MILITARY ACTIVITIES IN CYBER SPACE

CLASSIFICATION, ANALYSIS, ORGANIZATION, CONDUCTING

Lieutenant Colonel (ITAAF) Alessandro Chianello

NATO Science & Technology Organization - Office of the Chief Scientist – STRATCOM Officer

ISEG Evaluator Member

chianello.alessandro@hq.nato.int

OUTLINE

- **OVERVIEW**
- **CLASSIFICATION OF MILITARY ACTIVITIES CONTRIBUTING THE DEVELOPMENT OF CYBER MILITARY OPERATIONS**
- **ANALYSIS OF CYBER MILITARY ACTIONS**
- **BUILDING A CYBER DEFENSE CAPABILITY: A REAL EXAMPLE**
- **CYBER OPERATIONS PLANNING AND CONDUCTING**
- **RECOMMENDATIONS AND CONCLUSIONS**

References:

IT CHoD JIC-012 “Cyber-warfare”
NATO AJP-3.20 “Allied Joint Doctrine for Cyberspace Operations“

OVERVIEW

The implementation of the cyber defence requires the development of appropriate abilities to fit military operations in the cyber space

The awareness of a possible cyber-warfare matured recently. National and international juridical framework has not been adjusted to the forecast of a cyber-warfare yet.

- Cyber space can be exploited for operations. Cyber Activities can be developed and conducted from any point of the world and in extremely rapid, economic, anonymous way with devastating effects.

- Cyber operations are not limited to operating government. Contrarily to a conventional military attack, a cyber attack doesn't need/ask for the sponsorship of a State.

In the Cyber space domain the Defense Force, in respect of its uniqueness and assigned roles, has a double assignment:

- to develop some abilities and a doctrines such to be able to assure the Situational Awareness
- to operate with enough advantage in terms of initiative in comparison to enemies or potential opponents

LEGITIMATE USE OF THE “CYBER WEAPON”

Legal considerations

- There are neither agreed norms nor approved behaviors; all nations, groups, individuals and organizations have the flexibility to render an incident or attack, its seriousness and how to respond.

- There are no clear ‘boundaries’ to determine thresholds between persistent threat, use of force, everyday activity or an attack.

It is essential that commanders, planners and operators consult with legal advice during planning and execution of cyberspace operations.

commanders, planners and operators must
- understand the relevant legal framework and authorities under which they operate
- appropriately comply with applicable laws, treaties and policies.

SPECIAL FOCUS ON:

- **Dual use objects.** may have both military and civilian uses which may render these types of objects more difficult to identify as legitimate military targets.

- **Collateral damage estimation.** can be more difficult in the context of cyberspace operations compared to more traditional physical means or weapons.

CYBER MILITARY ACTIVITIES CLASSIFICATION

The classification process is a challenging process . It is affected by:

- missed distinction among different activity concept. Example: the information manipulation on a database is a "Cyber Attack" or an "Information Operation?"

- “non coherent” use of the definitions. Example: confusing use among terms like "Cyber Security", "Cyber Defence", and "Computer Network Defence" (CND).

- "non exhaustive" formal definitions. Example: it is a mistake to consider as "attack" activity like theft of identity, the non authorized access and the gathering of data, that are to frame as activity of intelligence or can be included in the domain of cyber crime.

CONSIDERATIONS FROM THE ACTUAL EXPERIENCE

Definition of basic parameters to classify Cyber Military Activities by a new and more articulated model of classification

Definition of Cyber Military Activities' details

CLASSIFICATION OF MILITARY ACTIVITIES CONTRIBUTING THE DEVELOPMENT OF CYBER MILITARY OPERATIONS

Definition of basic parameters to classify Cyber Military Activities

DEFINITIONS OF REFERENCE:

- MILITARY ACTIVITY : one or more military actions, aimed at the realization of a military operation

