European Defence Agency
Capabilities Directorate

COMMON STAFF TARGET FOR MILITARY COOPERATION ON CYBER RANGES IN THE EUROPEAN UNION

Version 1.0
Brussels, 14/November/2013

This page intentionally left blank

Executive Summary

The recently released Cyber Security Strategy for the EU recognizes Cyber Defence as one of the strategic priorities of the EU. The military requirements on Cyber Defence capabilities are to prepare for, prevent, detect, respond to, recover from and learn lessons from attacks, damage or unauthorized access affecting information infrastructures that support and enable the conduct of military tasks and operations.
Coherent to this, a vital aspect to protect effectively against Cyber Threat is the ability to detect and to properly react to and evaluate Cyber Threats. This requires well - trained personal on different training levels. Such training requires in most cases the availability of technical infrastructure that allows flexible scenario related training simulation and experienced personnel to simulate the attacker side.

The EDA has proposed in June 2012 an initial idea for a multinational cooperation for more coherent and sustainable Cyber Defence training, exercises and testing under the Pooling & Sharing agenda. This Common Staff Target (CST) for cyber ranges, prepared by AT, CZ, EE, EL, IE, FI, LT and NL with support from EDA within the cyber ranges Ad Hoc Working Group (AHWG), identifies the common functional requirements for cyber ranges and proposes the way ahead to fulfil the requirement.

The scope of the cyber ranges ad hoc project is to improve the usage of existing and future cyber ranges for conducting cyber defence training, exercises & testing. This should improve the cyber resilience and the levels of awareness, insight and expertise of national and EU personnel.

Interoperability of cyber ranges will have a positive effect on the interoperability of operational cyber defence systems, organisations and processes, thereby improving the effectiveness and efficiency of CSDP operations and multinational exercises.

The project will be carried out under the EU pooling & sharing agenda and should:
- Increase availability of existing cyber range facilities;
- Increase occupation rate and efficiency of existing cyber ranges and platforms;
- Mainstream and improve cyber defence training, exercises & testing at European level.

The document lists the requirements for the cyber ranges project organised according to the DOTMLPF-I methodology[1] and describes the way ahead to fulfil the requirements through an EDA ad hoc project on cyber ranges in a spiral approach within the timeframe from Mid 2014 (Initial Operational Capability) until early 2018 (Full Operational Capability).

The CST will be submitted for endorsement to the EDA Steering Board (SB) through a written procedure.

[1] **D**octrine, **O**rganisation, **T**raining, **M**ateriel, **L**eadership, **P**ersonnel, **F**acilities and **I**nteroperability

Contents

1. Introduction

1.1 Background

Cyber Space is today widely recognized as the 5th operational domain besides the traditional physical domains land, sea, air and space. The success of military operations in the physical domains is increasingly dependent on the availability of, and the access to, cyberspace. This paradigm shift should be considered in the preparation and conduct of EU-led operations as the unpredictability and asymmetry of cyber threats could impose tremendous limitations on the effectiveness of military operations.

The recently released Cyber Security Strategy for the EU (Reference 1) recognizes Cyber Defence as one of the strategic priorities of the EU. The European Defence Agency (EDA) has identified cyber defence as one of ten priorities in its Capability Development Plan (CDP) (Reference 2). The EU concept for cyber defence for EU-led Operations (Reference 3) defines the key responsibilities of strategic, operational and tactical commanders. The Cyber Defence Capability Requirements document (Reference 4) was agreed by the EU Military Committee (EUMC) in March 2013. On the basis of these requirements and the Strategic Context Case for the EDA Cyber Defence Project Team (PT) (Reference 5) EDA has undertaken action to identify collaborative options for cyber defence, including the training dimension at EU level. The recently released Estonian, Irish and Lithuanian Non-Paper on Cyber Security in view of the adoption of the Cyber Security Strategy of the European Union and the upcoming European Council addressing defence issues (Reference 6) highlighted the requirement for enhancing cooperation between all actors in the EU including technical incidence response, law enforcement and the cyber defence community.

One of the essential elements of the EU cyber defence capability is highly skilled and well-trained personnel. It is recognized that skilled and competent cyber defence operators are and will remain a scarce resource in the short to mid-term. It is concluded that the training dimension of the cyber defence capability offers opportunities for collaboration both in the field of concept development and for pooling and sharing of means and facilities. Furthermore multinational exercises can contribute greatly to enhancing the skills of cyber defence personnel.

Therefore, EDA has put forth initiatives that contribute to the development of mature cyber defence training in the EU: analysis of the cyber defence training Need and development of a cyber defence training curriculum. In conjunction with these activities the cyber ranges initiative forms a coherent package of training and exercises initiatives for cyber defence. These separate initiatives were launched and are synchronised by the EDA PT for cyber defence.

