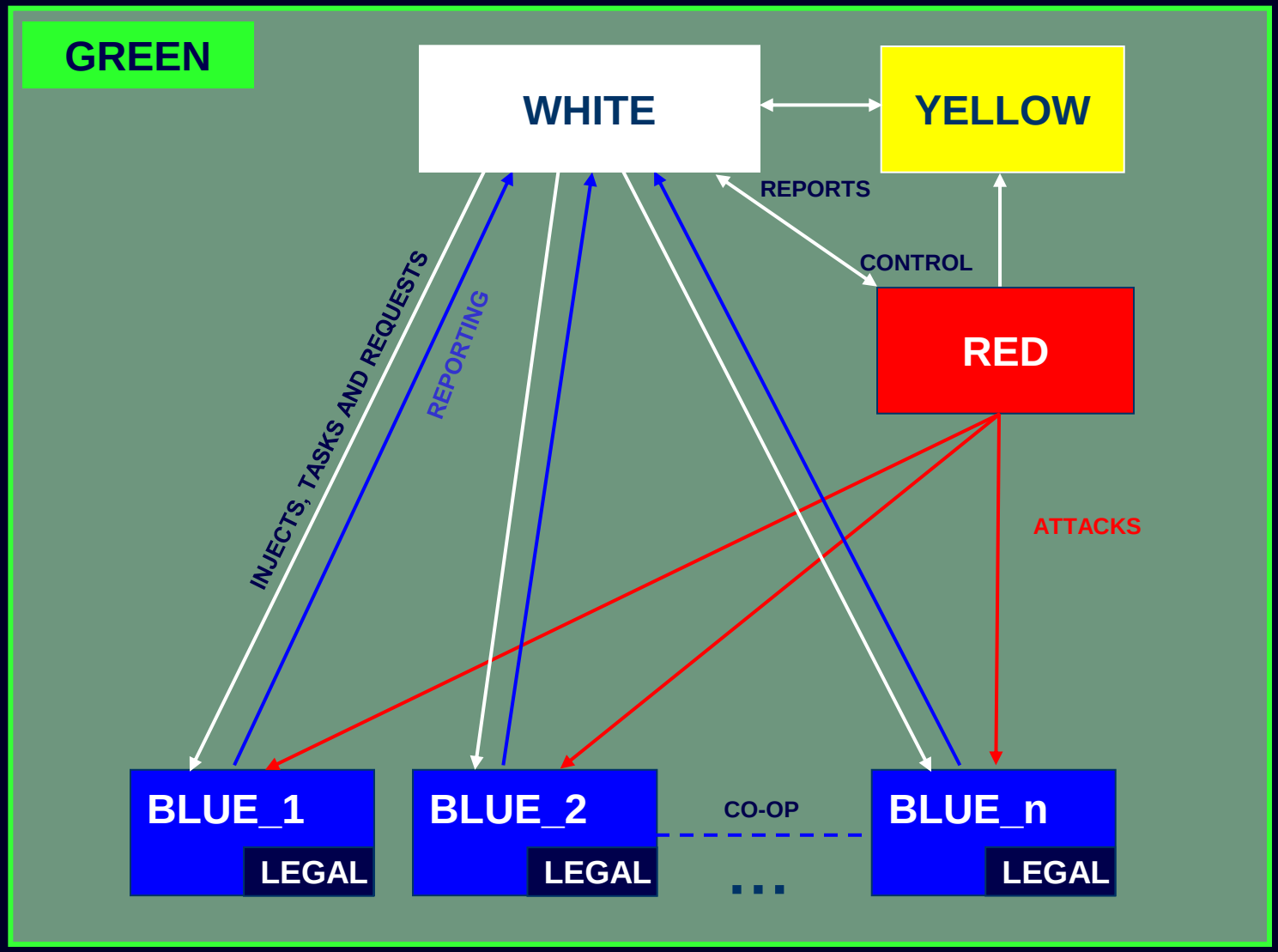
# LOCKED SHIELDS 2015 CONCEPT



- **Yellow Team** (x1, Tallinn), responsabile della *situational awareness* dell'esercitazione. Il suo compito è quello di analizzare informazioni provenienti da diverse fonti e fornire un feedback al White Team, al Red Team e ai Blue Team ("SA solutions").

# Esercitazione "Locked Shields"
## Relazioni tra teams





# LOCKED SHIELDS 2015
# AMBIENTE TECNICO



- I Blue Teams dovevano gestire una rete segmentata in un totale di 8 **zone**, nelle quali erano presenti le seguenti tipologie di macchine:
  - **Routers Cisco**
  - **Firewall basato su ipfilter Linux**
  - **Gateways VPN basati su OpenVPN**
  - **Workstations Windows XP, Windows 7 e Ubuntu**
  - **Controllers di dominio Windows**
  - **Servers web, DNS, SMTP, POP3, IMAP, FTP, SMB (su piattaforma Windows e Linux)**
  - **Sistemi VoIP basati su Asterisk**
  - **PLC Siemens** (automazione industriale)

