Council of the
European Union

**Brussels, 7 June 2019
(OR. en)**

7848/19

**EUMC 35
CSDP/PSDC 135**

COVER NOTE

From:	European External Action Service (EEAS)
To:	European Union Military Committee (EUMC)
Subject:	Training Requirements Analysis Report on Military Role in Cyber Defence EU Military Training Discipline

Delegations will find attached document EEAS(2019) 154 REV 6.

Encl.: EEAS(2019) 154 REV 6

European Union
EXTERNAL ACTION

European Union Military Staff

Working document of the European External Action Service
of 22/05/2019

EEAS Reference	**EEAS(2019) 154 REV6**
Classification	**PUBLIC**
From **To**	**European Union Military Committee (EUMC)** **European Union Military Committee (EUMC)** *CSDP/PSDC; EUMC*
Title / Subject	**Training Requirements Analysis Report on Military Role in Cyber Defence EU Military Training Discipline**
[Ref. prev. doc.]	**-**

Delegations will find attached the "Training Requirements Analysis (TRA) Report on Military Role in Cyber Defence (CD) EU Military Training Discipline".

This document was agreed by EUMC, by silence procedure, on Monday 13 May 2019.

REFERENCES

A. EU Policy on Training for CSDP (Council doc. 7838/17, adopted by the Foreign Affairs Council on 3 April 2017).

B. Implementing Guidelines for the EU Policy on Training for CSDP (Council doc. 5199/1/17 REV2, dated 17 January 2017).

C. Guidelines for EU Military Training Discipline Leader, doc. 11192/15, dated 23 July 2015

D. EU Concept For Cyber Defence for EU-led Military Operations, doc. EEAS(2016) 1597, dated 22 November 2016.

A. BACKGROUND[1]

1. In accordance with EU Policy on Training for CSDP (Ref. A), training for CSDP is driven by requirements, not events. The type, complexity and number of training activities related to a training discipline derive from requirements and shortfalls identified during the conduct of CSDP operations and missions, evolution of the security and defence environment, and civilian and military capability development processes. These requirements are agreed for each identified training discipline[2].

2. In accordance with Implementing Guidelines for the EU Policy on Training for CSDP (Ref. B), an EU Military Training Group (EUMTG) was established as the Council Preparatory body for the systematic process of managing CSDP Training Requirements for CSDP Military Training.

3. In accordance with its Terms of Reference (Ref. C), the EUMTG should propose strategic priorities for CSDP Military Training and Education (T&E) to the European Union Military Committee (EUMC). These priorities derive from political guidance (e.g. Conclusions of the European Council, Council

[1] The general overview of the management of the military training requirements at EU level is common for all the disciplines and their associated TRA reports. It is updated regularly with the latest training policy documents.

[2] Discipline for CSDP training: a functional training category that groups distinct training thematic and requirements in support of capabilities for CSDP missions and operations. Thematic are areas within each discipline that group individual and collective performance objectives on a functional basis (Ref. B).

Conclusions on CSDP, etc.), military capability development process, studies, military concepts, and analysis of lessons from operations and exercises, and other sources as required. The deliverable for this task is the EUMC Strategic Guidance on CSDP Military Training, which includes an annex on CD with the military role, tasks and priorities in the EU context.

4. On 17 December 2014, the EUMC agreed[3] to nominate France and Portugal as Discipline Leaders (DL) for the Military Role in CD EU Military Training Discipline. The DL have conducted a Training Requirements Analysis (TRA) to identify training gaps and propose appropriate corrective measures.

5. The DL started the TRA during the second semester 2015 taking into account the priorities set by the EUMC Strategic Guidance on CSDP Military Training, especially the annex on CD.

B. AIM

6. The aim is to present the conclusions of the TRA for the Military Role in CD EU Military Training Discipline and to recommend the adoption of corrective measures by the EU Member States (MS).

C. METHODOLOGY OF THE TRAINING REQUIREMENTS ANALYSIS (TRA)

7. DL organised several workshops with the MS to identify training requirements in the CD area.

8. Initially, DL defined a *Common taxonomy of terms and definitions* for a collective understanding of the concepts and to facilitate cooperation. Then a *Unified Cyber Competence Framework* was established, identifying competencies and skills requirements.

9. Later on, a first questionnaire was sent to MS in order to identify T&E needs and capture the insights of relevant stakeholders related to CD at National levels. Based on these declared needs, a *Theoretical Common Curriculum* was developed, linking the competencies to develop, the target audience

[3] Framework Process for Managing CSDP Military Training Requirements, para 16 and annex B, doc. 17087/14, dated 19 December 2014.

and the requested level of qualification. A modular approach was selected, to reduce the total amount of Courses needed to fulfil all the CD T&E.

10. DL sent then a second questionnaire to MS, to identify Courses proposed by MS. The DL assess that the results of this second questionnaire were not totally convincing, maybe because MS are reluctant to share their competencies and priorities. According to the DL, it appeared that all potential offers were neither shared nor existent, and that the gap covered the whole identified needs.

11. Therefore, the DL proposed corrective measures to cover the full CD spectrum, which had been described on *Cyber Competencies Career Path Matrix,* with a list of courses.

12. Along all this process, DL reported on a regular basis to the EUMTG on the progress achieved.

D. MAIN FINDINGS AND CONCLUSIONS

13. DL assess that the working plan goal was achieved.

14. EU Concept for Cyber Defence for EU-led Military Operations (Ref. D) defines the framework and responsibilities required to implement CD in CSDP and supports the CD capability requirements definition.

15. NATO Communications Information Systems School (NCISS) and NATO Cooperative Cyber Defence Centre of Excellence offer a large potential of T&E opportunities to EU MS, which can be considered as EU training opportunities, provided that their courses and procedures are re-rolled/adapted respectively, in such a way to be open to EU bodies and all EU MS. These training courses can be included in the next revision of the CD TRA, conducted within a common agreed timeline

16. Moreover, industry and civil sector also have lot to offer in the cyber T&E domain.

17. In terms of training needs, the main findings are :

    a. CD Awareness for all Information and Communication Technology (ICT) users is identified as a "common need".

b. Lack of specialists / SMEs, which increases the need for more T&E.

c. MS highlighted lack of training in their answers to the questionnaires.

18. During the analysis, the DL found out that;

a. There were few training offers from the MS.

b. The offers were mainly technical courses.

c. There was a lack of collective training.

d. Potential offers from MS are not shared or inexistent.

19. Based on a systematic approach, the DL underline in the report that a realistic solution for the abovementioned findings consists in covering the full CD Discipline spectrum, described in a Cyber Competencies Career Path Matrix, with a list of proposed courses.

20. With the Cyber Competencies Matrix Career Path Matrix, MS or EU bodies can conduct self-assessment in order to fill gaps individually or collectively.

21. Opportunities for cooperation are available through existing tools, such as the two coordinated initiatives, the EU CD Training and Exercises coordination Platform (TEXP), led by the European Defence Agency (EDA), or the Education, Training, Exercise and Evaluation (ETEE) platform, led by the European Security and Defence College (ESDC). CD TEXP has to be the central platform where all the cyber courses linked with CSDP should be registered. ESDC is fully engaged in the CD TEXP project and will manage it for the EU as soon as it is fully operational.

22. In Phase 5, DL propose sixteen solutions and some new initiatives in four main areas (IT Communications, System Administration, Cyber Education and Cyber Logistics) to cover the identified training gaps, encompassing the whole CD Discipline spectrum (Annex I).

23. The sixteen solutions are shortly described and cover the needs from of a simple ICT user to an expert level/CD specialist. An example of a Cyber Intel Course is developed (Annex H). These solutions are to be further developed, adapted or updated.

24. The report underlines that Cyber is a rapidly moving environment and, because of that, MS and EU Institutions should develop innovative and appropriate processes to adapt to a new reality. Empiric approach applied on proposed initiatives should lead to a fast increase of EU capabilities in the correspondent domains.

E. PROPOSED WAY AHEAD

25. It is proposed by the DL that MS and EU Institutions should carry this work forward and develop correspondent T&E courses[4] which would fill the Cyber Competencies Career Path Matrix.

26. The CD TEXP is expected to be able to support three different domains – EU, national and multinational – and will take a central role.

27. ESDC, in charge of "giving a training and education instrument that promotes a European security culture", could further develop the CD T&E capability in EU bodies and MS.

F. RECOMMENDATION

28. The EUMC is invited to:

    a. Note this Report.

    b. Agree that the proposed *Discipline Common Core Curriculum* and the solutions constitute the minimum common EU military training requirements on CD.

    c. Support the recommendations about Duality of E&T in the cyber domain, including the avoidance of gaps between the civil and military tools and the need to standardize E&T tools and processes.

    d. Task EUMTG, supported by DL Cyber Defence, EUMS and other relevant EU entities, notably ESDC, to further investigate ways to

[4] Taking into account the EU agreed terminology and definitions (presented in various EU documents e.g. the *EU Concept on Cyber Defence for EU-led Military Operations and Missions* or the *EUMC Glossary for Acronyms and Definitions*)

implement the proposed way ahead and recommendations and also to benefit from NATO E&T opportunities:

(1) consistent with EU-NATO Joint Declaration Implementation Plan (JDIP) Action 3.2 (strengthen cooperation on training) and JDIP Action 3.4 (strengthen cooperation in cyber exercises).

(2) open to EU bodies and all EU MS in a reciprocal way, respecting the principle of inclusiveness.

e. Support the recommendations about the NATO training opportunities, which can be considered as EU training opportunities, provided that their courses and procedures are re-rolled/adapted respectively, in such a way to be open to EU bodies and all EU MS.

f. Task the EUMTG to report back progress to the EUMC through the EU Military Training and Education Annual Report.

Annex

A. Final Report Training Requirements Analysis (TRA) for the discipline (Military contribution to) Cyber Defence – Version 2.1, April 2019

EUMTG

CD DISCIPLINE LEAD (FR-PT)

FINAL REPORT
(Version 2.1)

April 2019

INDEX

INDEX 1

PREFACE..2

ACKNOWLEDGEMENTS 3

EXECUTIVE SUMMARY 3

1. CD DISCIPLINE..4

a. Aim and Objectives 4

b. EU CD Capability Development Process (The role of E&T)..........................4

c. EU CD E&T Relevant Organisations 4

d. CD Discipline Framework 4

e. Background (chronology of events) 5

f. CD Discipline Members – Contributors 6

2. CD DISCIPLINE WORKING PLAN 6

a. CD Competencies and Skills (Phase 1)...6

b. CD E&T Needs (Phase 2) 8

c. Analysis of CD E&T Offer (Phase 3)..10

d. Gap Analysis (Phase 4)...11

e. Proposed Solutions (Phase 5)...11

f. New CD E&T Initiatives (Phase 6)...12

3. CONCLUSIONS 12

4. RECOMMENDATIONS..13

a. Duality of CD Discipline 13

b. Management of CD E&T 13

c. Necessity to Standardize CD E&T Tools and Processes 13

d. Way ahead 14

REFERENCES 15

ANNEXES 16

Annex A - CD Discipline Working Plan *(April 2015)* 17

Annex B - CD E&T Taxonomy used for this report 21

Annex C - Studies on Required Competencies & Skills......................................31

Annex D - CD E&T Needs Questionnaire...37

Annex E - CD E&T Existing Offers Questionnaire 43

Annex F - Cyber Competencies Career Path Matrix 47

Annex G - Example of a Gap Analysis (Module B3)...55

Annex H - Example of a proposed solution for a Cyber Intel Course..................60

ANNEX I - Proposed solutions 74

Annex J - Change Proposals 82

PREFACE

Cyberspace infrastructure is largely globally interconnected and far more than merely the internet. All devices reachable via cyberspace could be potential targets and potential threats. This includes networks and devices connected by wired connections, wireless-free connections and those that appear to be not connected at all. European Union (EU) and its MS (MS) can be targets.

Since a few years, EU's interest in CD (CD) and Security is increasing. This is translated in concrete actions promoted by Commission or other European External Action Service (EEAS) stakeholders such as European Union Military Staff (EUMS), Crisis Management and Planning Directorate (CMPD), Civilian Planning & Conduct Capability (CPCC). The duality of the Domain is obvious and this leads to the pertinence of works developed by EU agencies and bodies, among which you can find agencies like European Defence Agency (EDA) in the defence sector, European Police College (CEPOL) or European Union Agency for Network and Information Security (ENISA) in the security domain or European Security and Defence College (ESDC) in both.

The 2013 EU cyber security strategy (ref. A) is a practical expression of this interest and forms a fundamental start in the implementation of any European initiative in the domain.

The Commission 2016 action plan (ref. B) is clearly mentioning the creation of a cyber security training and education platform. Some on-going initiatives announced by the president of the Commission build on the initial idea.

All those political initiatives should then be translated in practical implementations. This is the ambition of the two discipline leaders and the participating MS to contribute via this report, to the improvement of the European military CD capability development.

The EU Military Training Group (EUMTG) conducted a CD Training Requirements Analysis (TRA). The final result of this TRA is a picture of the Education and Training (E&T) activities (courses, exercises, e-learning etc.) that is conducted by the relevant training actors at the MS and EU level, in this very technical and specific discipline, in order to cover the training gaps, to improve an existing training, to reach a certain level of quality (standard) or eliminate unnecessary redundancies.

There is a consensus that a rational and expedient approach is the conduct of TRA by lead nations/bodies, which can assume the role of EU discipline leaders, with subsequent validation of the TRA by the EUMTG. In order to avoid unnecessary duplication of efforts, it has been assessed that the role of the EU discipline leader has to be assumed, whenever possible and accessible to all EU MS, by the nation or the body having a similar role for NATO.

France and Portugal are strongly engaged at the development of an integrated and cooperative approach to CD Education and Training at both National and International (EU and NATO) levels.

ACKNOWLEDGEMENTS

The discipline leaders take the opportunity of this report to thank the small group of MS who regularly attended the workshops organized by discipline leaders and efficiently contributed to expand the viewpoint on the processes and results. By doing so, they gave the necessary legitimacy for this report to be presented for a collective appropriation within the EU MS community.

Thanks are also addressed to the other Cyber communities with whom fruitful exchanges led to a better result and also ensure potential synergies and interoperability. Namely, the works conducted within EDA project team, as well as in NATO Multinational CD Education and Training (MNCD E&T), have been of great interest and to a large extend incorporated in the work of our Discipline.

EXECUTIVE SUMMARY

Recognized as a priority for MS, the CD capability is developing, in which E&T plays a key role.

The main objective was to help EUMTG and MS to identify CD E&T requirements and needs, and fill the gaps deriving from their CD capability development process, without unnecessary duplicating MS or NATO existing capabilities.

During the 2nd Semester 2015, France and Portugal took the lead of the EU CD Discipline and decided to start a TRA, in accordance with a European Union Military Committee's (EUMC) strategic guidance (ref. C).

The first step was to define a Common Taxonomy of terms and definitions, in order to offer guidance for a collective understanding of the concepts and to facilitate cooperation. Then a 'Unified Cyber Competence Framework' (common for NATO and EU) was created, identifying competencies and skills requirements.

To identify E&T needs, a first questionnaire was sent to MS, to capture the insights of relevant stakeholders related with CD at National levels. Based on these declared needs, a "Theoretical Common Curriculum" was developed, linking the competencies to develop (in facts "segments": aggregations of competencies), the target audience and the requested level of qualification. A modular approach was selected, to reduce the total amount of Courses needed to fulfil all the CD E&T.

A second questionnaire was sent to MS, to identify Courses proposed by MS, but the result was not totally convincing, maybe because MS are reluctant to share their competencies and priorities. Therefore, the actual gaps appear to be the whole identified needs.

Based on a systematic approach, a realistic solution consists in covering the full CD Discipline spectrum, which had been described on a Cyber Competencies Career Path Matrix, with a list of proposed courses.

Now MS and Institutions should carry on this work and have to develop correspondent E&T courses which would fill the Cyber Competencies Career Path Matrix. The EU CD Training and Exercise coordination Platform (CD TEXP) is expected to be able to support three different domains – EU, national and multinational – and will take a central role.

Cyber is a rapidly moving environment and, in accordance, MS and Institutions should develop innovative and appropriate processes to adapt to a new reality and keep up-to-date. Empiric approach applied on our proposed initiatives should lead to a fast increase of EU capabilities in the correspondent domains.

1. CD DISCIPLINE

a. Aim and Objectives

Supported by the EUMS and building on EDA Training Needs Analysis (TNA), the CD Discipline aimed at identifying the military training requirements for the Common Security and Defence Policy (CSDP).

Given the EU CD Capability Requirements definition, the main objective of CD Discipline was to help the EU and MS to identify CD E&T requirements and needs, and to fill the gaps deriving from their CD Capability development process.

Reminder of the CD Discipline aims:

- offers MS CD E&T initiatives (from strategic to technical level) not available through national, bilateral or commercial arrangements;
- promotes Excellence and Certification – high quality of courses and interoperability of experts;
- has a Multinational Character – greater flexibility and benefits with participation of NATO, Academia, Industry and Partners;
- is open and inclusive to EU Bodies and all MS.

b. EU CD Capability Development Process (The role of E&T)

During the 2014 update of the Capability Development Plan (CDP), MS recognized CD as one of the Top 14 priority areas (ref. D). CD is also high on the agenda of the European Council, Foreign Affairs Council, EEAS and receive a high priority for CSDP current operations. The EU Concept for CD for EU-led Military Operations (ref. E) defined the framework and responsibilities required to implement CD in CSDP and supported the CD capability requirements definition.

c. EU CD E&T Relevant Organisations

Within EU, several actors are working to develop CD E&T capabilities, and are at different steps of maturity.

EDA received mandate to develop CD E&T and has also conducted preliminary studies about TRA.

Within EEAS, CMPD, CPCC and EUMS are collaborating to ensure comprehensiveness and non-duplication of efforts.

On February 2018, the steering board of ESDC decided the creation of an Education Training, Exercise and Evaluation (ETEE) platform (ref F). Within the college, the aim of the Cyber ETEE platform will be to address cyber security and defence training among the civilian and military personnel for the CSDP requirements for all CSDP training levels, as identified by the EU Military and Civilian Training Groups.

d. CD Discipline Framework

Complementarity and non-duplication

Following the 2016 EU-NATO joint declaration (ref. G), the NATO Smart Defence MNCD E&T project team is constantly exchanging with EU CD discipline leaders on the military strand of E&T. Currently, MNCD E&T has carried out the development of a strong model in competencies, work roles and carrier path. Answers from the nations and MS involved were not consistent enough to describe a precise gap analysis. However, due to the dynamic of the domain, some countries came up with proposals of cyber courses.

The NATO Communications Information Systems School (NCISS) moving to Oeiras (in vicinity of Lisbon), as well as the Tallinn NATO Cooperative CD Centre of Excellence (CCD COE) in Tallinn are offering a large potential of E&T opportunities to EU MS, which can be considered as EU training opportunities, provided that their courses and procedures are re-rolled/adapted respectively, in such a way to be open to all EU bodies and all EU MS

Industry and civil sector have a lot to offer in the cyber E&T domain to the military.

EU MS have developed their own capabilities, but the level of maturity is not equal in all states.

As an example, some like France in Rennes, have developed large national competency poles for the MoD and the industry while others are more relying on multinational initiatives or private education companies. More precisely, French *Pôle d'excellence cyber* located in Brittany relies on a strong layout of cyber expertise for education, research and development as well as industrial development. In the framework of the *Pôle d'excellence cyber*, the FR MoD has located in Rennes area key cyber assets, operational, technical and in the education. This decision is in line with the national strategy and allows the concentration of scarce resources.