The EDA has proposed in June 2012 (Reference 7) an initial idea for a multinational cooperation for more coherent and sustainable cyber defence training, exercises and testing under the Pooling & Sharing agenda. EDA organized two workshops with pMS and Nations with which EDA has Administrative Arrangements (AA nations) and Estonia hosted an additional workshop in Tallinn with the intention to assess the feasibility and interest in Multinational Cooperation on Cyber Defence Training, Exercise & Testing Ranges (“Cyber Ranges”, formerly MNCDR).

1.2 Aim

This Common Staff Target (CST) for cyber ranges identifies the common functional requirements for cyber ranges. It will be submitted to the EDA steering board (SB) for endorsement. The CST will be based on the high level concept for cyber ranges (Chapter 1.4).
It is the intention that, after Steering Board endorsement, implementation of the CST will be realised by an ad hoc project on cyber ranges.

1.3 Scope

The cyber ranges ad hoc project should improve the usage of existing and future cyber ranges for conducting cyber defence training, exercises & testing. This should improve the cyber resilience and the levels of awareness, insight and expertise of EU personnel.

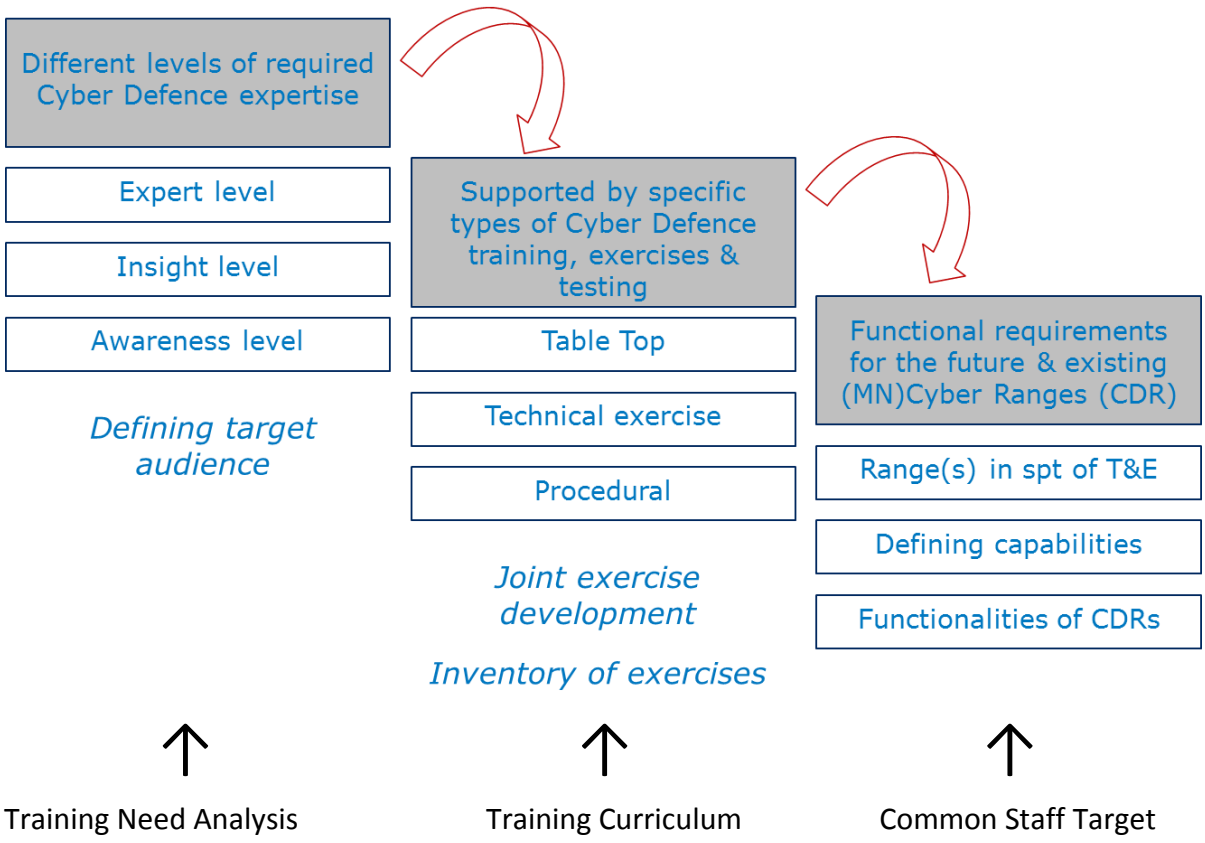
Interoperability of cyber ranges will have a positive effect on the interoperability of operational cyber defence systems, organisations and processes, thereby improving the effectiveness and efficiency of CSDP operations and multinational exercises.