# LOCKED SHIELDS 2015
# PROFILI E RUOLI RICHIESTI

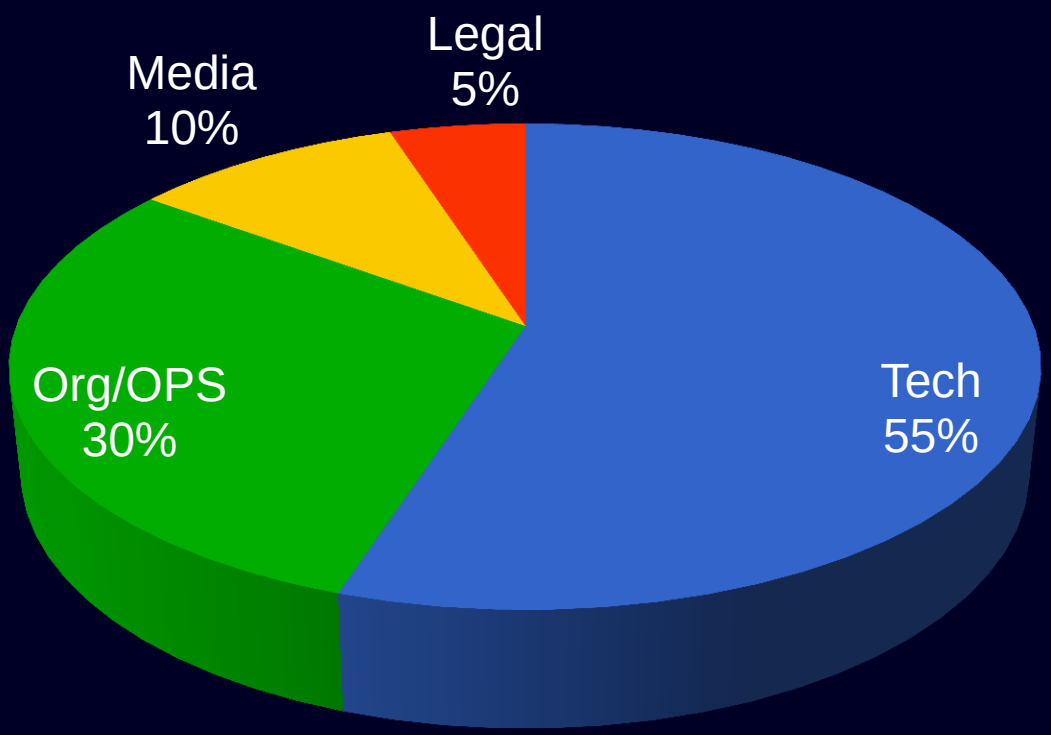


- **Tecnici** (configurazione, hardening, patching, detection e remediation):
  - **Sistemisti Cisco IOS** (routers)
  - **Sistemisti Windows** (XP, 7, Active Directory)
  - **Sistemisti Linux** (workstation e server)
  - **Web masters / developers** (server-side scripts)
- **Operatori per coordinamento di Incident Response** (information sharing e incident reporting)
- **Consulenti legali**
- **Addetti stampa** per comunicazioni ai media

