CYBERSPACE

- ⇨ *Hardware*
- ⇨ *Software*
- ⇨ Data
- ⇨ Users
- ⇨ Logical relations

Information Technology

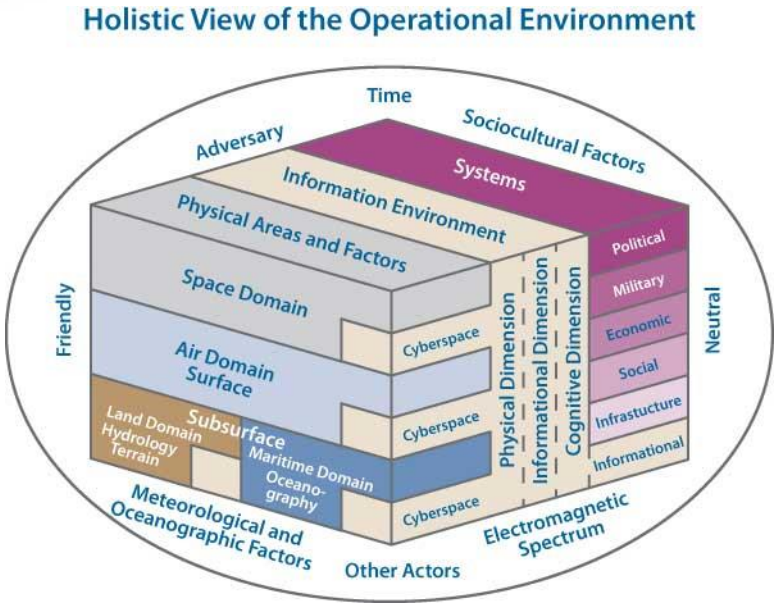
Operational Technology

Internet of Things

CYBERSPACE


NATO
OTAN
Warsaw
Varsovie
8-9 VII 2016
Summit | Sommet


Cyber Domain
Air
Sea
Space
Land


Holistic View of the Operational Environment
Time
Adversary
Sociocultural Factors
Systems
Information Environment
Physical Areas and Factors
Space Domain
Air Domain
Surface
Subsurface
Land Domain
Hydrology
Terrain
Maritime Domain
Oceano-
graphy
Cyberspace
Cyberspace
Cyberspace
Physical Dimension
Informational Dimension
Cognitive Dimension
Political
Military
Economic
Social
Infrastucture
Informational
Friendly
Neutral
Meteorological and
Oceanographic Factors
Other Actors
Electromagnetic
Spectrum

CYBER THREAT

- ⇨ Long range capabilities
- ⇨ Exploitation of vulnerabilities of systems, also sophisticated and protected
- ⇨ Defensive reactions ineffective due its time of action
- ⇨ Anonymity and deception