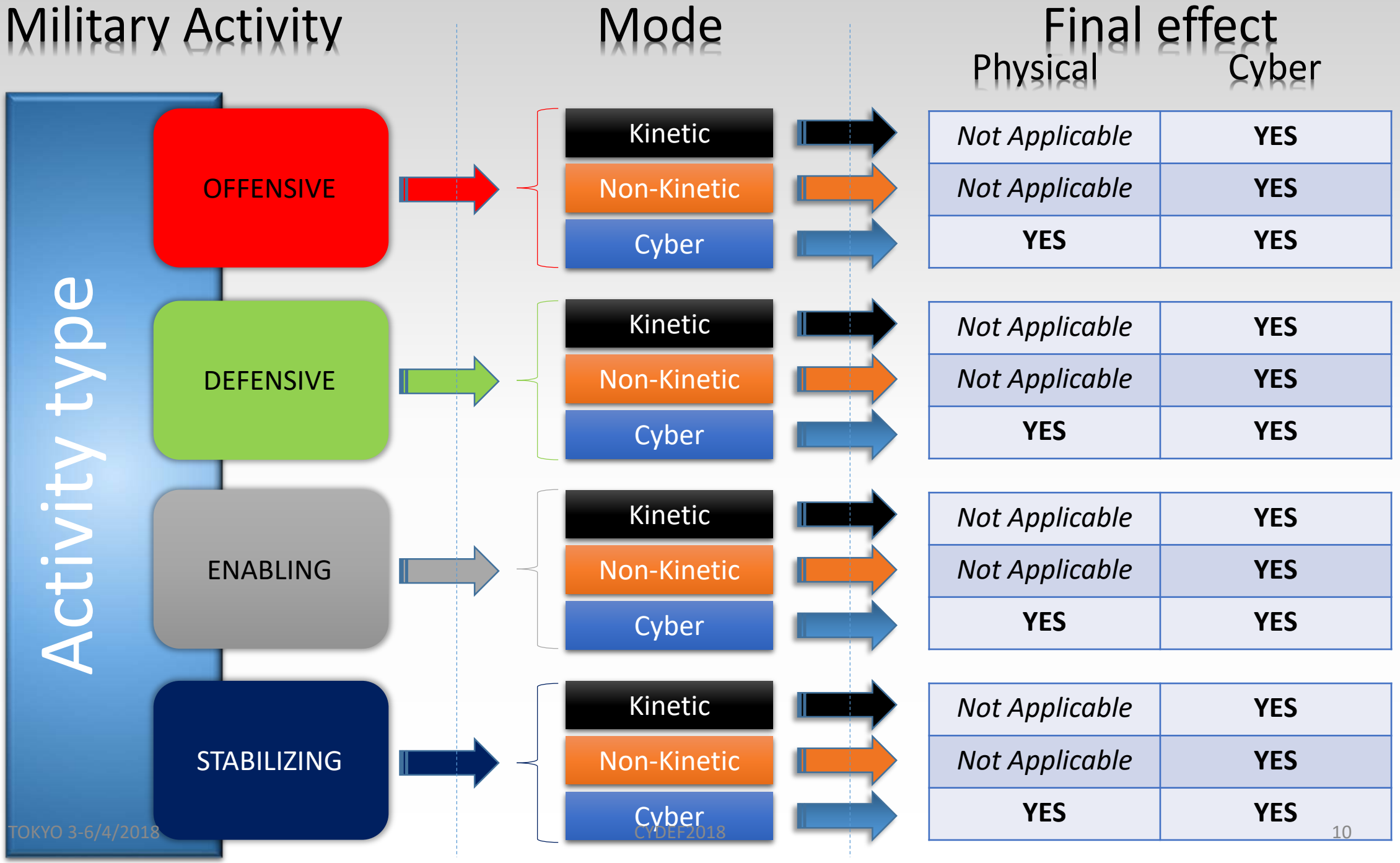
- CYBER MILITARY ACTION: Action conducted from military with military cyber orders, and not, in a military operation.