# LOCKED SHIELDS 2013
# INJECTS DI SCENARIO



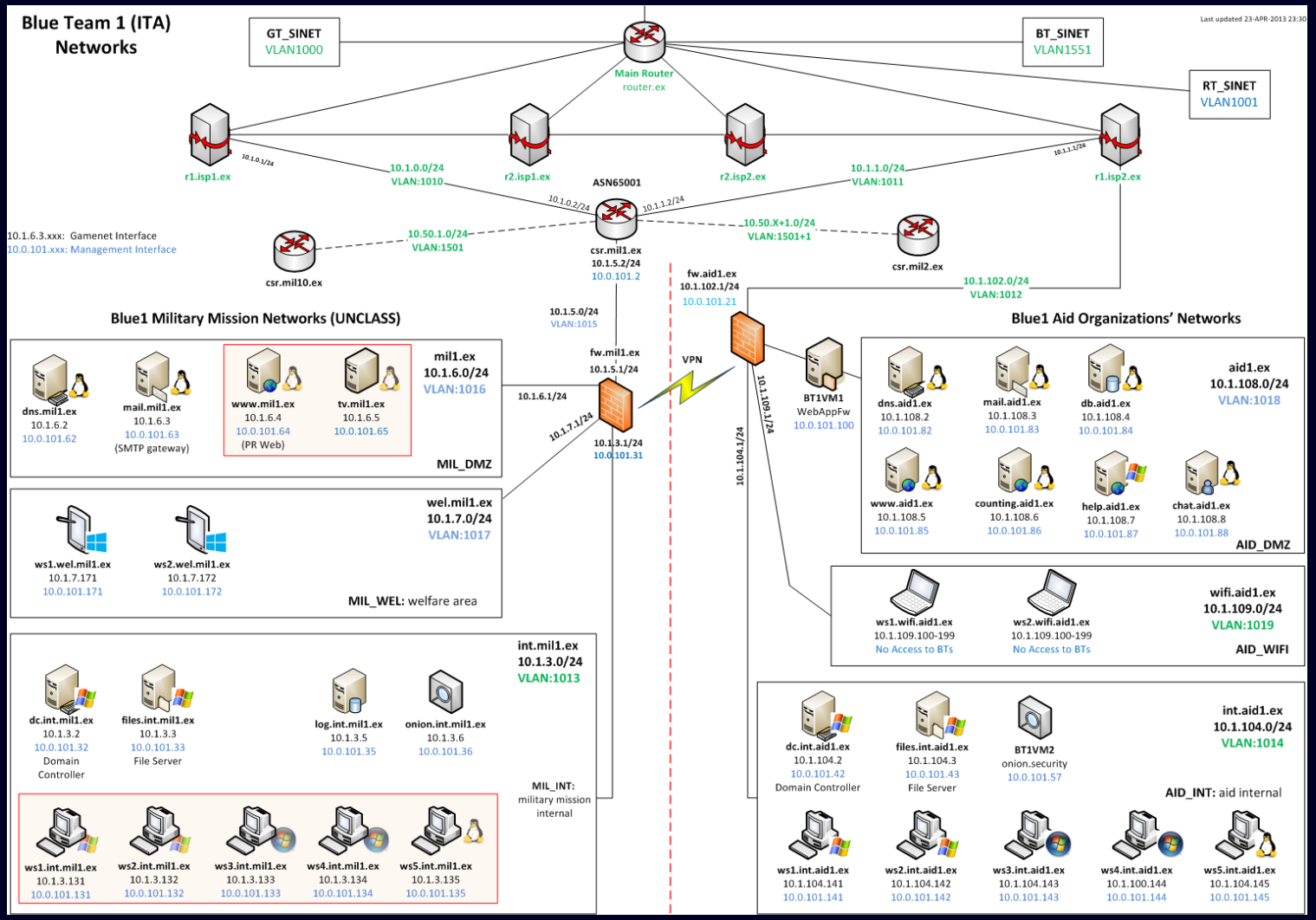
## TIPOLOGIE DI INJECTS



# Esercitazione "Locked Shields" 2013

("Live-fire Cyber Defense eXercise")