Cybercrime

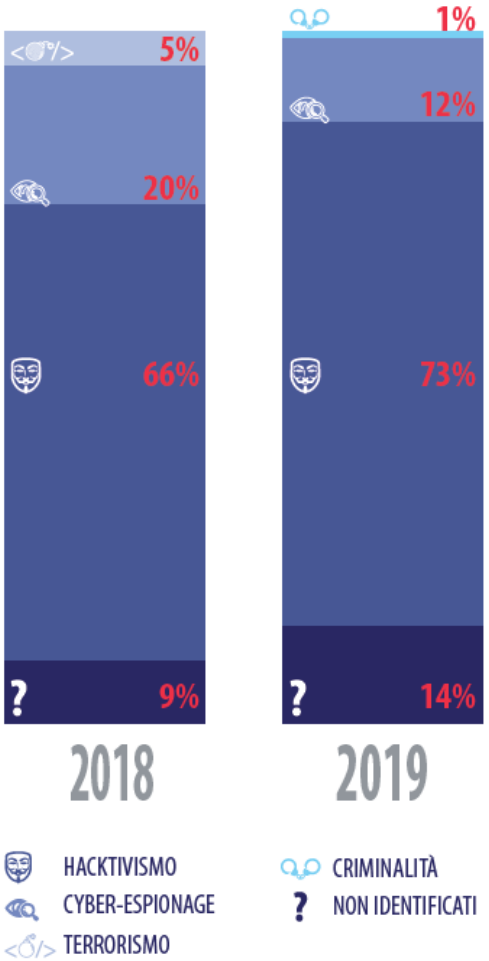
Cyber-espionage

Cyber-terrorism

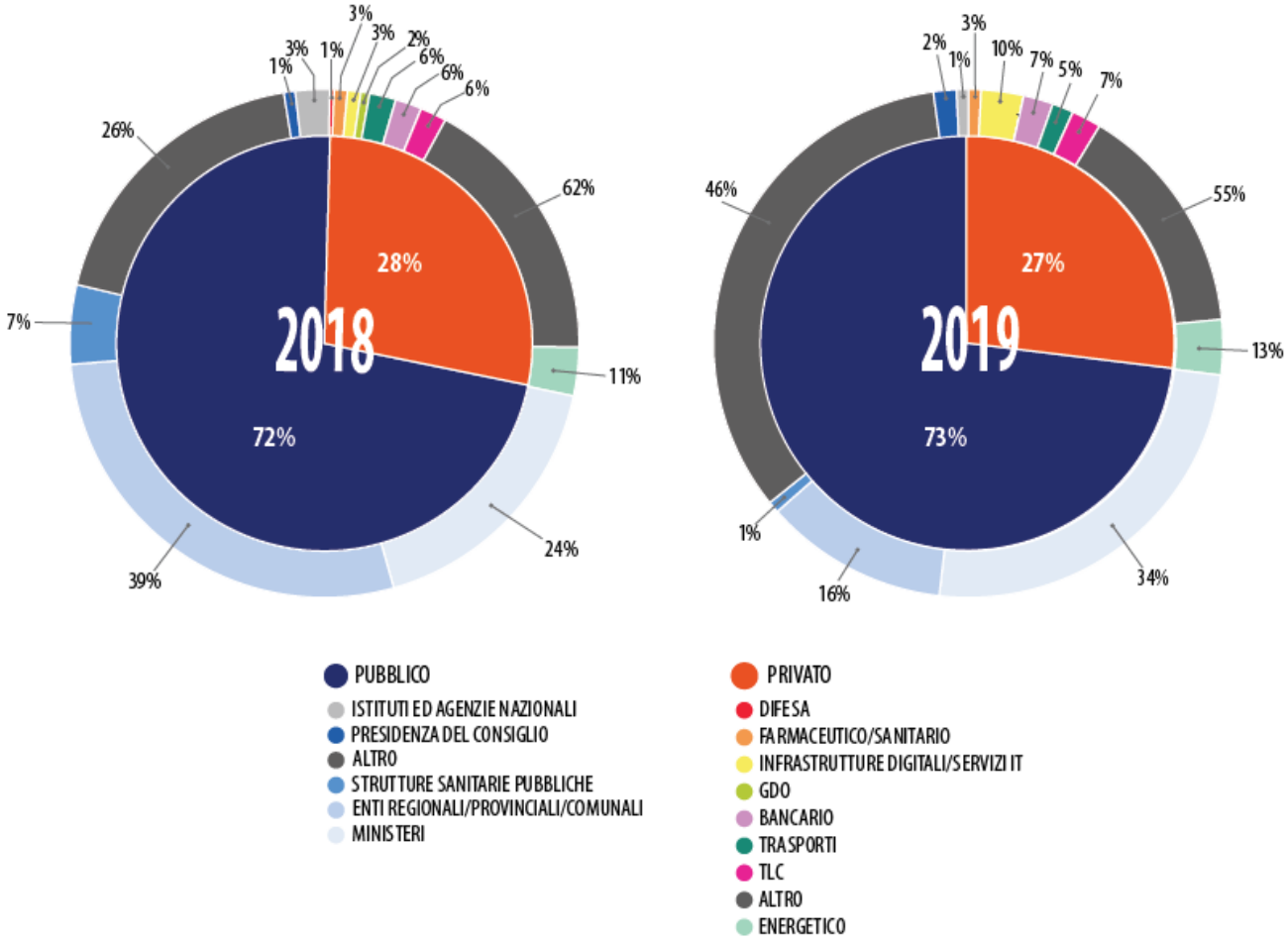
⇨ Cyber-warfare

CYBER THREAT

ATTACCHI PER TIPOLOGIA DI ATTORI



ATTACCHI PER TIPOLOGIA DI TARGET



CYBER THREAT

OPPORTUNISTIC

Methods based on:

⇨ known vulnerabilities;

⇨ supposed poor defensive measures.

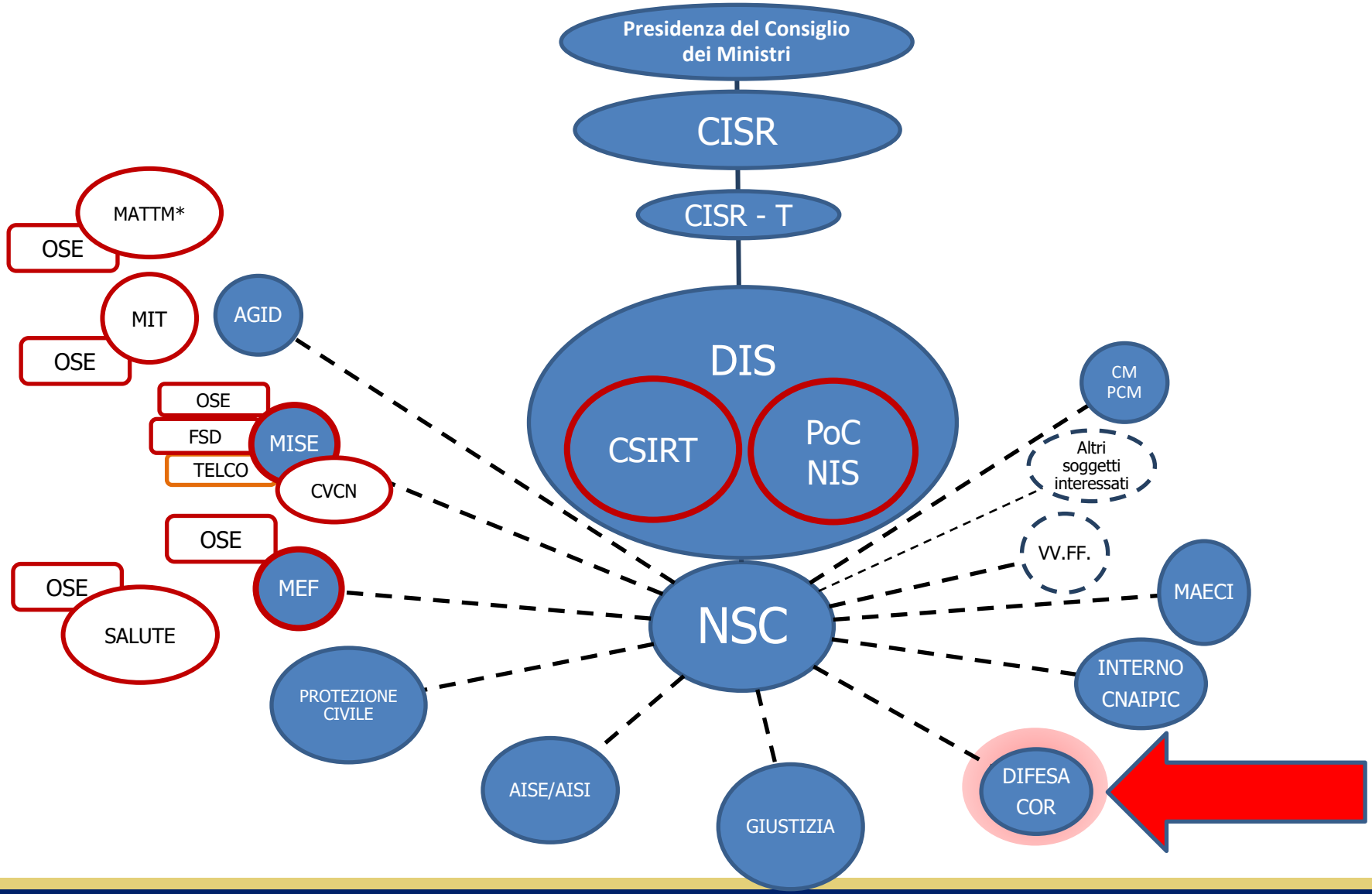
TARGET ORIENTED

Methods based on:

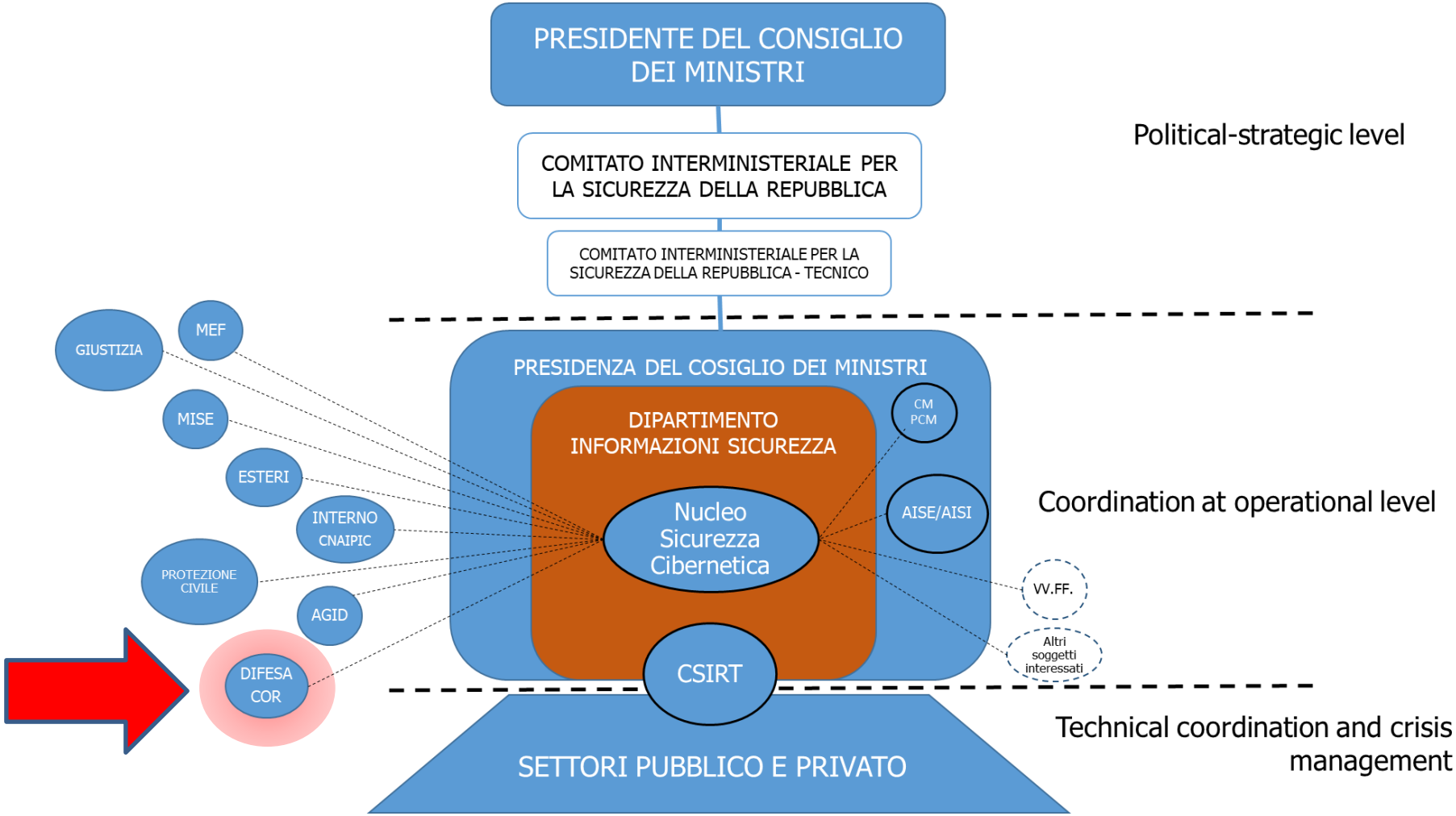
⇨ 0-day vulnerabilities;

⇨ supposed strong defensive measures (intelligence activity required).

ITALIAN CYBER ECOSYSTEM



ITALIAN CYBER ECOSYSTEM



ITALIAN CYBER ECOSYSTEM – DEFENCE MISSION

STRATEGIC LEVEL

⇨ To define and coordinate **military policy**, **governance** and **capabilities** within cyberspace

⇨ To plan, conduct and sustain military operations (**Computer Network Operations**) within cyberspace in order to counter and neutralize every threat and/or cyber hostile action to the defence services, both at **Homeland and abroad** (including Opeational Theatres)

⇨ To contribute to prevent and disrupt **terrorist activities**

- **Computer Network Attack;**
- **Computer Network Defence;**
- **Computer Network Exploitation.**

⇨ To preserve and defend the **new domain** (cyberspace)

ITALIAN CYBER ECOSYSTEM – DEFENCE MISSION

OPERATIONAL LEVEL

⇨ To **implement** operational capabilities of organizations in charge of defending cyberspace

⇨ To **develop** C2 (Command & Control) structures in charge of planning and conducting military operations within cyberspace, effectively, quickly and by a distributed organization

ITALIAN CYBER ECOSYSTEM – DEFENCE ORGANIZATION

JOINT CYEBR OPERATIONS COMMAND
2017 - 2020

TASK

⇨ To **plan**, **conduct** and **execute** military operation (full spectrum) within the cyberspace

⇨ To **counter** and **neutralize** every threat and/or cyber opposing action against defence networks, systems or services

SCOPE

⇨ To preserve **friendly forces freedom of action** within the cyberspace

⇨ To deny/limit **opposing forces freedom of action** within the cyberspace

⇨ To grant **freedom of action within all domains**

ITALIAN CYBER ECOSYSTEM – DEFENCE ORGANIZATION

Ministry of Defence Guidelines (2019)

NETWORK OPERATIONS COMMAND (COR)

