Cyber Defense Competencies

A structured approach for MN CD E&T towards cyber excellence

Allard Kernkamp MSc RO

Outline

- Definition Cyber Defense
- Overall perspective: Why do we need it?
- Who wants it?
- How do we get there?
- Where are we now?
- What to expect?

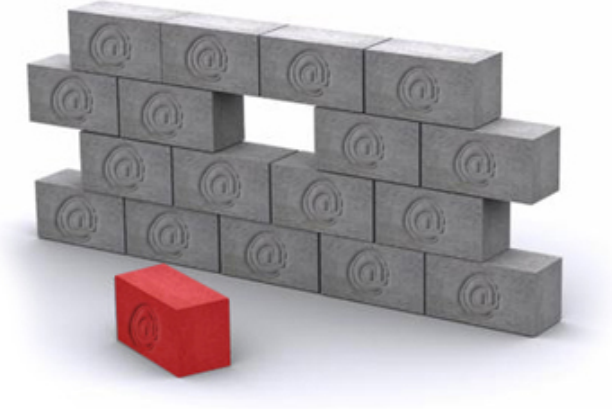
Cyber Defense

- **Prepare for, prevent**, **detect**, **respond to**, **recover from** and **learn lessons from** attacks, damage or unauthorized access affecting information infrastructures (**including military and civil networks)** that support and enable the conduct of NATO/National military tasks and Crisis Management Operations

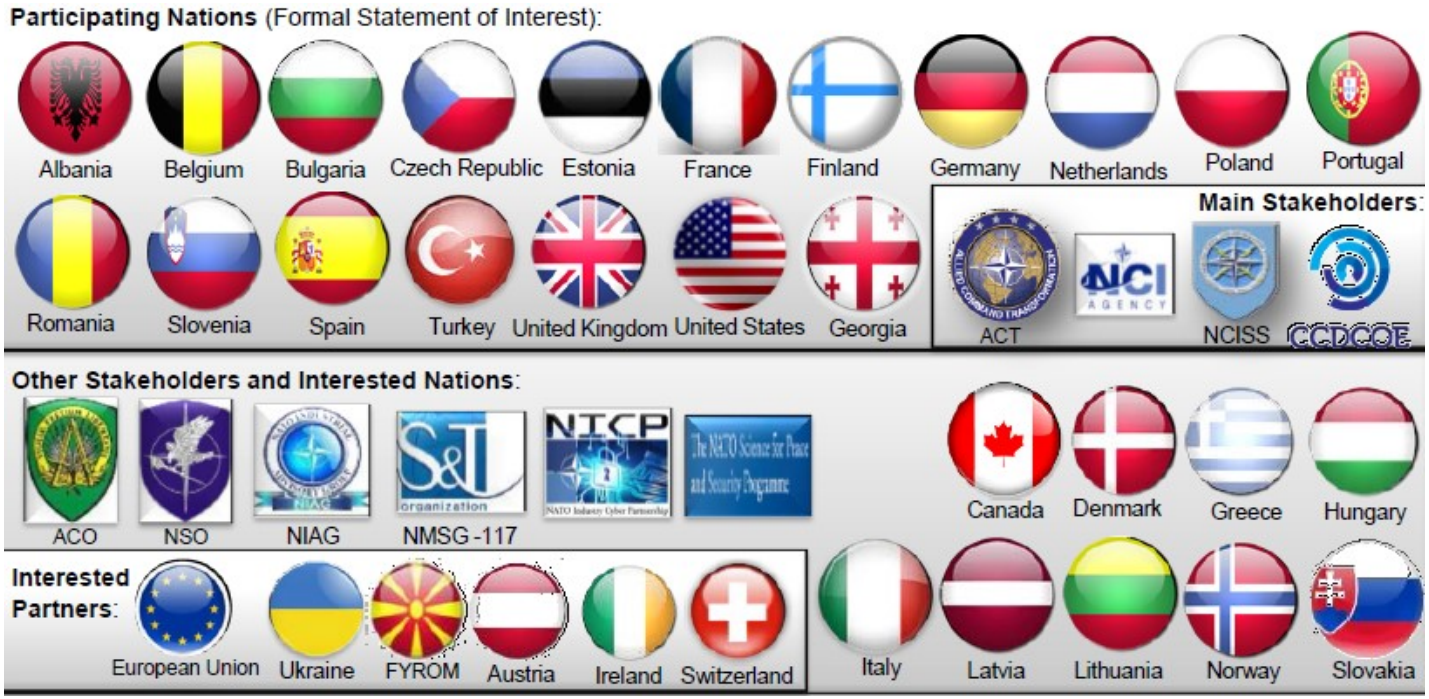
- So… this is applicable to the entire national MoD and NATO workforce: cyber awareness, policy decisions, intelligence gathering, international cooperation on CD, and other tasks