Portugal, for instance, with its Cyber Academia and Innovation Hub (CAIH), within cyber, stimulates Education, Training, Research Innovation and Industry development in order to provide its national ecosystem with the necessary competencies to address the needs of a new generation of professionals.

Finally, the relevance of these works is high for the civilian bodies and institutions which may conduct EU missions and operations. The duality of E&T is a source of savings and a potential growth factor for the EU capacity building, as long as we have avoided any unavailable drift from one to the other. We must, as far as possible avoid any gap between the civil and military tools, beginning with the vocabulary or the conceptual development.

e. Background (chronology of events)

The CD EUMTG Discipline plan of work is developed over several phases, integrating in each stage the results deriving from the different modules / areas identified as building blocks of CD E&T initiatives (identification of competencies and skills to be developed, analysis of E&T needs, analysis of existing initiatives and identification of gaps not yet fulfilled).

In accordance with the EUMC strategic guidance, the EUMTG has conducted a CD TRA. The final result of this TRA should be a clear picture of the E&T activities (courses, exercises, e-learning etc.) that should be conducted by the relevant training actors at the MS and EU level, in this very technical and specific discipline, in order to cover the training gaps[5], to improve an existing training, to reach a certain level of quality (standard) or eliminate unnecessary redundancies.

Taking on EUMC guidance and after the discussions held at the EUMTG on 16 December 14 and 28 April 15, France and Portugal took the lead of the EU military training discipline "CD" and decided to start a TRA during the 2nd Semester 2015. Since then, a succession of Workshops and reports to regular Headline Gold Task Force HTF/EUMTG meetings lead to the common

[5] To better understand whether, in the implementation process, training activities (e.g. courses, exercises etc.) manage to meet the military training requirements, quantitative and qualitative analyses are needed. For practical reasons and in order to approach training in an integrated manner, across all levels, for individual and collective needs alike, training requirements should be analyzed per each individual training discipline.

understanding of the needs. As well as, through a system of questionnaire, it also provided a theoretical view of the existing capacities. It has to be noticed that a stable view is quite impossible in the specific dynamic of the cyber domain. The operational requirement is in a continuous and rapid movement to adapt to threats and technical evolution.

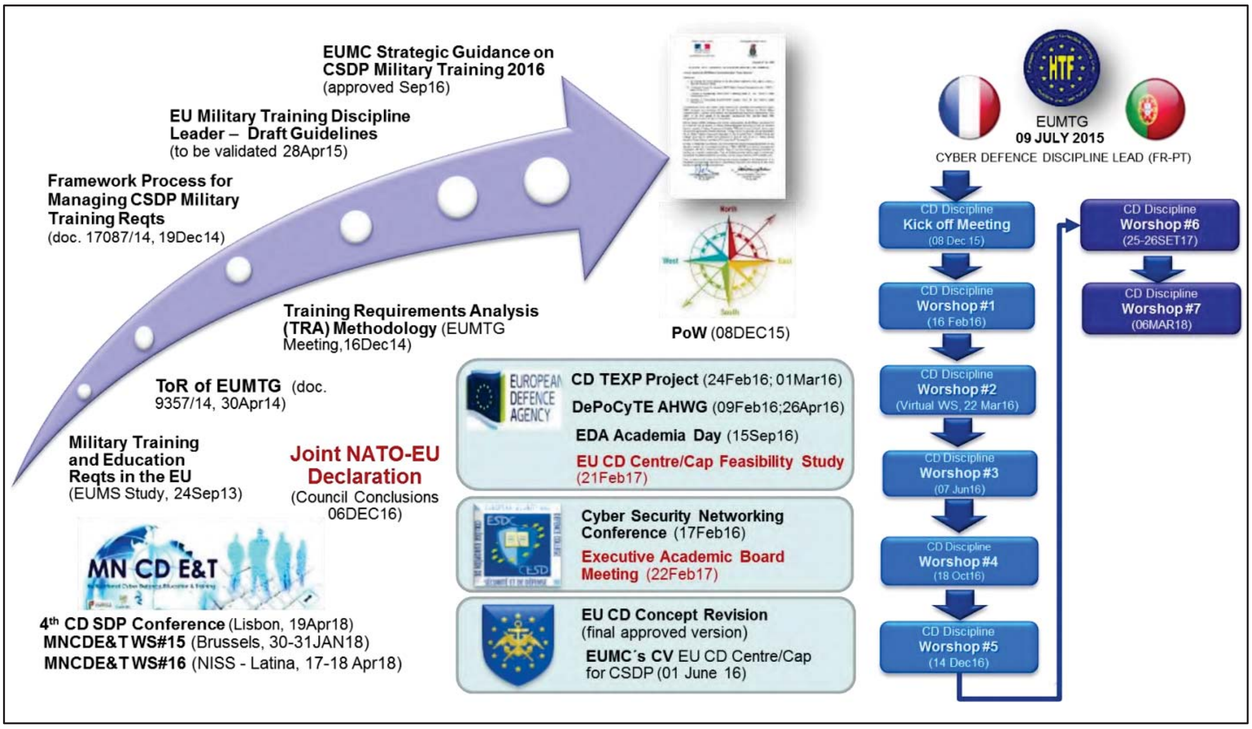

EUMC Strategic Guidance on CSDP Military Training 2016 (approved Sep16)
EU Military Training Discipline Leader – Draft Guidelines (to be validated 28Apr15)
Framework Process for Managing CSDP Military Training Reqts (doc. 17087/14, 19Dec14)
Training Requirements Analysis (TRA) Methodology (EUMTG Meeting,16Dec14)
ToR of EUMTG (doc. 9357/14, 30Apr14)
Military Training and Education Reqts in the EU (EUMS Study, 24Sep13)
Joint NATO-EU Declaration (Council Conclusions 06DEC16)
MN CD E&T
4th CD SDP Conference (Lisbon, 19Apr18)
MNCDE&T WS#15 (Brussels, 30-31JAN18)
MNCDE&T WS#16 (NISS - Latina, 17-18 Apr18)
PoW (08DEC15)
EUROPEAN DEFENCE AGENCY
CD TEXP Project (24Feb16; 01Mar16)
DePoCyTE AHWG (09Feb16;26Apr16)
EDA Academia Day (15Sep16)
EU CD Centre/Cap Feasibility Study (21Feb17)
Cyber Security Networking Conference (17Feb16)
Executive Academic Board Meeting (22Feb17)
EU CD Concept Revision (final approved version)
EUMC´s CV EU CD Centre/Cap for CSDP (01 June 16)
HTF
EUMTG
09 JULY 2015
CYBER DEFENCE DISCIPLINE LEAD (FR-PT)
CD Discipline Kick off Meeting (08 Dec 15)
CD Discipline Worshop #1 (16 Feb16)
CD Discipline Worshop #2 (Virtual WS, 22 Mar16)
CD Discipline Worshop #3 (07 Jun16)
CD Discipline Worshop #4 (18 Oct16)
CD Discipline Worshop #5 (14 Dec16)
CD Discipline Worshop #6 (25-26SET17)
CD Discipline Worshop #7 (06MAR18)

Figure 1: CD Discipline background

f. CD Discipline Members – Contributors

EU Members have been contributing to the study and constantly associated to the results. Even if some MS proved particularly active, a larger involvement, would have been a benefit.

During workshops and in line with the agendas, on a case by case basis, other stakeholders were invited to broaden the scope of the study, as well as ensuring coherence with other works conducted in the domain, in NATO, as well as within EU bodies.

EUMS was a systematic participant.

EDA, EEAS services, Commission, NATO have been invited and some industrial providers occasionally participated.

The multiplication of solicitations and the scarcity of experts showed the limits of a multinational exercise. Thanks to the proximity established between EUMTG and the MNCD E&T group from NATO, this « overheat » on the human resources has been partially mitigated.

2. CD DISCIPLINE WORKING PLAN

a. CD Competencies and Skills (Phase 1)

1) Common Taxonomy - see annex B

The first meetings, within EU and also NATO contexts, gave the opportunity to identify the necessity to create a Common Taxonomy of terms and definitions, in order to offer guidance for a collective understanding of the concepts and to facilitate cooperation between developers. This is beneficial for the stakeholders as well as the future beneficiaries of the CD Discipline conclusions. The Taxonomy is focused mainly on the practical meaning of the notions, on aspects that are useful and serve for the Discipline scope, and subsequently on the didactical and scientific accuracy of the definitions.

The document contains definitions for a set of concepts that are referential for understanding the CD Discipline scope. The final form of the definitions has been either taken as-is from some official documents, or adapted and commonly agreed inside the Discipline so as to best fulfil the Discipline's needs.

The document is focused on the needs for future development and interoperability between EU, NATO and other international organisations, concerning CD and Cyber Security topics. It also comprises an extensive list of technical terms that are described from different international perspectives, for a common understanding of the CD and Cyber Security areas of expertise. Since it is a continuously updating document, the version presented in this Final Report is a snapshot corresponding to the Discipline closing phase.

It offers a reference point for the future development processes and represents a solid support for current and future works that are conducted in the CD and Cyber Security domains.

Of course setting a list of agreed Cyber Definitions and Acronyms helped to create a common knowledge base.

2) CD Competencies and Skills - see annex D

The goal of the *CD Competencies and Skills phase* was to create a Cyber Competence Framework to educate and/or train all military and civilian personnel. The framework provides an overview of tasks accompanied with the needed *Knowledge, Skills and Abilities* (competencies) in order to perform roles as proficient as possible.

MNCD E&T is conducting, within NATO, a parallel work on E&T. The deliverables are, to a large extend, relevant for EU military cyber capacities. A "Unified Cyber Competence Framework" (UCCF) ties the frameworks from the EDA Landscaping Study (2013) and the NIST SP 800-181 NICE Cyber Workforce Framework (NCWF) together.

The UCCF contains a rich selection of building blocks allowing you to:

- Task 1: use the UCCF as a Rosetta stone to express or describe (part of) a cyber-organisation.
  Using the framework to describe national cyber organisations makes it easier to relate different national cyber organisations e.g. to train their personnel and share education with other nations in the future. The building blocks are also useful when your cyber organisation is growing or restructuring. NB: the framework might not contain all building blocks to describe all particular parts for all types of cyber organisations.
- Task 2: structure and describe a work role.
  People often have more work roles comprising of core tasks and support tasks. Identifying the core tasks of a role helps to structure the work and workload of personnel. It also facilitates structuring additional work roles within a cyber-organisation. The competencies in the UCCF allow you to define the prerequisite competencies.
- Task 3: identify core competencies to select a course or training.

Having identified the work role and the corresponding core tasks allows you to identify the core competencies to be trained to improve the task proficiency. The list of core competencies also helps to identify training to ensure a proficient task execution over time.

- Task 4: identify core competencies to develop a course or training.
  The result of the previous task (3) could also lead to the recognition that currently no course or training are available. Having identified the core competencies will help to develop a curriculum to address the gap.

b. CD E&T Needs (Phase 2)

Based on the tasks to be performed and in the identified competencies and skills requirements (Phase 1), we intended to identify the needs of E&T on CD at all levels – EU CSDP related Bodies and MS.

Deliverables: Common CD E&T Curriculum (preliminary version).

A questionnaire about CD E&T needs was sent to MS. Its aim was to capture the insights of relevant stakeholders related with CD at National levels. It is explained in Annex D.

The CD Discipline leaders thank those MS who answered and gave a view of CD E&T needs. Some general conclusions can be highlighted: CD Awareness for all ICT users is identified as a "common need"; Lack of Specialists (having the necessary knowledge in advance) increase the need for more education; all MS answers identified the lack of training, in general**.**

Based on the CD E&T needs, a "Theoretical Common Curriculum" was developed, as depicted below:

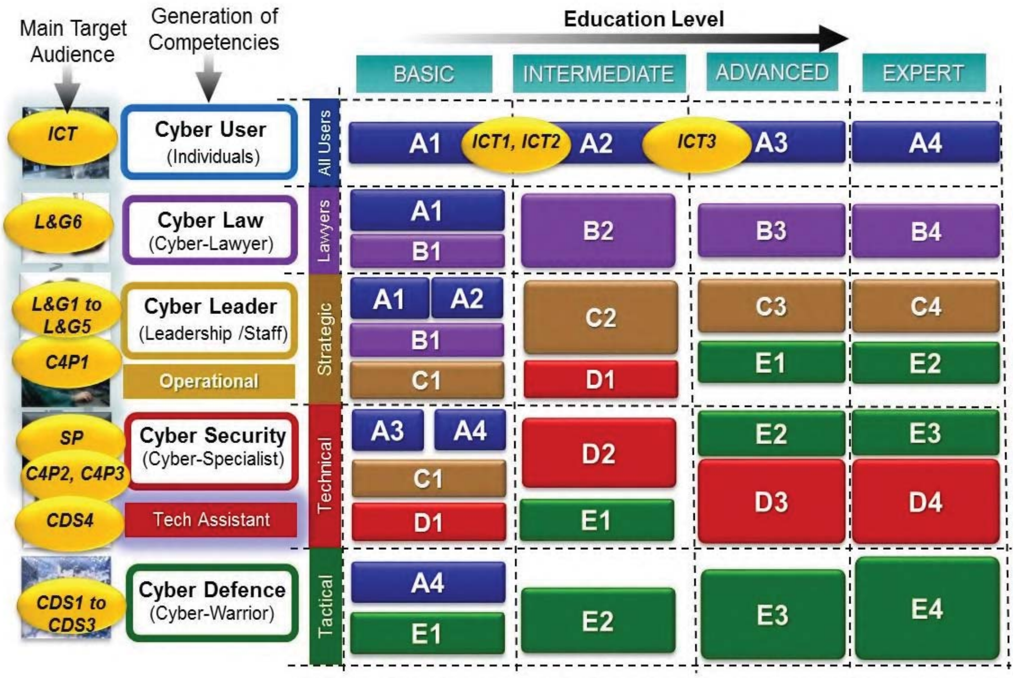


Figure 2: Common Curriculum (Nunes V., 2016)

Vertically, from top to bottom, the various Target Audiences (TA) can be found: from "ICT users" until "CD Specialist".

Under "Generation of Competencies", a designation is used to define an aggregation of competencies related with various "Segments" or subsets of the TA.

At the Education Level, four different Depth of Knowledge (DoK) levels are recognized: Basic, Intermediate, Advanced and Expert.

The blocks use a Colour Code and Letters, directly linked to the “generation of competencies” and therefore to the TA. The numbers relate to the DoK.

It is important to understand that similar blocks are found in different places through the Curriculum. Actually, it is on purpose and a real advantage because it permits a modular approach that will allow the reutilization of the same courses for different TA, depending on each DoK. As an example, E1 course content can deserve C4P1 at an Advanced level, and also CDS1 to CDS3 at a Basic level.

A modular approach will reduce the total amount of Courses needed to fulfil all the CD and CS E&T. Furthermore, it will allow students to attend less different courses, to facilitate career evolution or career paths changes.

At this stage, it is convenient to introduce a strong link with the works conducted by the ESDC in the cyber domain and especially the equivalence of proficiency levels.

Correspondences UCCF – EQF – SQF – DoK

The Unified Cyber Competence Framework (UCCF) developed by the EUMTG CD Discipline is a competence framework relevant for EU's CSDP. It is a kind of International Sectorial Qualifications Framework (ISQF) since it is structured with different levels of knowledge, skills and responsibility/autonomy (KSR/A)[6] required by individuals to act in a specific field of activity or to perform specific job roles[7]. A similar product has been developed by the ICT community (the European e-Competence Framework[8] and its levels of proficiency have been related to relevant levels of the European Qualifications Framework - EQF). The EQF is a reference framework that captures eight European generic levels of learning. Each level is defined in terms of knowledge, skills and responsibility/autonomy in relatively abstract terms. All types and levels of qualifications are covered, including those resulting from formal education and training at all levels, but also private sector qualifications and international (sectorial) qualifications.

Level 1 represents the lowest level of proficiency, level 8 the highest. In principle all possible ways of learning can lead to the learning outcomes corresponding to the eight levels, including non-formal and informal learning. The EQF has been conceived as a "translation tool" between National Qualifications Frameworks (NQF), to promote transparency, comparability and understanding of qualifications held by individuals.

The modules of the Core curriculum associated to the UCCF may lead to a qualification that could be assimilated to one of the EQF levels. Within this context, there is merit to informally assign the proficiency levels described by UCCF to the relevant EQF levels. However, the formal referencing of UCCF levels to EQF implies formal recognition by the MS through referral in their NQF.

ESDC has developed a SQF for young officers (OF1) corresponding to level 6 of EQF[9] and will develop a complete SQF for junior (OF 2/3) and senior military officers (OF 3/4). This SQF applies only to common modules and programmes organised as part of military education and training of young officers (under so called Military Erasmus). UCCF levels (1-basic, 2-intermediate, 3-advanced and 4-expert) include competencies that are achieved through programmes identified by the core curriculum with various degrees of complexity (Depth of Knowledge - DoK). For example, the learning outcomes at level 1 – basic will be achieved through modules taught at DoK levels 100, 300 and 400, depending on the audience. DoK indicates the degree of immersion into acquiring the knowledge and could range from 100 to 400, where 100 means basic and 400 means expert level.

Following the agreement by the MS of the UCCF and core curriculum, all cyber security/defence education and training programmes/courses will have to be referenced against UCCF/core curriculum.

c. Analysis of CD E&T Offer (Phase 3)

At this stage we intended to analyse the existing offer of CD E&T (nationally and internationally) in order to support personnel participating at EU missions and CSDP Operations and at National CD related activities. A questionnaire had been envisaged as a valuable and structured way to obtain the relevant information related with the existing CD E&T Offer.

Deliverables: List of available CD E&T activities.

[6] The Council Recommendation of 22 May 2017 on the European Qualifications Framework changes the term 'competence' as heading for the third column of the EQF descriptors (Annex II to the 2008 Recommendation on EQF) into 'Responsibility/Autonomy' as the term 'competence' was not used consistently in the 2008 EQF.
Therefore, the current taxonomy for describing competences is knowledge, skills and responsibility/autonomy.

[7] Working definition used by the EC Directorate-General for Employment, Social Affairs and Inclusion Unit Skills and Qualifications, Study on International Sectoral Qualifications Frameworks and Systems Final Report, Monika Auzinger, Julia Fellinger, Karin Luomi-Messerer, Luca Mobilio, Daniela Ulicna, Ali Zaidi. July 2016.

[8] www.ecompetences.eu

[9] Comparison of courses based on competencies, doc. IG/2014/002 (Rev 4), dated 24/09/ 2014

In order to gather offers in a format that can be exploited in conformity with the latest outputs from the WS#6, a questionnaire (explained in Annex E), containing more accurate questions was issued again, to complement and give more relevance to the Phase 4 gap analysis.

The CD Discipline leaders thank those MS who answered and gave a practical view of existing offers. This contribution cannot address the full spectrum of requirements. Nevertheless, some general conclusions can be emphasized: the offers were mainly technical courses and there is a lack of Collective Training.

At this point, the information retrieved from the questionnaires was not enough precise in order to propose a full picture of the available CD E&T activities.

It is possible that MS really do not have activities to offer at this time or they are reluctant to share this kind of information.