The project is carried out under the EU pooling & sharing agenda and should:

- Increase availability of existing facilities;
- Increase occupation rate and efficiency of existing cyber ranges and platforms;
- Mainstream and improve cyber defence training, exercises & testing at European level.

1.4 High level concept

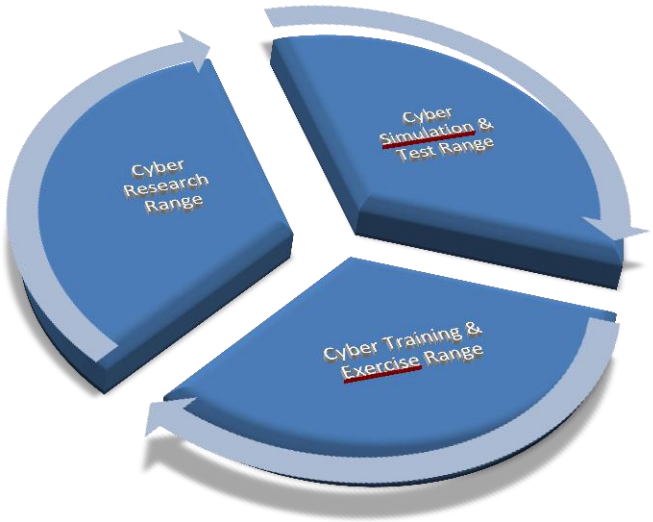
The CST will be based upon the following high level concept.



Picture 1: High Level Concept for cyber ranges

The training need analysis, that defines the target audience, will be performed as a work package of EDA's Frame Cyber Cap study (12.CAP.OP.332). The inventory of exercises will be developed on the basis of the cyber defence training curriculum as another work package of the same EDA study.

Both these results will provide the basis for the identification of the functional requirements for cyber ranges. It should be noted that the picture does not imply a 'waterfall' model. All types of exercises will be available for training on every expertise level. All requirements can support any level of expertise and any type of exercise.



Picture 2: Cyber range components

In the context of this CST a cyber range is defined as follows (see picture 2):

a *multipurpose* environment in support of 3 primary processes: knowledge development, assurance and dissemination. It consists of three complementary functionality packages:

- **Cyber Research Range (CRR)**

A facility where in close cooperation with research centers, private sector, academic institutions knowledge development (research) takes place. Where newly gained knowledge can be utilized in new products, processes and/or services (development). A facility where e.g. ICT, Network Information & Architecture (NII) in a variety of configurations and circumstances can be analyzed. Currently used systems can be analyzed as well.

- **Cyber Simulation & Test Range (CSTR)**

A facility within the cyber range where the current ICT-reality of a specific network configuration can be simulated, in which possible effects of cyber operations can be tested. The CSTR enables experimental testing of cyber capabilities in a realistic manner, but in a safe, isolated setting.

- **Cyber Training & Exercise Range (CTER)**

In order to achieve the necessary growth and sustainability in human capital a state-of-the-art training & exercise functionality is needed. Modeling & Simulation is a valuable

asset where knowledge and skills concerning cyber capabilities and cyber operations can be trained and tested. A setting where cyber operators under simulated circumstances can be trained for utilizing cyber capabilities.

A cyber range conceptually consist of a research range, a simulation & test range and a training & exercise range (see picture 2). This CST will above all focus on the training & exercise part of the cyber range, because this is considered to be the area where pooling and sharing will give the highest pay off in the near future.

2. Mission analysis

The military requirements on cyber defence capabilities are to 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, systems using computer systems as well as programs and data used within) that support and enable the conduct of military tasks and operations.

Coherent to this, a vital aspect to protect effectively against cyber threat is the ability to detect and to properly react to and evaluate cyber threats. This requires well - trained personal at different competence levels. Such training requires in most cases (with exception of procedural training) the availability of technical infrastructure that allows flexible scenario related training simulation and experienced personnel to simulate the attacker side.

In order to achieve and maintain the necessary skill sets of cyber defence personnel, in most cases hands-on training is required. Such hands-on training necessitates the availability of a technical infrastructure (virtual battle space) that allows flexible scenario related training simulation and experienced personnel to simulate the aggressor.

For smaller pMS it is a challenge to provide and maintain the necessary resources to implement and to operate such a training infrastructure in a cost efficient manner. Even for bigger pMS it is a challenge to have a sufficient occupancy rate of cyber ranges and the related resources to make it run economically sound.