ELEMENTS OF CLASSIFICATION:

- purpose of the military activity (Defensive, Offensive, Enabling, Stabilization)

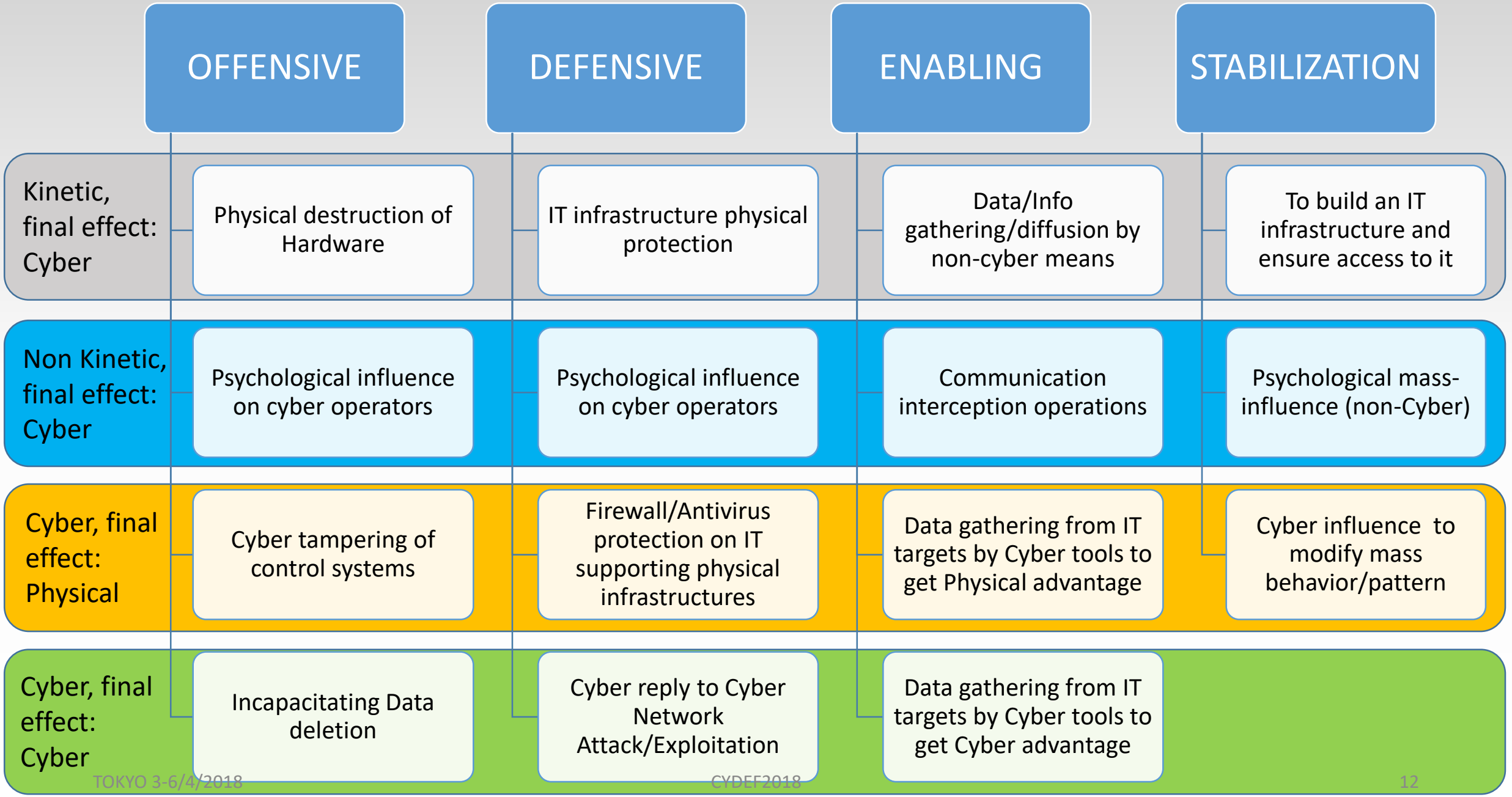
- Modes (kinetic, non kinetic, cybernetic)

- Type of final effect (physical or not physical)


Military Activity
Mode
Final effect
Physical
Cyber
Activity type
OFFENSIVE
DEFENSIVE
ENABLING
STABILIZING
Kinetic
Non-Kinetic
Cyber
Not Applicable
YES
Not Applicable
YES
YES
YES
Kinetic
Non-Kinetic
Cyber
Not Applicable
YES
Not Applicable
YES
YES
YES
Kinetic
Non-Kinetic
Cyber
Not Applicable
YES
Not Applicable
YES
YES
YES
Kinetic
Non-Kinetic
Cyber
Not Applicable
YES
Not Applicable
YES
YES
YES

