Multinational Cyber Defence Capability Development (MNCD2)

Cyber Defence Smart Defence Projects Conference

Lisbon – 28th of April 2016

NATO UNCLASSIFIED

SMART DEFENCE?

'It is a renewed culture of cooperation that encourages Allies to cooperate in ***developing****,* ***acquiring*** *and* ***maintaining*** *military capabilities to undertake the Alliance's essential core tasks agreed in the new NATO strategic concept.'*

'That means ***pooling*** *and* ***sharing*** *capabilities,* ***setting priorities*** *and* ***coordinating efforts*** *better.'*

AGENDA

1. MNCD2 background
2. Project portfolio
   - CIICS
   - CDSA
   - DMCCI
   - CSAT
3. Future developments
4. What's in it for you?
5. Questions

MNCD2 background

PARTICIPATING NATIONS:

PROJECT OFFICE:

NCI AGENCY
NATO Communications and Information Agency
Agence OTAN d'information et de communication

PARTNERING:

NCIRC
NATO COMPUTER INCIDENT RESPONSE CAPABILITY

ALLIED COMMAND TRANSFORMATION

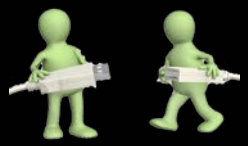
CORE VALUES & PRINCIPLES

Synergy

Efficiency

Industry & academia

Agile



Born-interoperable

Legal framework

€ 2.591.024

2013

Project portfolio

CIICS

- Cyber Information and Incident Coordination System

CDSA

- Cyber Defence Situational Awareness

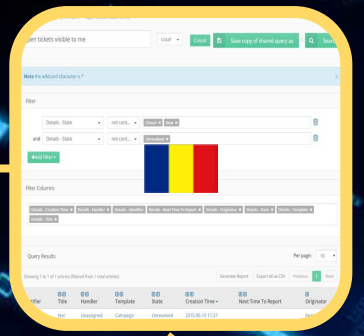
DMCCI

- Distributed Multi-sensor Collection and Correlation Infrastructure

CSAT

- Cyber Security Assessment Team

Project portfolio: CIICS



(Technical) Information Sharing:

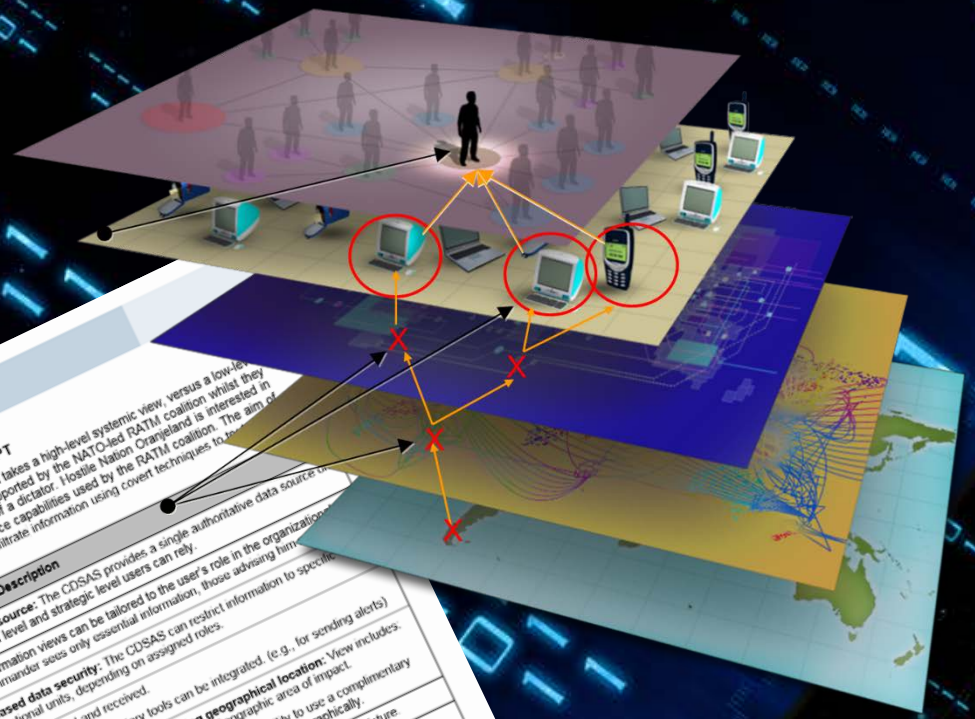
1. Ticketing incident data
2. Threat, vulnerability, other CD data