Why

- Understand what competencies are needed
  - for which audience
  - to perform CD tasks as part of their job
- Identify solid knowledge requirement basis for CD E&T purposes
- Based on existing studies and frameworks

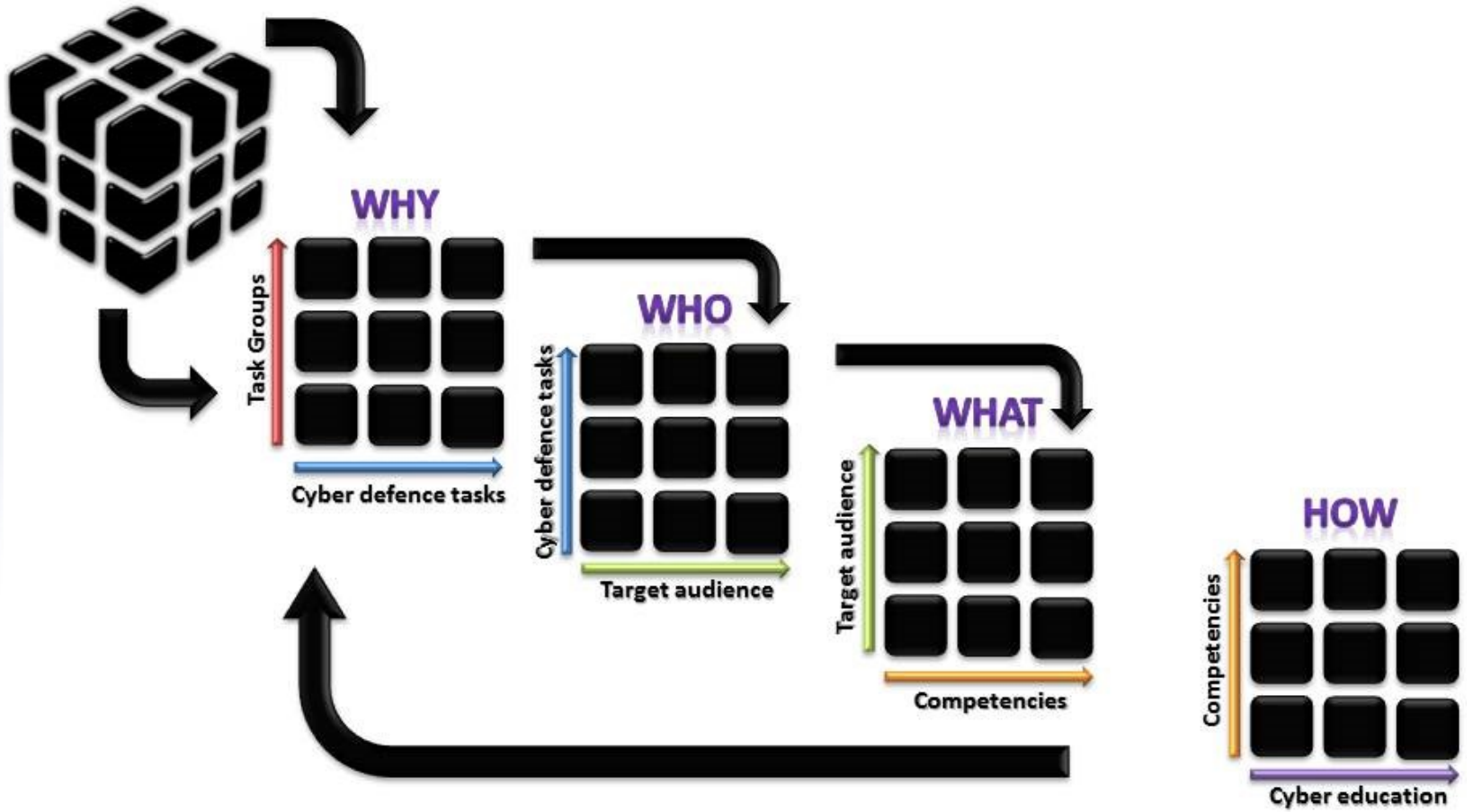


Who



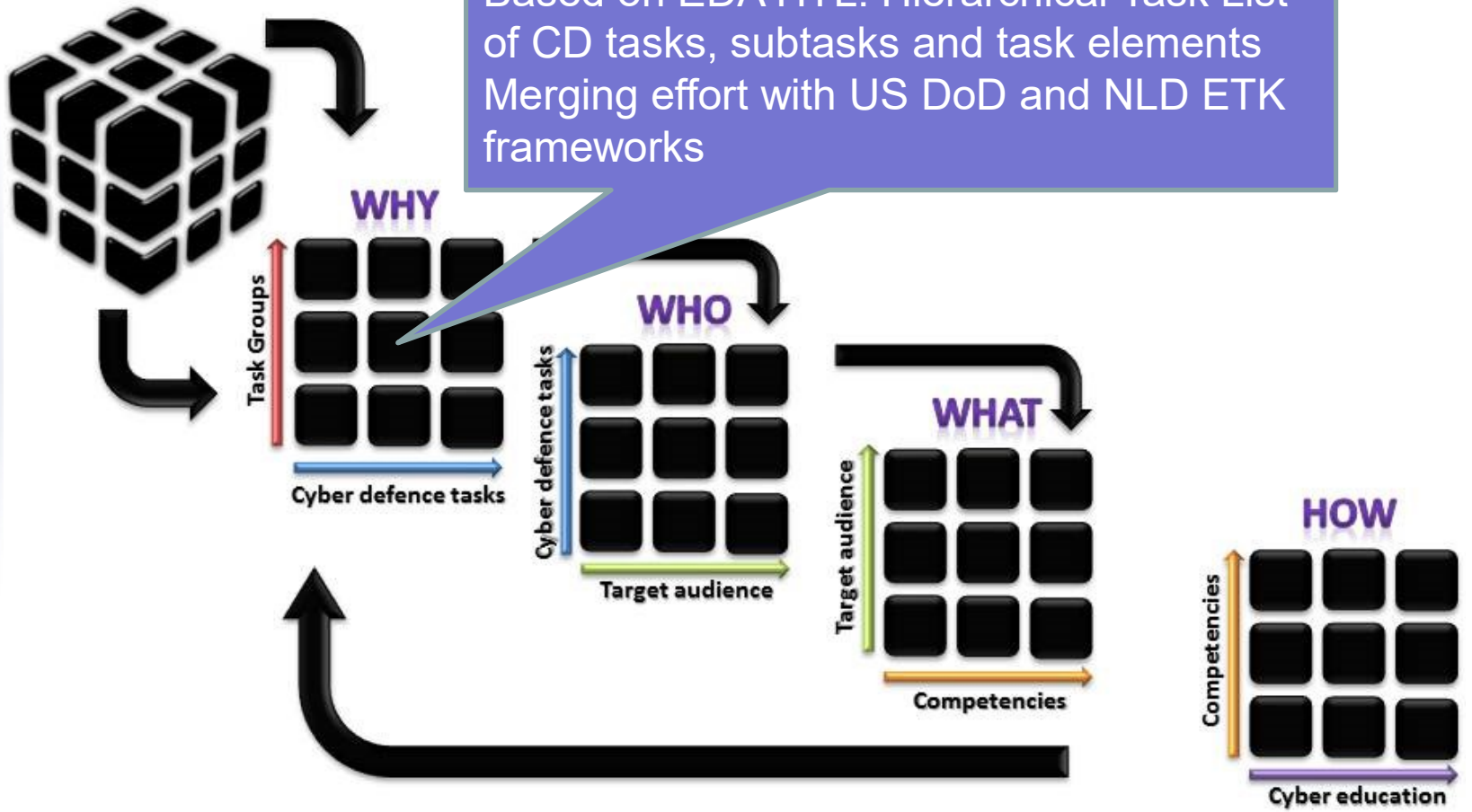
- NATO common description
- National level
- Academia, E&T solution providers to build and adapt curricula