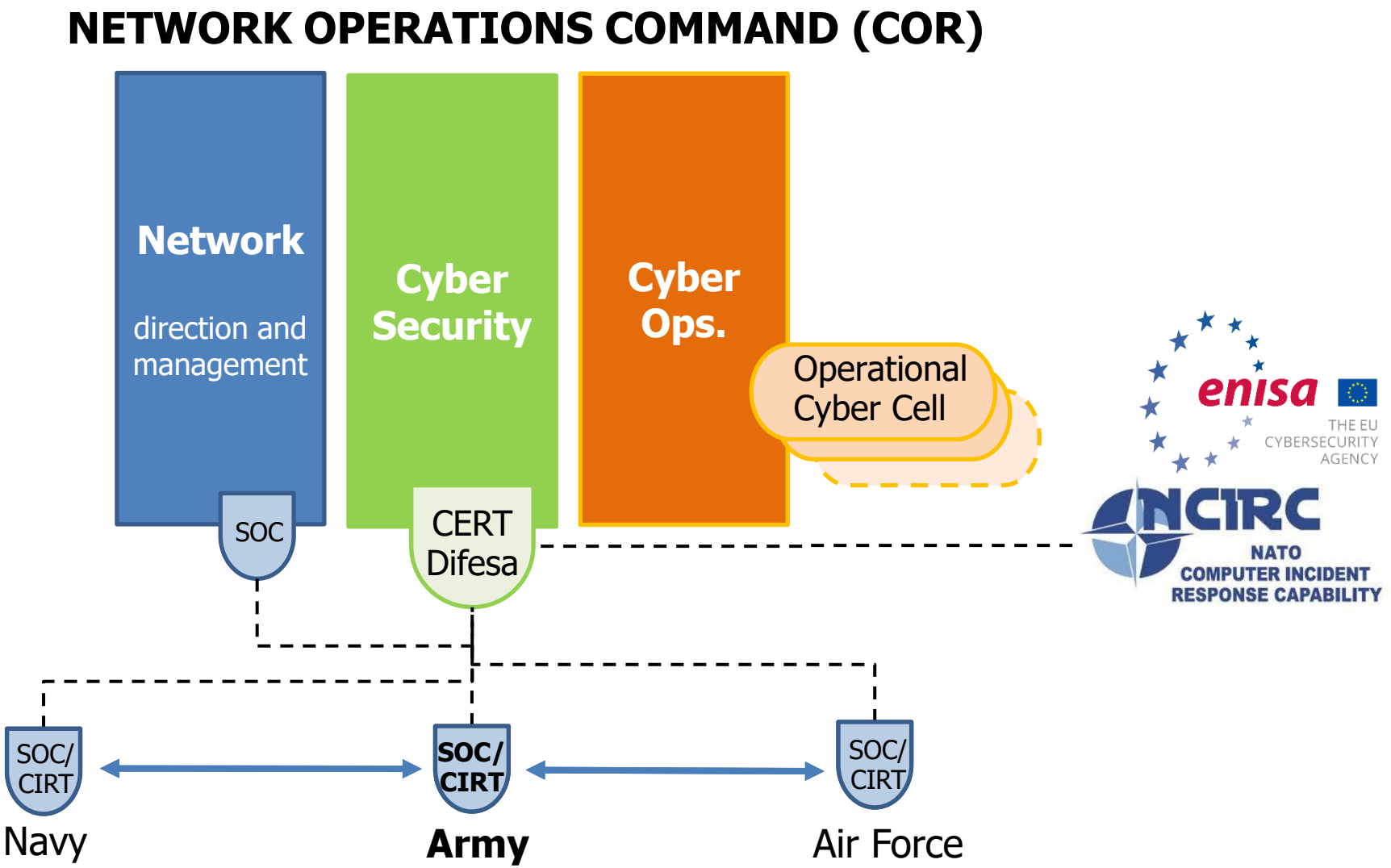
To **unify direction** of joint Information and Communications Technology (ICT), cyber security and cyber operations, in order to **harmonize** and **rationalize** Defence organization

Chief of Defence Strategic Concept 2019

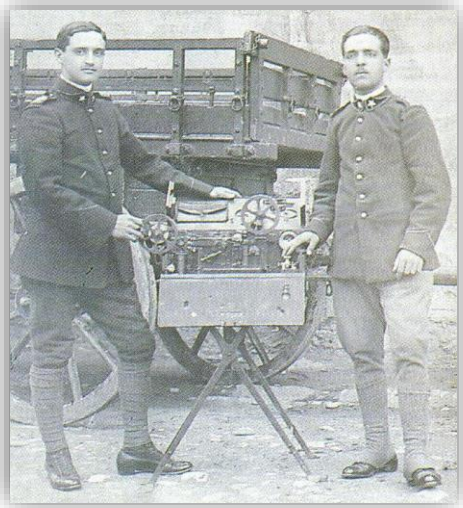
COR **responsible** for cyber environment (lead)

- Technical direction of joint ICT
- Protection of joint ICT
- Computer Network Operations

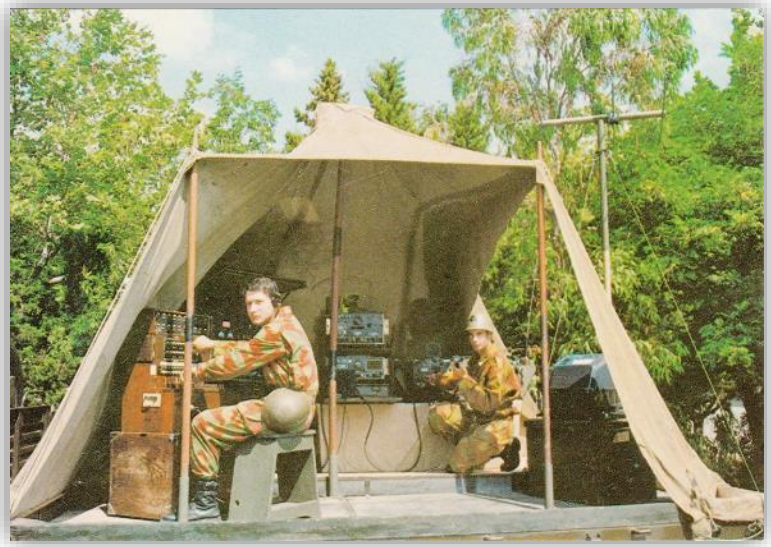
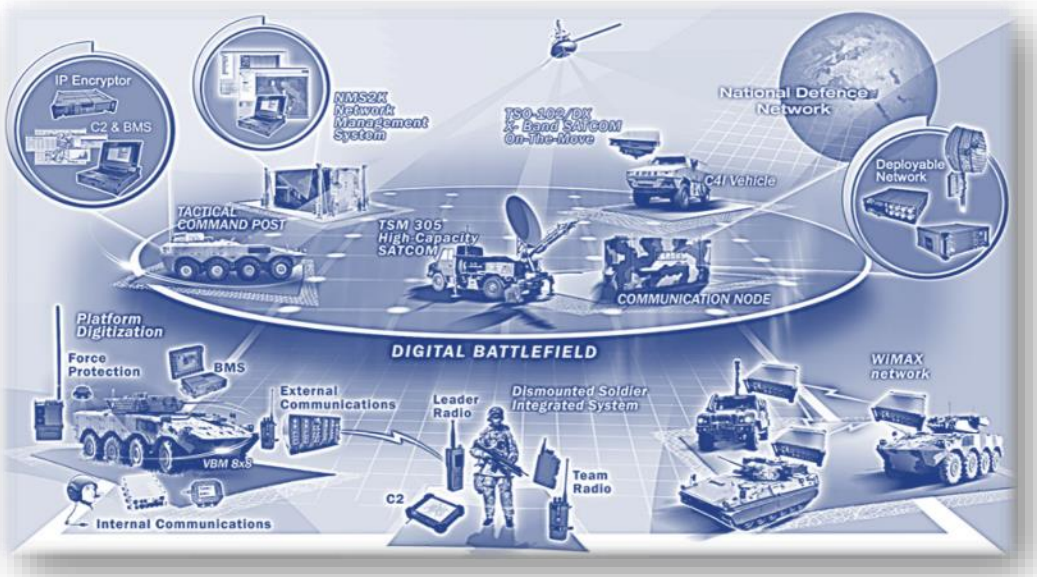
ITALIAN CYBER ECOSYSTEM – DEFENCE ORGANIZATION