STAND-ALONE & FEDERATED

Obtain a license?
ncia.mncd2@ncia.nato.int

NATO UNCLASSIFIED

Project portfolio: CDSA



NATO UNCLASSIFIED

SCENARIO 1 SUMMARY – ORANJELAND APT

This scenario is focussed at the strategic level and takes a high-level systemic view versus a low-level technical view. Country Appelestan is being supported by the NATO-led RATM coalition whilst they rebuild a stable government following the fall of a dictator. Hostile Nation Oranjeland is interested in understanding the technologies and intelligence capabilities used by the RATM coalition. The aim of Oranjeland is to infiltrate the network and exfiltrate information using covert techniques to [illegible] detection.

Step	Related use case	Activity Description
1-1	UC10	**Single authoritative data source:** The CDSAS provides a single authoritative data source from which both the operational level and strategic level users can rely.
1-2	UC04	**Hierarchical view:** Information views can be tailored to the user's role in the organization hierarchy (e.g. the commander sees only essential information, those advising him/her more detail).
1-3	UC05	**Unit and location based data security:** The CDSAS can restrict information to specific missions and organizational units, depending on assigned roles.
1-4	UC14, UC09	**Alerting:** Alerts can be triggered and received.
1-5	UC01	**Use a complimentary tool:** Complimentary tools can be integrated. (e.g., for sending alerts)
	UC09	**View current risk list, ordered by impact, showing geographical location:** View includes: impact (to hosts, services, missions), Risk, Likelihood, Geographic area of impact.
1-6	UC03	**Use a complimentary tool:** The system may demonstrate its ability to use a complimentary tool, by interfacing to a separate geo server to display information geographically.
1-7	UC30	**Drill down / roll up:** Drill down for more detail, and roll up to get a higher level picture.
1-8	UC12	**Investigate specific incident:** The system shows the affected service from the host information included in the alert / incident ticket information using system search capability.
1-9	UC11, UC09	**View connections of asset:** Strategic command then identifies services dependent upon the server by bringing up a dependency tree showing services.
		View interconnectivity: Strategic command also checks the logical and physical connections of the asset to see which routes the APT could use, and affected assets.
		Use a complimentary tool: Additional information is gathered from a complementary tool (e.g., Online Computer Forensics (OCF)), and shown in CDSAS.
1-10	UC19	**Collect dependencies:** The system automatically collects and builds the dependency graphs. The user can add, edit, and delete elements of these dependencies.
1-11	UC06	**View dependencies:** Dependent or affected missions, operations, services, and network infrastructure are shown. For courses of action, potential impacts are shown.
1-12	UC08	**Generate and select from Courses of Action:** Options for alternative courses of action are shown with likelihoods, benefits, and costs of the CoAs presented.
1-13	UC07	**View incidents by geographic region:** Check system availability and level of degradation across network. Incident impacts are shown.
1-14	UC02	**Reporting:** System generates reports that are tailorable, and system can inform other actors.

CDSA PROBLEM SPACE

- New missions & priorities
- Constant change
- Constant attack
- Cascading dependencies
- Conflicting information
- Limited resources