How


WHY
Task Groups
Cyber defence tasks
WHO
Cyber defence tasks
Target audience
WHAT
Target audience
Competencies
HOW
Competencies
Cyber education

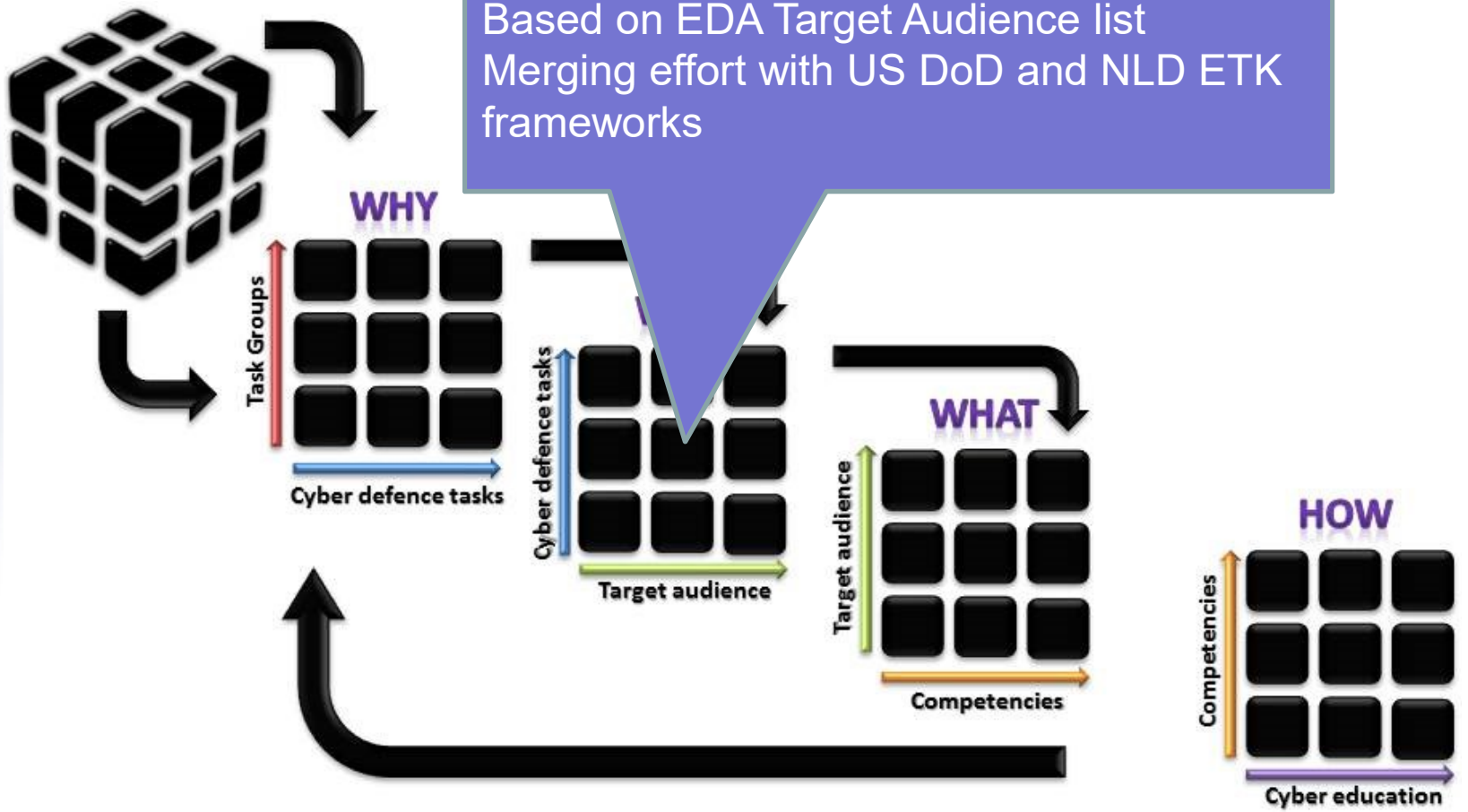
How

Based on EDA HTL: Hierarchical Task List of CD tasks, subtasks and task elements
Merging effort with US DoD and NLD ETK frameworks