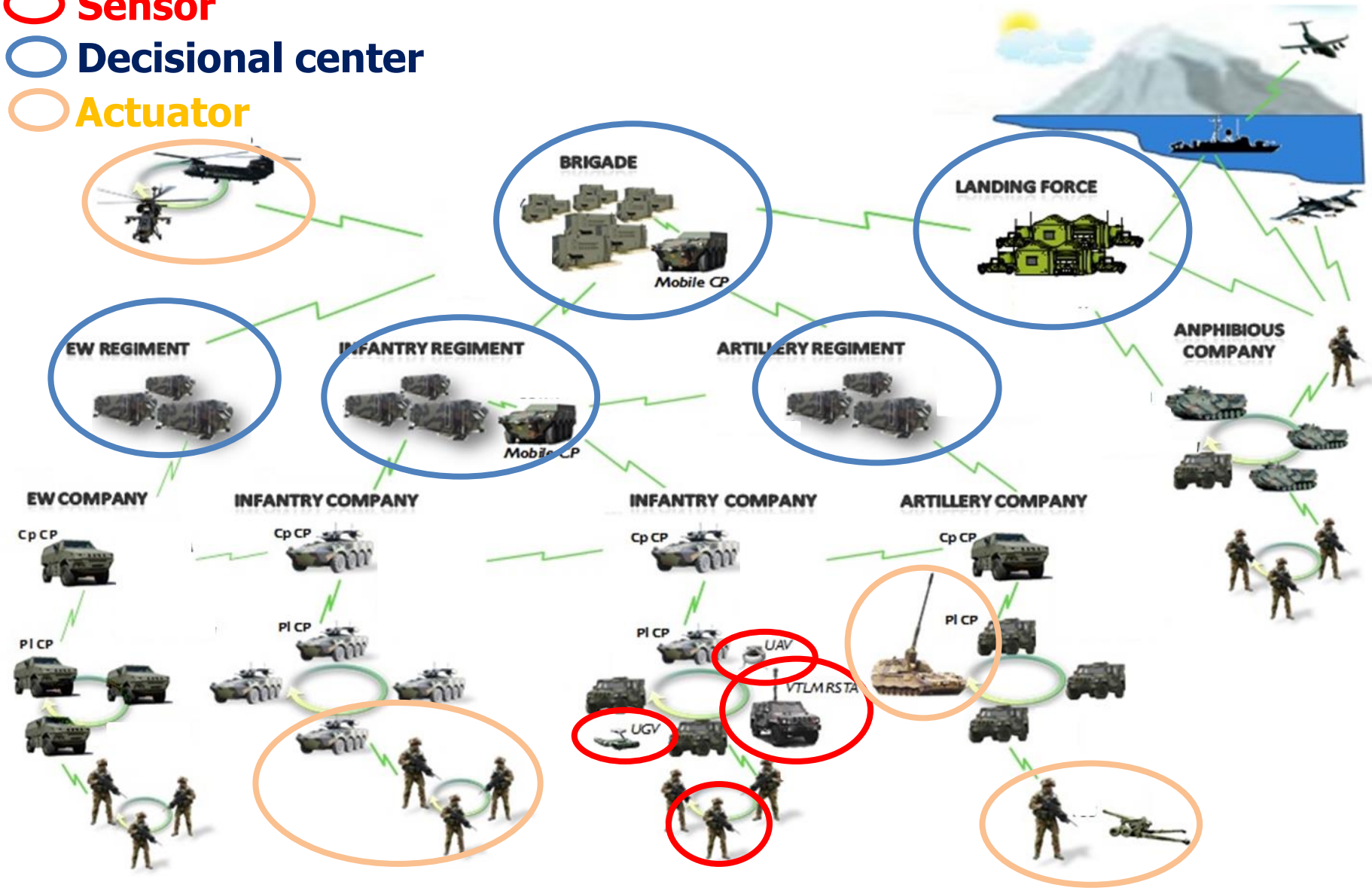

COMMAND & CONTROL

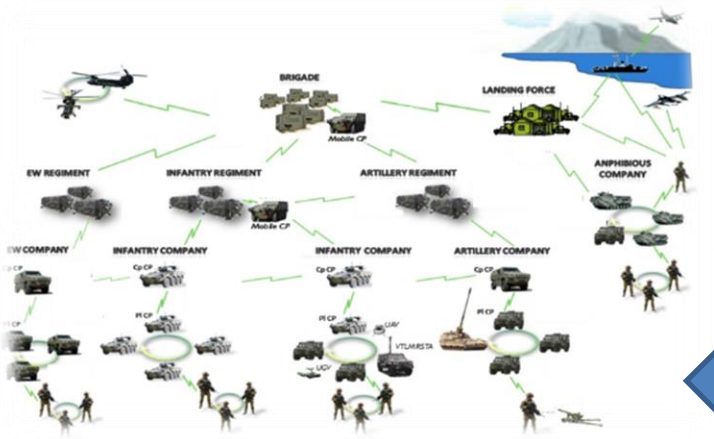
Sensor

Decisional center

Actuator



CYBERSPACE THREE-LAYER STRUCTURE



PHYSICAL

LOGICAL

COGNITIVE (CYBER-PERSONA)