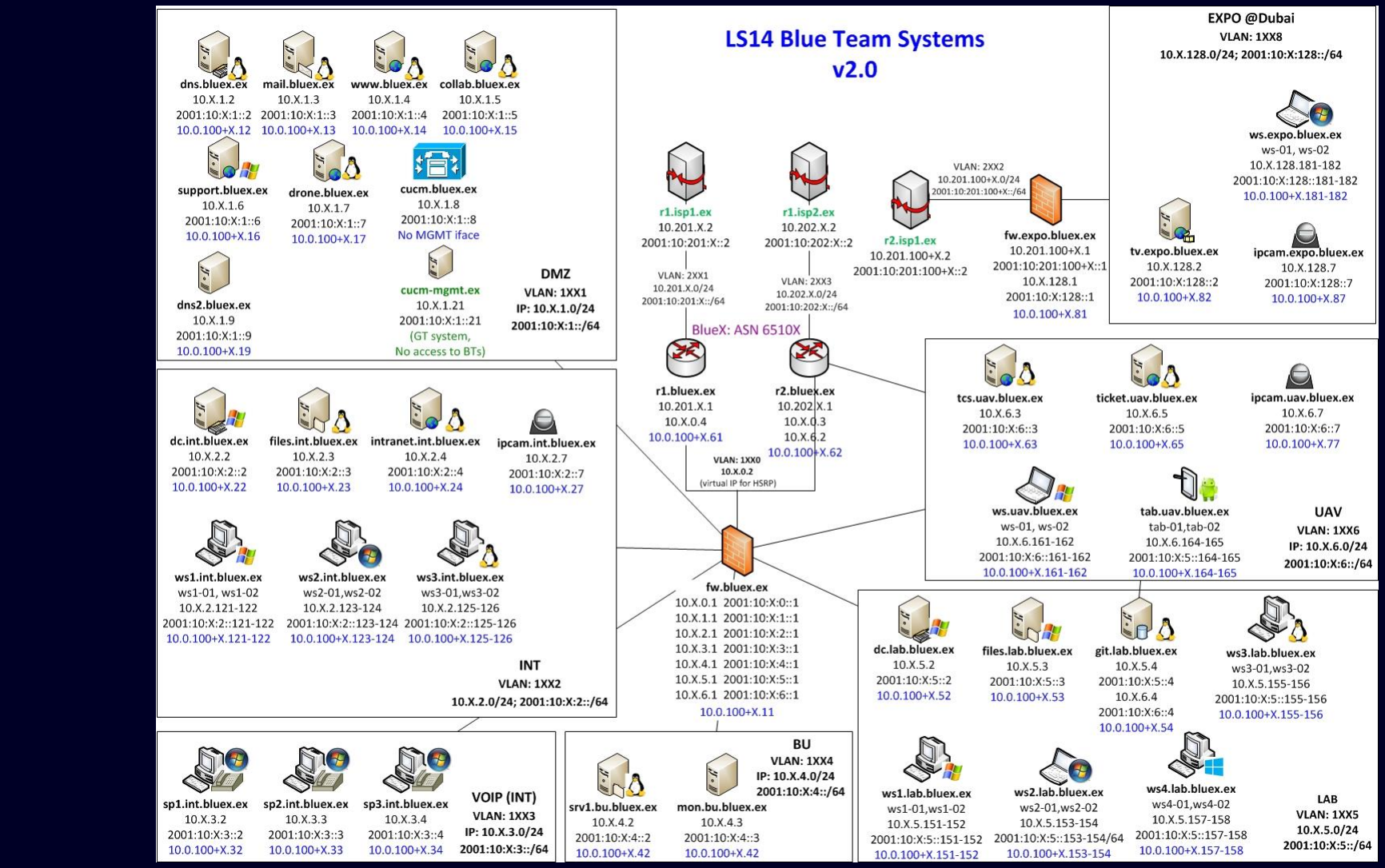
Comando C4 Difesa



# Esercitazione "Locked Shields" 2014

("Live-fire Cyber Defense eXercise")