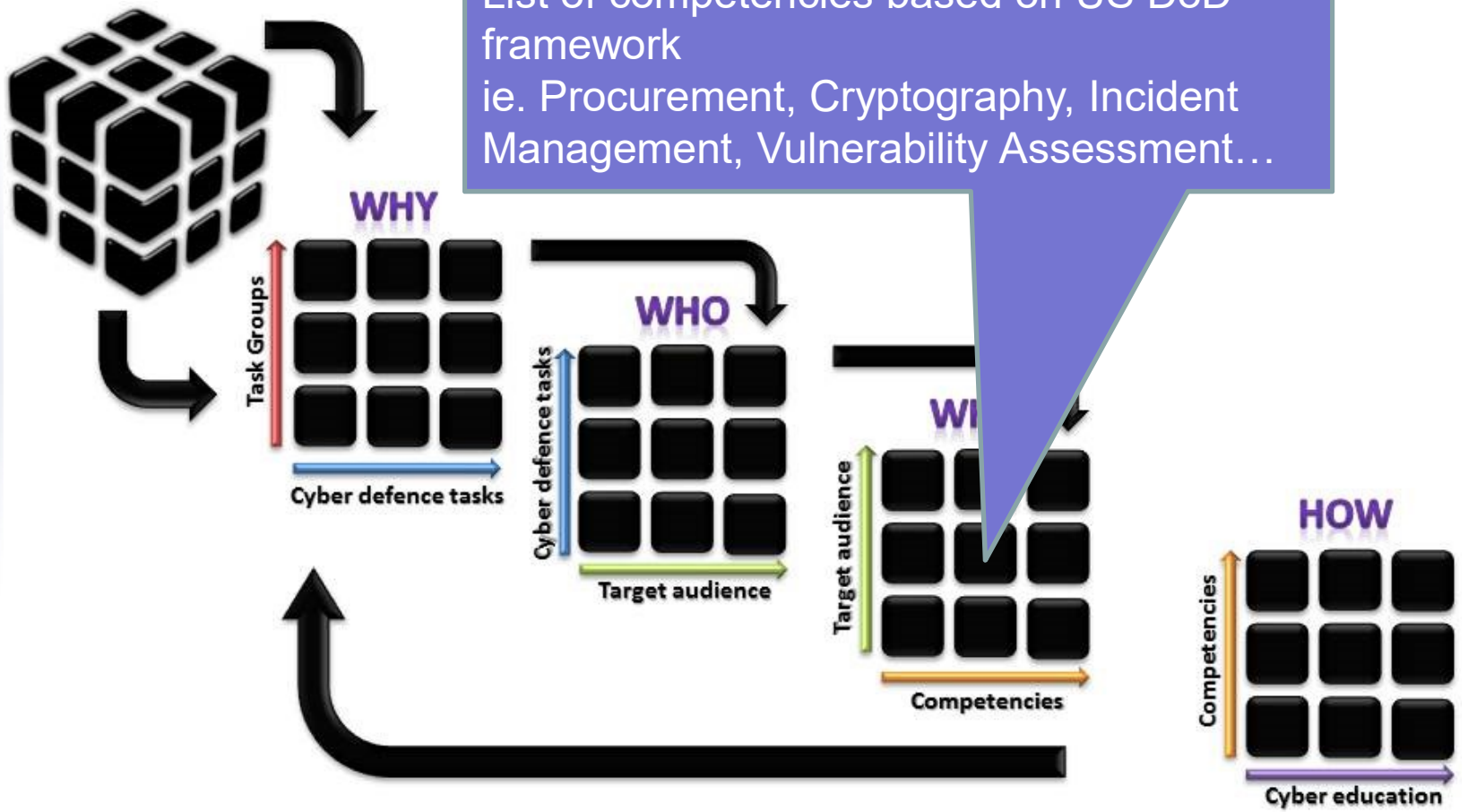
How

Based on EDA Target Audience list
Merging effort with US DoD and NLD ETK frameworks

