EUROPEAN DEFENCE AGENCY

2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, 23-24 Sep 2013,

Mr. Wolfgang Roehrig,
Project Officer Cyber Defence

Mainstreaming European Military Cyber Defence Training & Exercises

Mission

So we do for Cyber Defence in CSDP

Agenda

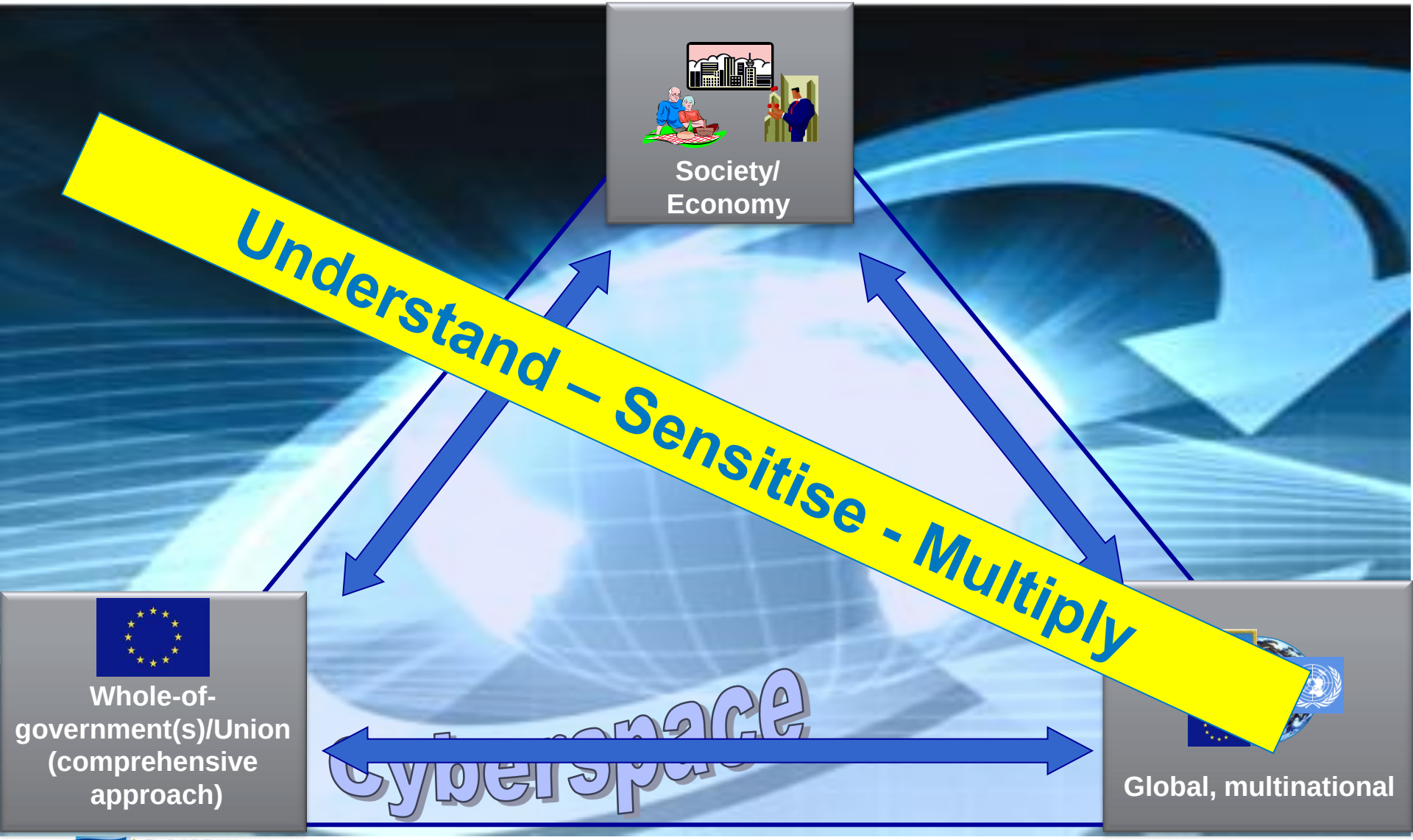
- Cyber Security Strategy for the EU and the related military concepts
- The EDA Project Team Cyber Defence and its development
- Training related findings of the EDA Cyber Defence Landscaping Study
- Cyber Defence Training Need Analysis and Training Curriculum
- Cyber Ranges Ad Hoc Project
- Opportunities for Civil-Military Cooperation on Training & Exercises

Cyber Security Strategy for the EU: The key military aspects

"Cyber security efforts in the EU also involve the cyber defence dimension."