The CST for cyber ranges does not purely focus on equipment and facilities. In order to gain momentum it is important to provide a framework for pooling and sharing that allows for multinational use of existing and emerging facilities for cyber defence training & exercise. In this way filling a capability gap in one EU nation can at the same time raise the occupancy rate of another nations facilities to an economically sustainable level.

To validate the concept of cyber ranges it is considered important to hold one or more international exercises in which the cyber ranges are used in practice. Such an exercise and the evaluation of the results should be an integral part of the ad hoc project.

2.1 Global description

The CST on Cyber ranges aims at the following functionality:

- Providing technical platform(s), which allows both on-site training and distributed/ remote training of Cyber Defence personnel on a technical level for various customers (military and civil) of cMS and EU organisations.
- Providing technical platform(s) for distributed multinational Cyber Defence exercises.
- Providing a platform for concept development & experimentation with a focus to validate concepts for various customers (military and civil) of cMS and EU organisations.
- Investigating the feasibility to support equipment and software testing with a focus to assess their resilience against Cyber Attacks for various customers (military and civil) of cMS and EU organisations through the use of such an infrastructure.
- Providing a coordination mechanism for matching supply and demand for the usage of cyber ranges.
- Organising a multinational exercise to evaluate the concept of cyber ranges

2.2 Scenarios

In times of austerity Pooling and Sharing of existing facilities and joint development of future cyber ranges can be appropriate means to tackle the challenges of budget restrictions and scarce expertise. A multinational project with partners from cMS and/or cAA nations can help to overcome the economical, efficiency and military know-how related challenges.

Time slots not utilized for training and exercises could be used for research, equipment testing and simulations to ensure a sufficient occupancy rate. The usage of cyber ranges could be arranged on a member state-specific reimbursement scheme, depending on the participation/contribution status in the project.

The federation of existing and future cyber ranges in cMS into a "Cyber Ranges Network" (CRN) will drastically reduce efforts and resources required to set-up larger scale or more complex cyber defence exercises at national or multinational level.

The cMS participating in cyber ranges have intentions that can be categorised as follows:

1. Improve a nation's own cyber range and streamline training and exercise formats;
2. Use cyber ranges of cMS or offer national range for shared use by cMS ("shared ranges");
3. Interconnect cyber ranges of cMS into a network to form together a bigger range for larger scale and more complex exercises ("Cyber Ranges Network").

To operationalize the scenarios above, the following products and actions require development in an ad hoc project on cyber ranges (Figures in parenthesis indicate which of the above intentions are addressed by the product/action):

- Platform for exchange of information and experience (1, 3);
- Arrangements with agreed terms and conditions for multinational usage of cyber ranges (legal and financial) (2);
- Agreed common framework for training and exercises (1);
- Agreed training curriculum (1);
- Logical and technical interface specifications for interconnection of cyber ranges (3);
- Legal, organisational and procedural arrangements for interconnection of cyber ranges (3);
- Procedures, organisation and tools to publish, plan and coordinate the availability and occupancy of cyber ranges (2);
- Generic re-usable concepts/models/tools/procedures for training and exercise (1);
- Common architecture for cyber ranges (1).

3. Requirement

3.1 General operational and functional aspects

As part of the drafting process of the CST, cMS reacted to a questionnaire with respect to their motivation, ambitions, intentions and expectations with regard to the EDA cyber ranges project. The nations participating in cyber ranges have indicated their ambitions as follows:

	AT	CZ	EL	EE	FI	IE	LT	NL
Improve own range (1)	X	X	X	X	X		X	X
Sharing ranges (2)	X		X	X*	X*	X	X	X*
Federation of ranges (3)	X		X	X	X	X	X	X

Chart 1: cMS ambition with respect to the different options

*) Estonia, Finland and Netherlands offer (part of) their (future) national cyber facilities for sharing by cMS to improve the occupation rate of their facilities.

In the short term some cMS are developing their own cyber capabilities, including cyber ranges, based on national requirement statements. They want to share information, experiences and raise cyber awareness. Some cMS want to close a national capability gap by using other cMS' ranges. Interconnection of ranges is considered challenging, but profitable in support of (multi)national and complex exercises. cMS indicated that option 3 is the mid to long-term goal.

3.2 Requirement in more detail and structure

The following subparagraphs list the requirements for the cyber ranges project organised according to the DOTMLPF-I methodology[2].

3.2.1 Doctrine

- Improve national and EU Cyber Defence doctrine procedures, terminology and metrics.
- Share lessons learned and common practices.
- Develop practice-oriented guidelines for further development in the Cyber Defence domain.
- Use cyber ranges as a platform for testing, validating, experimenting and exercising the above products.
- Improve cyber defence measures implementation.

3.2.2 Command and Control

- Validate and improve command structures and procedures to integrate cyber operations into general operational decision making and planning by providing a platform for cyber operations simulation and war gaming. This will also improve the implementation of cyber defence measures.