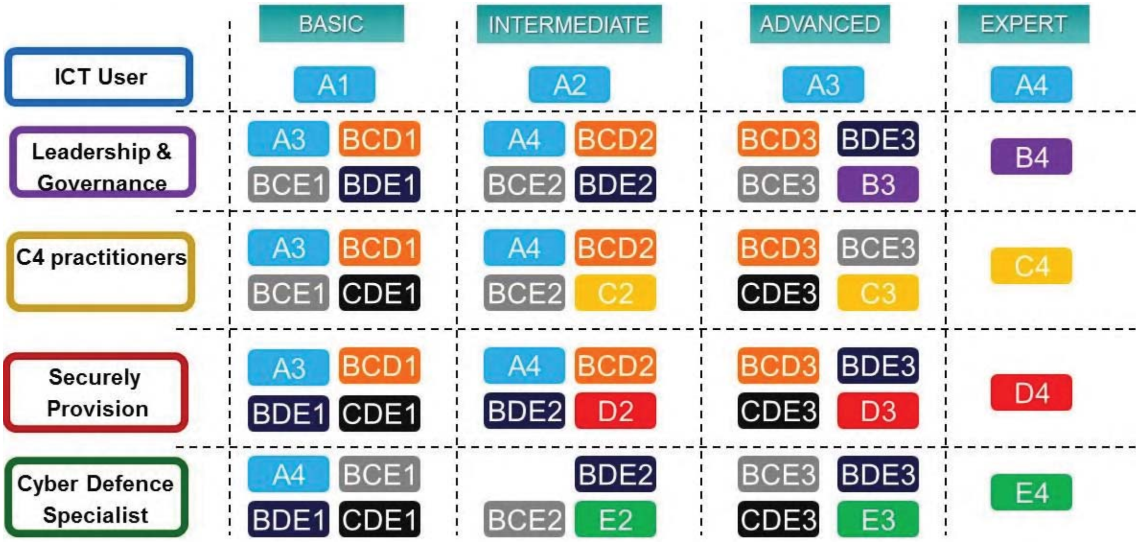
For the remaining phases, we will assume there is no available offer.

d. <u>Gap Analysis (Phase 4)</u>

Confronting the needs of E&T previously identified (Phase 2) with the existing offer (Phase 3), a gap analysis was held in order to identify CD E&T shortfalls.

Deliverables: Report on the gap analysis and resulting CD E&T Shortfalls.

As we have seen in phase 3, it appears that all the potential offers were not shared or inexistent. As a result, based on a systematic approach, we came to a realistic solution covering the full CD and cyber security spectrum, which can be visualized on the "Cyber Competencies Career Path Matrix" (detailed in Annex F).



	BASIC	INTERMEDIATE	ADVANCED	EXPERT
ICT User	A1	A2	A3	A4
Leadership & Governance	A3 BCD1 BCE1 BDE1	A4 BCD2 BCE2 BDE2	BCD3 BDE3 BCE3 B3	B4
C4 practitioners	A3 BCD1 BCE1 CDE1	A4 BCD2 BCE2 C2	BCD3 BCE3 CDE3 C3	C4
Securely Provision	A3 BCD1 BDE1 CDE1	A4 BCD2 BDE2 D2	BCD3 BDE3 CDE3 D3	D4
Cyber Defence Specialist	A4 BCE1 BDE1 CDE1	BDE2 BCE2 E2	BCE3 BDE3 CDE3 E3	E4

Figure 3: Cyber Competencies Career Path Matrix

Therefore, we have developed a tool that allows each MS or institution to conduct self-assessment in order to fill gaps individually (or collectively). Any potential contributor may feel free to share opportunities for cooperation through existing tools, such as CD TEXP or ETEE.

In Annex G, we can see an example of a possible contribution: module B3, to fulfil a gap on "cyber leadership and governance at an advanced level," is reported.

e. Proposed Solutions (Phase 5)

Taking into account CD E&T shortfalls (Phase 4) new solutions should be proposed.

Deliverables: CD E&T Coordination Platform. New proposals of CD E&T solutions (CD enhanced curriculum, special CD E&T equipment and infrastructures requirements, etc.).

The development of a centralized CD E&T coordination platform was envisaged at that stage by EDA: CD TEXP. This would help participating Nations to fill their gaps and will be focused on providing concrete answers to EU and MS' CD E&T requirements.

Within the cyber curriculum framework and to fill gaps identified by EDA's training needs analysis and ACT's CD training requirements analysis, the CD Discipline proposed new CD E&T solutions that are targeting academia, industry and other pooling and sharing projects.

Proposed solution follows (Annex I):

- Information security management
- Software and application security
- Digital forensics
- Social Engineering
- Digital crime and investigation
- Cyberspace and cyber operations legal framework
- Penetration testing and ethical hacking
- Cyber operations and planning
- Cyber intelligence and situational awareness
- Protection of critical infrastructures and systems
- Cyber capability development
- Cyberspace crisis management (exercise)
- Risk and incident management
- Information warfare
- Digital leadership and team management
- CD advisor

f. New CD E&T Initiatives (Phase 6)

Based upon viable solutions identified in phase 5, CD E&T sub-projects might be conducted in order to fill the remaining shortfalls

Deliverables: New CD E&T initiatives.

The proposed solutions presented in phase 5 are covering a great part of the competencies needed for the cyber landscape. It was identified four main areas that were not totally covered, related with: IT communications, Systems Administration, Cyber Education and Cyber Logistics.

New CD E&T initiatives should take into consideration the existing technical Courses from private sector. For further development, ESDC as well as other EU stakeholders, MS and NATO CD E&T training facilities outcomes should also be taken into consideration.

The EUMTG proposes that MS and institutions keep on working along those lines and develop correspondent E&T courses which would fill the Cyber Competencies Career Path Matrix. Those potential contributions could be voluntarily shared with other EU stakeholders through a proper channel.

The EU centralized CD TEXP is expected to be able to support three different domains – EU, national and multinational – and will take a central role in developing future cyber E&T initiatives. This platform will be crucial in proposing a set of courses and sharing valuable information with other platforms developed by nations (or international bodies).

3. CONCLUSIONS

After some years, the EU Military Training Group (EUMTG) "CD (CD) Discipline" achieved the working plan goal.

Having followed a systematic approach, the EUMTG CD Discipline defined first a Common Taxonomy, a Unified Cyber Competence Framework (UCCF), a common Cyber Curriculum and, taking into account the MS needs and offers, a Cyber Competencies Career Path Matrix.

Sixteen solutions and some new initiatives were proposed, covering the whole CD Discipline spectrum, and which can be now developed, adapted or maintained updated.

Cyber is a rapidly moving environment and, because of that, MS and Institutions should develop innovative and appropriate processes to adapt to a new reality. Empiric approach applied on our proposed initiatives should lead to a fast increase of EU capabilities in the correspondent domains.

The CD Discipline lead was pleased to work in an international environment and had the opportunity to work on an important topic for EU and MS. CD Discipline could benefit, at this stage, from new points of view. The actual CD Discipline leaders are opened to share their experience and lessons identified for a process which can always be improved.

4. RECOMMENDATIONS

After completion of this phase, the CD Discipline can provide some recommendations to further develop CD E&T capability in EU bodies and MS. ESDC, in charge of “giving a training and education instrument that promotes a European security culture”, could take a lead on that process.

a. Duality of CD Discipline

Cyber is a recent domain, sensitive and dual use in nature.

- We should merge the military reflexion with the civilian one, particularly within EU, to avoid unnecessary redundancies.
- The civilian sector (e.g. CEPOL, Academia and Industry framework) has expertise and can add value in the E&T fields.
- Cooperation with International Organisations is beneficial to avoid unnecessary duplication and also because of their interaction with the private sector.

b. Management of CD E&T

CD E&T has to be managed at different levels.

CD E&T courses must follow a process of EU accreditation and certification. The courses, will need to be reviewed in a regular basis, based on evaluations and lessons learned in order to improve and follow new trends.

An updated list of Cyber E&T Subject Matter Experts (SME), MS Points of Contact should be kept and one annual conference or seminar should be held to discuss CD E&T in EU.

c. Necessity to Standardize CD E&T Tools and Processes

The first next step should be the standardisation of all CD E&T Tools and Processes, in order to facilitate the management of CD E&T: exchanges, interoperability, and improvement.

- The standardisation has to be conducted according to the templates provided by EU and UCCF.
- CD TEXP has to be the central platform where all the cyber courses linked with CSDP should be registered.

d. Way ahead

- Note the revised report made by the CD Discipline Leaders.
- Final report will be presented at HTF/EUMTG Meeting, and finalised during April / May 2019.

REFERENCES

A. Cyber Security Strategy for the EU : an open, safe and secure cyberspace (Feb 2013)

B. Commission 2016 action plan

C. EUMC Strategic Guidance on CSDP Military Training 2016

D. Capability Development Plan, Emerging trends and key priorities (2014)

E. EU Concept for CD for EU-led Military Operations (2012, 2016)

F. Cyber ETEE platform, ESDC (Feb 2018)

G. EU-NATO joint declaration (Dec 2016)

H. European Council 19/20 December 2013, Conclusions (doc. EUCO 217/13, dated 20 December 2013).

I. EU CD Policy Framework (doc. 15190/14, dated 11 November 2014)

J. CD – Capability Requirements (doc. EEAS 00713/13, dated 27 March 2013).

K. Framework Process for Managing CSDP Military Training Requirements (doc. 17087/14, dated 19 December 2014).

L. Terms of Reference of EU Military Training Group (doc. 9357/14, dated 30 April 2014).

M. Guidelines for EU Military Training Discipline Leader (doc. 11192/15, dated 23 July 2015).

N. Military Training and Education in the EU - Draft Action Plan for the short term proposals (doc. EEAS 02648/13, dated 19 December 2013).

O. Council Conclusions on CSDP (doc. 15992/13, dated 25 November 2013).

P. Bi-SC Education and Individual Training Directive (E&ITD) 075-007

Q. Cyber Intelligence Tradecraft Project (http://www.sei.cmu.edu/about/organization/etc/citp-summary.cfm)

R. SANS-FOR578: Cyber Threat Intelligence (https://www.sans.org/course/cyber-threat-intelligence)

S. NIST Special Publication 800-181: National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF), 2017

T. The US department of Homeland Security webpage (http://niccs.us-cert.gov/glossary#letter_c)

U. IEEE Std 610.12-1990

V. NIST SP 800-12

W. IR 7298 Revision 2, Glossary of Key Information Security Terms (NIST, 2013)

X. CD Training Needs Analysis: Framework project on developing CD Capabilities for the Military (frameCyberCAP) – 12.CAP.OP.332, 2014

The following documents have been taken into consideration

Y. AC/322-N (2014)0072 NATO CD Taxonomy and Definitions

Z. AC/322-N (2014)0072 NATO CD Taxonomy and Definitions

AA. NATO CD Education and Training Plan

BB. 5000/TSC FCX 0010/Ser:NU0006 NATO CD Awareness, Education and Training Concepts

CC. ATrainP-1 Training and Education for Peace Support Operations (NATO, 2014)

DD. BiSC 75-2 Education and Training Directive (NATO, 2013)

EE. BI-SC 075-007 Education and Individual Training Directive (NATO, SEP2015)

ANNEXES

Annex A – CD Discipline Working Plan

Annex B – CD E&T Taxonomy

Annex C – Studies on Required Competencies & Skills

Annex D – CD E&T Needs Questionnaire

Annex E – CD E&T Existing Offers Questionnaire

Annex F – Cyber Competencies Career Path Matrix

Annex G – Example of Gap Analysis

Annex H – Example of a proposed solution for a CIC

Annex I – Proposed solutions

Annex J – Change Proposals

Brussels, April 2019

The CD Discipline Leaders

Annex A - CD Discipline Working Plan *(April 2015)*

CD Discipline Working Plan

1. WORKING PLAN

a. In accordance with the guidelines defined by EUMTG, this working plan defines the way how the CD Discipline Leading Nations intends to support the management of the EU CSDP CD military training requirements in a coherent and integrated way.

b. Given the EU CD Capability Requirements definition, the main objective of this working plan is to help the EUMTG and MS to identify CD E&T requirements and needs and fill the gaps deriving from their CD Capability development process.

c. The CD Military Training Discipline plan of work is developed over several phases, integrating in each stage the results deriving from the different modules / areas identified as building blocks of CD E&T initiatives (identification of competencies and skills to be developed, analysis of E&T needs, analysis of existing initiatives and identification of gaps not yet fulfilled). Within this context, the working plan develops along the following phases:

- Phase 0 – Approval of the Working Plan by the EUMTG

  Development of the Working Plan and its validation by the EUMTG.

  Deliverables: CD Military Training Discipline Working Plan.

- Phase 1 – Competencies and Skills Requirements

  The main purpose of this stage is to identify and define the competencies and skills considered as necessary to achieve the general and specific performance objectives associated with the EU CD Capability. This process will be based upon the analysis of the Generic Military Task List (GMTL) and the task requirements associated with the CS and CD military capabilities. EDA's CD TRA[10] and other relevant NATO[11] inputs will be taken into consideration.

  Deliverables: Report on required CD Competencies and Skills.

- Phase 2 – E&T Needs

  Based on the tasks to be performed and in the identified competencies and skills requirements (Phase 1), we intend to identify the needs of E&T on CD at all levels – EU CSDP related Bodies and MS.

  Deliverables: Common CD E&T Curriculum (preliminary version).

- Phase 3 – E&T Offer

  At this stage we intend to analyse the existing offer of CD E&T (nationally and internationally) in order to support personnel participating at EU missions and CSDP Operations and at National CD related activities. A questionnaire should be envisaged as a

[10] EDA has established in 2011 a Project Team on CD (PT CD) and developed an EU CD Stocktaking Study were an initial CD Training Needs Analysis was conducted. As a result of this study several CD Education and Training (CD E&T) gaps were identified at both EU and MS level. At this area, the EU CD Policy Framework emphasized the need to develop programs for different audiences in the CSDP chain of Command.

[11] Namely NATO SACT's TRA and MNCDE&T Project deliverables should be taken into account.

valuable and structured way to obtain the relevant information related with the existing CD E&T Offer.

Deliverables: List of available CD E&T activities.

- Phase 4 – Gap Analysis

  Confronting the needs of E&T previously identified (Phase 2) with the existing offer (Phase 3), a gap analysis will be held in order to allow the identification of CD E&T shortfalls.

  Deliverables: Report on the gap analysis and resulting CD E&T Shortfalls.

- Phase 5 – Proposed Solutions

  Taking into account CD E&T shortfalls (Phase 4), not yet fulfilled by the available offer, new initiatives should be proposed. The development of a centralized CD E&T coordination platform should be envisaged at this stage. EDA intends to acquire a similar platform in 2015. This should help participating Nations to fill their gaps and will be focused on providing concrete answers to EU and MS' CD E&T requirements. The civilian Goalkeeper Schoolmaster Project and the Schoolmaster Application Portal could also be considered to support CSDP Training.

  Deliverables: CD E&T Coordination Platform. New proposals of CD E&T initiatives (CD enhanced curriculum, special CD E&T equipment and infrastructures requirements, etc.).

- Phase 6 – Implementation of New Initiatives

  Based upon viable solutions identified in phase 5, CD E&T sub-projects might be conducted in order to fill the identified shortfalls. ESDC as well as other EU, MS and NATO CDE&T training facilities should be considerate at this stage.

  Deliverables: New CD E&T initiatives.

- Phase 7 – Preparation of the Final Report.

  Deliverables: Final Report.

d. CD Discipline Lead (France and Portugal) plans and coordinates the work conducted at each phase. Relevant EU Bodies, MS' SME and other Participants provide the added value of their expertise in order to support all the planned activities.

e. The CD Discipline Lead Nations will organize workshops and questionnaires in order to consolidate the activities and the work conducted at each phase of the working plan. Partial results will be presented, discussed and integrated at workshops in order to enhance and consolidate the outputs and deliverables. Progress will be reported to EUMTG in a periodical and regular basis.

f. EU and NATO have already expressed willingness to develop CD cooperative efforts, namely at the CD E&T arena. Therefore, staff-to-staff EU-NATO cooperation should be envisaged at the various phases of this Program of work.

2. PLANNED ACTIVITIES

a. In the view to develop a coherent approach and foster future cooperation, the CD Discipline Leaders (France and Portugal) will present at the next EUMTG meeting (end of June / early July 2015) an initial working plan, with a view to allow its preliminary discussion with EU Agencies/Organizations (EEAS, EUMS, EDA, CMPD, ESDC) and MS that would be interested to engage and actively participate at both TRA and TNA Workshops and related activities.

b. Given the fact that there are already several on-going initiatives at EU (EEAS, EDA, ESCD), National and NATO (SACT and MNCDE&T) levels, the intention is to incorporate all these inputs and to complete this working Plan in 2016.

c. In order to set time limits adjusted to the fulfilment of the proposed objectives, the following activities / initiatives were scheduled to be developed in a comprehensive and sequential manner:

Location/Dates	**Content**
EUMTG WS (28 Apr 15)	Presentation of the Draft Proposed Working Plan by the CD Discipline Lead Nations (France and Portugal)
May – June 15	Declaration of interest by EU Agencies/Organizations and MS to participate at TRA and TNA Workshops and related activities
EUMTG WS (July 15)	Presentation and preliminary approval of the Working Plan (by EUMTG)
CD Discipline (July 15)	CD TRA Kick Off Meeting (back to back with EUMTG WS)
CD Discipline (September 15)	**Workshop 1** (Phase 0 and Phase 1)
CD Discipline (November 15)	**Workshop 2** (Consolidation of Phase 1 and Phase 2 preliminary results)
CD Discipline (February 16)	**Workshop 3** (Consolidation of Phase 2)
CD Discipline (May 16)	**Workshop 4** (Phase 3 preliminary results)
CD Discipline (July 16)	**Workshop 5** (Consolidation of Phase 3 and modular results Phase 4)
CD Discipline (Oct / Nov 16)	**Workshop 6** **(Consolidation of Phase 4 and 5 – Final Report 1st Draft)**
CD Discipline (Jan-Nov 16)	**New CD E&T Initiatives** (Phase 6 - Filling CD E&T identified gaps – Courses and Training Delivery)
EUMTG WS (December16)	Presentation of the Final Project Report to EUMTG (Phase 7)

Annex B - CD E&T Taxonomy used for this report

CD E&T Taxonomy used

Introduction

1. The CD Discipline requires a list of agreed cyber definitions and acronyms since it will help to create a common knowledge base, EU, as well as NATO references related to CD education and training, and include additional definitions that might be considered necessary for future work. Dealing with military matters, this Taxonomy largely builds on agreed references, but most can be replicated in a civilian environment.

Taxonomy structure

2. The definitions are structured into the following groups:
   - Definitions related to CD Discipline
   - Definitions related to CD and adjacent domains
   - List of acronyms

3. The terms related to CD Discipline reflect education and training in CD from a EU perspective, for a common understanding within the Discipline and further CD E&T within EU framework.

4. Whereas definitions related to CD in this document were formulated to reflect both EU and MS' perspective, the Annex lists already existing definitions articulated by EU, NATO, NIST and ISACA.

Glossary

5. Definitions related to CD Discipline

(Course) Accreditation	The process resulting in recognition that an institution has met standards established by an external body/agency.
(Attendee/ Participant) Certification	The process of officially recognizing that organizations, individuals, materiel or systems meet defined standards or criteria.
Competence	Ability to perform a particular skill or a range of skills to a prescribed standard under prescribed conditions.
Competency	A behavioural indicator of competence, which includes the set of knowledge, skills, abilities or other characteristics which may vary among individuals, that contributes to effective performance.
Competency profile	A list of skills and knowledge necessary to successfully fulfil a task or job.
Curriculum	The combination of strategies and learning employed in an attempt to fulfil specific learning objectives of an educational institution or training unit.

CD Awareness Program	An awareness program addressing CD knowledge as a part of CIS Security, use of personal devices, and social engineering and promoting personal investment in threat prevention.	
CD Education	The process to impart knowledge related to CD through formal and informal study, in order to achieve competencies and skills to fulfil specific tasks or duties.	
CD Exercise	A planned event during which an organization simulates a cyber disruption in order to test the effectiveness of capabilities such as preventing, detecting intrusions or weaknesses, mitigating, responding to or recovering from the disruption.	