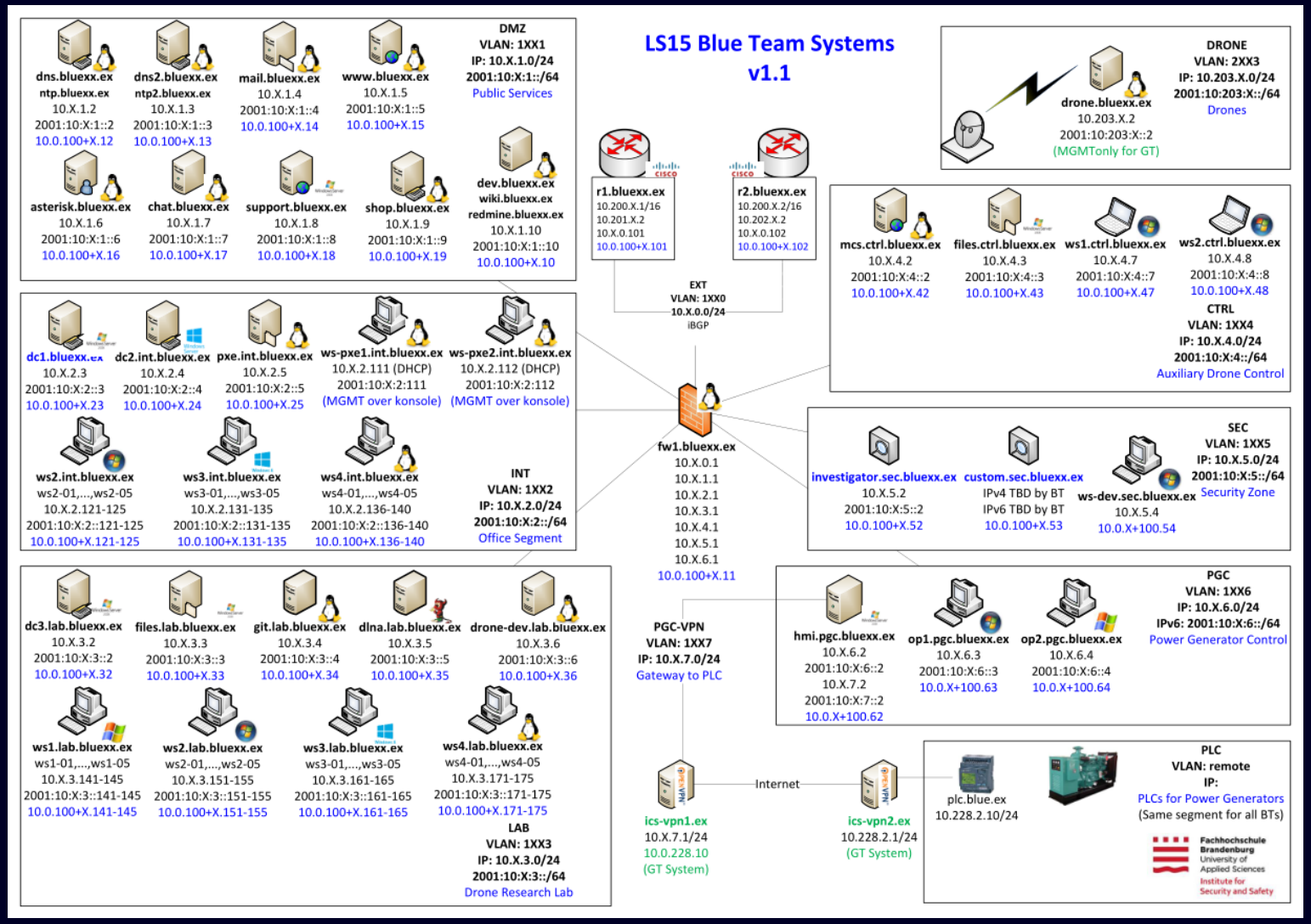
Comando C4 Difesa



# Esercitazione "Locked Shields" 2015

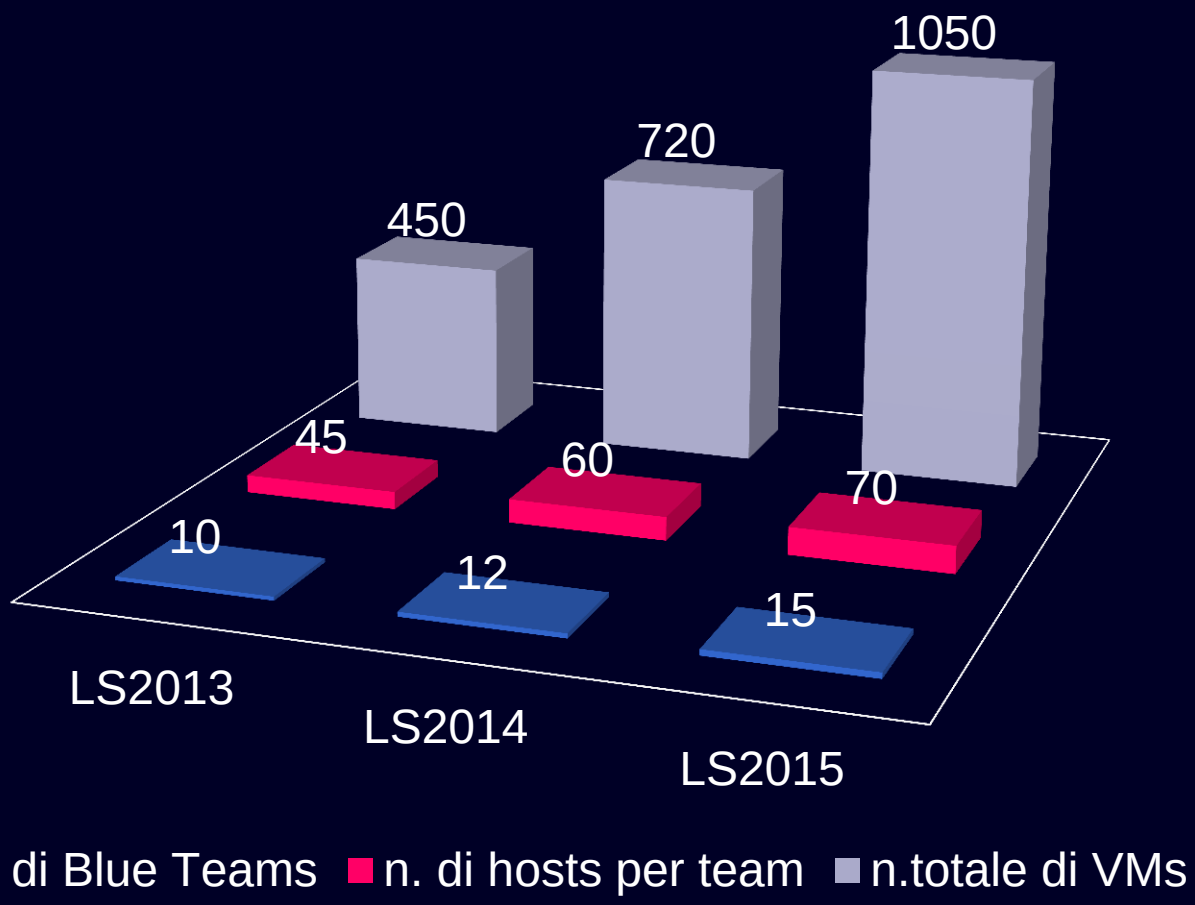
("Live-fire Cyber Defense eXercise")

Comando C4 Difesa



# LOCKED SHIELDS
# EVOLUZIONE DELLA COMPLESSITA'





# Esercitazione "Locked Shields" 2014

("Live-fire Cyber Defense eXercise")

Comando C4 Difesa

# LOCKED SHIELDS
## Valutazione e punteggio



- Ogni Blue Team viene valutato in termini di punteggio in base alle attività effettivamente condotte in modo da motivarli e misurare i loro skills.
- La valutazione avviene in modo automatico tramite scoring bots e uno scoring server, supervisionata e integrata/corretta dal White Team.
- **TUTTE LE ATTIVITA' DI COMPETENZA PRECEDENTEMENTE ELENCATE SONO OGGETTO DI VALUTAZIONE!**


# LOCKED SHIELDS 2013
# CLASSIFICA FINALE GENERALE

Comando C4 Difesa

| Posizione | | Nazione | Punteggio | Team |
|---|---|---|---|---|
| **1** | | **NATO** | **41944** | **BT 5 (NCIRC)** |
| 2 | | ESTONIA | 37742 | BT 8 |
| 3 | | OLANDA | 29916 | BT 2 |
| 4 | | GERMANIA | 26957 | BT 10 |
| 5 | | SPAGNA | 25996 | BT 7 |
| 6 | | SLOVACCHIA | 25768 | BT 4 |
| 7 | | POLONIA | 23739 | BT 6 |
| 8 | | ITALIA | 18396 | BT 1 |
| 9 | | LITUANIA | 16963 | BT 3 |
| 10 | | FINLANDIA | 13881 | BT 9 |