Definition of cyber military activities' details

- Decomposing the military activities related to cyber military operations in ***component actions***
- Defining the typology and analysis of the ***component actions***


OFFENSIVE
DEFENSIVE
ENABLING
STABILIZATION
Kinetic, final effect: Cyber
Physical destruction of Hardware
IT infrastructure physical protection
Data/Info gathering/diffusion by non-cyber means
To build an IT infrastructure and ensure access to it
Non Kinetic, final effect: Cyber
Psychological influence on cyber operators
Psychological influence on cyber operators
Communication interception operations
Psychological mass-influence (non-Cyber)
Cyber, final effect: Physical
Cyber tampering of control systems
Firewall/Antivirus protection on IT supporting physical infrastructures
Data gathering from IT targets by Cyber tools to get Physical advantage
Cyber influence to modify mass behavior/pattern
Cyber, final effect: Cyber
Incapacitating Data deletion
Cyber reply to Cyber Network Attack/Exploitation
Data gathering from IT targets by Cyber tools to get Cyber advantage

CYBER MILITARY ACTIONS ANALYSIS
1-DEFENSIVE, 2-INTELLIGENCE, 3- OFFENSIVE

Planning, and conducting basic criteria

- **ETHIC**
- **JURIDICAL** (juridical-legal national and juridical- legal international)
- **POLITICS-STRATEGIC**
- **OPERATIONAL**
- **DECISION-MAKING**
- **CONSEQUENCE MANAGEMENT**

DEFENSIVE ACTIONS
- Analysis -

JURIDICAL

- the compliance with ICT, Information Assurance normative and (above all) the privacy protection

OPERATIONAL

- there are no constrains related to the principle of self-defence that legitimates the defensive actions

CONSEQUENCE MANAGEMENT

- there are no elements of particular attention. In case of an incident or in presence of attack, the active reaction must be balanced between a possible partial impairment or unavailability of some services of public utility for a limited time up to the full safe restoration. An effective redundancy could avoid limitations in defensive actions.

INTELLIGENCE, SURVEILLANCE & RECONNAISANCE ACTIONS
- Analysis -

They are conducted in anonymity and without producing harmful effects or damages on the networks, systems and infrastructures

INCLUDE

- The OSINT (Open Source Intelligence) always conducted in the full respect of the law,
- The SIGINT (SIGnals INTelligence)
- the “surgical” actions of active nature like the Cyber Access Operations
- The use of software tools of offensive nature, but opportunely set to satisfy intelligence requirements and not to destroy or to make direct damages.

The opponent could read as offensive actions

OFFENSIVE ACTIONS
-Analysis-

With regard to the ***limited or moderate*** use of force

Cyber Soft Kill (CySK):

Temporary effects

With regard to the ***proportional*** use of force

Cyber Offensive Attack (CyOA):

Permanent effects of destruction and/or permanent modifications

OFFENSIVE ACTIONS – Analysis - in relationship to the ***limited or moderate use of force***

ETHIC

- the action to attach an enemy's asset without damaging in concrete terms, but interrupting its functionalities in a timeframe, could be justified as "limited use of force",

JURIDICAL

- despite the action doesn't cause permanent damages, it can be in contrast with the law. Within military operations such typologies of actions should be included in the Rules of Engagement (RoE);

POLITICS-STRATEGIC

- From the political-strategic point of view, such actions are intended like demonstrative. In absence of permanent cyber damages they are a tool used to support Communication / Propaganda activity, rather than a real cybernetic operations

DECISION MAKING

- The decision to use Soft Kill rather than Hard Kill to pursuit a task or to determine the origin of an action, requires evaluations comparable to the use of soft or hard kill in the most traditional domains. Therefore, this process must be strongly tied up to the situational awareness

CONSEQUENCE MANAGEMENT

- Throughout the planning phase it is necessary to evaluate possible direct or indirect dependences reducing the risk of possible collateral damages.

OFFENSIVE ACTIONS – Analysis - in relationship to the ***proportional use of force***

ETHIC

- a cybernetic attack is comparable to a traditional attack (with kinetic systems of weapon) pointing the destruction of a computer system, therefore is a hostile action. The "not kinetic“ attribute of some action (cancel / modify information without destruction of hardware) gives the option to adopt the defensive principles of proportional use of force.