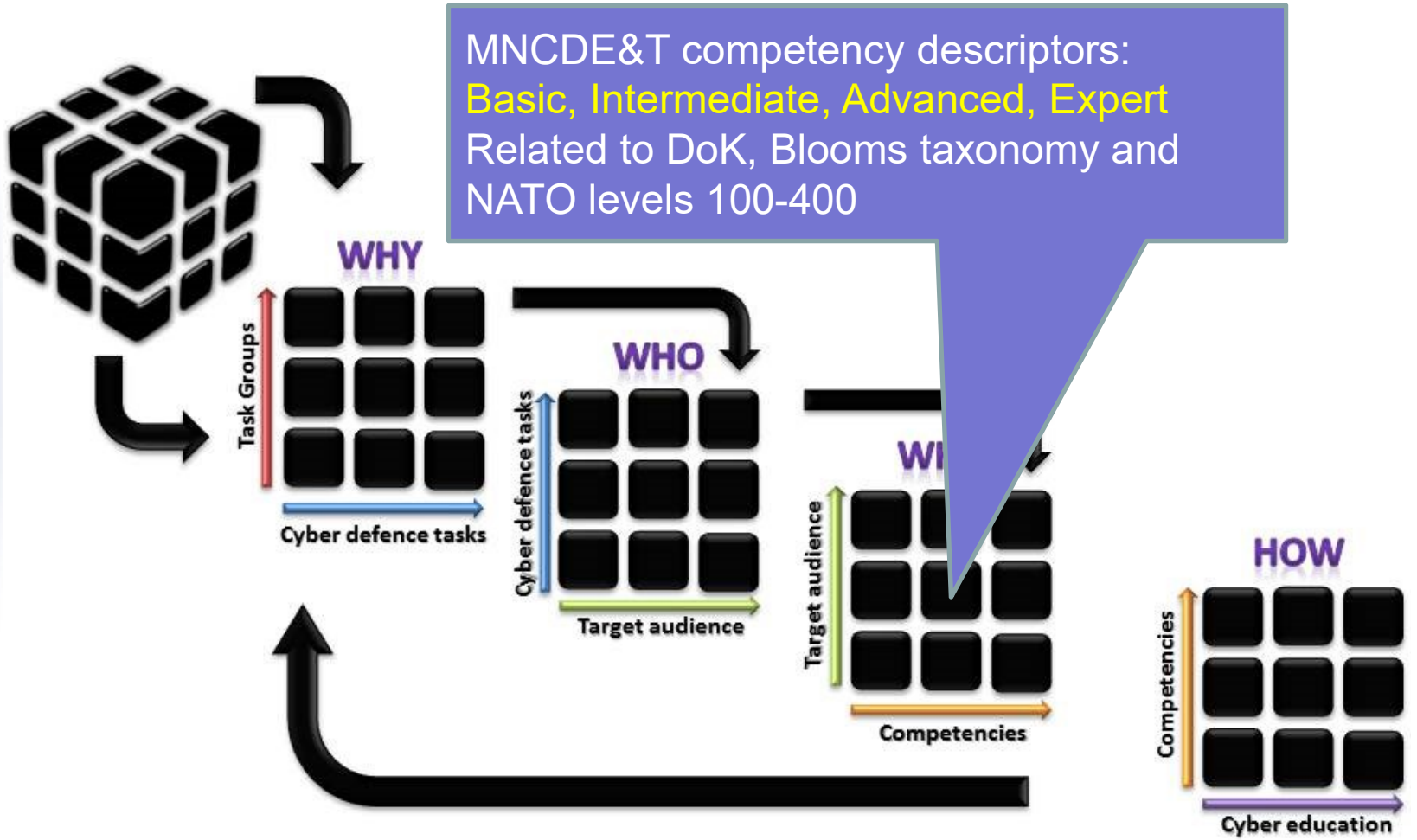


How

List of competencies based on US DoD framework
ie. Procurement, Cryptography, Incident Management, Vulnerability Assessment…



How


MNCDE&T competency descriptors:
Basic, Intermediate, Advanced, Expert
Related to DoK, Blooms taxonomy and
NATO levels 100-400
WHY
Task Groups
Cyber defence tasks
WHO
Cyber defence tasks
Target audience
Target audience
Competencies
HOW
Competencies
Cyber education

Competencies

- Observable, measureable patterns of knowledge, skills, abilities and other characteristics (KSAOs) that an individual needs to perform work roles or occupational functions successfully.

Example (1/2)

Task Group	Task	Sub-Task Description	Task Element Description
2.0 - PREVENT (Mitigate Cyber risks through the management of CIS security architectures, testing and audit functions)	2.1 - Test and Audit	2.2.2 - Manage the security of the support systems, facilities and personnel	2.2.2.1 - Manage the security of the supply chains for CIS and other information-reliant systems
	…	…	…

Example (2/2)

Basic
Intermediate
Advanced
Expert

CSDP Senior Decisionmakers 2/4)		CSDP C4 Practitioners (3/6)			CSDP CD Specialists (2/7)	
Senior military and civilian personnel, who engage in policy, strategy, concept, doctrine and/or capability development	**Chief Information Officer, Senior Information Risk Owner, or similar Information Governance roles**	**Military and civilian personnel, who engage in policy, strategy, concept, doctrine and/or capability development**	**Legal Advisors**	**Deliver CIS services**	**CD Architect, Accreditor and Auditor functions**	**Design and deliver individual and collective training interventions for CD specialists**
Knowledge of the organization's core business/mission processes.	Knowledge of capabilities and requirements analysis	Knowledge of capabilities and requirements analysis	Knowledge of applicable laws	• Knowledge of supply chain risk management standards, processes, and practices	Knowledge of supply chain risk management standards, processes, and practices	Knowledge of supply chain risk management standards, processes, and practices
Knowledge of the organization's enterprise information technology (IT) goals and objectives	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Knowledge of the organization's enterprise information technology (IT) goals and objectives	Knowledge of the organization's core business/mission processes		Ability to apply supply chain risk management standards	Ability to apply supply chain risk management standards
	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure					Knowledge of applicable laws

Status

- Starting point: EDA Landscaping study and HTL
- Framework comparison and refinement
- Framework mapping is difficult: Scope EDA HTL is on strategic/operational level, NLD and US DoD frameworks focus mostly on tactical level

What to expect?

- Recommendation for framework refinement
  - Task list
  - Target audiences
  - Best-of both-worlds approach from US DoD / NLD ETK frameworks
  - US DoD competency framework is the most mature → use it
- Validate framework output with academia
- Use outcome in next WP to match TNA and available E&T offer

Allard Kernkamp MSc RO
M: +31 6 20542148
E: ac.kernkamp@mindef.nl