CYBER THREAT

COMMUNICATIONS SYSTEMS

DEGRADATION/DISRUPTION/
DESTRUCTION

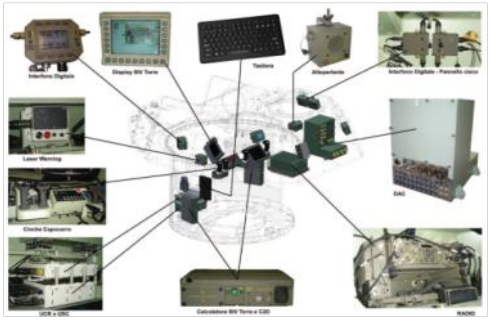
DATA AND INFORMATION

DISRUPTION/DESTRUCTION
EXFILTRATION
MANIPULATION

COMMAND & CONTROL/INFORMATION SYSTEMS

DEGRADATION/DISRUPTION/
DESTRUCTION

COMBAT PLATFORMS



DEGRADATION/DISRUPTION/DESTRUCTION

NO COMBAT PLATFORMS

DEGRADATION/DISRUPTION/
DESTRUCTION

CYBER THREAT

HOST NATION CRITICAL INFRASTRUCTURES

DEGRADATION/DISRUPTION/ DESTRUCTION

HOST NATION POPULATION

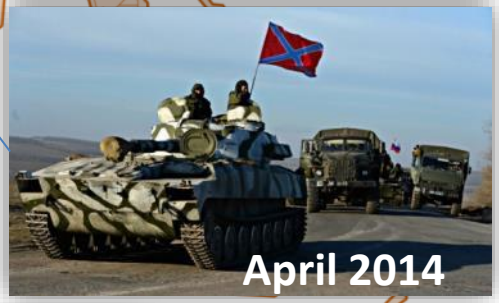
PSYCOLOGICAL OPERATIONS INTELLIGENCE

FRIENDLY FORCES/FAMILIES

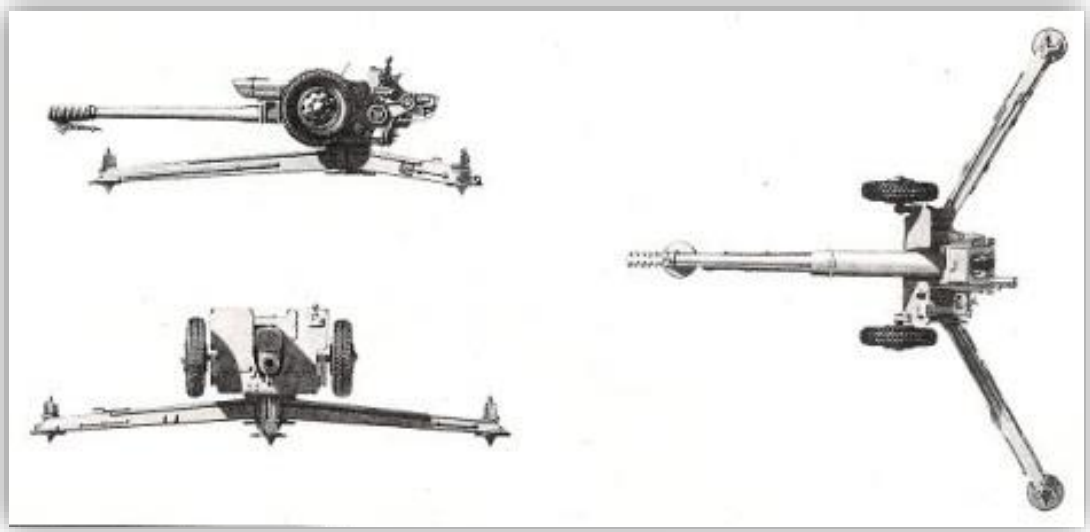
PSYCOLOGICAL OPERATIONS INTELLIGENCE

CYBER THREAT

D-30 CASE STUDY (UKRAINE, 2014-16)



D-30 CASE STUDY (UKRAINE, 2014-16)



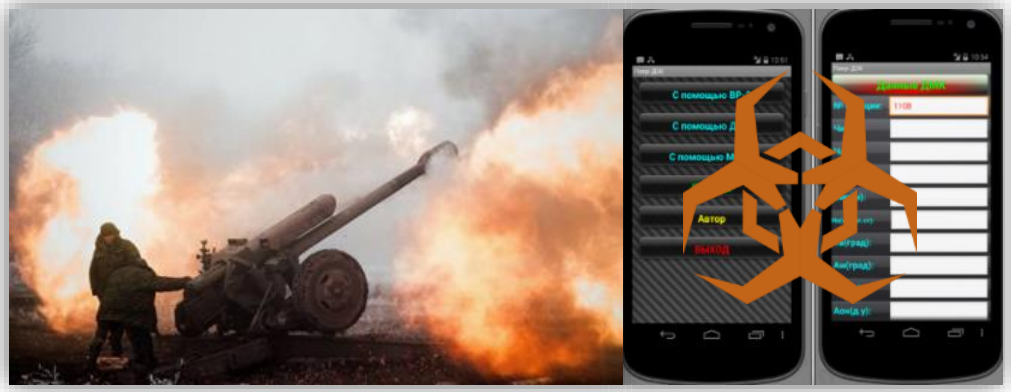
HOWITZER D-30	
Year	**1960**
Weight	3210 kg
Length	5,4 m
Barrel length	4,875 m
Caliber	122mm
Shooting speed	1 shot per minute
Maximum range	15.400m (22 km with rocket propelled rounds)
Elevation	-7° ÷ 70°