JURIDICAL

- **National**: Cyber attack is legitimate under all those conditions in which other conventional forms of offensive military would be conducted by kinetic weapon.
- **International**: U.N. limits "the use of force" or the behaviour of "armed attacks" against other members states. But about the use of systems able to inflict damages to an aggressor for strategic purposes, defensive restrictions don't exist;

POLITICS-STRATEGIC

- A Cyber Offensive Action highlights the availability of a cyber capability from the aggressive Nation and shows the ampleness of possible/future targets. Such action can easily be extended to all the sectors of the public and social life of a nation

ORGANIZATION

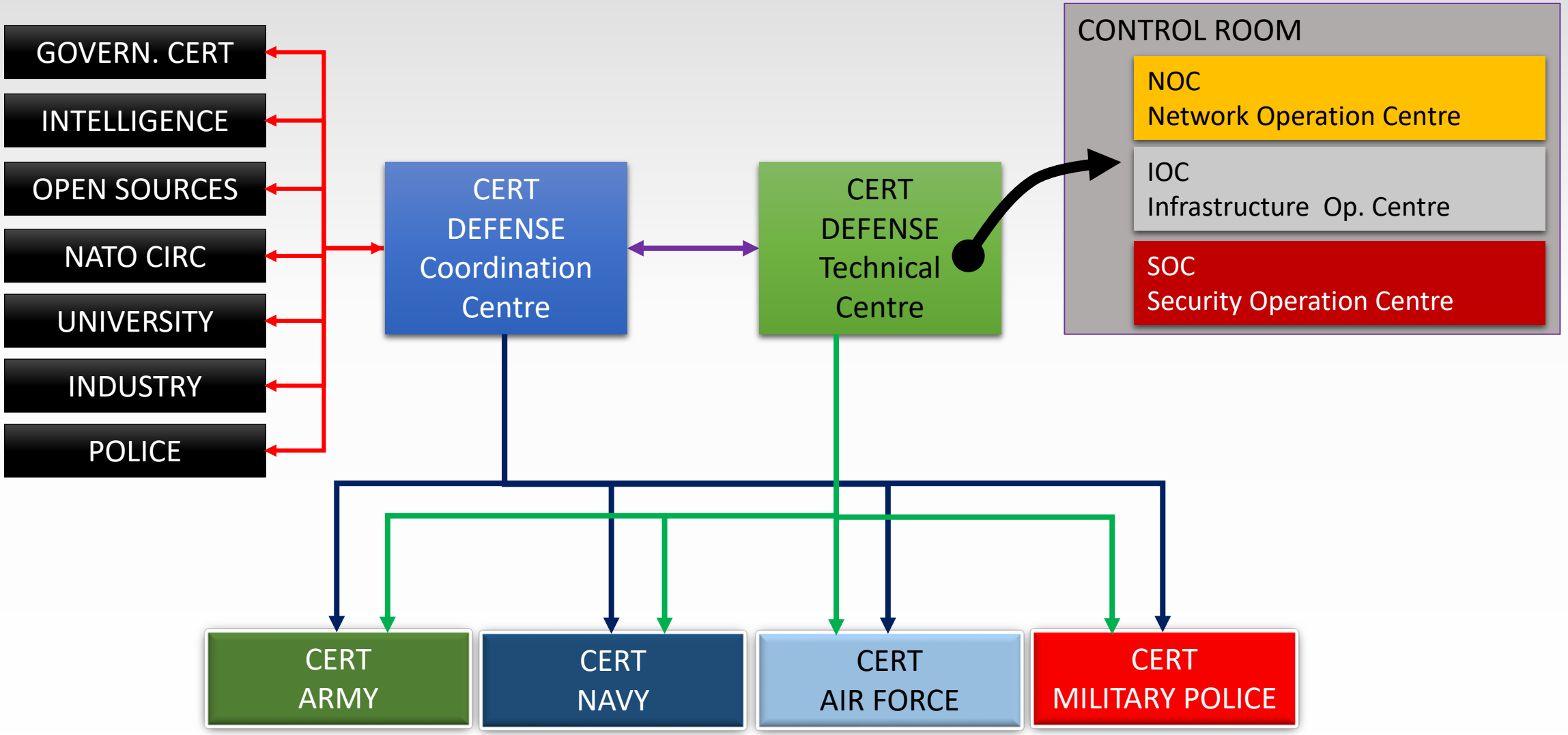
- Cyberspace operations can achieve targets or create effects on its own. Such effects have to be synchronized with other effects and capabilities of the overall operation to create synergy.