3.2.3 Organisation

- Improve performance of national cyber organisations by validating and testing them in national and multinational exercises by using cyber ranges.

[2] **D**octrine, **O**rganisation, **T**raining, **M**ateriel, **L**eadership, **P**ersonnel, **F**acilities and **I**nteroperability

- Explore whether new, innovative organisational models can be more effective for the cyber domain.

3.2.4 Training

- Improve cyber training through the exchange of best practices and by facilitating joint and combined exercises.
- Enable and stimulate pooling and sharing of cyber training capacities. Multinational exercises and pooling and sharing of training capabilities will be boosted by a common cyber training curriculum and the definition of standard training sessions for user-groups at different skill levels.
- Support Red and Blue Team exercises.
- Training audience for cyber ranges are cyber defence experts, operators, commanders, staff personnel and trainers.
- Stimulate and enable the interconnection of national cyber training facilities to provide a bigger platform for multinational and complex exercises.
- Training on specific military aspects of cyber defence that are not covered by the civil market.

3.2.5 Materiel

- Identify technical requirements for national cyber range capabilities by sharing information and experience.
- Facilitate and stimulate pooling and sharing of national assets by harmonisation of technical requirements for cyber ranges.
- Provide a test bed for testing cyber resilience of hard- and software.
- Develop a technical architecture and technical security requirements for cyber ranges.
- Provide a platform for better system integration and optimization of hardware and software.

3.2.6 Leadership

- Improve leadership in the cyber domain and cyber security awareness of commanders and planners by participating in multinational exercises.
- Develop, validate and improve the cyber defence decision making process.
- Test the ability of commanders with responsibility for cyber defence to effectively implement the decision making process.
- Raise the cyber security awareness and improve the decision making and information sharing of critical (information) infrastructures providers.

3.2.7 Personnel

- Improve the cyber defence knowledge and skills of technical operators, planners, instructors and commanders.
- Raise the cyber security awareness of personnel to evolving/new cyber threats.
- Harmonise cyber security awareness of personnel in cMS to create common ground for CSDP operations and multinational exercises.
- In-house education on specific military aspects of cyber defence that are not covered by the civil market.
- Determine the required qualifications and security requirements for cyber ranges personnel.
- Determine the required qualifications for cyber defence instructors.

3.2.8 Facilities

- Initiate and facilitate the pooling and sharing of cyber range facilities in support of cMS that currently have insufficient cyber range facilities.

- Improve the efficiency and occupation rate of cyber range facilities.
- Develop arrangements and procedures (legal and administrative) to allow pooling and sharing of cyber facilities between cMS.
- Create the conditions under which a cyber range network can be established by interconnecting cyber ranges of cMS.
- Develop a management system and mechanism that matches the availability with the demand of cyber range facilities.

3.2.9 Interoperability

- Support testing of cross-border linkage of cyber early warning systems and processes.
- Identify and agree on common technical standards, procedures and legal conditions for the interconnection of Cyber ranges.
- Use existing standards/de facto standards.
- Interconnect cyber ranges to increase the capacity, performance of national ranges, thereby creating scalability and diversity that would not be achievable on a national scale.

3.3 Security aspects

Currently the following security aspects/requirements were identified by the cyber ranges AHWG, which need further detailing during the development of the project:

- Comply with existing national security measures/regulations for facilities that host cyber ranges;
- Establish information exchange on national security requirements and measures/ regulations for cyber ranges;
- Agree on minimum security requirements for cyber ranges;
- Establish security requirements for the interconnection of cyber ranges;
- Establish security requirements for cyber ranges with regard to instructors, trainees, exercise participants, range personnel;
- Investigate the necessity for security accreditation of cyber ranges;
- Determine the required security level of the EDA ad hoc project on cyber ranges;
- Investigate the necessity to establish non-disclosure agreements.

4. Way ahead

4.1 Measures, means and process description to fulfil the requirement

cMS are currently in the process of establishing or developing national cyber ranges independently of each other. Thus it is important that the results of the cyber ranges projects can be utilised the very moment they emerge. To facilitate that concept, a spiral development approach would be a practical approach. With the start of each new spiral the deliverables of the previous spirals will be evaluated and adapted/improved as necessary. Additionally each spiral will result in new products/deliverables. Following spirals are foreseen at the moment:

4.1.1 Spiral 0 (in parallel with pre-project phase for spiral 1-4)

- Agree on arrangements with terms and conditions for multinational usage of cyber ranges (legal and financial) until July 2014; (Initial Operational Capability);
- AT and EE will take the lead to develop the draft arrangements. Validate results in a proof of concept demonstration (e.g multinational exercise)
- Validate results in a proof of concept demonstration (e.g multinational exercise)