# LOCKED SHIELDS 2014
# CLASSIFICA FINALE GENERALE

Comando C4 Difesa

| Posizione | | Nazione | Punteggio | Team |
|---|---|---|---|---|
| **1** | | **POLONIA** | **27603** | **BT 6** |
| 2 | | LETTONIA+REP.CECA | 24966 | BT 10 |
| 3 | | ESTONIA | 22003 | BT 4 |
| 4 | | AUSTRIA+LITUANIA | 20663 | BT 5 |
| 5 | | ITALIA | 19644 | BT 3 |
| 6 | | FINLANDIA | 18666 | BT 11 |
| 7 | | NATO (NCIRC) | 16806 | BT 1 |
| 8 | | TURCHIA | 12024 | BT 7 |
| 9 | | GERMANIA+OLANDA | 10517 | BT 2 |
| 10 | | UNGHERIA | 9189 | BT 8 |
| 11 | | FRANCIA | 8047 | BT 12 |
| 12 | | SPAGNA | 6460 | BT 9 |

# LOCKED SHIELDS 2015
# CLASSIFICA FINALE GENERALE

Comando C4 Difesa

| Posizione | | Nazione | Punteggio | Team |
|---|---|---|---|---|
| **1** | | **NATO CIRC (NCIRC)** | **25631** | **BT06** |
| 2 | | ESTONIA | 24526 | BT11 |
| 3 | | POLONIA | 22648 | BT09 |
| 4 | | LITUANIA + LETTONIA | 20827 | BT12 |
| 5 | | FRANCIA | 19324 | BT05 |
| 6 | | SLOVACCHIA | 17753 | BT10 |
| 7 | | REPUBBLICA CECA | 17448 | BT04 |
| **8** | | ITALIA | 16829 | BT02 |
| 9 | | GRECIA | 16449 | BT01 |
| 10 | | GERMANIA+OLANDA | 14960 | BT03 |
| 11 | | FINLANDIA | 11146 | BT15 |
| 12 | | AUSTRIA | 10233 | BT14 |
| 13 | | SPAGNA | 8369 | BT13 |
| 14 | | TURCHIA | 6244 | BT07 |
| 15 | | UNGHERIA | 2815 | BT08 |

# LOCKED SHIELDS 2015
# PUNTEGGIO PER TEAM / TIPOLOGIA

Comando C4 Difesa

| TEAM | GR 9 blue01 | ITA 8 blue02 | D+NL 10 blue03 | CZ 7 blue04 | FR 5 blue05 | NATO 1 blue06 | TUR 14 blue07 | HUN 15 blue08 | POL 3 blue09 | SVK 6 blue10 | EST 2 blue11 | LT+LV 4 blue12 | ESP 13 blue13 | AUT 12 blue14 | FIN 11 blue15 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SCORE TYPE: attack | -13500 | -17450 | -13950 | -13775 | -20300 | -10100 | -15800 | -17150 | -11975 | -11900 | -13050 | -11050 | -15950 | -16675 | -20250 |
| availability | 16775 | 15405 | 11714 | 15109 | 17837 | 15504 | 12658 | 9821 | 14938 | 12872 | 16486 | 16501 | 11660 | 15786 | 15784 |
| coop | 3974 | 1639 | 739 | 2379 | 2777 | 2392 | 2596 | 264 | 2450 | 4582 | 760 | 806 | 1064 | 1167 | 2817 |
| inject | 4100 | 10360 | 9715 | 7180 | 11010 | 14310 | 4920 | 5630 | 9385 | 3695 | 9705 | 8945 | 6270 | 3505 | 5170 |
| revert | -700 | -1050 | | | -350 | -1050 | -1700 | | -350 | -1050 | | -700 | -700 | | -350 |
| situation report | 3900 | 6000 | 6250 | 5400 | 6300 | 6750 | 5450 | 1700 | 4600 | 6680 | 5100 | 4000 | 4000 | 2300 | 5800 |
| special | -250 | -600 | -1008 | -2520 | -650 | -4000 | -3750 | -1150 | 500 | -51 | 2000 | -250 | -150 | 1400 | |
| usability | 2150 | 2525 | 1500 | 3675 | 2700 | 1825 | 1850 | 3700 | 3100 | 2925 | 3525 | 2575 | 2175 | 2750 | 2175 |
| | 16449 | 16829 | 14960 | 17448 | 19324 | 25631 | 6224 | 2815 | 22648 | 17753 | 24526 | 20827 | 8369 | 10233 | 11146 |

NON CLASSIFICATO

# LOCKED SHIELDS 2015
# SUB-TEAM DEL BLUE TEAM ITALIANO

Comando C4 Difesa

## PUBLIC INFORMATION

## LEGAL

## SYSTEM ANALYSTS

## MALWARE ANALYSTS

## FORENSIC

## NETWORKING

## REPORTERS

# EVOLUZIONI CD
# VIRTUAL CYBER DEFENCE BATTLE LAB



## Comando C4 Difesa

⇩

***Virtual Cyber Defence Battle Lab***

- Piattaforma di simulazione (ambiente di virtualizzazione) e locali di fruizione installati presso il Comando C4 Difesa
- Coniugazione di risorse elaborative virtuali (VMs) e reali (network appliances)
- Utilizzabile per: **ricerca**, **testing**, **addestramento**, **esercitazioni**
- Possibilitá di sinergia con molteplici partecipanti (Forze Armate, Istituzioni, Ministeri, Accademia, NATO, industria, etc.)