- Assess operational **EU cyber defence requirements** and promote the development of EU cyber defence capabilities and technologies to address all aspects of capability development … *including training & exercise dimension*;
- Develop the **EU cyber defence policy framework** to protect networks within CSDP missions and operations;
- Promote **civil-military dialogue in the EU** and contribute to the coordination between all actors at EU level;
- Ensure **dialogue with international partners**, including NATO, other international organisations and multinational Centres of Excellence.

Civil-Military Cooperation



EDA Project Team Cyber Defence

Start: Nov 2011

Aim: Within the remit of the Cyber Security Strategy for the EU to assess short, medium and long term Cyber Defence capability requirements and to identify collaborative options in order to improve Cyber Defence resilience of pMS and CSDP operations

pMS: **EE/IT (rotational chair)**, AT, BE, BG, CY, CZ, DE, EL, ES, FI, FR, HU, IE, LT, LV, NL, PL, PO, RO, SE, SI, SK plus CH, NO on a regular basis plus EUMS, Council GSC, CION, ENISA, EC3, ESA, EU SatCen

EDA to-date Achievements on Cyber Defence:

- Contribution to the Cyber Security Strategy for the EU (2012-2013)
- Cyber Defence Landscaping study (2012)
- Liaison Agreement with CCD COE, Tallinn (2013)
- Acceptance of EDA Steering Board MoDs to add Cyber Defence to the Pooling & Sharing (P&S) agenda (2012);
- Delineation & Coordination of EDA R&T with CION with respect to FP7 under the European Framework Cooperation (EFC);
- Initiation of an adhoc Project on Cyber Ranges
- Initiative on deployable Cyber Defence Situational Awareness Kits for OHQ/FHQ
- Initiative on improved APT Detection

Cyber Defence Lines of Development – DOTMLPF-I - a holistic approach

The Stocktaking Study: Some training & exercise related recommendations for EU institutions

- Deepening Incident response capabilities;
- Creating a culture of cyber-security (good practices, training, awareness raising);
- Promulgating standards and security tools;
- Reinforcing links between EU/NATO for cyber defence issues.

The Stocktaking Study: Some Training & exercises related recommendations for member states