Android Software Application to facilitate fire direction

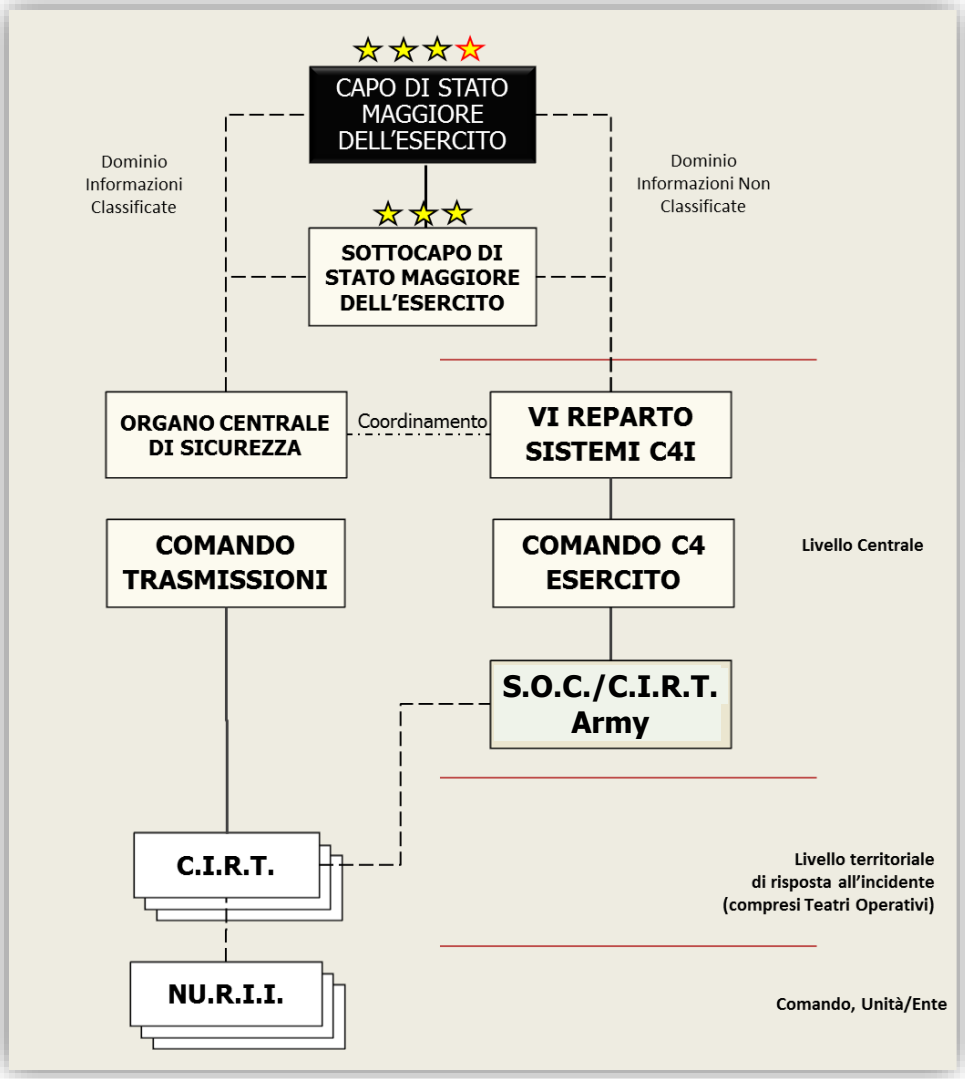
D-30 CASE STUDY (UKRAINE, 2014-16)

Fancy Bear/ATP28/Pawn Storm/Sofacy Group/Sednit/Strontium

MORE THAN 20% OF D-30 UKRAINE HOWITZER DAMAGED/DESTROYED



MORE THAN 9.000 DOWLOAD OF POISONED VERSION (X-AGENT) OF SOFTWARE



Set of **doctrine**, **organization** and **activities** aimed to **prevent**, **detect**, **limit** and **counter** the effects of attacks conducted through the cyberspace, in order to damage at least one of its component.

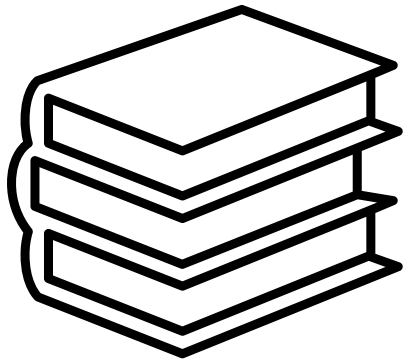
C4I: Command, Control, Comunications, Computer e Information
C.E.R.T.:Computer Emergency Response Team
C.I.R.T.: Computer Incident Response Team
NU.R.I.I.: Computer Incident Response Cell

SECURITY OPERATIONS CENTRE

- ⇨ **Prevent and detect** cyber incidents/attacks
- ⇨ **Minimize** cyber incidents/attacks impact
- ⇨ **Support** recovery activities
- ⇨ **Advise** and cooperate for *Cyber Defence* education, training and awareness

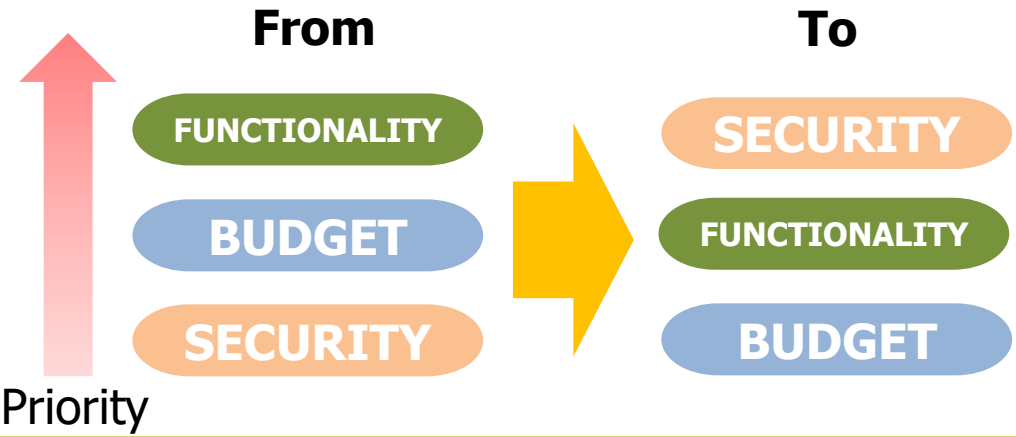
Awareness

Doctrine & Regulations



Education and Training

Procurement



GOVERNANCE ADAPTATION

- From «CERT – Army» to «SOC/CIRT – Army»
- Cyber incidents response procedures

DEPLOYABLE CYBER DEFENCE CAPABILITIES PROGRAM

- Support capabilities development of COR (Army role)
- Develop deployable cyber capabilities similar to Allies and Partner Nations ones (Army Staff Talks)
- Fulfil NATO requirements for deployable Headquarters

"*CYBER DEFENCE CAPABILITY* – E.I."