Project portfolio: CDSA

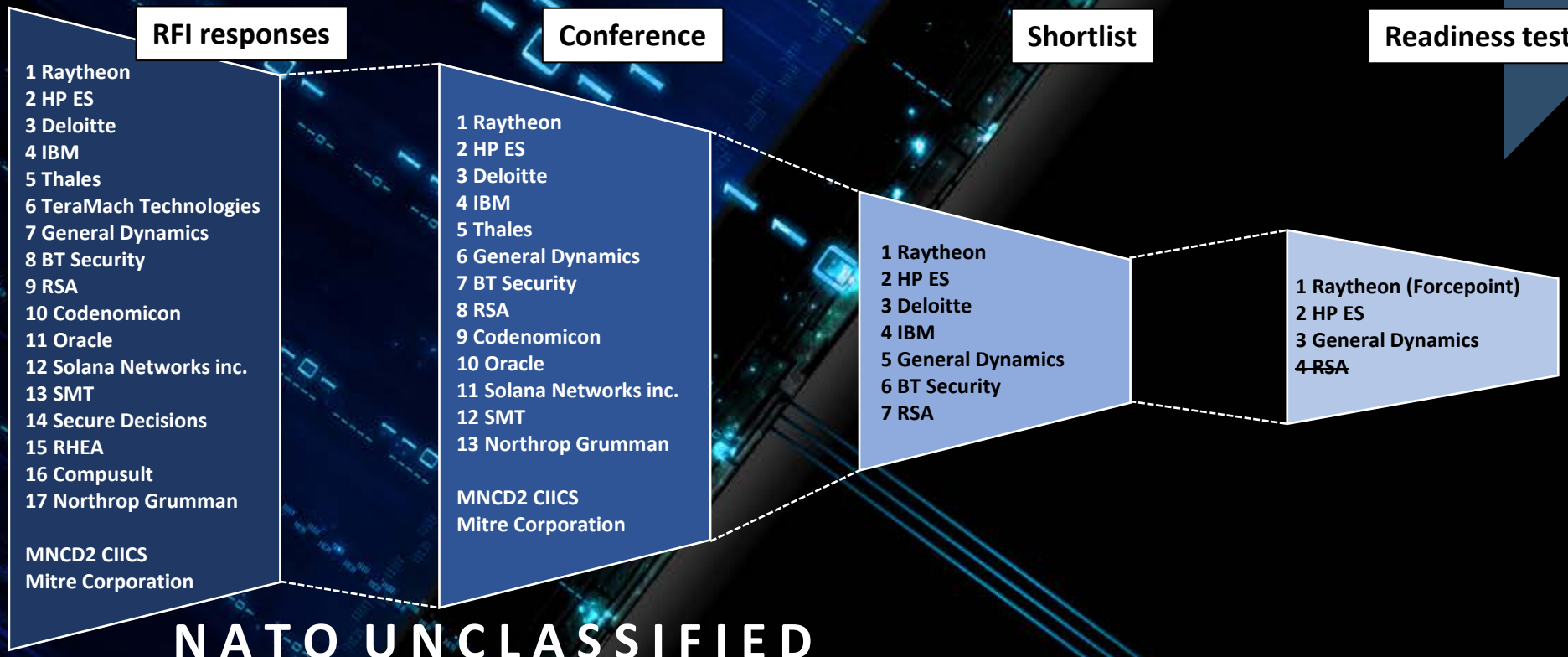
Requirements gathering and use case prioritization (2013-2014)

Request for Information; conference; selection (2015)

Pre-contract testing (Jan-May 2016)

Tailoring and high-fidelity demonstration (May-Nov 2016)

Implementation recommendations; Virtual machines for testing (Jan 2017)



Project portfolio: DMCCI

Targeted
An individual organization, nation state or even specific technology is the focus. Infiltration is not accidental.

Advanced
An unknown, zero day attack that has malware payloads and uses kernel rootkits and evasion-detection technologies.

Persistent
It doesn't stop. It keeps phishing, plugging and probing until it finds a way in to serve malware.

'... any mechanism that gives deeper insight into the unusual, abnormal and potentially malicious in an organization would be a great addition to the arsenal of tools available ...'

- **STORAGE**
- **PARSING**
- **CORRELATION**

Project portfolio: CSAT

Overarching concept

- Goals and objectives
- Governance
- Emulated threats
- Assessment activities
- Assessment lifecycle

CSAT ConOps

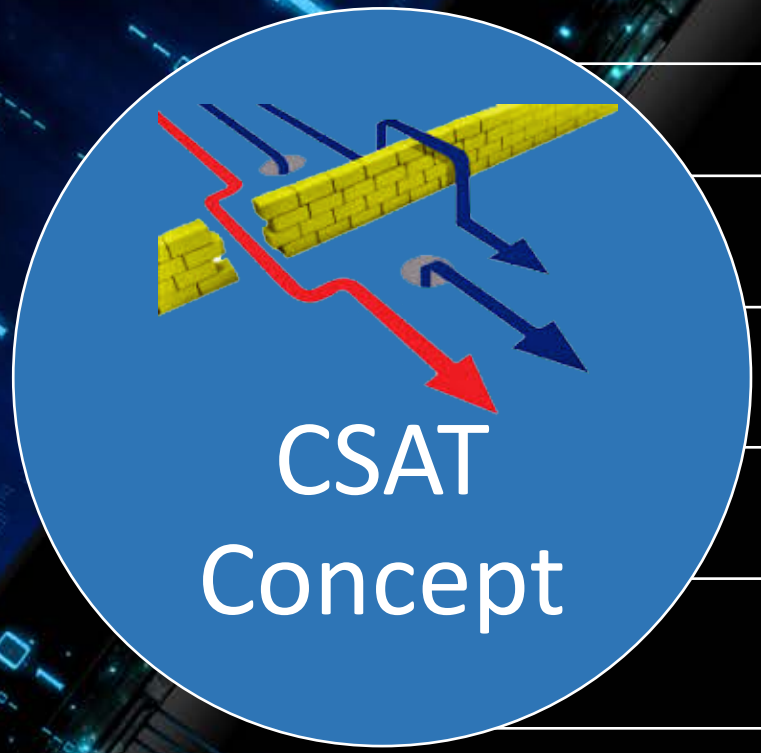
- Organizational structure & staffing
- Facilities & equipment
- Documentation