CD Organizational Framework	A generic CD framework which contains all identified CD roles and their assigned tasks. It spreads across all levels:
	– Strategic Level;
	– Operational Level;
	– Tactical Level.	

CD Training	The process of improving the skills and competencies related to CD, in order to ensure effective responses in CD operations.	
Depth of Knowledge (DoK) levels (as used by NATO)	Level 100: General Knowledge	Requires a level of understanding that will enable a learner to recall elements and details of structure or process and recognize or identify specific information.
	Level 200: Foundation Skills and Competences	Requires a level of comprehension that will enable a learner to use foundational conceptual and procedural knowledge in a controlled working environment with ease and with minimum supervision.
	Level 300: Advanced Skills and Competences	Requires a level of comprehension that will enable a learner to reason, analyse and interpret concepts, patterns and relationships to develop a plan and sequenced steps. This requires the ability to make some decisions and justification using abstract and complex analytical thinking skills and to offer more than one possibility to solve a problem.
	Level 400: Expert Skills and Competences	Requires a level of comprehension that will enable a learner to investigate and apply solutions to complex problems. This requires the ability to research and process multiple conditions of the problem or task, based on in-depth complex reasoning, planning and development skills that have been acquired across disciplines and over an extend period of time.

	Level 500: Master Skills and Competences	Requires a learner to have the full extent of comprehension that will enable a level of forward leadership reasoning and strategic thinking skills to see outward and immediately plan for today to achieve strategic goals of the future in the most effective, efficient and affordable way possible.

Education and Training Audiences (Target Audiences)	A reference to the courses' targeted audiences, which depicts the correspondence between the personnel, the job description inside the CD Organizational Framework and the training requirements.
	Includes the following specialization levels:
	– ICT users (ICT);
	– Leadership and Governance (L&G);
	– Command, Control, Communications and Computers (C4) Practitioners;
	– Securely Provision (SP);
	– CD and Security (CDS) Specialists.	

	ICT users	This category is represented by all military and civilian personnel within the TA Boundary interacting with networked digital data through officially-provided and/or privately-owned ICT devices. Because of this, they are potential vectors for (and may be conscious or unwitting agents of) cyber attacks. Some (but not all) people within the ICT User Category will have a role which makes them also a member of one of the other three TA categories. The ICT user TA category is super-ordinate to the other three categories, as members of the latter are necessarily also members of the former.
	Leadership and Governance	This category encompasses all of the senior military and civilian personnel within the TA Boundary who are required to make decisions which should be informed by CD considerations. Whilst their staff can and do provide them with CD informed advice and recommendations, it is clearly important for Senior Decision Makers themselves to be able to make CD-informed decisions. The Senior Decision Maker TA category is usually bounded by military officers from NATO Grade OF-6 (in some cases OF-5) and the equivalent civilian grade upwards.

	Command, Control, Communications and Computers (C4) Practitioners	This category encompasses the many junior and middle-ranking military and civilian personnel within the TA Boundary who have generalist or non-CD specialist roles. Such personnel are not required directly to implement CD measures, but may still oversee, work closely with, or support those who do. They themselves often have to make routine decisions in which CD should be a key consideration. Their roles also entail the provision of CD-informed advice to, and the development of CD-informed plans for Senior Decision Makers. The C4 Practitioner upper boundary is NATO military Grade OF-5 and the equivalent civilian grade.
	Securely Provision	This category encompasses military and civilian personnel within the TA Boundary who have a supporting role in the cyber operations domain by securely providing systems and services. They Conceptualize, design, and build secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.
	CDS Specialists	This category encompasses military and civilian personnel working in CD specific roles who are required to undertake relatively narrowly-bounded and/or technically complex CD activities. They adopt CD measures in order to prevent, protect against, detect or react to cyber-attacks. The CD Specialists upper boundary is NATO military Grade OF-5 and the equivalent civilian grade.
(CD Education and Training) Initiative	An undertaking (i.e. training, course, exercise, etc.) that is aimed at providing CD skills or competencies to fulfil CD education and training shortfalls at EU and/or at organizational/multi-national level. Examples of initiatives defined in CD Discipline: - CD Awareness Course; - Cyber Security and CD International Master; - Cyber Law and CD International Master; - Cyber Intelligence Course; - CD Staff Officers' Course;	

		- CD Capability Development Course. …….
Knowledge, Skills and Abilities (KSAs)		Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and Training.
Learning objectives		Articulate knowledge and skills students are expected to acquire by the end of a course or training.
Levels of proficiency		A reference to the levels of competency targeted by the courses
	Basic	Specific: – The individual can identify basics aspects of CD in his/her function/role. – The individual can perform basic or developmental level work in activities requiring this competency. The individual is capable of demonstrating this competency after being given specific instructions and guidance and can engage in general conversation about this competency. – Depth of Knowledge level 1. – Equal to NATO level 100.
	Intermediate	Specific: – This individual demonstrates an understanding of CD for his/her organization. – He/ She is considered someone who has the capability to fully perform work that requires application of this competency in routine situations and can contribute with knowledge or new ideas in applying this competency. The individual consults co-workers at advanced level for unknown situations. – Depth of Knowledge level 2. – Equal to NATO level 200.
	Advanced	Specific: – The individual has a broad understanding of the CD domain, and applies strategic thinking to put (aspects of) CD in the bigger picture. – An individual is able to perform tasks related to this competence successfully in non-routine and sometimes complicated situations. The individual is confident in serving as an advisor and is sought out to provide insight into the application of this competency. – Depth of Knowledge level 3. – Equal to NATO level 300.
	Expert	Specific: – The individual has in-depth-knowledge of (several) CD aspects. – The individual is able to perform successfully in complex, unstructured situations. He/ She validates

	(new) ideas and develops criteria to judge the quality of work (of others). He/ She serves as a resource and provide guidance to others. – Depth of Knowledge level 4. – Equal to NATO level 400.
Lifelong learning	All learning activity undertaken throughout life with the aim of fostering continuous improvement of knowledge, skills and competences needed for employment and personal development.
Cyber Range Capability	A distributed and federated, simulated, environment in which CD operators can administer and undertake training; develop tactics, techniques and procedures to counter evolving threats; and test technologies to ensure they are ready to meet head-on challenges.
Training Needs Analysis	A process conducted to identify specific key components that will affect the curricula and the depth of knowledge that must be achieved to attain the correct level of critical thinking. TNA defines learning and enabling objectives required to eliminate Performance Gaps, and systematically delivers a training opportunity.
Training Requirements Analysis	A systematic yet flexible process, vital to ensure that a holistic representation of the education and training environment is produced. TRA is a process used to systematically identify relationships between the target audience, Depth of Knowledge and competencies required for personnel and/or functions.

6. Definitions related to CD and adjacent domains

Accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
CIS Security	The application of security measures (technical and non-technical) for the protection of communication, information and other electronic systems, and the information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, authentication and non-repudiation.
Cyber Attack	An act or action initiated in cyberspace to cause harm by compromising communication, information or other electronic systems, or the information that is stored, processed or transmitted in these systems.
Cyber Capability	The combination of people, means and procedures to achieve a cyber-effect which contributes to a (mission) goal.
Cyber Crime	Any illegal activity that uses information systems or networks as its primary means of commission.

Cyber Crisis	An unauthorized of unexpected CIS event where automated measures have failed, whose impact is considered severe and recovery cannot be achieved through the involvement of cyber experts.
CD	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 EU/National military tasks and Crisis Management Operations.
Cyber Event	An unauthorized and unexpected CIS event whose impact is minimal and recovery is easy or automatic.
Cyber Incident	An unauthorized or unexpected CIS event where automated measures have failed, whose impact is not severe and recovery can be achieved through the involvement of cyber experts.
Cyber Resilience	Ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from deliberate cyber attacks, accidents or naturally occurring threats or incidents.
Cyber Security	The application of preventive, protective, responsive and recovery security measures for the protection of the information, resources, public and private services running into cyber space, with respect to confidentiality, integrity and availability.
Cyber Security Workforce	Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defence actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.
Cyber Space	Global domain made from the network of information technology infrastructures (including the Internet), telecommunications networks, information systems, processors and integrated control mechanisms Cyber space includes transported digital information as well as operators' network infrastructures of online services.
Cyber Space Effects Workforce	Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.
Cyber Space IT Workforce	Personnel, who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.
Cyber Space Workforce	Personnel who build, secure, operate, defend, and protect EU cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and

	portions of the Intelligence workforce.
Cyber Operations	Actions to achieve (military) goals using cyber capabilities.
Cyber Threat	Any potential malicious action of either intentional or unintentional character associated with exploitation of a vulnerability in cyber space that could lead to loss of availability, integrity and confidentiality of CIS.
Information Assurance	A set of measures to achieve a given level of confidence in the protection of communication, information and other electronic systems, non-electronic systems, and information that is stored, processed or transmitted in these systems with respect to confidentiality, integrity, availability, non-repudiation and authentication.
Information System	Organized set of resources (hardware, software, personnel, data and procedures) allowing to collect, process, maintain, use, share and disseminate information.
Intelligence Workforce (Cyber Space)	Personnel who collect, process, analyse, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.
Vulnerability	A development fault or other weakness in a system that can be exploited in order to allow an attacker to compromise confidentiality, availability or integrity of the system. Vulnerabilities can originate from flaws on the design of the system, defects in its implementation, problems with its operation or intended malicious behavior of the system.

7. Acronyms

CC	Cyber Coalition
CD	CD
CDS	CD and Security
CIS	Communication and Information Systems
COE	Centre of Excellence
CS	Cyber Security
EDA	European Defence Agency
E&IT	Education and Individual Training
E&T	Education and Training
ETEE	Education, Training, Exercise and Evaluation
JFT	Joint Force Trainer
MTEP	Military Training and Exercise Programme

TA	Training Audience
TNA	Training Needs Analysis
TRA	Training Requirements Analysis

Annex C - Studies on Required Competencies & Skills

Studies on Required Competencies & Skills

“The goal of the CD Competencies and Skills phase was to create a Cyber Competence Framework for EU bodies and EU MS to educate and/or train all of their military and civilian personnel. The framework provides an overview of tasks accompanied with the needed *Knowledge, Skills and Abilities* (competencies) in order to perform roles as proficient as possible.

From now on only the term competencies will be used, indicating Knowledge, Skills and Abilities.

To understand what competencies are needed, it is necessary to determine a comprehensive list of Target Audiences, cyber (defence) tasks and competencies in order to execute these tasks effectively. The used approach is to combine two existing frameworks using a method that has already been developed in the context of the (military) cyber domain:

- EDA Landscaping Study (2013)
- NIST SP 800-181 NICE Cybersecurity Workforce Framework (2017)
- Dutch Cyber Cube method (2014)

The Dutch Cyber Cube method (see figure below) is a method developed by the Dutch MoD and ties the frameworks from the EDA Landscaping Study and the NIST SP 800-181 NICE Cyber Workforce Framework (NCWF) together in a Unified Cyber Competency Framework (UCCF). Although the two frameworks have an overlap, there are also differences:

- The EDA Landscaping study focuses on EU using a Hierarchical Task List, defined on a high and more strategic oriented level whereas the NCWF has a limited focus on strategic tasks and roles, but more on the tactical and technical level roles;
- The EDA Landscaping study contains 18 target audience segments, whereas the NCWF defines 52 roles;
- The EDA Landscaping study differentiates between core and supporting tasks, and addresses proficiency levels to indicate significant tasks whereas the NCWF lists them in-discriminatory to each of the 52 defined roles;
- The NCWF defines an elaborate set of competencies to each of the 52 defined roles, whereas the EDA Landscaping study does not;
- The EDA landscaping study was developed as an EDA project in 2013, whereas the NCWF was built upon several US frameworks, using both military and civilian experts in a joint effort over a period of 7 years.

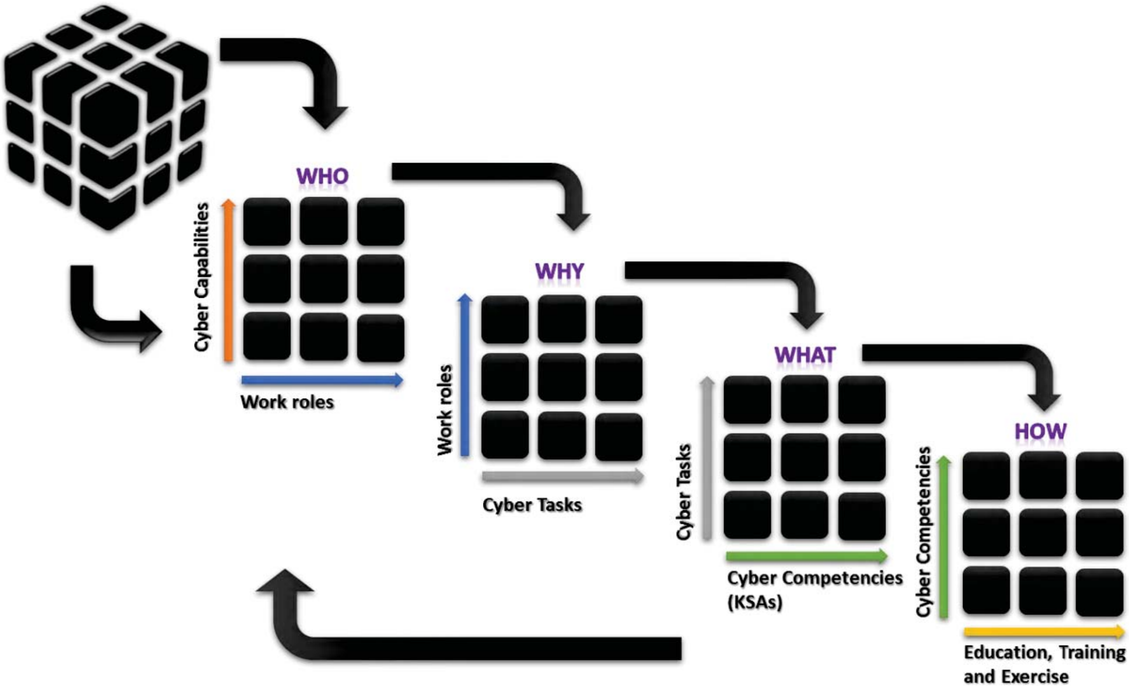


Figure 1: The Dutch Cyber Cube method

The process of combining the two frameworks into an UCCF was performed by the following stepped approach, using the Dutch Cyber Cube method and starting with the ‘WHO’.

1. **WHO**

a) The EDA HTL was discussed by the MNCDE&T project team and declared fit for purpose after a few additions in the Target Audience definitions to address both the NATO enterprise and the MoDs of the participating nations.
b) The Target Audience list from the EDA HTL was matched with the 52 work roles from the NCWF. The NCWF work roles were grouped along the Target Audience list from the EDA HTL where possible. Some roles did not fit directly in the framework, so an additional segment was made to incorporate all of the 52 work roles in a combined Target Audience list (for instance the roles under the segment Securely Provision).
c) A segmentation of four distinct proficiency levels was developed, based on Webb’s Depth of Knowledge (DOK) model, Bloom’s taxonomy and the NATO level 100-500 classification. The four proficiency levels have a separate definition for the CD Task level and the corresponding Competency level.

2. **WHY**

a) After a trial-and-error approach, a direct mapping of the (~1000) CD tasks of the NCWF in the EDA HTL (at the lowest level of sub-sub-tasks) was assessed as unsuccessful. Therefore, the highest segmentation of the EDA HTL was taken (Prepare, Prevent, Detect, Respond, Enable) to cluster all of the CD tasks of the NCWF. This was performed in several iterations and by assessing each of the described tasks (and the work roles they are linked with to gain as much context as possible) using a workshop approach.
b) The clustering approach from step 1 resulted in an adapted hierarchy of (sub)task levels, based on the highest segmentation level of the EDA HTL.

Where possible the next level was used. In the figure below a mindmap with a collapsed (highest level of) tasks levels is shown. The total mindmap overview of the UCCF task levels can be found in the Annex D-1. Each task level has an added task level description.

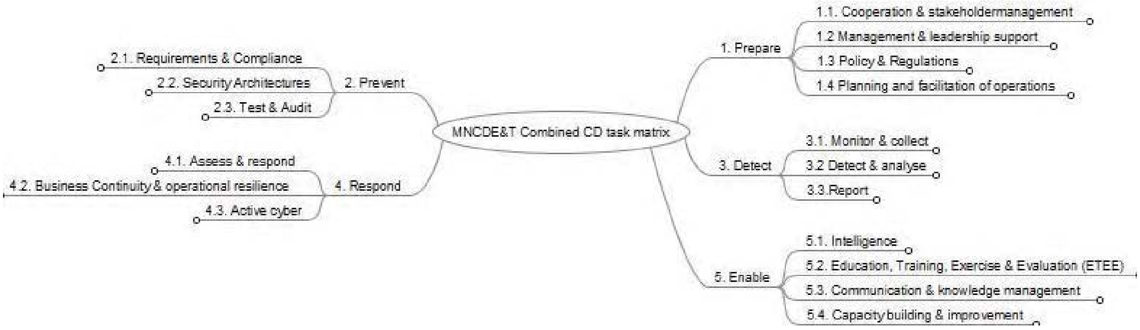

MNCDE&T Combined CD task matrix
1. Prepare
1.1. Cooperation & stakeholdermanagement
1.2 Management & leadership support
1.3 Policy & Regulations
1.4 Planning and facilitation of operations
2. Prevent
2.1. Requirements & Compliance
2.2. Security Architectures
2.3. Test & Audit
3. Detect
3.1. Monitor & collect
3.2 Detect & analyse
3.3.Report
4. Respond
4.1. Assess & respond
4.2. Business Continuity & operational resilience
4.3. Active cyber
5. Enable
5.1. Intelligence
5.2. Education, Training, Exercise & Evaluation (ETEE)
5.3. Communication & knowledge management
5.4. Capacity building & improvement

Figure 2: Highest level of UCCF task description

c) The UCCF tasks levels have been reviewed and updated in the task level overview. A specification of proficiency level per task and per work role has not been made, as this was too dependent on where (for instance a nation) the UCCF would be implemented. It could be done across nations (to get an average rating) however this would require a large amount of effort to perform this analysis from many nations.

d) The UCCF tasks and their clusters have been placed in an Excel. Per UCCF task and overview has been made to link the respective task (WHY) with the corresponding Target Audience (WHO), based on the existing NCWF information.

3. WHAT

The UCCF contains an overview (matrix) of tasks and target audiences. The NCWF also contains a list of competencies (divided in Knowledge, Skills and Abilities) that are linked per work role. As the work roles are used with the UCCF in a combined Target Audience List, a ‘translation’ can be made to identify the competencies per Target Audience Segment.

4. How to use the UCCF

The UCCF can be used in different ways. The most important thing to remember is that the UCCF is a framework that contains building blocks. These building blocks are a way to structure and describe (part of) a cyber organisation.

Although the UCCF is originally built to identify the core competencies to select a course or training for an individual (task 3 in the list below), the current framework can also be used to support other tasks that we describe below.

The UCCF contains a rich selection of building blocks allowing you to:

- Task1: Use the UCCF as a Rosetta stone to express or describe (part of) a cyber organisation; Using the framework to describe national cyber organisations makes it easier to relate different national cyber organisations e.g. to train their personnel and share education with other nations in the future. The building blocks are also useful when your cyber organisation is growing or restructuring. NB. The framework might not contain all building blocks to describe all particular parts for all types of cyber organisations.