4.1.2 Spiral 1

- Revisit Spiral 0 deliverables;
- Develop generic re-usable concepts/models/tools/procedures for the usage of cyber ranges;
- Develop a pool of exercise scenarios (initially NL offers 1 scenario that can be used for the project and/or for national use by cMS) ;
  Initially on top of NL offer:
  - 1 exercise scenario (e.g. along Locked Shields scenario)
  - 1 scenario evaluation of assets, procedures etc. (testing & simulation module)
  - 1 test case for research module
  - Take training & coordination platform into account as host for the pool including catalogue of:
    - Ranges,
    - exercises,
    - outcome/inputs
    - scenarios
    - …
    - Knowledge Managent platform
- Develop a training and exercise curriculum for training and exercises that are supported by cyber ranges. The Training Need Analysis (TNA) and the training curriculum of the on-going EDA frameCyberCAP study (12.CAP.OP.332) will be used as starting point for this project element;
  -
- Validate results in a proof of concept demonstration (e.g multinational exercise).

4.1.3 Spiral 2

- Revisit Spiral 0-1 deliverables;
- Agree a common framework for the usage of cyber ranges by cMS;

- Agree a common framework for collaboration with third parties (government, academia, industry etc.) with respect usage of cyber ranges;
- Develop and implement a platform for exchange of information and experience on cyber ranges and their usage;
- Develop procedures, organisation and tools to publish, plan and coordinate the availability and occupancy of cyber ranges;
- Validate results in a proof of concept demonstration (e.g multinational exercise).

4.1.4 Spiral 3

- Revisit Spiral 0-2 deliverables;
- Develop common architecture for cyber ranges and cyber ranges network;
- Validate results in a proof of concept demonstration (e.g multinational exercise).

4.1.5 Spiral 4

- Revisit Spiral 0-3 deliverables;
- Develop logical and technical interface specifications for interconnection of cyber ranges;
- Develop legal, organisational and procedural arrangements for interconnection of cyber ranges;
- Demonstrate the feasibility of interconnection of cyber ranges;
- Implement interconnection of cyber ranges;
- Validate results in a proof of concept demonstration (e.g. multinational exercise).

4.2 Expected Results along Timelines

The different steps, deliverables and milestones are depicted in Annex A in a GANTT chart format. Currently the timelines are estimates that will require further detailing in a business case with respect to necessary resource assessments and a CSR with respect to the functional requirements of the different components/deliverables of the different spirals of the cyber ranges project. The business case should be developed in parallel with the CSR for the cyber ranges project but with an earlier delivery date (summer 2014) in order to allow cMS the allocation of budgets for the project starting in 2015.

4.3 Tools

For the pre-project phase of the cyber ranges project a Forum for the work of the cyber ranges AdHoc Working Group (AHWG) was initially established at the EDA EXTRANET. This forum will be utilized for the entire pre-project phase. The AHWG will identify, which additional existing EDA tools (e.g. CODABA) can support the project.

Spiral 2 foresees the development and implementation of an information sharing and coordination platform on cyber ranges. The project will investigate whether the requirements of this tool can be pooled/integrated with other existing training coordination tools or whether existing architectures/designs could be reused.

4.4 Risk Analysis

Each project has inherent risks. Initially the following risks, that might affect the success of the project, and related risk mitigation options were identified by cMS:

Risk	Risk Mitigation Options
Lack of capacities (personnel on working level) to develop necessary arrangements	• Increase time to develop the arrangements; • More cMS then one is doing the specific work package.
Work on legal challenges significantly delays the project	• Include as soon as possible the legal community in the preparation work; • Use as far as possible existing MOU(s).
Lack of resources to run and maintain developed platforms on daily basis	• Address operation and maintenance of the cyber ranges in the business case and resource plan; • Investigate EDA support options.
Opting out of one or more cMS due to necessary efforts/resources or other initiatives in this field (e.g. NATO)	• Hold the affordable project resources as low as possible; • Meet the time lines; • Check the common grounds and aims periodically; • Adapt Project to meet cMS changed expectations (change horses).
Lack of availability of a critical mass of Cyber Range-capacity due to national occupation	• Check the actual occupation rate; • Renegotiation with the offering cMS.
Failure in operationalizing the agreements and procedures in day to day business	• Give sufficient time in advance to implement; • Establish a governance body that accompanies this initial phase.
Restructuring and new competencies (cMS, EDA) cause delays	• High degree of pre-planned and authorized work packages; • Situational awareness.
Work packages are delayed and do not meet the timelines therefore: • Loss of momentum and interest in cMS; and/or • Lack of support on decision making level	• Meet the timelines; • Inform relevant bodies and decision makers on a regular base (internal Marketing).