CORE ConOps

- Services
- Organizational structure & staffing
- Facilities & equipment
- Documentation

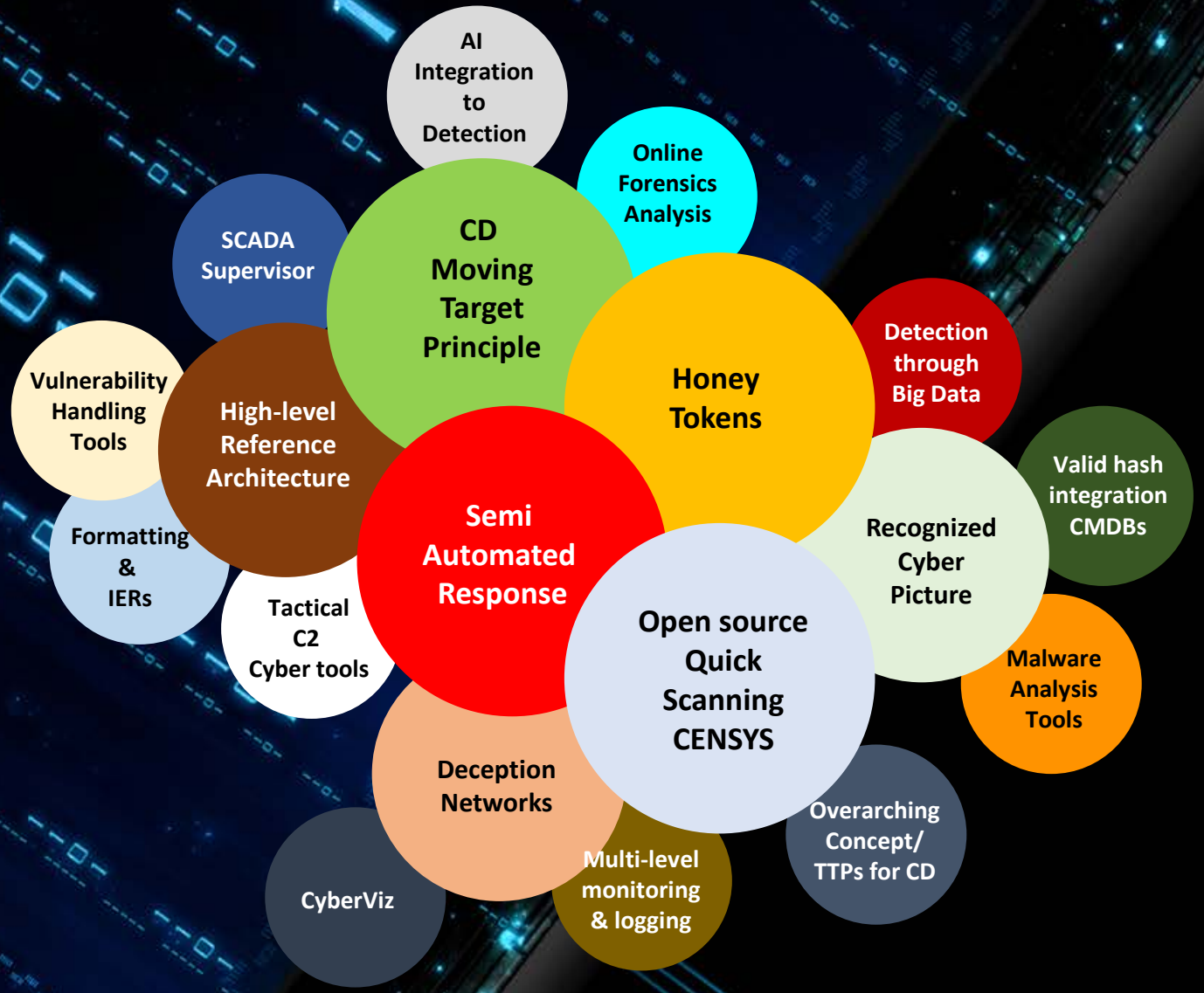
Implementation

- Implementation options
- Implementation plan
- Business case

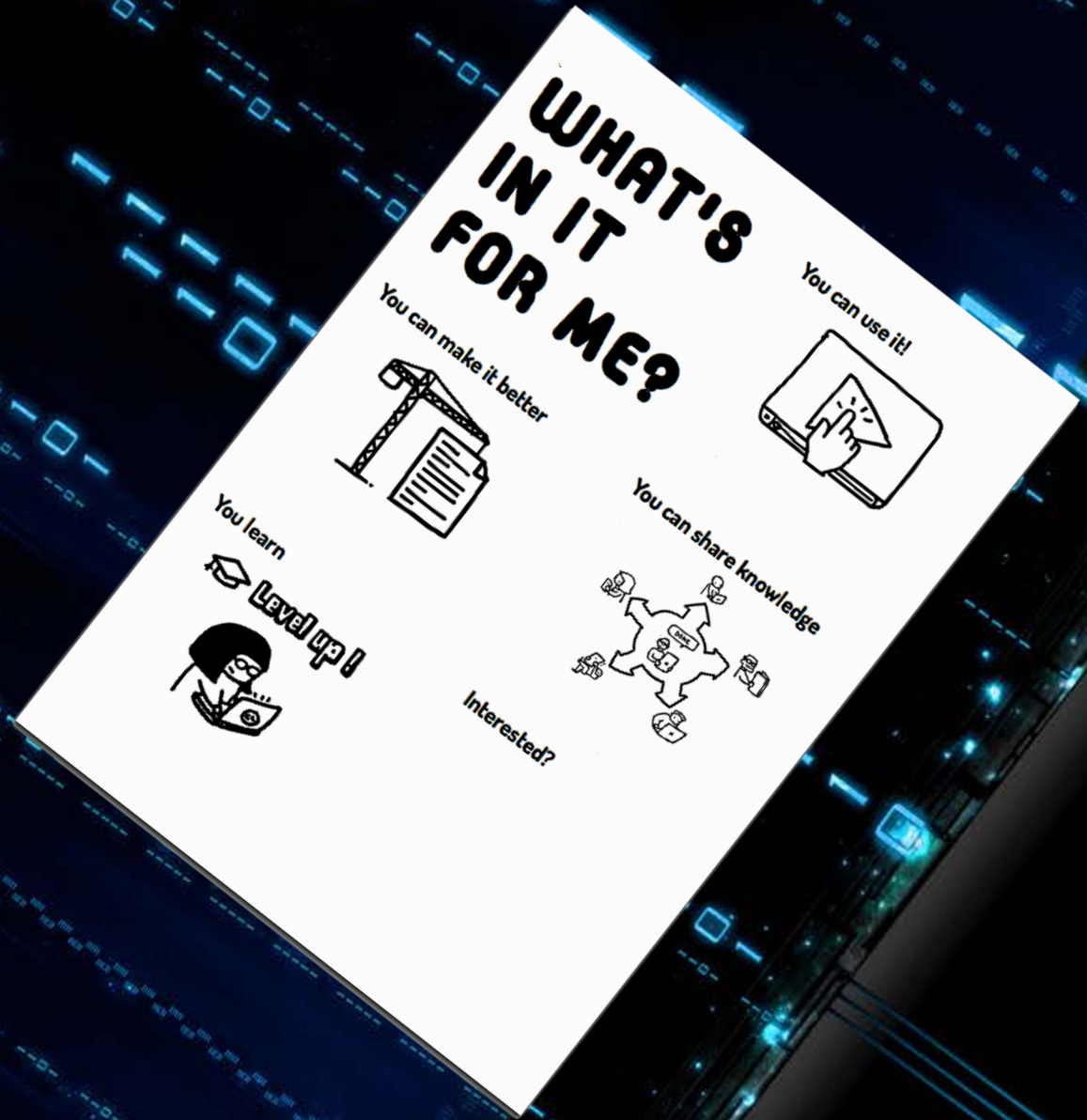


- Independent assessment
- Assess overall effectiveness of security measures
- Testing of Operational CIS
- Demonstrate mission impacts through cyber domain
- Provide mission assurance to stakeholders and senior decision makers
- Improve the ability of users and operators to detect and respond to cyber attacks

New capabilities?



What's in it for you?



- In-depth information
  - Licensed use (CIICS)
- Adopt results (CDSA)
  - Share the other way around

Questions

Management structure