- Task 2: Structure and describe a work role; People often have more work roles comprising of core tasks and support tasks. Identifying the core tasks of a role helps to structure the work and workload of personnel. It also facilitates structuring additional work roles within a cyber organisation. The competencies in the UCCF allow you to define the prerequisite competencies.
- Task3: Identify core competencies to select a course or training; Having identified the work role and the corresponding core tasks allows you to identify the core competencies to be trained to improve the task proficiency. The list of core competencies also helps to identify training to ensure a proficient task execution over time.
- Task 4: Identify core competencies to develop a course or training. The result of the previous task (3) could also lead to the recognition that currently no course or training are available. Having identified the core competencies will help to develop a curriculum to address the gap.

5. Typical setup

The following paragraph describes a typical setup that can be used to carry out tasks 3 and 4: Identifying core competencies to select/develop a course or training. We describe these steps at a high level, as most organisations will have a dedicated department and specific procedures for this. It is advised to apply these steps to the available procedures in your organisation.

- Create a diverse consultative group that will support you to identify the core competencies for the task(s). The group could contain for example representatives that perform the task(s), have a role in education and training, and of the human resource department.
- As a curriculum is usually developed around one or more tasks, the first goal would be to select the task(s) and create a common understanding of the task. Identify the work role(s) that carry out the task(s).
- Select the core-, support- and prerequisite-competencies. Create a common understanding of the competencies.
- Define the proficiency level for the task(s) and the set of core competencies with your consultative group. You can also define the proficiency level for the support competencies and the prerequisites; however, we assume at this moment that the course has or will have a focus on the core competencies.
- To combine, align or extrapolate learning goals and possible topics for courses from the competencies. This step could be done using your consultative group, but it may be easier to do this with an education and training specialist first and then check with the rest of the group.
- Use the learning goals and topics to either find an existing course or start the process to develop a course (or training).”

6. Mindmap overview of the UCCF task levels (PDF)

MNCDET Combined
CD task matrix 2.3.4

7. Unified Cyber Competence Framework

20171129 Unified
Cyber Competence F

8. EDA TNA

frameCyberCAP WP2
TNA report v0.pdf

Annex D - CD E&T Needs Questionnaire

CD E&T Needs Questionnaire

Based on the tasks to be performed and in the identified competencies and skills requirements (Phase 1), a questionnaire[12] about CD E&T needs was sent to MS to identify the needs at all levels. Its aim was to capture the insights of relevant stakeholders related with CD at National levels.

Based on the CD E&T Questionnaire results, a 'Theoretical Common Curriculum' was developed, as described in Main Body, §2.e.

1. QUESTIONNAIRE OVERVIEW

a. Questionnaire Instructions

Answers to the CD E&T Requirements questionnaire were attended NLT 30MAY18.

At National level, questionnaires had to be directed to the relevant Organizations and practitioners of CD (e.g. CD Centre/Command, MoD CD E&T, etc.) and Cyber Security (e.g. National Cyber Security Centres, National CERTs, and Networks).

The main Target Audience for answering this questionnaire was the Cyber E&TE related Management authorities, taking into consideration their respective areas of responsibility.

The following phased and sequential approach was recommended to the various POCs:

- PHASE 0 – Identification of National CD/Cyber Security E&TE related decision makers.
- Output – List of all the Target Decision Makers that will be answering the questionnaires (National Level).
- PHASE 1 – Meeting with the relevant stakeholders that will be answering the questionnaire.
- Output – Common understanding of the aim and expected outputs of the questionnaire.
- PHASE 2 – Delivery of a pilot questionnaire (selected CD/cyber security organization).
- Output – Validation of the questionnaire at a National level.
- PHASE 3 – Delivery of the TNA questionnaire to the entire selected community (identified at PHASE 0). Deadline to receive answers and a helpdesk should be provided.
- Output – National CD/Cyber Security E&T relevant organizations fill in and return their answers to the National POC.
- PHASE 4 – Compilation of the questionnaire answers by the National POCs.
- Output – Summary of TNA findings derived at National Level.
- PHASE 5 – Fulfilment of the National response to the questionnaire by the National POC.
- Output – National answer to the questionnaire.
- PHASE 6 – Delivering National answers to the questionnaire.
- Output – National POC send the answer to the CD Discipline Management Team.

[12] This questionnaire is extracted from a NATO survey, part of the CD Training Needs Analysis (TNA) conducted by the NATO Smart Defence Project 1.36 - Multinational CD Education & Training (MNCDE&T). This survey was it-self adapted from a study that was conducted by the European Defence Agency (EDA) and undertook by RAND Europe, TNO, Vedette Consulting and FRS.

Taking into consideration that organizations related with CD and Cyber Security tend to be very specific and diverse from country to country, National POCs felt the need to balance their answers (according with their relative importance) against the need to produce a single and integrated national answer.

The synthesis of the different answers received had therefore to be weighted according with the relevance of each organization within the National CD/Cyber Security framework and its responsibility towards the ET&E requirements definition. Nations were invited to adopt the following weights:

WEIGHT	ORGANIZATION
5	CD Organization
4	Cyber Security Organization
3	Military Organization involved in cyber crisis operations
2	Civilian Organizations involved in cyber crisis operations
1	Other Organizations Cyber related

b. Target Audience Categories

The Target Audience (TA) was bounded for the purpose of the studies to for categories of users:

- Information & Communications Technology (ICT) user: all military and civilian personnel within the Target Audience Boundary will interact with networked digital data through officially-provided and/or privately-owned Information and Communication Technology (ICT) devices. Because of this, they are potential vectors for (and may be conscious or unwitting agents of) Cyber Attacks. Some (but not all) people within the ICT User Category will have a role which makes them also a member of one of the other 3 TA Categories. The ICT User TA Category is superordinate to the other 3 Categories, i.e. encompasses members of all three categories.
- CD Specialist: this Category encompasses military and civilian personnel within the Target Audience Boundary working in CD specific roles who are required to undertake relatively narrowly-bounded and/or technically complex CD activities. These attributes distinguish CD Specialists from personnel in the C4 Practitioner and Senior Decision Maker TA Categories.
- C4 practitioners: this Category encompasses the many junior and middle-ranking military and civilian personnel within the Target Audience Boundary who have generalist or non-CD specialist roles. Such personnel are not required directly to implement CD Measures, but may still oversee, work closely with, or support those who do. They themselves often have to make routine decisions in which CD should be a key consideration. Their roles also entail the provision of CD informed advice to, and the development of CD-informed plans for, Senior Decision Makers.
- Senior CD Decision maker: This Category encompasses all of the senior military and civilian personnel within the Target Audience Boundary, who are required to make decisions which should be informed by CD considerations. Whilst their staffs can and do provide them with CD-informed advice and recommendations, it is clearly important for Senior Decision Makers themselves to be able to make CD-informed decisions.

2. QUESTIONNAIRE STRUCTURE

a. Section 1 – About Organisation

- Type of Organisation.
- Location.
- Relevance of the TA bounding.

- Number of people within each TA category.

b. Section 2 – Task Analysis

The purpose of this part of the questionnaire was gathering data on the performance requirements of personnel engaged within the CD domain. This allowed us to understand what tasks they carry out, as well as understand to what standard these tasks must be performed.

For each of the following tasks, MS had to indicate:

- the frequency with which tasks are performed by each TA Category (Never, Several times a day, Daily, Several times a week, Weekly, Several times a month, Monthly, Several times a year, Annually);
- the level of competence expected (Not required, Awareness, Practitioner, Expert).

- List of tasks (can be extended by MS):
- take preventive actions against malicious Cyber Attacks;
- take protective actions against malicious Cyber Attacks;
- undertake actions that detect malicious Cyber Attacks;
- undertake actions responding to malicious Cyber Attacks;
- recover from malicious Cyber Attacks;
- learn lessons from attacks, damage or unauthorised access.

c. Section 3 – Existing and Future Training Provision

MS had to answer following questions:

- Are personnel within your organisation expected to participate in security awareness training? When is the awareness training undertaken? How often does the awareness training need to be undertaken?
- Does the security awareness training include details on how to prepare for, prevent, detect, respond to, recover from and learn lessons from attacks?
- Overall, do you consider there to be sufficient training and education provision for CD aspects of EU/National military tasks and Crisis Management Operations? If not, please indicate your top three suggestions for what might be done?
- In order to gain insights into the level of priority for CD training of segments of people within MS organisations, MS had to choose for each following segment:
- the level of priority (no, low, medium, high) currently placed on CD Training;
- the current training provision (0 - Not currently being trained in CD, 1 - Trained on-the-job, 2 - National Defence Training institution, 3 - National Commercial Training Institution, 4 - International Defence Training Institution, 5 - International Commercial Training institution, 6 - Both national and international training);
- the training preference in the future (Select people who have this competence in advance, Formal training as part of induction, On the job training, Formal training within first year of role, Same as currently provided, No training required).

List of segments:

- Senior military and civilian personnel working in EU, National MOD and HQs, who engage in policy, strategy, concept, doctrine and/or capability development.

- Senior military and civilian personnel working within the EU, National MOD and Joint HQs, who plan, inform, implement and support CRO and National CMO.
- Senior military officers in, or liable for, command appointments at the Operational, Force, Component Command and HQ echelons of CRO and National CMO.
- Senior military and civilian personnel working within the EU, Nations' MOD and Joint HQs, filling Chief Information Officer, Senior Information Risk Owner, or similar Information Governance roles.
- Military and civilian personnel working within the EU, Nations' MOD and Joint HQs who engage in policy, strategy, concept, doctrine and/or capability development.
- Military and civilian personnel working within the EU, Nations' MOD and Joint HQs who plan, implement and support CRO and National CMO missions.
- Military staff officers and civilian advisors assigned to ‘at readiness’ and ‘committed’ Operational HQs, Force HQs, Component Command HQs.
- Legal Advisors who provide advice and make recommendations to Senior decision makers, and to their supporting staff officers and advisors.
- Military and civilian personnel who deliver CIS services in support of the Alliance, CRO and National Military CMO, and to ‘at readiness’ and ‘committed’ Operational HQs, Force HQs, Component Command HQs.
- Military and civilian personnel who design and deliver education, and individual and collective training interventions for C4 Practitioners and Senior Decision Makers.
- Military and civilian personnel who undertake CD Architect, Accreditor and Auditor functions.
- Military and civilian personnel who undertake CD Monitoring, Analysis and Response functions in support of day to day activities, CRO and National Military CMO.
- Military and civilian personnel who undertake CD Investigator functions in support of day to day activities, CRO and National Military CMO.
- Military and civilian personnel who provide specialist CD advice to Senior Decision Makers and C4 Practitioners engaged with day to day activities, CRO and National Military CMO.
- Military and civilian personnel who design and deliver individual and collective training interventions for CD specialists who support CRO and National Military CMO.
- Military and civilian personnel who undertake CIS-specific physical and personnel security functions in support of day to day activities, CRO and National Military CMO.
- Military and civilian personnel who direct, collect, process and disseminate all-source intelligence about cyber threats to day to day activities, CRO and National Military CMO.
- All personnel within the EU who interact with digital data via networks.
- All National personnel in MOD and those working for the Alliance as well as those who are held 'at readiness' for, or are committed to military missions, who interact with networked digital data.
- MS had to indicate how and where coordinated EU involvement could enhance most effectively the CD capability at EU and National level.

d. Section 4 – Preferred Learning Strategies, Training Setting & Learning Media

MS had to indicate the most preferred:

- Learning Strategies: Lectures, Workshops, Discovery learning, On-the-job training, other.
- Training Strategies: International Institution, Individual instruction, Classroom training, Collective operational unit training, On-the-job training, E-learning (at home), E-learning (classroom), National exercises, International exercises, other.
- Learning Media: Virtual Simulators, Reading material, Operationally used equipment, Operationally used software, other.

Annex E - CD E&T Existing Offers Questionnaire

CD E&T Existing Offers Questionnaire

The CD E&T Existing Offers Questionnaire aimed to analyse the existing offer of CD E&T (nationally and internationally) in order to support personnel participating at EU missions and CSDP Operations and at National CD related activities.

This questionnaire had been envisaged as a valuable and structured way to obtain the relevant information related with the existing CD E&T Offer.

In order to gather offers in a format that can be exploited in conformity with the latest outputs from the WS#6, this questionnaire was issued to complement and give more relevance to the Phase 4 gap analysis (described in Main Body, §2.4).

Structure of the CD E&T Existing Offers Questionnaire:

For each Course:

- Individual CD training
  - Section 1 - Course Identification
    - Name of Course
    - Organization that provides the Course
    - Requirement on which was built
    - Periodicity
  - Section 2 - Intended Training Audience
    - TA Category: ICT, ICT + DM, ICT + C4P, ICT + CD, ICT + DM + C4P, ICT + DM + CD, DM, DM + C4P, DM + CD, DM + C4P + CD, C4P, C4P + CD, CD, All
    - TA Segment: ICT1 (NATO), ICT2 (National), DM1 (Strategy & Policy), DM2 (Senior Planners), DM3 (Senior Commanders), DM4 (CIS Governance), C4P1 (Strategy & Policy), C4P2 (OP Planners), C4P3 (Advisors), C4P4 (Legal), C4P5 (CIS Support), C4P6 (E&T), CD1 (Design&Audit), CD2 (Response), CD3 (Forensics & Investigation), CD4 (Advisors), CD5 (E&T), CD6 (CIS OPSEC), CD7 (Intelligence)
    - TA Physical Location / Origins
  - Section 3 - CD E&T Outcomes
    - Performances Objectives
    - Learning Objectives
    - Deep of Knowledge: Basic, Intermediate, Expert, Basic+ Intermediate, Intermediate+Expert, All
  - Section 4 - Course Control
    - Course Control Documents
    - Analysis used to build the course
    - Classification
  - Section 5 – Cooperation Framework
    - Open to EU?
    - Open to NATO?
    - Restrictions to Partner Nations?
  - Section 6 – Estimated Cost
    - Costs
    - Comments

- Collective CD training
    - Section 1 - Exercise Identification
        - Name of Exercise
        - Organization that conducts Exercise
        - Requirement on which was built
        - Periodicity
    - Section 2 - Intended Training Audience
        - TA Category: ICT, ICT + DM, ICT + C4P, ICT + CD, ICT + DM + C4P, ICT + DM + CD, DM, DM + C4P, DM + CD, DM + C4P + CD, C4P, C4P + CD, CD, All
        - TA Segment: ICT1 (NATO), ICT2 (National), DM1 (Strategy & Policy), DM2 (Senior Planners), DM3 (Senior Commanders), DM4 (CIS Governance), C4P1 (Strategy & Policy), C4P2 (OP Planners), C4P3 (Advisors), C4P4 (Legal), C4P5 (CIS Support), C4P6 (E&T), CD1 (Design&Audit), CD2 (Response), CD3 (Forensics & Investigation), CD4 (Advisors), CD5 (E&T), CD6 (CIS OPSEC), CD7 (Intelligence)
    - Section 3 - Exercise Specifications
        - Exercise Specifications
        - Exercise Objectives
        - Performance Objectives
        - Classification
    - Section 4 – Cooperation Framework
        - Open to EU?
        - Open to NATO?
        - Restrictions to Partner Nations?
    - Section 5 – Estimated Cost
        - Organisation
        - Participation Fee: 0-500, 500-1000, 1000-5000, 5000-10000, Above 10000
        - Comments

Available Offer Questionnaire (example)

Name of the Course: Information Systems Security

Target Audience: Cyber Security and CD International Law Master Students / C4P4

University/School: UCP - Faculdade de Filosofia e Ciências Sociais

1 Week ☐
2 Weeks ☒
1 Month ☐
1 Semester ☐
Other ☐
____

Learning Objectives / Outcomes: This curricular unit aims to raise the awareness to the risks associated with the benefits created by the Information and Communication Technologies (ICT) and to allow students to meet the resources available for ICT protection. In the end, students will be able to: •Explain the concepts defined by the International Standards of Security Management •Apply, in a real or in a simulated environment, the processes defined by the International Standards of Security Management •Describe the resources available for increasing the security of information systems •Describe the way that adopting ICT based processes represents, along with all the benefits, a risk for States and organizations. •Identify the authentication and/or identification processes that best suit one determined scenario. •Use tools aiming to insure confidentiality, integrity and authenticity of the information.

Syllabus Topics:

- Introduction to Information and Communication Security
- Information Warfare and Competitive Intelligence
- Malicious Software
- Authentication and Identification
- Protection of electronic communications
- Secure data storage
- Information Security Policy and Contingency Plan
- Social networks, privacy and security.

E-learning platform ☒
Cyber Lab ☐
Cyber Range ☐
Scenario Tool ☒
Other ☐ ____________

Teaching and learning methodologies: This unit will have, as main methodology, expositive classes, followed by debate. Some issues will use a case study approach.

Assessment: The assessment will be made through a small original essay, between 3000 and 4000 words, that the student will write on a subject to his choice, related to the ICT security issues (75% - 65% to the written work and 10% to a short presentation) and through the evaluation of the attitudes in the classroom, particularly during the debates.

Main Bibliography: Tenreiro de Magalhães, et al. 2008. Using technology to overcome the password’s contradiction. In Handbook of Research on Social and Organizational Liabilities in Information Security, 398 - 414. . USA: IGI Global .
Tenreiro de Magalhães, S; Rios, M. J; Santos, L.; Jahankhani, H.. 2009. "The People’s Republic of China – the emerging cyberpower", In Proc. of the 5th Int. Conf. on Global Security, Safety & Sustainability, London UK.

Annex F - Cyber Competencies Career Path Matrix

Cyber Competencies Career Path Matrix

The theoretical common curriculum is useful to transmit an idea of the various courses throughout all the TA, organized following a strategic / operational / tactical approach and 4 different DOK.

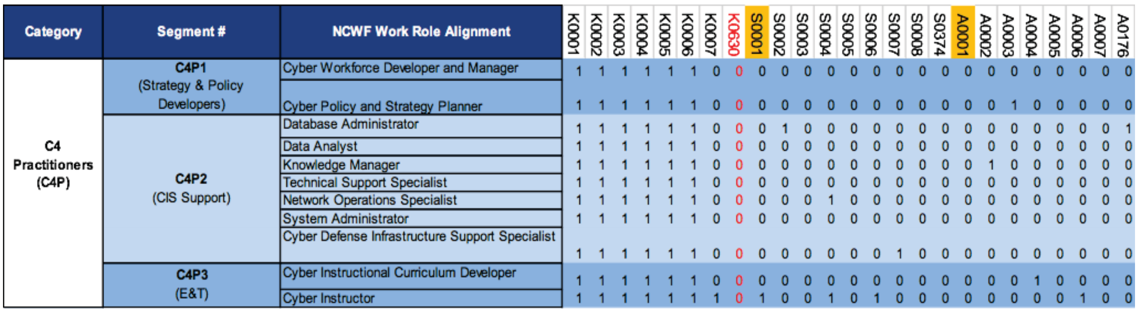
Using the same logic, and all the information delivered so far, an updated Common Curriculum will be presented, as a "*Cyber Competencies Career Path Matrix*".

1. COMPILING DATA

Firstly, we compile all the information from the UCCF so far in the same matrix.

Horizontally, we list the four TA, divided by their subsets and subdivided by their several work roles (a total of 52). Vertically, we list all the Knowledge, Skills and Abilities (KSA). We have a total of 1180 KSA: Knowledge (630), Skills (374) and Abilities (176).

Each KSA has a number which corresponds to a definition that can be found under the NICE Framework. Let us give an example to illustrate.