Along with the project development a risk management process should be established to mitigate risks in order to ensure the success of the cyber ranges project.

4.5 Project Documentation Classification

The classification of the cyber ranges project documentation will depend on several security aspects (see Chapter 3.3), which will be detailed along the project development. In the pre-project phase information exchange and project documentation of the cyber ranges project (e.g. CSR and business case) is at unclassified/LIMITE UE level. cMS can raise the classification of the documentation at any stage of the project if national and/or EU security requirements deem this appropriate.

4.6 Strategic Communication

cMS together with EDA will develop a communication strategy to inform stakeholders in cMS, other pMS and third parties about the cyber ranges project. Currently following activities could be foreseen:

- Information of cMS stakeholders, other pMS and AA nations through EDA meetings (e.g. PT Cyber Defence, IDT Command & Inform, SB Cap) and established communication channels (e.g. EXTRANET Forum Cyber Defence)
- Presentation of the cyber ranges initiative at selected conferences in 2014;
- Development of a standard presentation and information paper (fact sheet) explaining the project;
- Organisation of a cyber ranges workshop within the context/agenda of a Cyber Security/Defence conference with a world-wide reputation (e.g. CCD COE organized CYCON 2014)

4.7 Entrance Points for other pMS and AA nations

All pMS and AA nations are invited to join in the cyber ranges project at any time. Terms and conditions of joining will depend on the date of joining and the progress of the project. For pMS/AA nations joining in the pre-project phase terms and conditions will be determined by the Cyber Ranges AHWG. For joining in the project phase the terms and conditions will be determined by the Cyber Ranges Project Management Group (PMG) (see Annex A).

List of acronyms

AA	Administrative Arrangement
AA nation	Nation with which EDA has Administrative Arrangements
AHWG	Ad Hoc Working Group
AT	Austria
cAA nation	Nation with which EDA has Administrative Arrangements and which contributes to an EDA ad hoc project
Cap	Capabilities
CCD COE	Cooperative Cyber Defence Center of Excellence (Tallinn)
CDP	Capability Development Plan
CDR	Cyber Defence Range
CION	Commission of the EU
cMS	(Project) contributing Member State
CODABA	Collaborative Data Base
CRN	Cyber Ranges Network
CRR	Cyber Research Range
CSDP	Common Security and Defence Policy
CSR	Common Staff Requirement
CSTR	Cyber Simulation & Test Range
CTER	Cyber Training & Exercise Range
CST	Common Staff Target
CYCON	CCD COE annual Cyber Conflict Conference
CZ	Czech Republic
DOTMLPF-I	Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities and Interoperability
EE	Estonia
EEAS	European External Action Service
EL	Greece
EDA	European Defence Agency

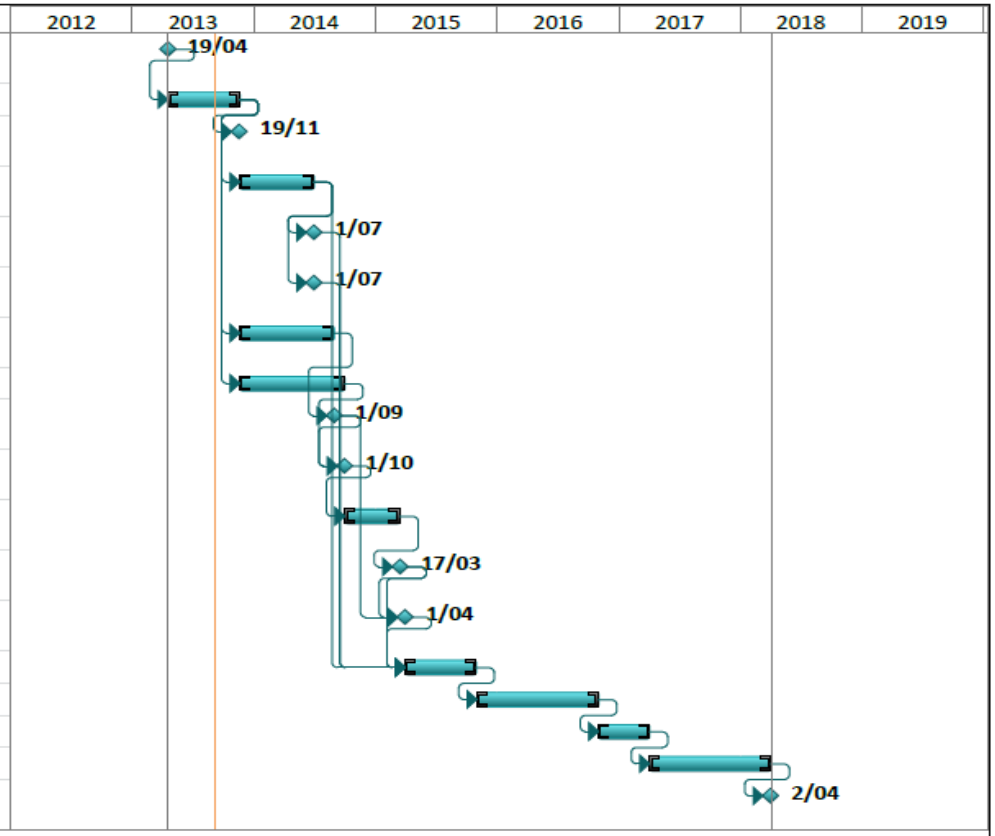
EU	European Union
EUMC	EU Military Committee
EUMS	EU Military Staff
FI	Finland
FOC	Full Operational Capability
ICT	Information and Communication Technology
IDT	Integrated Development Team
IE	Ireland
IOC	Initial Operational Capability
MNCDR	Multinational Cyber Defence Training & Exercise Range
NL	Netherlands
NII	Network & Information Infrastructure
PMG	Project Management Group
pMS	participating Member State to EDA
PT	Project Team
SB	EDA Steering Board
TNA	Training Need Analysis
T&E	Training & Exercises