- In addition to traditional targets, cyberspace operations add potential opportunities to the range of objectives

Cyberspace operations is now an integral part of joint operations

Real case: Italian Cyber Defense Organization (Current)

Type: PASSIVE DEFENSE

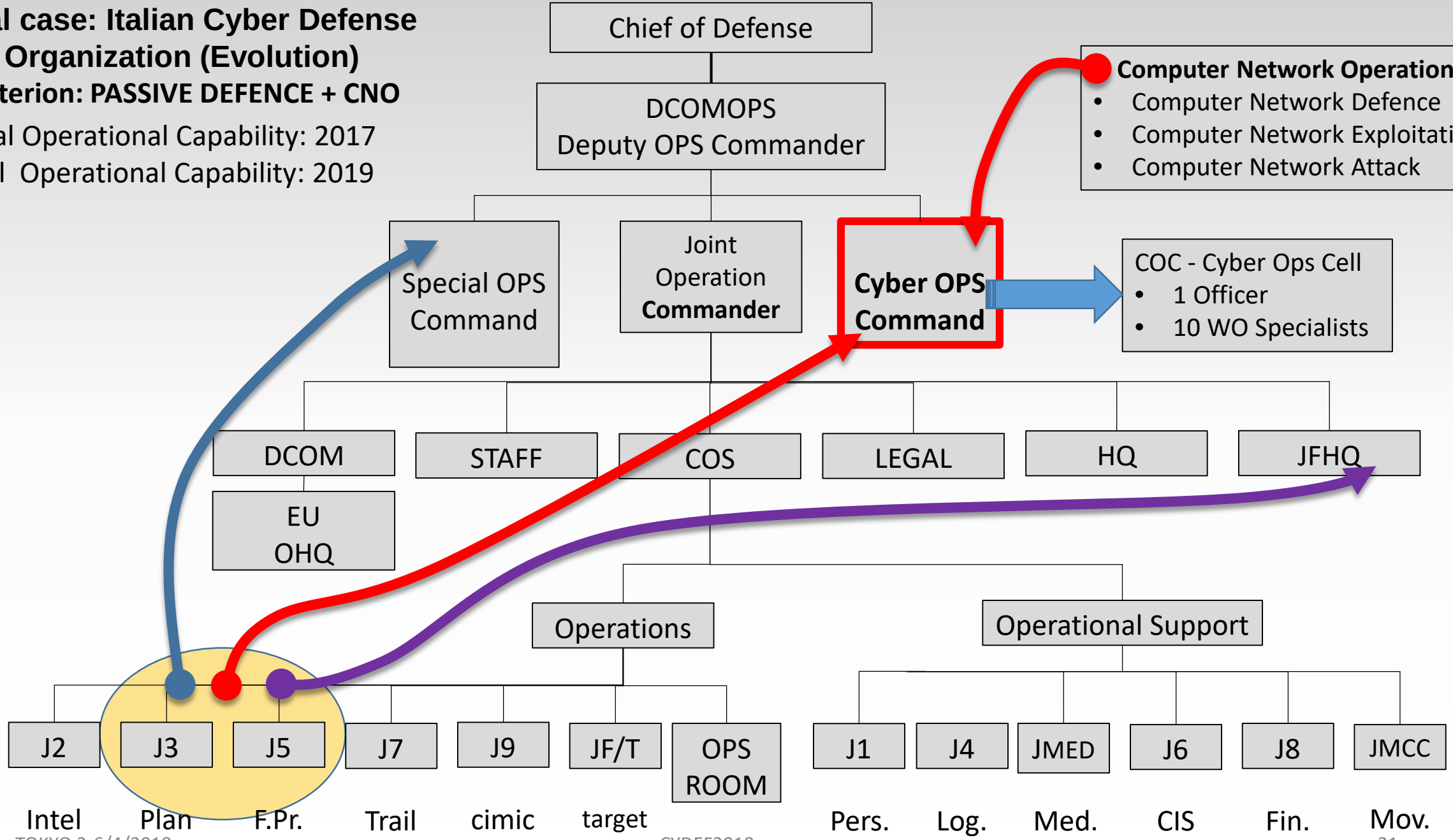


Real case: Italian Cyber Defense Organization (Evolution)