Category	Segment #	NCWF Work Role Alignment	K0001	K0002	K0003	K0004	K0005	K0006	K0007	K0630	S0001	S0002	S0003	S0004	S0005	S0006	S0007	S0008	S0374	A0001	A0002	A0003	A0004	A0005	A0006	A0007	A0176
C4 Practitioners (C4P)	C4P1 (Strategy & Policy Developers)	Cyber Workforce Developer and Manager	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		Cyber Policy and Strategy Planner	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
	C4P2 (CIS Support)	Database Administrator	1	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
		Data Analyst	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		Knowledge Manager	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
		Technical Support Specialist	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		Network Operations Specialist	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0
		System Administrator	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
		Cyber Defense Infrastructure Support Specialist	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0
	C4P3 (E&T)	Cyber Instructional Curriculum Developer	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
		Cyber Instructor	1	1	1	1	1	1	1	0	1	0	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0

Table 1 - TA vs all KSA extract

In the table above, an extract of the matrix is represented for the C4 Practitioners' TA, with its 3 different segments (subsets) and Work Roles, throughout the 1180 KSA.

For each work role, each time we have a match of a KSA, a "1" is introduced. Otherwise, when a specific competency is not found for that work role, a "0" is introduced in the matrix.

That kind of approach permits data analysis.

2. DATA ANALYSIS

For an easier comprehension and, later on, to relate with the Theoretical Common Curriculum, we will abbreviate the TA using the following notation:

TARGET AUDIENCE GROUP	ABBREVIATED DESIGNATION
ALL ICT USERS (ICT)	A
Legal & Governance (L&G)	B
C4 Practitioners (C4P)	C
Securely Provision (SP)	D
CD Specialist (CDS)	E

Table 2 - Target Audience abbreviated notation

Thus, when we refer TA B, we actually mean Target Audience "Legal & Governance".

The TA A has no KSA listed. It was already assumed by NLD, and identified under their WP. A solution will be proposed later on, in this document. Meanwhile TA A is discarded from the data analysis phase.

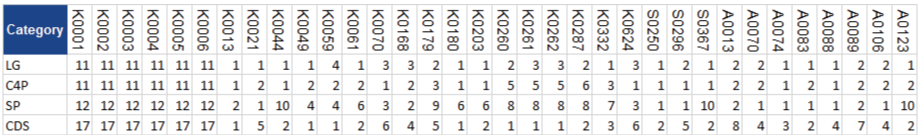
We can observe that:

- 34 KSA are matching all TA. That means, all TA need that 34 competencies;
- 69 KSA are matching at least 3 different TA.
- More than 1100 KSA and 52 work roles are still big numbers.
  Therefore, we need to find a method to group the KSA in such a way that the competencies are more easily handled. As for now, we propose to study and compare two different Courses of Action (COA).

a) COA 1

We will consider that the 34 KSA matching all TA are core KSA, thus can be applied as prerequisite to everybody, so shall be inserted to TA A (ICT).

The summary of the table is presented below:



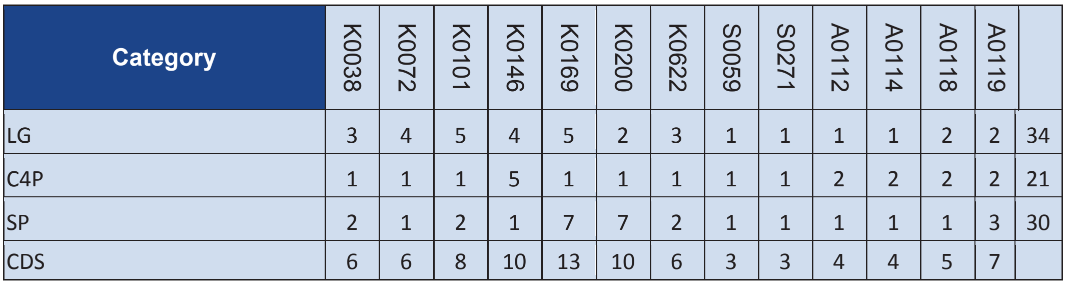
Category	K0001	K0002	K0003	K0004	K0005	K0006	K0013	K0021	K0044	K0049	K0059	K0061	K0070	K0168	K0179	K0180	K0203	K0260	K0261	K0262	K0287	K0332	K0624	S0250	S0296	S0367	A0013	A0070	A0074	A0083	A0088	A0089	A0106	A0123
LG	11	11	11	11	11	11	1	1	1	1	4	1	3	3	2	1	1	2	3	3	2	1	3	1	2	1	2	2	1	1	1	2	2	1
C4P	11	11	11	11	11	11	1	2	1	2	2	2	1	2	3	1	1	5	5	5	6	3	1	1	1	1	2	2	1	2	1	2	2	2
SP	12	12	12	12	12	12	2	1	10	4	4	6	3	2	9	6	6	8	8	8	8	7	3	1	1	10	2	1	1	1	1	2	1	10
CDS	17	17	17	17	17	17	1	5	2	1	1	2	6	4	5	1	2	1	1	1	2	3	6	2	5	2	8	4	3	2	4	7	4	2

Table 3 - 34 common KSA

The numbers depicted are the frequency of each KSA for each TA.

Moreover, when we try to check which KSA have 3 TA matches out of 4, we find 4 different possibilities:

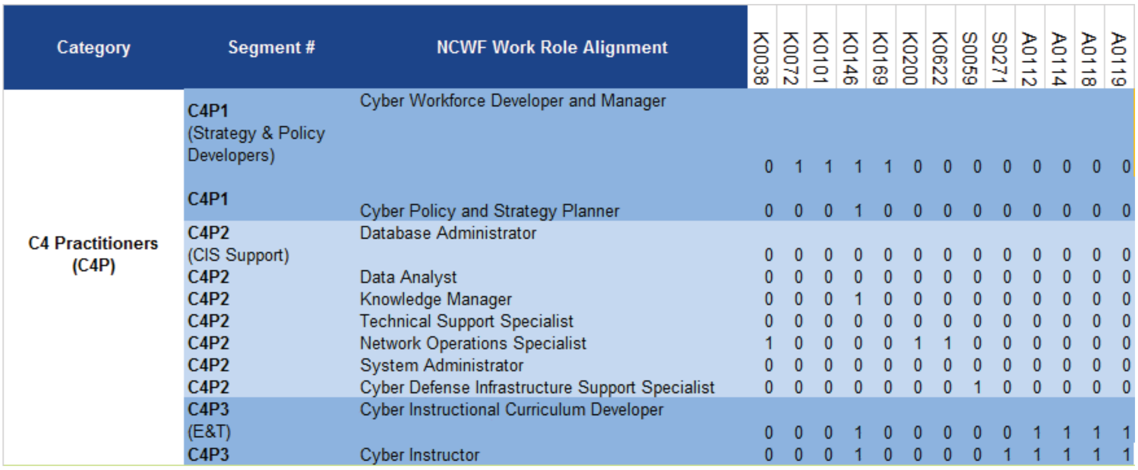
- BCD: KSA which are common to TA B and C and D.
- BDE: KSA which are common to TA B and D and E.
- BCE: KSA which are common to TA B and C and E.
- CDE: KSA which are common to TA C and D and E.
  As an example, we present a summary of the common KSA found for TA B, C and D, called BCD:



Category	K0038	K0072	K0101	K0146	K0169	K0200	K0622	S0059	S0271	A0112	A0114	A0118	A0119	
LG	3	4	5	4	5	2	3	1	1	1	1	2	2	34
C4P	1	1	1	5	1	1	1	1	1	2	2	2	2	21
SP	2	1	2	1	7	7	2	1	1	1	1	1	3	30
CDS	6	6	8	10	13	10	6	3	3	4	4	5	7	

Table 4 - BCD summary KSA table

Let us have a more detailed view of TA C (C4 Practitioners), from the example above, to illustrate further our data analysis:

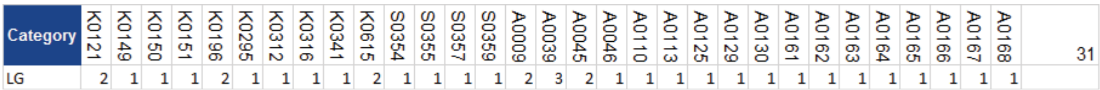


Category	Segment #	NCWF Work Role Alignment	K0038	K0072	K0101	K0146	K0169	K0200	K0622	S0059	S0271	A0112	A0114	A0118	A0119
C4 Practitioners (C4P)	C4P1 (Strategy & Policy Developers)	Cyber Workforce Developer and Manager	0	1	1	1	1	0	0	0	0	0	0	0	0
	C4P1	Cyber Policy and Strategy Planner	0	0	0	1	0	0	0	0	0	0	0	0	0
	C4P2 (CIS Support)	Database Administrator	0	0	0	0	0	0	0	0	0	0	0	0	0
	C4P2	Data Analyst	0	0	0	0	0	0	0	0	0	0	0	0	0
	C4P2	Knowledge Manager	0	0	0	1	0	0	0	0	0	0	0	0	0
	C4P2	Technical Support Specialist	0	0	0	0	0	0	0	0	0	0	0	0	0
	C4P2	Network Operations Specialist	1	0	0	0	0	1	1	0	0	0	0	0	0
	C4P2	System Administrator	0	0	0	0	0	0	0	0	0	0	0	0	0
	C4P2	Cyber Defense Infrastructure Support Specialist	0	0	0	0	0	0	0	1	0	0	0	0	0
	C4P3 (E&T)	Cyber Instructional Curriculum Developer	0	0	0	1	0	0	0	0	0	1	1	1	1
	C4P3	Cyber Instructor	0	0	0	1	0	0	0	0	1	1	1	1	1

Table 5 - BCD KSA table for TA C

Finally, a set of KSA are not common to all TA, nor to 3 out of 4 TA. Those specific only KSA subsets are designated B, C, D and E, as they remain only for those TA.

To illustrate, please look at the table below, for TA B:



Category	K0121	K0149	K0150	K0151	K0196	K0295	K0312	K0316	K0341	K0615	S0354	S0355	S0357	S0359	A0009	A0039	A0045	A0046	A0110	A0113	A0125	A0129	A0130	A0161	A0162	A0163	A0164	A0165	A0166	A0167	A0168	31
LG	2	1	1	1	2	1	1	1	1	2	1	1	1	1	2	3	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	

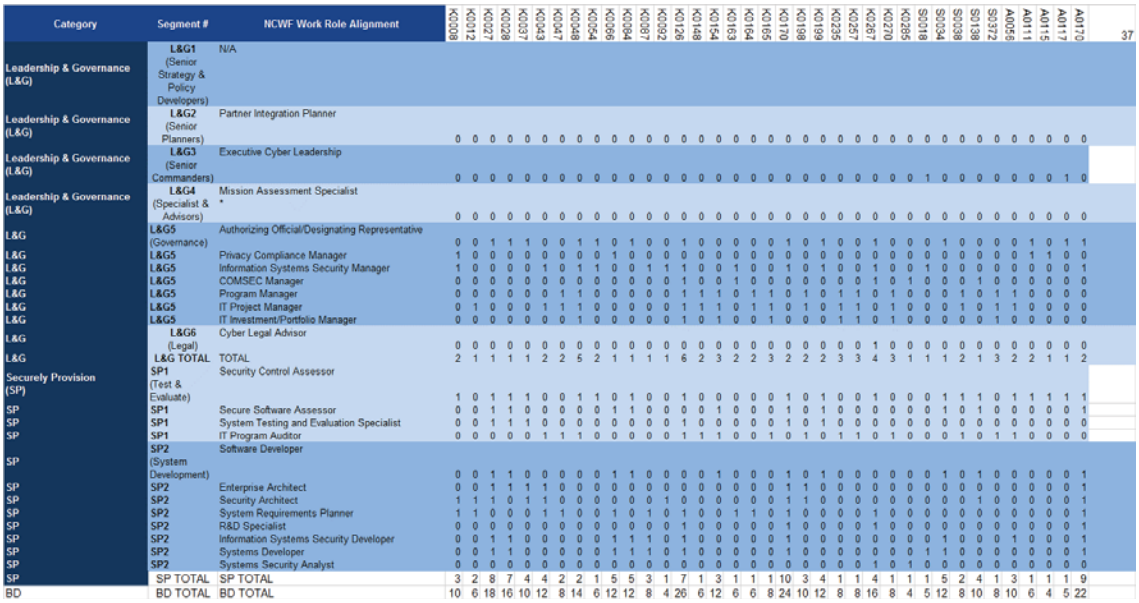
Table 6 - B summary KSA table

b) COA 2

For this COA, we decide to analyse one step lower, that is, group 3 or more similar KSA for TA A, group the KSA matching two different TA and, finally, the remaining specific KSA for each TA.

In that case, we find 103 KSA which have a match to at least 3 TA.

Grouping KSA similar to 2 TA, gives us 6 different possibilities: BC, BD, BE, CD, CE and DE.



Category	Segment #	NCWF Work Role Alignment	K0008	K0012	K0027	K0028	K0037	K0043	K0047	K0048	K0054	K0066	K0084	K0087	K0092	K0126	K0148	K0154	K0163	K0164	K0165	K0170	K0198	K0199	K0235	K0257	K0267	K0270	K0285	S0018	S0034	S0038	S0138	S0372	A0056	A0111	A0115	A0117	A0170	37
Leadership & Governance (L&G)	L&G1 (Senior Strategy & Policy Developers)	N/A																																						
Leadership & Governance (L&G)	L&G2 (Senior Planners)	Partner Integration Planner	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
Leadership & Governance (L&G)	L&G3 (Senior Commanders)	Executive Cyber Leadership	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	
Leadership & Governance (L&G)	L&G4 (Specialist & Advisors)	Mission Assessment Specialist *	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
L&G	L&G5 (Governance)	Authorizing Official/Designating Representative	0	0	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	0	0	0	0	1	0	1	1	
L&G	L&G5	Privacy Compliance Manager	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	
L&G	L&G5	Information Systems Security Manager	1	0	0	0	0	1	0	1	1	0	0	1	1	1	0	0	1	0	0	1	0	1	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	
L&G	L&G5	COMSEC Manager	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	0	0	
L&G	L&G5	Program Manager	0	0	0	0	0	0	1	1	0	0	0	0	0	1	1	1	0	1	1	0	1	0	1	1	0	1	0	0	0	1	0	1	1	0	0	0	0	
L&G	L&G5	IT Project Manager	0	1	0	0	0	1	1	1	0	0	0	0	0	1	1	1	0	1	1	0	1	0	1	1	0	1	0	0	0	1	0	1	1	0	0	0	0	
L&G	L&G5	IT Investment/Portfolio Manager	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	
L&G	L&G6 (Legal)	Cyber Legal Advisor	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	
L&G	L&G TOTAL	TOTAL	2	1	1	1	1	2	2	5	2	1	1	1	1	6	2	3	2	2	3	2	2	2	3	3	4	3	1	1	1	2	1	3	2	2	1	1	2	
Securely Provision (SP)	SP1 (Test & Evaluate)	Security Control Assessor	1	0	1	1	1	0	0	1	1	0	1	0	0	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	1	1	1	0	1	1	1	1	1	
SP	SP1	Secure Software Assessor	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	
SP	SP1	System Testing and Evaluation Specialist	0	0	1	1	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
SP	SP1	IT Program Auditor	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	1	0	0	1	0	1	0	1	1	0	1	0	0	0	1	0	1	1	0	0	0	0	
SP	SP2 (System Development)	Software Developer	0	0	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	0	0	0	1	
SP	SP2	Enterprise Architect	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	
SP	SP2	Security Architect	1	1	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	
SP	SP2	System Requirements Planner	1	1	0	0	0	1	1	0	0	1	0	1	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	
SP	SP2	R&D Specialist	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	
SP	SP2	Information Systems Security Developer	0	0	1	1	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	
SP	SP2	Systems Developer	0	0	1	1	0	0	0	0	0	1	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	1	
SP	SP2	Systems Security Analyst	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	
SP	SP TOTAL	SP TOTAL	3	2	8	7	4	4	2	2	1	5	5	3	1	7	1	3	1	1	1	10	3	4	1	1	4	1	1	1	5	2	4	1	3	1	1	1	9	
BD	BD TOTAL	BD TOTAL	10	6	18	16	10	12	8	14	6	12	12	8	4	26	6	12	6	6	8	24	10	12	8	8	16	8	4	5	12	8	10	8	10	6	4	5	22	

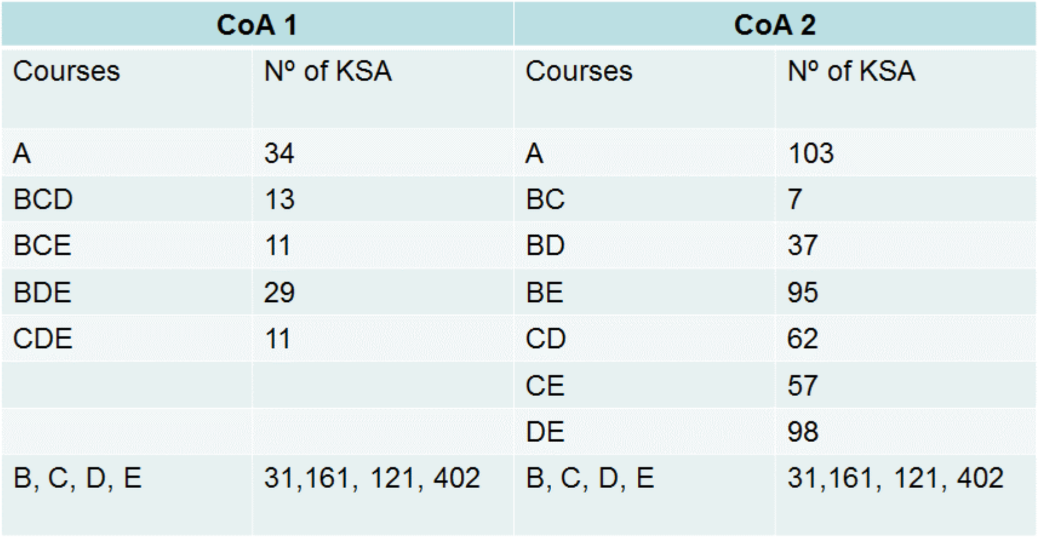
Table 8 - BD KSA table for TA B and D

On the table above, it is possible to identify which KSA are common to TA B and TA D, and the frequency of occurrence.

Finally, the remaining group of specific TA KSA, just as it has been presented on COA1.

c) COA comparison

In order to compare the two COA, we are using the following table:



CoA 1		CoA 2	
Courses	Nº of KSA	Courses	Nº of KSA
A	34	A	103
BCD	13	BC	7
BCE	11	BD	37
BDE	29	BE	95
CDE	11	CD	62
		CE	57
		DE	98
B, C, D, E	31,161, 121, 402	B, C, D, E	31,161, 121, 402

Table 9 - COA comparison matrix

As we can see, there is no real benefit to follow COA 2, because we can achieve a lower number of curriculum in COA 1, and the number of KSA is not much different from the COA2 approach.

Therefore, COA1 is chosen.

3. CYBER COMPETENCIES CAREER PATH MATRIX

As we have seen, more than 1100 KSA are defined for CS and CD. Using COA1, we are able to join them under 9 different subsets, whereas the KSA are common to all TA, common to at least 3 different TA or, are uniquely found in a particular TA.

A major point to clarify is that the same competency can be taught at 4 different DOK. Let us give a simple example, using KSA, "*K0138 - Knowledge of Wi-Fi*". A basic "Knowledge of Wi-Fi" can be a broad explanation of that technology, used by wireless equipment. On the other hand, an advanced "Knowledge of Wi-Fi" can address deeper understanding of the Wi-Fi radio spectrum or the security protocols used.