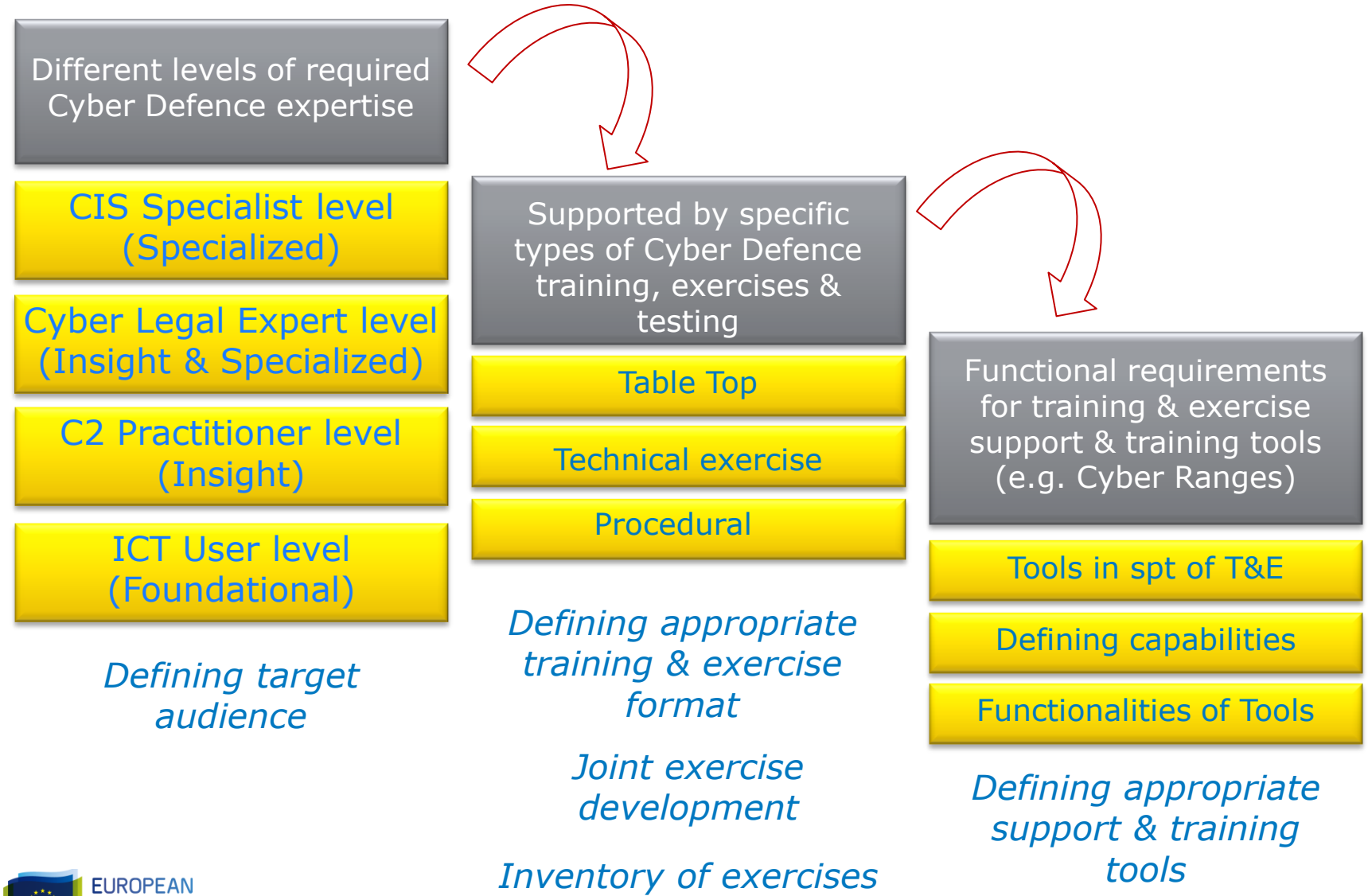
- Improve Exchange of best practices on doctrine (D);
- Ensure CD is not just a IT related function (O);
- **Mainstream cyber defence training (T);**
- **Encourage participation in exercises (T);**
- Explore better identification of lessons learned and trusted information sharing (T);
- **Pooling and sharing of testing platforms for patches; exploits and reverse engineered code (F);**
- Use of a common Cyber defence interoperability frameworks across the public sector (I).

EDA Project: Cyber Defence Training Need Analysis and Training Curriculum

Provide an assessment of cyber defence learning needs and propose solutions:

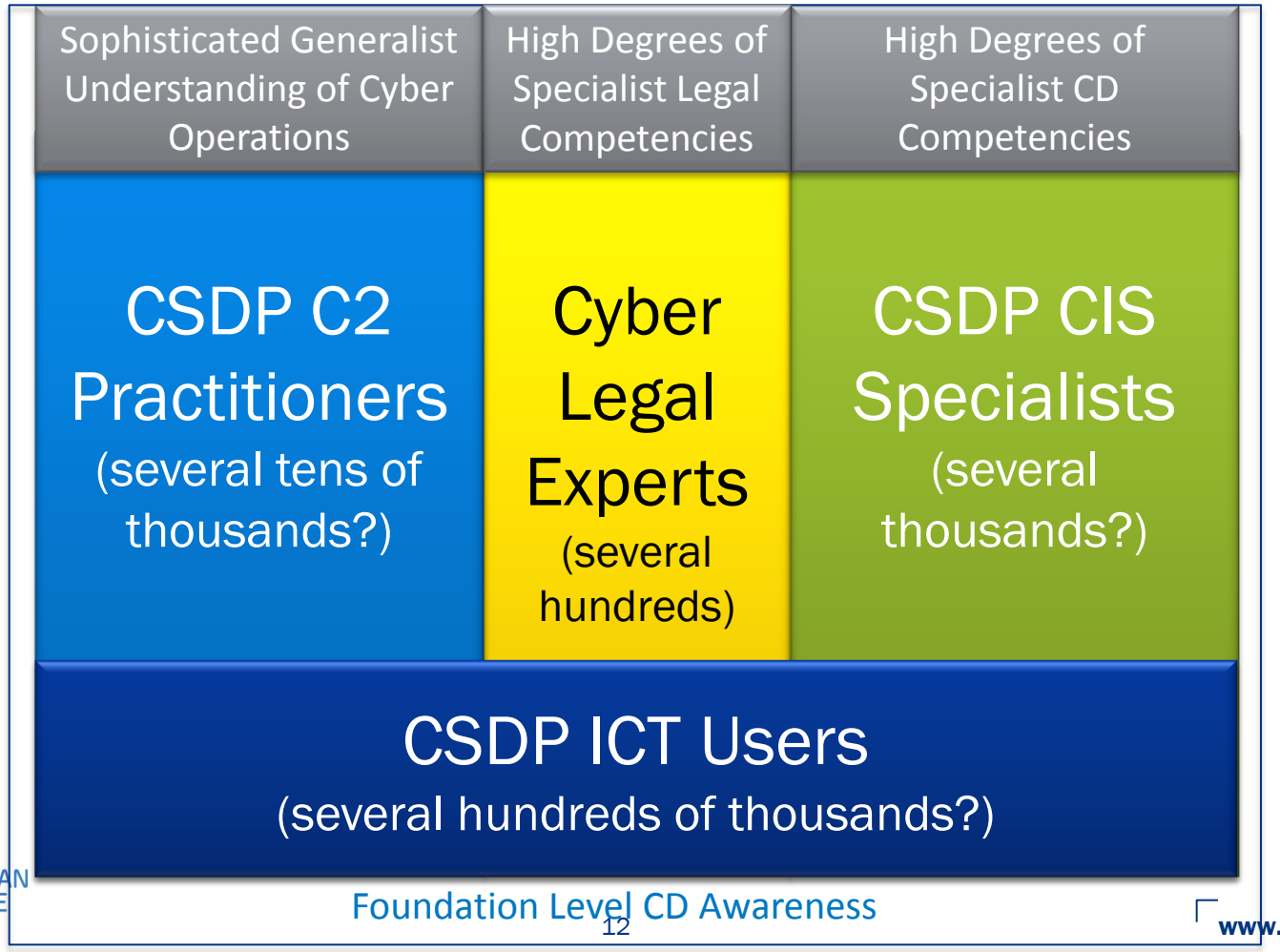
- Define and segment training audiences;
- Describe skills and competencies needed;
- Define learning requirements;
- Scope existing delivery streams and identify gaps;
- Identify multinational training & exercise opportunities;
- Explore synergies with civilian training infrastructures;
- Explore modern training and exercise methods and formats;
- Explore and describe support and training tools required;
- Define comprehensive set of required Cyber Defence courses.