# EVOLUZIONI CD
# VIRTUAL CYBER DEFENCE BATTLE LAB



## Cisco UCS blade servers

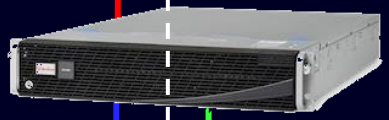
- Potenza (~ 200 VMs)
- Modularitá (8 blades)
- Semplicitá di gestione (web GUI)

# EVOLUZIONI CD
# VIRTUAL CYBER DEFENCE BATTLE LAB

Comando C4 Difesa

INTERNET

ATD (Advanced Threat Defence) device



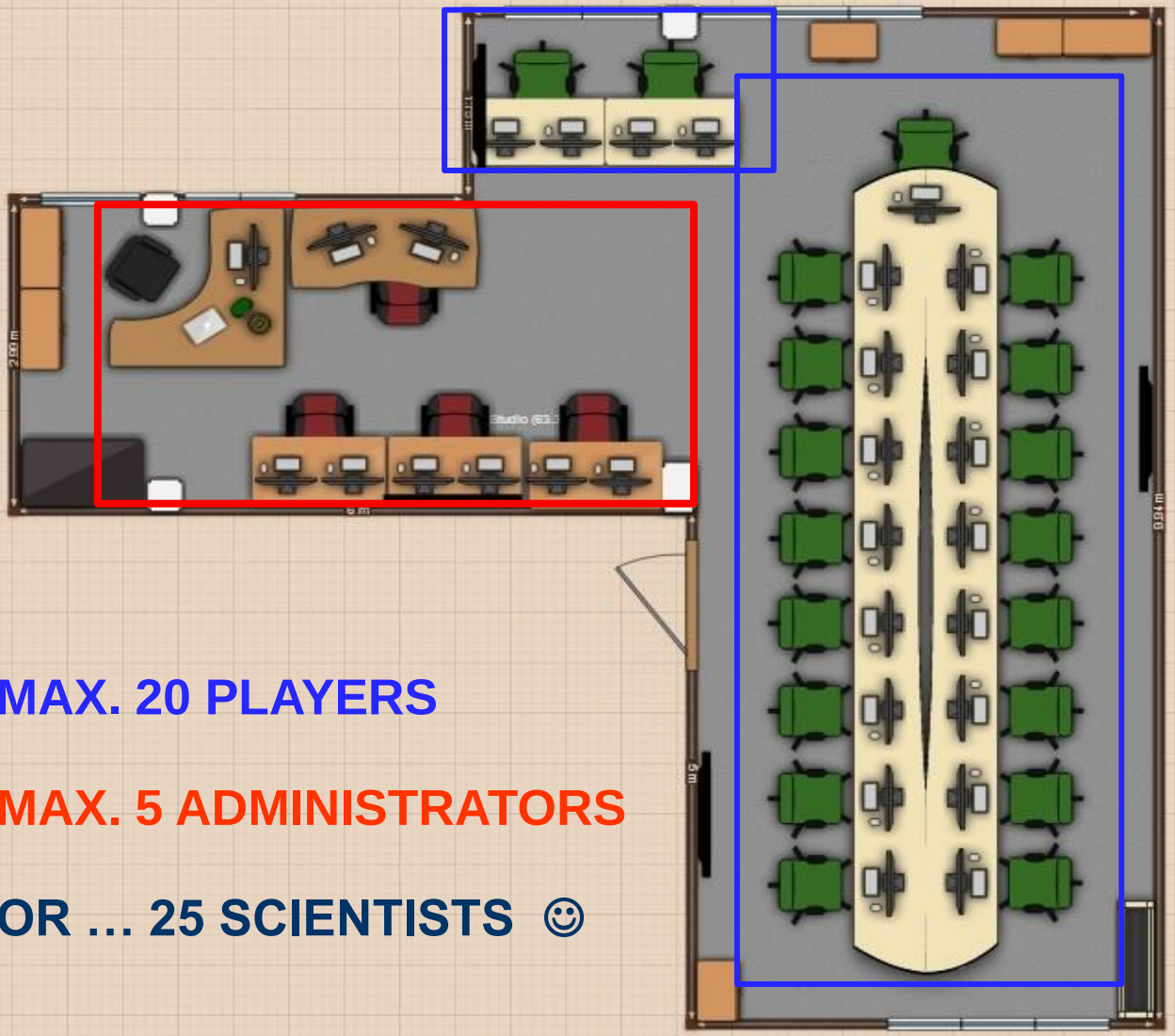
**DIFENET** (PRODUCTION NETWORK)