So, in order to cover all the CS and CD education, we will ideally need a total of 36 different subsets.

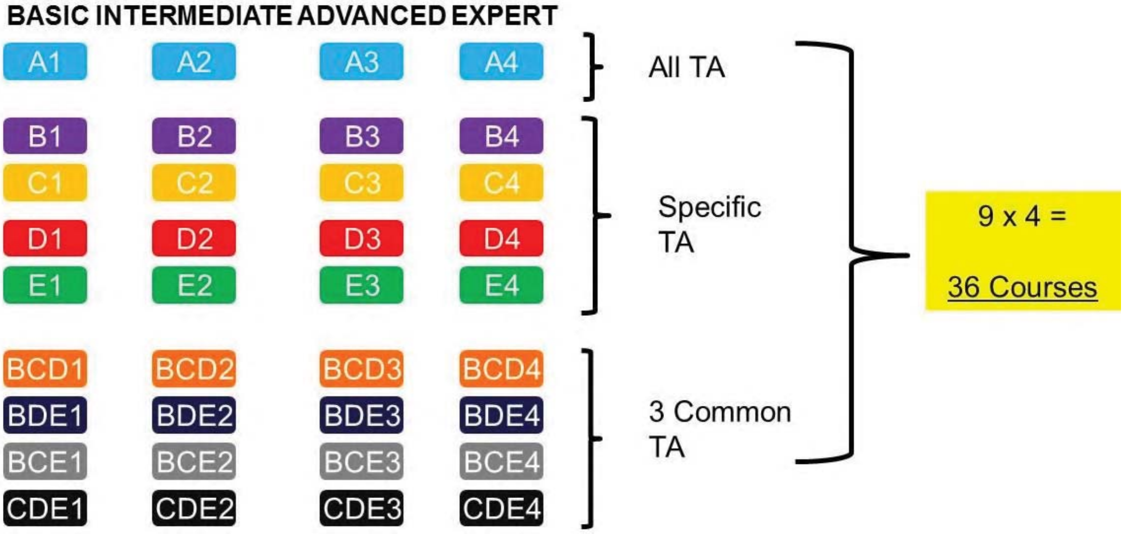


Figure 10 - All courses throughout 4 DOK

On the Figure above, each box is related to a subset of KSA. The number added refers to the subset's DOK. The various boxes are simply called "courses", independently of the number of KSA and the time needed to teach all the KSA inside the box. Instead of "courses", we should use the term "module".

As we can see, 36 "modules" are still a lot of possibilities. We need to find a way to reduce that number, and still, be able to cover as close as possible all E&T for CS and CD.

On a first "safe" reduction, we have not considered the KSA that are specific only to a TA, at the Basic levels, because those competencies will be obtained at other more levels. Following a similar logic with an opposite view of the DOK's spectrum, we have not considered the KSA common to more than 3 TA, at the Expert levels, because TA specificities shall be privileged.

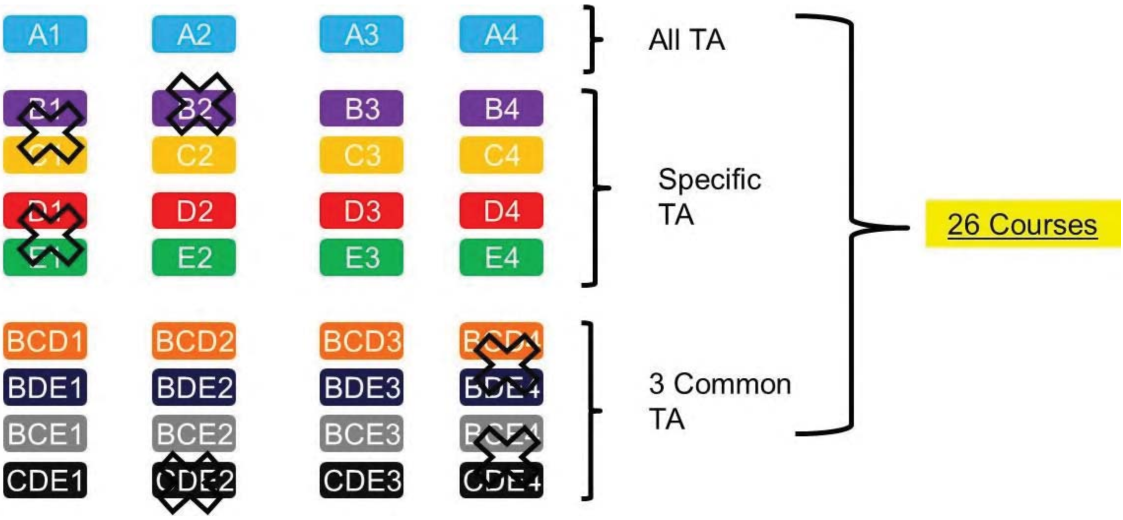


Figure 11 - Safe reduction of courses throughout 4 DOK

For experiment purposes, we also conducted a drastic reduction, with the same logic but pushing even further until level intermediate and advanced. In that case, the result was a total of 20 modules, not substantially different from the "safe" reduction. Considering the cost of reduction vs the benefit on the total output of modules, we recommend the "safe" reduction.

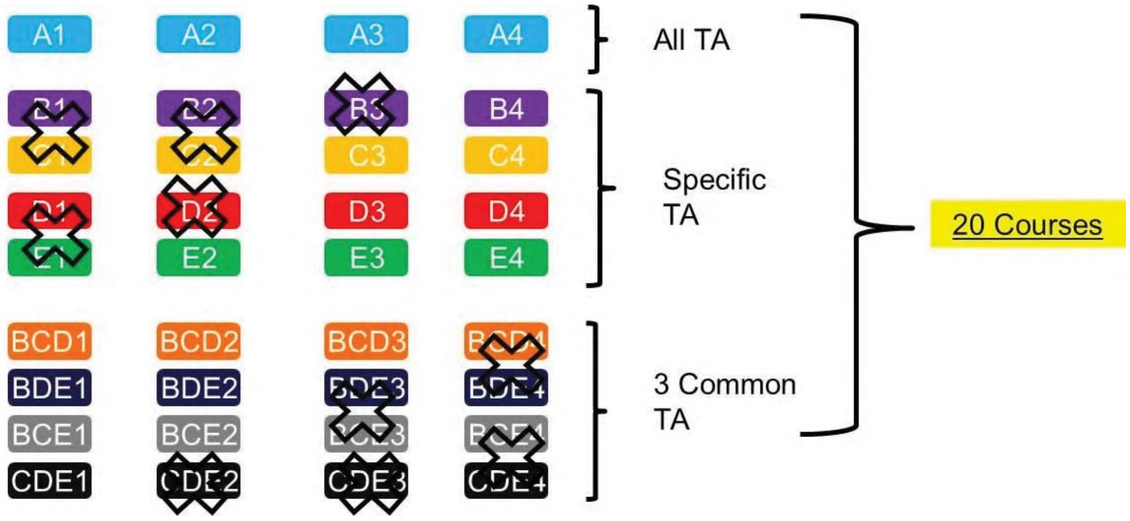
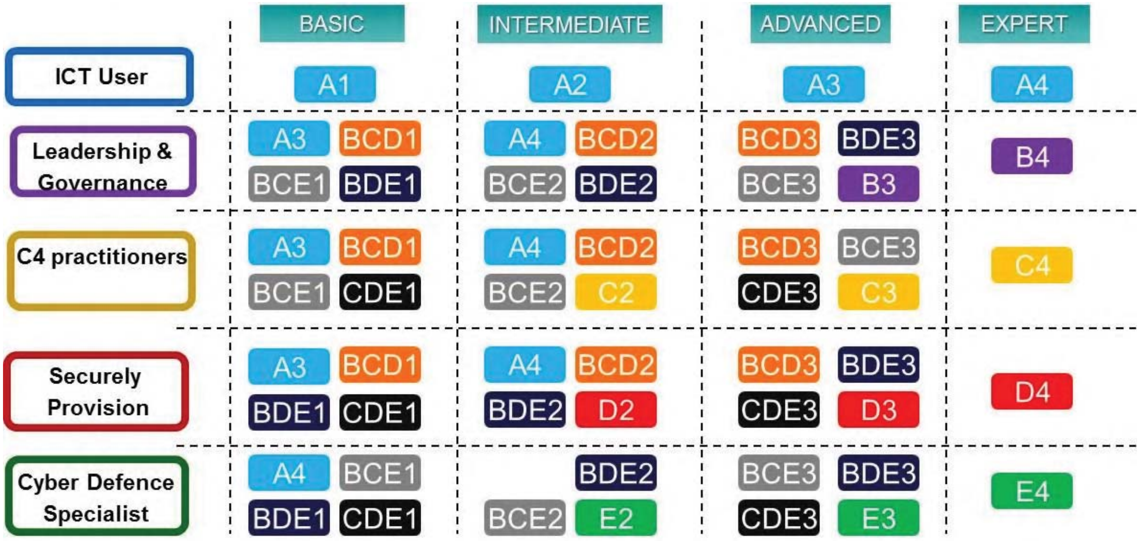


Figure 12 - Drastic reduction of courses throughout 4 DOK

Our last step consists on applying the 26 modules inside a Common Curriculum framework, based on the Theoretical model explained earlier. Our proposal follows:



	BASIC	INTERMEDIATE	ADVANCED	EXPERT
ICT User	A1	A2	A3	A4
Leadership & Governance	A3 BCD1 BCE1 BDE1	A4 BCD2 BCE2 BDE2	BCD3 BDE3 BCE3 B3	B4
C4 practitioners	A3 BCD1 BCE1 CDE1	A4 BCD2 BCE2 C2	BCD3 BCE3 CDE3 C3	C4
Securely Provision	A3 BCD1 BDE1 CDE1	A4 BCD2 BDE2 D2	BCD3 BDE3 CDE3 D3	D4
Cyber Defence Specialist	A4 BCE1 BDE1 CDE1	BDE2 BCE2 E2	BCE3 BDE3 CDE3 E3	E4

Figure 13 - Cyber Competencies Career Path Matrix

We are going to illustrate how this curriculum can be used, through some examples.

- ICT Users (TA A), four different initiatives shall be developed: A1 to A4.
- Basic Level of Leadership and Governance TA. It consists of of 4 initiatives: A3, BCD1, BCE1 and BDE1. Beginning at A3 means that A1 and A2 are not in depth enough for the Basic level needed by L&G, but are still pré-requisites. A student shall be tested before entering a program, in order to verify if he possesses the competencies up to the new course.
- Advanced level of Securely Provision, consists of initiatives: BCD3, BDE3, CDE3 and D3. Please notice that, for instance BCD3, is an initiative used by other TA. The Curriculum follows a modular approach that have a double

benefit: initiatives deserving multiple TA can lower the cost of courses, serve larger groups of students and facilitate the migration of students between TA.

- Expert level of CD Specialist TA, consists of only one initiative, E4, specific to that TA. At the expert level, it is fair to assume that the competencies are tailored to the TA. Nevertheless, an E4 initiative can be lengthy, expensive and difficult.

Annex G - Example of a Gap Analysis (Module B3)

Example of a Gap Analysis (Module B3)

MODULE B3: CYBER LEADERSHIP AND GOVERNANCE COURSE (ADVANCED)

1. Course Title: Cyber Leadership and Governance Course (advanced)

2. Identification Number: CYB B3

3. Purpose of the course
   "Leadership and Governance" is one of the Training Audiences identified.
   This course will give the cyber competencies that are specific to that TA, at an advanced level.
   This course is designed for Senior Strategy and Policy Developers, Senior Planners, Senior Commanders, Specialists and advisers, Governance and Legal professionals who seek to develop their career with cyber knowledge at and advanced level.

4. Learning objectives
   This course consists of four main Learning Objectives:
   a. Project management for Advanced Legal and Governance users in Cyber security;
   b. Cyber security Operations for Advanced Legal and Governance users;
   c. Laws, regulations and policies in cyberspace for Advanced Legal and Governance users;
   d. Communications Security for Advanced Legal and Governance users.

5. Qualification obtained
   "EU Advanced Cyber Leadership and Governance Course"

6. Student criteria
   The candidate must be:
   a. Selected for an assignment to …..
   b. Has met the background knowledge prerequisites for this course
   c. Has at least one year…

7. Rank
   a. OR 4 to …
   b. OF 1 to …
   c. Civilian equivalent

8. Language proficiency:
   English Level …..

9. Security clearance
   EU CONFIDENTIAL

10. Course length
    2 working days

11. Special instruction

12. Class size (max/ recommended/ minimum)
    30 / 20 / 12

13. Nomination procedure

14. Pre-course study material

15. Location

16. Prerequisites

17. TA: B – Leadership and Governance

18. Competencies

	DEFINITION	UNIT / LEARNING OBJECTIVE	TIME
K0121	Knowledge of information security program management and project management principles and techniques.	Project management for Advanced Legal and Governance users in Cyber security	0.6
S0355	Skill in negotiating vendor agreements and evaluating vendor privacy practices.		0.6
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.		0.6
A0039	Ability to oversee the development and update of the life cycle cost estimate.		0.6
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.		0.3
A0129	Ability to ensure information security management processes are integrated with strategic and operational planning processes.		0.6
A0161	Ability to integrate information security requirements into the acquisition process; using applicable baseline security controls as one of the sources for security requirements; ensuring a robust software quality control process; and establishing multiple sources (e.g., delivery routes, for critical system elements).		1
A0162	Ability to ensure information system security, acquisition personnel, legal counsel, and other appropriate advisors and stakeholders are participating in decision making from system concept definition/review and are involved in, or approve of, each milestone decision through the entire system life cycle for systems.		1
K0149	Knowledge of organization's risk tolerance and/or risk management approach.		0.3
A0009	Ability to apply supply chain risk management standards.		0.6
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	Cyber security Operations for Advanced Legal and Governance users	0.3
K0151	Knowledge of current and emerging threats/threat vectors.		0.3
K0295	Knowledge of confidentiality, integrity, and availability principles.		0.3
K0312	Knowledge of intelligence gathering principles, policies, and procedures including legal authorities and restrictions.		0.3
K0316	Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.		0.3
S0357	Skill to anticipate new security threats.		0.6
A0130	Ability to ensure that senior officials within the organization provide information security for the information and systems that support the operations and assets under their control.		0.3

K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	Laws, regulations and policies in cyberspace for Advanced Legal and Governance users	0.3
K0341	Knowledge of foreign disclosure policies and import/export control regulations as related to cyber security.		0.3
K0615	Knowledge of privacy disclosure statements based on current laws.		0.3
S0354	Skill in creating policies that reflect the business's core privacy objectives.		1
A0046	Ability to monitor and assess the potential impact of emerging technologies on laws, regulations, and/or policies.		0.6
A0110	Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.		0.6
A0113	Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.		0.6
A0125	Ability to author a privacy disclosure statement based on current laws.		0.3
A0162A	Ability to recognize the unique aspects of the Communications Security (COMSEC) environment and hierarchy.	Communications Security for Advanced Legal and Governance users	0.3
A0163	Ability to interpret Communications Security (COMSEC) terminology, guidelines and procedures.		0.3
A0164	Ability to identify the roles and responsibilities for appointed Communications Security (COMSEC) personnel		0.3
A0165	Ability to manage Communications Security (COMSEC) material accounting, control and use procedure.		0.3
A0166	Ability to identify types of Communications Security (COMSEC) Incidents and how they're reported.		0.3
A0167	Ability to recognize the importance of auditing Communications Security (COMSEC) material and accounts.		0.3
A0168	Ability to Identify the requirements of In-Process accounting for Communications Security (COMSEC).		0.3
🟩			16 timeslots

Annex H - Example of a proposed solution for a Cyber Intel Course

Example of a proposed solution for a Cyber Intel Course

CD CYBER INTELIGENCE COURSE

Version: 2.00

03NOV2017

References

A. AC/322-N(2014)0072 NATO CD Taxonomy and Definitions

B. NATO CD (CD) Education and Training Plan.

C. Bi-SC Education and Individual Training Directive (E&ITD) 075-007

D. Cyber Intelligence Tradecraft Project (http://www.sei.cmu.edu/about/ organization/etc/citp-summary.cfm)

E. SANS-FOR578: Cyber Threat Intelligence (https://www.sans.org/course/cyber-threat-intelligence)

F. NIST Special Publication 800-181, NICE Cybersecurity Workforce Framework (NCWF).

Aim

This initiative should take into account the training requirements of different Intelligence Analysts (Cyber and others), located at different planning levels (Strategic, Operational and Tactical).

Key notes

According to the Project's Taxonomy (draft), the Intelligence Workforce is the personnel who collect, process, analyse, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

The Intelligence Workforce include mainly the Work Roles described into the Categories Analyse (AN) and Collect and Operate (CO) at Reference F. To be more precise work roles related with cyber intelligence are: Warning Analyst, Cyber Operator, Exploitation Analyst, All-Source Analyst, All-Source Collector, All-Source requirements, Target Developer, Target Network Analyst, Multi-Disciplined Language, Cyber

Intel Planner and Cyber Ops Planner. These roles fit into the category CD Specialists (subcategories Response (CDS1), Intelligence (CDS3) and Planners (CDS4)).

Category	Segment #	NCWF Work Role Alignment
CD Specialists (CDS)	**CDS1** (Response)	Warning Analyst Cyber Operator
	CDS3 (Intelligence)	Exploitation Analyst All-Source Analyst All-Source Collection Manager All-Source Requirements Manager Target Developer Target Network Analyst Multi-Disciplined Language Analyst
	CDS4 (OP/TAC Planners)	Cyber Intel Planner Cyber Ops Planner

Figure 3: CD Specialists

It is difficult to plan and program different courses for every work role above mentioned. In the other hand some tasks are common for them. For these reasons we have included a single list of Knowledge, Skills and Abilities (KSA) to achieve in a single course: the CIC..

In order to avoid a very long course, some of the knowledge could be defined as pre-requisite, since it is generally demonstrated through previous relevant experience or performance-based education and training. Annex 2 contains those prerequisites. This knowledge could be demonstrated with a previous exam.

A syllabus has been derived from the tasks proposed in the Combined Task List (CTL). In this way we may find an alignment between the modules and the CTL. This proposed syllabus has considered inputs and the syllabus is included containing the KSA to be achieved in every subject and other content to be provided to the students during the CIC.