EDA Project: Cyber Defence Training Need Analysis and Training Curriculum



Target Audience Categorisation (1)

Target Audience Boundary: *'Those who set out the policy and strategy for, implement, support, are held at readiness for, and deploy on CSDP Crisis Management Operations, and who have a Cyber Defence learning need.'*



Target Audience Categorisation (2)

Audience Category	Definition	Rationale
CSDP CIS Specialists	**J6 and CD specialist military personnel:** within EU Institutions bearing responsibility for CIS and CD aspects of CSDP; those within pMS Defence entities with similar responsibilities, and those who are held at readiness for, or committed to, the CIS and CD support of CSDP operations/missions	Need for high levels of competency in narrowly-bounded and specialist CD activities
Cyber Legal Experts	**Civilian and military officials :** within EU Institutions and bearing responsibility for legal assessment of activities in cyber space and/or providing related legal advice to decision makers; within pMS MOD HQs and Joint HQs bearing similar CSDP-specific responsibilities, and those who are held at readiness for, or committed to the legal advice for CSDP operations/missions	Need for a sophisticated, but non-specialist understanding of Cyber Operations and high level of competency on their legal implications
CSDP C2 Practitioners	**Civilian officials and military commanders and generalist staff officers:** within EU Institutions and bearing responsibility for CSDP policy, strategy and implementation; within pMS MOD HQs and Joint HQs bearing similar CSDP-specific responsibilities, and those who are held at readiness for, or committed to the C2 of CSDP operations/missions	Need for a sophisticated, but non-specialist understanding of Cyber Operations and their potential impact on military capability effectiveness and operation/mission outcomes
CSDP ICT Users	**All personnel:** in the pMS and the EU Institutions with CSDP-specific roles, and who are held at readiness for, or committed to CSDP operations/missions, who must interact with networked digital data	Need for a foundation-level awareness of CD 'hygiene' principles

Military Training & Exercise Requirements

- Procedural Training & Exercises
  - C2 Practitioners (strategic, operational & tactical level Cyber Defence decision making and dynamic risk management;
  - Cyber Defence Legal Experts (integration of legal advice on cyber in the decision making process);
  - milCERT-Leaders (communication with C2 Practitioners);
  - milCERT (CERT-internal procedures and communication with technical experts);
  - (govCERTs).
- Specialists Training & Exercises (hands-on)
  - CSDP CIS Specialists:
    - System and Network Administrators of military information infrastructures;
    - Mil SOC Operators
    - Cyber Defence Instructors;
    - milCERTs;
    - (govCERTs).
  - Legal Experts (Evaluation of cyber incidents with respect to legal implications).
- ICT Users
  - General Awareness and Threat Awareness
  - Recognition of malfunctions and/or potential incidents (e.g. spearphishing)
  - General “CD Hygiene”
  - Reporting

EDA adhoc Project: CYBER RANGES

Scope of the Ad Hoc project is the Pooling and Sharing of Cyber Ranges:

- Increase availability of existing Cyber Ranges;
- Increase occupation rate/efficiency of existing Cyber Ranges;
- Federate existing and future Cyber Ranges into a Cyber Ranges Network (CRN) for large scale and complex exercises;
- Mainstreaming and Improving Cyber Defence Training, Exercises & Testing at European level.

- cMS: AT, CZ, EE, EL, FI, IE, NL (CH following the development in an associated role); LoI signed 30 May 2013;
- Spiral development in 5 spirals;
- IOC (MoU Increment) planned to be in place mid 2014;
- FOC (Cyber Ranges Network/Federation) April 2018.

Areas for Civil-Military Cooperation on Training and Exercises

- Shared Risk Assessment
- Alignment of civil and military Cyber Training curricula
- Coordination of civil and military Cyber Training/Exercise schedules
- Participation of govCERTs (observer and/or active) in national and multinational military exercises with Cyber Threads, e.g.:
  - EU MILEX/Multilayer Exercise serials
  - CCD COE exercise serials (Locked Shields 2012)
- Participation of military Command & Control structures and milCERTs (observer and/or active) in national and multinational civil crisis management exercises with Cyber Threads, e.g.:
  - DE LÜKEX serials
  - Cyber Europe serials
  - Cyber Atlantic serials
- Shared use of Training & Exercise Platforms

EUROPEAN DEFENCE AGENCY

2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises,
23-24 Sep 2013,
Mr. Wolfgang Roehrig,
Project Officer Cyber Defence

Thank you for your attention

EUROPEAN DEFENCE AGENCY

European Defence Agency
Rue des Drapiers 17-23
B-1050 Brussels (Belgium)

www.eda.europa.eu