LAB NETWORK

**Cyber lab virtualization infrastructure**

# Virtual Cyber Defence Battle Lab

Comando C4 Difesa



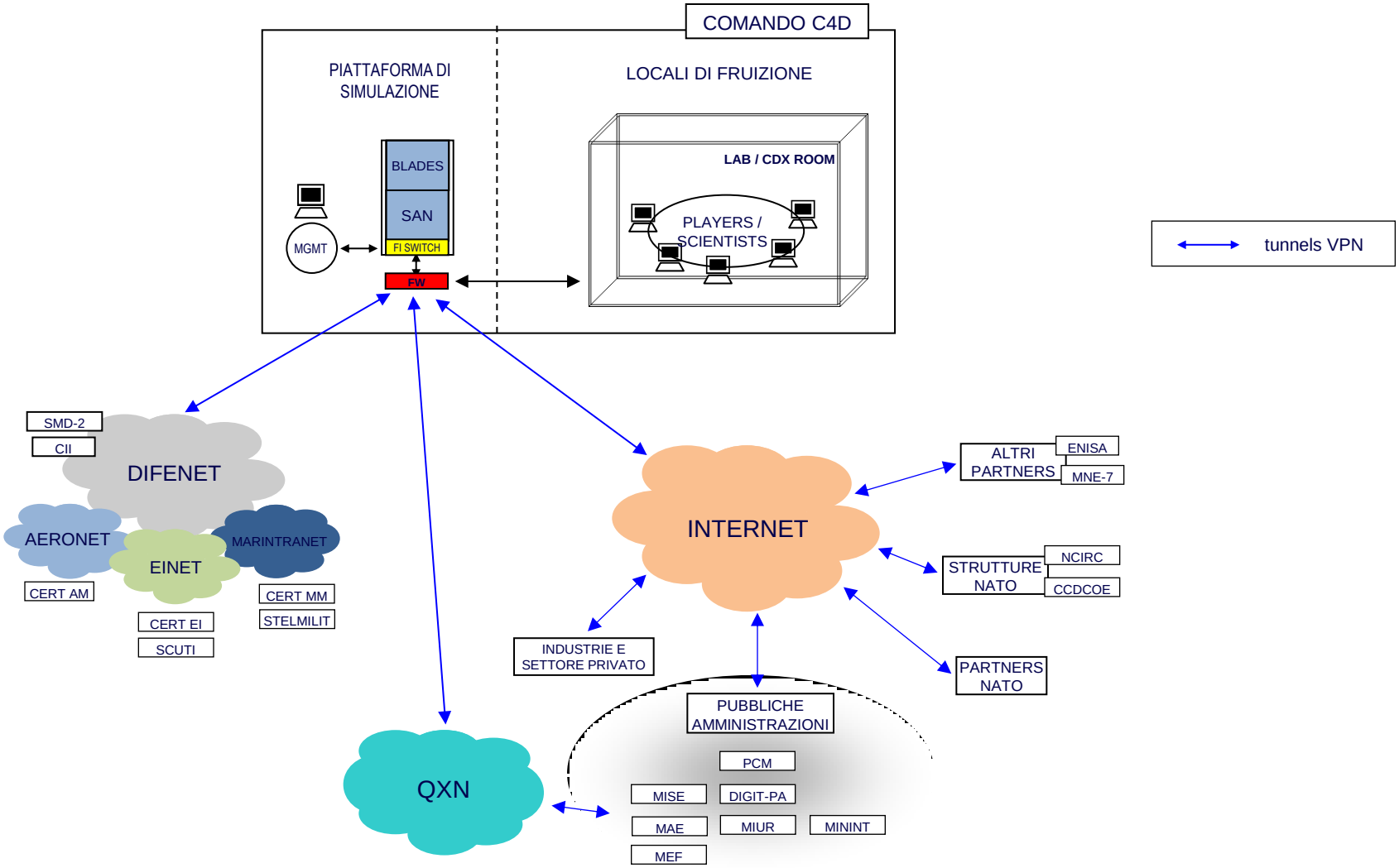
**MAX. 20 PLAYERS**

**MAX. 5 ADMINISTRATORS**

**OR … 25 SCIENTISTS ☺**

# EVOLUZIONI CD
# VIRTUAL CYBER DEFENCE BATTLE LAB





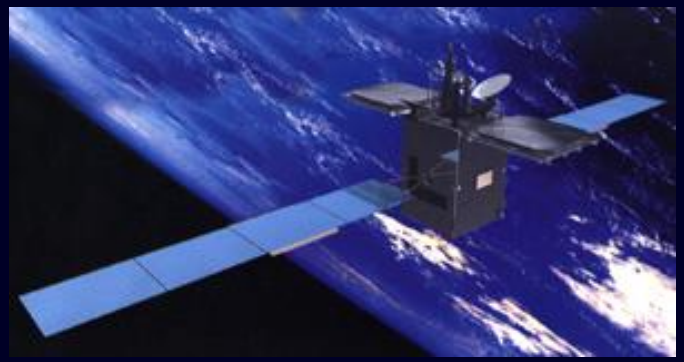
# CYBER SECURITY

## Cyber Defence Exercise «Locked Shields»



# COMANDO C4 DIFESA





Domande?