MODULES	TASKS/ SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
Cyber Intelligence Fundamentals	5.1.1, 4.2.1, 5.4.2	Introduction to Cyber Threat Intelligence for Intrusions	K0005, K0352,K0435,K0436 S0244	Why CTI? Collection Requirements/Motivations
				Traditional Intelligence Cycle
				Sources of intelligence
				Lexicon and Definitions
				Roles of CTI Analysts
				Risk
		Current Threat Landscape	K0474,K0612, S0229	Defining Threats and Abstractions
				What IS NOT a Threat?
				How Does CTI Work?
		Intelligence in Computer Network Defense	K0006, K0009, K0347, K0350, K0361, K0453, K0469, K0475, K0523, K0572, K0574, K0576, K0579, K0599, K0600, K0613, K0614, S0025, S0027, S0036, S0054, S0057, S0066, S0078, S0096,S0178, S0184, S0199, S0207, S0208, S0215, S0236, S0239, S0240, S0241, S0242, S0258, S0260,	Detection of unusual behaviors on networks
				Indicators of compromise (IOC)
				Examples of Indicators
				Setting up IOC
				Understanding Signatures as Expressive CTI
				Indicator Sources
				Vulnerability management

			S0263,S0269,	
		Threats at Organizational and National Levels	S0330 ?	State-sponsored cyber threats attribution APT Campaigns
				Understanding threats and their actions at the strategic and operational level
				Abridged history of threats in cyberspace influencing the CTI domain

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
Data Collection and examination	5.1.3, 1.2.4, 1.4.2, 3.3.2	OSINT	K0447, K0558 S0194, S0195, S0196, S0197, S0198, S0235, S0289, S0295	OSINT tools
				Social Media
				Tools to anonymize
				Legal considerations
		All sources	K0380, K0364, K0120, K0368, K0386, K0577, K0602, K0449 S0063, S0181, S0183, S0200, S0202, S0352, S0353, S0217, S0218, S0219, S0220, S0268,	Threat Intel Collaborations
				Sharing Platforms
				CTI Feeds
				Information Sharing and Analysis Centres (ISACs) and Fusion Centres

CD Military Training Discipline

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
			S0272, S0277, S0297, S0393, S0304, S0310, S0313, S0325, S0322, S0342, S0346, S0347, A0066,A0079, A0099, A0100, A0109	
Processing and analysis	5.1.2, 3.1.2, 3.2.1	Intelligence analysis	K0357,K0358, K0371, K0388, K0401, K0404, K0476, K0517, K0571, K0605 S0187, S0191, S0227, S0232, S0233, S0245, S0247,S0254, S0261, S0278, A0080, A0083, A0084, A0085, A0087, A0091, A0101, A0106, A0107, A0107,	Analytical Process and Scientific Methods
				Analysis of Competing Hypotheses
				Biases in Intel Analysis
				Counterintelligence
		Diamond Model		Intrusion analysis (adversary, infrastructure, capability, victim)

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
		Kill Chain	K0131, K0142, K0143, K0177, K0356, K0362, K0389, K0390, K0391, K0405, K0408, K0418, K0424, K0440, K0536, K0562 S0187, S0250 to S0299 A0093	Analytical Aspects of the Kill Chain
				Scenarios-based Kill Chain Analysis
				Multi-Stage Intrusions and Kill Chain Sequencing
				Intel Gain/Loss Considerations
				Prioritization of Detections and Response
				The Kill Chain and Intelligence in Conventional Incident Response
				Analytical Completeness Guided by Kill Chain Analysis
		Courses of Action Matrix	S0185, S0186, S033, A0097	
		Additional, Alternate, and Emergent Models for analysis purposes	S0337	Model Definition
				Application to Indicators and Signatures
				Maturity models
				CBEST model
		Historical Unsuccessf	S0025, S0120	Relationship to Present Incident
				When to Analyse Unsuccessful Attempts

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
		ul Intrusion Attempt: Phishing Attempt		Analytical Completeness in Unsuccessful Intrusions
		Campaign Definitions	K0448, K0460, K0481, K0492, K0526, K0567, K0606 S0317, S0360	Key Indicators
				Exploratory Techniques for Campaign Analysis, graph-based Tools
				Tactics, Techniques, and Procedures in Detail
		Correlation	K0607, K0483 S0211, S035, S0336, S0222, S0321, S0287, S0288 A102	Distinguishing Correlative and Actionable Intelligence
				Completing the Picture with Available Intelligence
				Interpreting Campaign Intersections
				CTI Analysis with Excel
				Cross-Incident Correlation
				Pitfalls in Correlating Intrusions
		Pivoting, Hunting, and External Intelligence Exploitation	K0430, K0433, K0493 S0294	Passive Network Activity
				Malware Repositories
				Domain and Organizational Data
				Configuration Block Data

CD Military Training Discipline

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
Communication and Collaboration		Technical Writing and Writing for Leadership	S0271, S0300, S0301, S0302, S0210, S0213, S0250 A0070, A0071, A0072, A0105	
		Public Speaking and defending Assessments	S0331, S0344, S0249, A0069, A0013	
		Intelligence Sharing Purposes and Considerations	S0212, S0214	
		Extracting Tactical Threat Intelligence	K0578, K0596	Indicators of Compromise (IOC) Formats
		Intelligence Knowledge Managemen	K0376,K0377,K0379, K0409, K465, K0466, K0467,	Strategic, Operational, and Tactical Threat Intelligence
				Non-disclosure Agreements (NDAs), Classifications, and Other Restrictions

MODULES	TASKS SUBTASKS (CTL)	SUBJECT	KSA (NCWF)	ADDITIONAL CONTENTS
		t	K0477, K0500, K0501, K0507, K0509, K0510, K0514, K0587, K0588, K0594, K0595 S0179, S0243,S0305	Technologies
				Standards
		Threat Intel Sharing and Peer Collaboration	K0457, K0354, K0355, K0359, K0394, K0407, K0421, K0422, K0423, K0451, K468, K0508, K0521, K0522, K0575, K0601 A0073,A0074,A0076,A0078,A0082, A0088, A0089, A0090, A0096	Threat Intelligence for Network Security Monitoring
				Threat Intelligence for Incident Response
				Threat Intelligence for Threat and Environment Manipulation
				Approaches for peer collaboration
				Risks of peer collaboration
				Benefits of peer collaboration
				Selecting the Right Groups and Forums

Integration in Cyber Operations	1.4.3, 5.1.4, 1.4.2, 1.4.3, 2.1.3, 4.3.1, 4.3.2, 4.3.3	Cyber as an intelligence asset in Cyber operations	K0382, K0383, K0384, K0387, K0454, K0456, K0003, K0442, K0461, K482, K0502, K0351, K0353, K0399, K0400, K0402, K0403, K0410, K0411, K413, K0414, K0416, K425, K0432, K0445, K0446, K0463, K0464, K0494, K0495, K0496, K0497, K0498, K0499, K0503, K0504, K0505, K0506, K0512, K0513, K0518, K0519, K0524, K0525, K0534, K0552, K0553, K0554, K0557, K0563, K0566, K0568, K0569, K0570, K0580, K0581, K0582, K0583, K0584, K0585, K0586, K0589, K0590, K0591,	

			K0593, K0597, K0598, K0603 S0189, S0193, S0201, S0204, S0216, S0223, S0273, S0296, S0306, S0308, S0312, S0314, S0315, S0316, S0317, S0318, S0319, S0320, S0321, S0322, S0323, S0324, S0327, S0328, S0329, S0330, S0334 S0338, S0339, S0341, S0341, s0343, s0345, S0348, S0349, S0350, S0351 A0067, A0068, A0077, A0160,A0081,A0095,A0098, A0104	

		Targeting process for Cyber operations	K0381, K0426, K0439, K0478, K0484, K0520, K0532, K0533, K0535, K0533, K0535, K0538, K0539, K0540, K0541, K0542, K0543, K0544, K0545, K0546, K0547, K0548, K0549, K0550, K0551, KA592, K0604 S0177, S0182, S0188, S0203, S0205, S0225, S0226, S0224,S0228, S0231, S0234, S0235, S0237, S0248, S0251, S0253, S0256, S0259, S0262, S0264, S0265, S0274,S0279, S0280, S0283,S0284, S0286,S0291, S0292,S0293,S0299, S0307, S0309, S0340,	

			A0086, A0092, A0094,A0103,A0108	
		Collaboration and coordination with Electronic Warfare	S0273	Collaboration and coordination with Information Warfare

ANNEX I - Proposed solutions

INFORMATION SECURITY MANAGEMENT	
This course aims to present an approach to Information Security as a management process, using as main base the ISO / IEC 27001 standard. It starts by characterizing a simple Risk Analysis model adequate to support decision-making regarding the security controls required to mitigate security risks. Specific Security Controls to protect all security properties are also characterized. Finally, it will be discussed the issues of information security evaluation and monitoring, to measure and ensure efficiency of the security controls in a typical management cycle (PDCA).	Upon completion of the course, the qualified student will be able to: Describe the Information Security Management process based on the PDCA model, following ISO/IEC 27001 standard; Perform an information security risk assessment and produce security countermeasures to mitigate identified risks; Prepare policy, programs, and guidelines for Information Security Management implementation; Identify security requirements specific to an information technology (IT) system in all phases of the system lifecycle.

SOFTWARE AND APPLICATION SECURITY	
This course aims to develop the capabilities needed to identify vulnerabilities in computer applications and their impacts, to know and apply security testing methodologies and to adopt good coding practices for secure applications.	Upon completion of the course, the qualified student will be able to: Know the most common types of vulnerabilities in applications, with an emphasis on Cyber applications, and their potential impact; Understand and apply software security methodologies (Secure SDLC); Audit, from the point of view of security, computer applications in the different states of its development cycle; Adopt best software and application security practices; Actively participate in incident response groups

DIGITAL FORENSICS	
Digital forensics is dedicated to the collection, identification, preservation, documentation, analysis and presentation of digital evidence from computers, data networks and other electronic devices. The digital forensics field can be divided into: computer forensics, data networks forensics and mobile forensics.	Upon completion of the course, the qualified student will be able to: Identify the different types of digital forensic evidence; Know the terminology, techniques and processes of a digital forensic investigation; Collect digital evidence from storage media; Know the limitations of digital forensics current techniques; Understand the scientific method and the need for its use; Apply the scientific method in a digital forensics investigation; Use digital forensics' tools and techniques;

	Comprehend forensic analysis reports.
SOCIAL ENGINEERING	
Identify human vulnerabilities and learn how to mitigate and/or explore them, not only from a technical point of view but also from a social and/or behavioural.	Upon completion of the course, the qualified student will be able to: Protect the organization from the human side of (in)security; Produce security policies and procedures, related to Telephone traffic, E-mail traffic and Internet searches, Employee behaviour and general safety level of installations; Produce crisis response procedures related to Social Engineering; Produce materials to promote employee awareness of how to respond to current crashes and future attacks on Social Engineering
DIGITAL CRIME AND INVESTIGATION	
This curricular unit has the laboratory aim to apply the techniques, methodologies and tools associated to the forensic analysis of digital evidences in several practical scenarios, namely personal computers and mobile devices. Students will apply the knowledge gained by performing various practical assignments.	Upon completion of the course, the qualified student will be able to: Collect data on storage media, data networks and volatile memory; Obtain digital evidence from different operating systems; Obtain digital evidence from data networks; Obtain digital evidence from mobile operating systems; Create and use hash sets; Create geo-location maps; Apply basic encryption data recovery techniques; Identify and contain malware; Correlate events from different media or devices; Create reports and report results of forensic analysis.
CYBERSPACE AND CYBER OPERATIONS LEGAL FRAMEWORK	
The course aims to develop capabilities in the Law, in the area of cyberspace and cyber operations	Upon completion of the course, the qualified student will be able to: Understand the main legal framework applicable to cyberspace; Understand how the transnational nature of the cyberspace is dealt with by the law; Understand the main legal obligations impending over the different players acting in cyberspace;

	Understand civil liability in cyberspace; Understand the main legal framework applicable to cybercrime; Understand the attribution process under applicable law; Understand the main Public International Law applicable to cyberspace; Understand the admissible conducts of States under Public International Law.
PENETRATION TESTING AND ETHICAL HACKING	
The curricular unit of Penetration Tests and Ethical Hacking, provides a global knowledge about the methodologies and processes involved in a professional Penetration Test and a practical use approach to its technical implementation.	Upon completion of the course, the qualified student will be able to: Understand the various methodologies for penetration testing; Use the Linux Kali distribution in a simple way; Efficient use of information gathering tools and techniques on the Internet; Use simple tools and techniques to identify open services in computer systems; Efficiently use vulnerability identification tools and techniques; Simple use of exploit development environments; Efficient use of passwords attacking tools and techniques; Plan and perform professional penetration testing on computer systems.
CYBER OPERATIONS AND PLANNING	
This unit contributes to the development of an integrative vision of Cyberspace (Cyber domain) in the Operational context, recognizing its transversal nature and identifying its implications in the various functions of staff functions, operational processes and systems	Upon completion of the course, the qualified student will be able to: Characterize the key components and critical aspects that need to be managed in the planning and conduct of Operations in Cyberspace, in a global context and in a broad-spectrum security environment; Analyse case studies and scenarios associated with the conduct of Cyber Operations in order to identify lessons learned; Perform a critical analysis of Cyber policies, strategies and doctrines; Identify the planning assumptions and conditioning factors associated with the Commander operational vision; Apply best practices and operational procedures in a dynamic operational environment and in continuous change; Advise a primary stakeholder and propose a direction to follow regarding

	Operations in Cyberspace.
CYBER INTELLIGENCE AND SITUATIONAL AWARENESS	
Give a general overview of cyberspace and how to use the available intelligence information in it, as well as the correct methodologies and techniques to do it.	Upon completion of the course, the qualified student will be able to: The context of intelligence and its analysis; The main activities and responsibilities of those who deal with intelligence; The main competencies of those involved in/with intelligence information; The main methodologies for obtaining information in cyber-space; The main techniques of analysis of intelligence data.
PROTECTION OF CRITICAL INFRASTRUCTURES AND SYSTEMS	
A solid training in cybersecurity, and particularly in issues related to critical infrastructure protection, draws on knowledge of paradigms and architectures typical of industrial automation and control systems, knowledge of models and techniques for protection of these systems, and knowledge on the application of these techniques and on tools used to conduct and protect infrastructure	Upon completion of the course, the qualified student will be able to: Identify and characterize a critical infrastructure, namely considering industrial automation and control infrastructures; Characterize the various architectures, components and protocols used in industrial automation and control; Analyse a critical infrastructure and identify its main security problems; Characterize the main frameworks for critical infrastructure protection and associated methodologies.
CYBER CAPABILITY DEVELOPMENT	
This unit aims to contribute to the development of a common vision and a deeper knowledge of the process of developing Cybersecurity and CD Capabilities, both nationally and internationally. In this context, in order to promote an integrated approach, the various framework vectors of a capacity (DOTMLPFI) and the different methodologies, associated with the capacity development processes, already existing at the level of the North Atlantic Treaty Organization (NATO) and of the European Union (EU). Merging between organizational efforts and national and international cybersecurity and cyber-defence capacity building processes is intended to contribute to the creation of a common vision and interoperability between them.	Upon completion of the course, the qualified student will be able to: To characterize the fundamentals and the framework of the process of development of the National Security and Defence Capacities; Identify the structuring concepts and principles of capacity development and carry out a critical analysis of its application to the context of Cybersecurity and CD; Characterize the structuring elements of a Capacity Development Plan (organizational, national and international); Identify the principles associated with Risk Management and apply them to the Management of Capabilities Gaps; Analyse and recognize the implications of the implementation of the

	Capacity Development Plan at the various levels (Strategic, Operational, Tactical and Technical); Apply best practices and methodologies for capacity development in the area of Cybersecurity and CD; Advise a primary stakeholder and propose a direction to follow regarding the development of Cybersecurity and Cyber-Defence Capabilities.
CYBERSPACE CRISIS MANAGEMENT (EXERCISE)	
This course aims to teach students how to develop scenarios, plan exercises and promote their execution according to the EU-NATO Crisis Management Exercises framework	Upon completion of the course, the qualified student will be able to: To assess the political and strategic implications of Cyberspace and to analyse its impact in the political, economic and military scopes; Identify the principles associated with the planning of the EU-NATO Crisis Management Exercises and in the area of CD; Analyse methodologies for assessing threats, vulnerabilities and risks; Develop Scenarios to Support Crisis Management in Cyberspace; Identify cybersecurity and CD initiatives that reduce the impact of cyber-attacks and facilitate crisis management in cyberspace; Mitigate its consequences and reduce the likelihood of them occurring again; Planning and executing Crisis Exercises in Cyberspace.
RISK AND INCIDENT MANAGEMENT	
This unit provides the student with the skills to effectively carry out risk and cybersecurity incidents management	Upon completion of the course, the qualified student will be able to: The most current models, methodologies and practices in the area of the Incident and Risk Management and its application; Decision-making in the field of investments in cybersecurity and in the scope of system architectures in organizations; Construction and management of contingency plans for security, emergency, contingency, disaster recovery and the its framework for the business continuity of organizations; Creation and preparation of teams and development of processes to respond to security incidents of various types. Organizational Resilience

	and Crisis Management.
INFORMATION WARFARE	

This Course aims to develop the capabilities needed to conduct a critical analysis of the competitive use of Information. Discuss and establish relationships between a number of terms such as Information warfare and information operations, effect based operations and network centric operations, Economic Warfare and competitive and economic intelligence. Lastly to discuss National Information Strategy composition and its relationship with CD and Cybersecurity.	Upon completion of the course, the qualified student will be able to:
	Differentiate Competition and Conflict in the Information Domain;
	Relating Geopolitics of Cyberspace with the National Information Strategy (NIE);
	Recognize the economic area as the center of modern conflict, where the military plays a secondary position in the resolution of conflicts;
	Relate Competitive Intelligence and Economic Intelligence with Economic Warfare;
	Define operational planning and explain how this applies to Information Warfare;
	Recognize examples of Effect-Based Operations (EBO's);
	Explain the Role of Network-centric Operations in Conducting EBO's;
	Explain the role of Information Operations in the conduct of the Information Warfare;
	Define National Information Policy and Strategy (NIE);
	Characterize the various components of NIE;
	Distinguish Cybersecurity from CD and its relationship with NIE.

DIGITAL LEADERSHIP AND TEAM MANAGEMENT	
In general seeks to acquire skills needed to critically analyse and understand the behaviour of individuals and groups in the organizations - from the point of view of human sciences and the experiences of the managers and leaders in different situations.	Upon completion of the course, the qualified student will be able to: Understanding the evolution of leadership and management in cyberspace environment; Developing skills to lead and manage groups vs teams in cyberspace environment; Develop skills to solve problems and make decisions in virtual team; Communicate effectively in cyberspace environment; To inspire, encourage and motivate virtual teams; Managing conflict and organizational stress in virtual teams.
CD ADVISOR	

The purpose of the course is to provide student with the high-level knowledge, skills and experience required for describing and evaluating the risks and threats of cyber space, improving CD measures and providing advice to decision makers.
The student will be able to re-asses the risks and opportunities during the planning, preparation and execution of operations, elaborating operational risk and opportunities
	Upon completion of the course, the qualified student will be able to:
	CIS & Vulnerabilities;
	Critical Infrastructure & Vulnerabilities;
	Cyber Threats and Mission Risks from CIS & Critical Infrastructure;
	EU CD & Policy;
	EU (Cyber) Intelligence and Mission Risks;
	EU CD Legal issues and Risks;
	EU CD Capabilities and Measures;
	EU CD in Operations (Situational awareness, Assess, Advise);
	EU CD Advice (case study 1, case study 2).

Annex J - Change Proposals

The matrix shown below will be used to record comments during the staffing. The column headings depicted on the matrix are self-explanatory. However, the following guidelines apply to the matrix. All comments will be numerically numbered and arranged in chronological order. The comments will be categorized in the following manner: C – Critical (Contentious issue that will cause non-concurrence with publication), S – Substantive (Factually incorrect, misleading, etc.), E – Editorial (grammar, punctuation, style, etc.). The originator, and paragraph, sub-paragraph and line is self-explanatory. Comment should be placed in the Comment column. Comments should be line-in/out format and propose a recommended course of action. General observations without proposed solutions should not be submitted. Rationale will be submitted for all comments. The adjudication column is used by the custodian to record the adjudication of the comment. The responses are Accepted (A), Accepted w/ Amendment (AA), Withdrawn (W), or Not Accepted (NA). All amendments to a comment are recorded on the matrix. The matrix becomes the record of decisions for the publication review.

Change Proposals

Serial	C/S/E	Originator	Page/	Sub-	Line	Comment	Rationale	Adjudication
			Para	Para		*New writing suggestion*	*Explanation about comment*	
1.								
2.								
3.								
4.								
5.								
6.								
7.								
8.								
9.								
10.								
11.								
12.								
13.								
14.								