Criterion: PASSIVE DEFENCE + CNO

Initial Operational Capability: 2017

Final Operational Capability: 2019



PLANNING AND CONDUCT

PLANNING

Ongoing situational awareness/horizon-scanning

Includes an analysis of cyberspace to generate a ***recognized cyberspace picture***

Operations planning process

Planning for cyberspace operations follows the overall seven steps in the operations planning process , however, activities in cyberspace might not be directly represented in each step.

Initiation. : process developed through:

- **Mission analysis:** Made by the planning staff In coordination with other branches and capabilities
- **Course of action development and analisys**. Using the outputs from the mission analysis, the planning staff assist in the course of action COA development
- **COA validation and Commander's decision.** The planning staff must provide the commander with a recommendation of how possible cyberspace operations best contribute to mission success

Risk management : iterative process, to be handled continuously. The right balance between creating an effect and risk must be carefully considered. It requires a deliberate decision:

- whether a risk is unacceptable or acceptable, and
- if the risk can be mitigated

CONDUCTING – PREPARATION

- **Forming the force.** For cyberspace operations it is possible to source forces and capabilities within a coalition, an Alliance or potentially involving voluntary national contributions.

- **Command and control.** the commander must understand the mechanisms that are integrating cyberspace operations in the campaign. (again, the ***recognized cyberspace picture)***

- **Pre-deployment training.** Before deploying the operation

- **Preparing the joint operations area.** Shaping, securing and maintaining access to the joint operations area, is a pre-condition for mission success and must be coordinated with the joint force commander.

CONDUCTING – EXECUTION

- **Operations management.** Integrating force elements is the most effective way to conduct operations

- **Battlespace management and synchronization.** Coordination and de-confliction are conducted through battlespace management at the joint forces level. Cyberspace operations will, to the extent possible, require coordinating and/or de-confliction with other capabilities/functions.

- **Situational awareness and Analysis of opponent's cyberspace operations**. continual situational understanding is required in cyberspace.

- **Assessment.** Assessment is integrated into all phases of the planning and execution processes. Measures of effectiveness and measures of performance need to be objective where possible, never subjective.

- **Plan refinement**. Cyberspace changes and evolves continuously; this requires a thorough interaction across all staff branches.

RECOMMENDATIONS

The implementation of the cyber defence requires the development of appropriate abilities to fit military operations in the cyber space

Must be achieved by:

- urgent prioritization
- planning of appropriate financial resources
- Selecting personnel holding a suitable professional skill
- effective interoperability between the national orders and those of the allied / partner countries
- **developing a strong collaboration among military, industry and academia**

RECOMMENDATIONS

- To select personnel, either military or civil servant, holding a professional background at high level in computer science, telecommunications, electronics, intelligence and human factor
- To foresee special educational training
- To activate collaborations between military components and academic / industrial entities
- To take in account the importance of "ethical hacking" and "penetration testing" activities
- To define a set of safety measures (minimum requirements) to protect information and computer systems
- To develop a trial capability to guarantee the protection of networks and Communication / Information also in the domain of UNCLASSIFIED systems connected (or not) to internet

CONCLUSIONS

- Cyber military activities is a specific subset of the National Defense System related to the cyber space

- Military entities must be considered linked with other bodies at inter-government, industrial and academic level

THE FUTURE BATTLEFIELD WILL BE THE FIFTH DOMAIN, INTANGIBLE, PERVASIVE AND DIFFICULT TO CONTROL. INNOVATION MUST HAPPEN …NOW!

Thank you!

どうもありがとうございます

Lieutenant Colonel (ITAF) Alessandro Chianello
chianello.alessandro@hq.nato.int