Renew Cyber Defence capabilities (static) implementing a new state-of-art technological platform, interopable with joint one (focus on Army C4 Command).

CYBER DEFENCE TRAINING FACILITY

Infrastructure dedicated to support basic education, training, familiarization and awareness on Cyber Defence (focus on Signals Command).

CYBER SECURITY UNIT

REQUIREMENTS

- To fulfil NATO operational requirements for deployable Headquarters
- To support COR for Cyber Operations (personnel)
- To be able to deploy Cyber Defence capabilities in operations
- To improve technical education, training and familiarization with Army systems and network difesa cibernetica)

SOLUTION

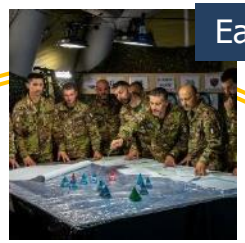
- Cyber Security specialized Unit, at Battalion level
- Deployable teams of high specialized personnel
- Modular capabilities (flexible number and composition of teams)
- Integration with Signals Units
- Cyber Defence Training Facility

CYBER SECURITY UNIT

FACTS

Est. - 2019, 1st April

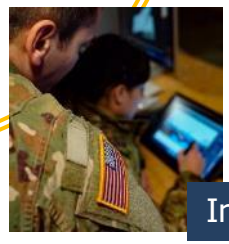
IOC - 2019, 20th June



Eagle Meteor 19

Joint Stars 19

Atlante 19



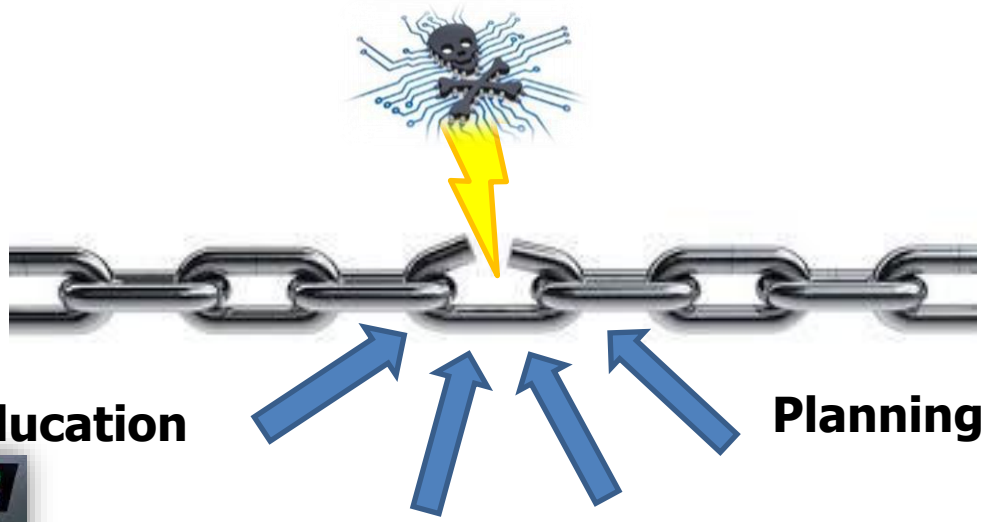
Intrepid Knight 19

Cyber Coalition 19

Exercices

SANS - 2019, December

- ⇨ *Hardware*
- ⇨ *Software*
- ⇨ Data
- ⇨ **Users**
- ⇨ **Logical relations**



List of references:

Italian cyber ecosystem

https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/quadro-strategico-nazionale-cyber.pdf
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2017/05/piano-nazionale-cyber-2017.pdf
https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2019-09-21;105!vig=
https://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/decreto-legislativo-18-maggio-2018-n-65.html
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2019/11/GAZZETTA-UFFICIALE-CSIRT.pdf
https://www.difesa.it/Primo_Piano/Documents/2015/04_Aprile/LB_2015.pdf
https://www.difesa.it/SMD_/CaSMD/concetto_strategico_casmd/Pagine/default.aspx
https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2020/03/RELAZIONE-ANNUALE-2019-4.pdf

Studies and reports

http://documenti.camera.it/leg17/resoconti/commissioni/bollettini/pdf/2017/12/20/leg.17.bol0935.data20171220.com04.pdf
http://documenti.camera.it/leg18/dossier/pdf/DI0162.pdf
https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf

Hearings & speeches

http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/html/0104/audiz2/audizione/2017/06/14/indice_stenografico.0002.html
http://documenti.camera.it/leg17/resoconti/commissioni/stenografici/pdf/04/indag/c04_cibernetico/2017/01/25/leg.17.stencomm.data20170125.U1.com04.indag.c04_cibernetico.0009.pdf
http://www.esercito.difesa.it/organizzazione/capo-di-sme/Documents/Audizione-del-capo-di-SME-20-settembre-2018.pdf
https://www.camera.it/leg18/1132?shadow_primapagina=8537
http://documenti.camera.it/leg18/resoconti/commissioni/stenografici/html/0109/audiz2/audizione/2019/10/08/indice_stenografico.0001.html
http://www.cesmamil.org/wordpress/wp-content/uploads/2018/02/2-_-Gen.-BA-F.-Vestito-_-Propsettive-sulla-Sicurezza-Cibernetica-della-Difesa.pdf

Documents from Italian Army

http://www.esercito.difesa.it/comunicazione/Le-5-Sfide/Documents/Italian%20Army%20-%20Preparing%20together%20for%20the%20challenges%20of%20tomorrow.pdf
http://www.esercito.difesa.it/comunicazione/Le-5-Sfide/Documents/FOE-INGLESE191205.pdf
http://www.esercito.difesa.it/Rapporto-Esercito/Documents/RE17%203101%20MEDIUM%20PER%20INTERNET.pdf
http://www.esercito.difesa.it/Rapporto-Esercito/Documents/RE-2018-rid-190329.pdf
http://www.esercito.difesa.it/Rapporto-Esercito/Contenuti-multimediali-RE-19/Documents/2019/RE19_ITA_INTERNET_A4_200317.pdf

NATO and miscellaneous

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf
https://www.nato.int/cps/en/natohq/topics_78170.htm
http://www.iai.it/sites/default/files/iaiq_02.pdf