References

1. CION/EEAS JOIN(2013) 1 final, dated, 7 February 2013, Cyber Security Strategy for the European Union
2. Capability Development Plan Update 2011
3. EEAS 02305/12, dated 20 December 2012 , EU Concept for Cyber Defence for EU-led Operations
4. EEAS 00713/13, dated 27 March 2013, Cyber Defence Capability Requirements
5. Strategic Context Case of the EDA Project Team Cyber Defence (as approved by the EDA SB Cap in October 2012)
6. Non-Paper: Estonian, Irish and Lithuanian views on Cyber Security in view of the adoption of the Cyber Security Strategy of the European Union and the upcoming European Council addressing defence issues (July 2013)
7. EDA Multinational Cyber Ranges (MNCDR) Initiative, dated 29 May 2012

Annex A

ID	Task Name	Duration	Start	Finish
1	Milestone; EDA SB MoD; Cyber Ranges AHWG establishment	0 days	Fri 19/04/13	Fri 19/04/13
2	Cyber Ranges CST Development	153 days	Fri 19/04/13	Tue 19/11/13
3	Milestone; EDA SB MoD; CST Approval	0 days?	Tue 19/11/13	Tue 19/11/13
4	Cyber Ranges Spiral 0; Arrangements development	159 days?	Wed 20/11/13	Mon 30/06/14
5	Milestone; Cyber Ranges Arrangements set in force	0 days?	Tue 1/07/14	Tue 1/07/14
6	Milestone; Cyber Ranges Initial Operational Capability (IOC)	0 days?	Tue 1/07/14	Tue 1/07/14
7	Cyber Ranges Business Case Development	203 days?	Wed 20/11/13	Fri 29/08/14
8	Cyber Ranges CSR Development	225 days?	Wed 20/11/13	Tue 30/09/14
9	Milestone; Business Case agreed by cMS	0 days?	Mon 1/09/14	Mon 1/09/14
10	Milestone; EDA SB Cap; CSR Approval	0 days?	Wed 1/10/14	Wed 1/10/14
11	Cyber Ranges Project MoU development	119 days?	Wed 1/10/14	Mon 16/03/15
12	Milestone; Cyber Ranges Project MoU Agreement	0 days?	Tue 17/03/15	Tue 17/03/15
13	Milestone; Cyber Ranges Project Management Group established	0 days?	Wed 1/04/15	Wed 1/04/15
14	Cyber Ranges Spiral 1	153 days	Wed 1/04/15	Fri 30/10/15
15	Cyber Ranges Spiral 2	262 days?	Mon 2/11/15	Tue 1/11/16
16	Cyber Ranges Spiral 3	109 days?	Wed 2/11/16	Mon 3/04/17
17	Cyber Ranges Spiral 4	261 days?	Tue 4/04/17	Tue 3/04/18
18	Milestone; Cyber Ranges Full Operational Capability (FOC)	0 days?	Mon 2/04/18	Mon 2/04/18



Project: 20130909 Cyber ranges P
Date: Mon 9/09/13

Task		External Milestone		Manual Summary Rollup	
Split		Inactive Task		Manual Summary	
Milestone		Inactive Milestone		Start-only	
Summary		Inactive Summary		Finish-only	
Project Summary		Manual Task		Deadline	
External Tasks		Duration-only		Progress	

Page 1