Objectives of the Workshop

- Communicate and clarify the context of Cyber Defence within NATO
- Present ACT’s Cyber Defence R&D Strategy
- Review the technical challenges associated with three areas:
  - Consolidated Information Assurance Picture (CIAP)
  - Dynamic Risk Assessment (DRA)
  - Remote Data Aggregation Capability (RDAC)
- Gather feedback from Industry and establish a dialogue
Industry Charge

★ You are here for a reason. Our reason for this forum, however is for you (Industry) to assist us (NATO) to ensure our priorities are coherent with Industry and for you (Industry) to assist us (NATO) to overcome our capability development challenges.

★ NATO challenges you to step up!
Next Steps...

✿ Continuous dialogue and collaboration through:

✿ Further development of the CD/IA framework
✿ Distributed Networked Battle Lab (DNBL) Testing activities
✿ Others?
Context
Afghan Mission Network

- LCSS Canada
- Caesar (Italy)
- Centrixs ISAF
- Overtask (UK)
- Other Nations
- ISAF Secret

NATO UNCLASSIFIED
NATO should recognize that cyber attacks are a growing threat to the security of the Alliance and its members. Accordingly:

- A **major effort** should be undertaken to increase the monitoring of NATO’s critical network and to assess and furnish remedies to any vulnerabilities that are identified.

- Allies should expand **early warning capabilities** in the form of a NATO-wide network of monitoring nodes and sensors.

- Over time, NATO should plan to mount a **fully adequate array of cyber defence capabilities**, including **passive and active elements**.
Context: NATO Computer Incident Response Capability (NCIRC)

NATO Cyber Defence Management Board
(Senior Management)

CD Co-ordination and Support Centre
(Brussels, Belgium)

NCIRC Technical Centre (FOC)
(Mons, Belgium)

NATO Computer Networks
(~70,000 computers in 58 Locations in 31 Countries)
Context : NCIRC Activities
Context: NCIRC Services

Outputs from NCIRC

- Incident Management (SIEM Services)
- INFOSEC Support (IA, VA, Audit, Compliance)
- Information Assurance
- Response Services (Forensics, Advanced Analysis)

Inputs for NCIRC

- NS
- MS
- NR
- NU

IT systems and infrastructures support NATO’s missions, users and processes

Users

Missions

Processes
Context : NCIRC FOC

✧ NCIRC FOC design will:
  ✧ Support Federated Operations
  ✧ Be implemented with a COTS strategy
    ✧ Employ a standards based approach
    ✧ Incorporate a service oriented paradigm
  ✧ Have a Scalable infrastructure
  ✧ Be transparent to end-users
Context: NCIRC FOC

2002
Programme established

2006
Initial Operating Capability

2009
Final Operating Capability

4Q 2010: Cost estimate.
2Q 2011: Invitations for Bids
4Q 2012: Implementation accomplished

Increment #1 (Core)
✓ Ticketing
✓ Storage
✓ Consolidated Information Assurance Picture v1
✓ Security Incident & Event Management v1
✓ Central Management of all NCIRC functional services
✓ Reference System
Increment #2 (spiral development)
✓ Intrusion Detection / Prevention
✓ Full Packet Capture
✓ Online Vulnerability Assessment
✓ Forensics capabilities

Increment #3 (maturing capabilities)
✓ Dynamic Risk Assessment
✓ Forensics Evidence Management
✓ Alternate capability
Research Strategy
Research Strategy

- Sponsored by ACT
- Develops and validates concepts and specifications
- Done in cooperation with other national entities:
  - Defence Research and Development Canada (DRDC)
  - Délégation Générale pour l‘Armement (DGA)
  - MITRE (US)
- Seeks synergy with other POW:
  - NCIRC Scientific POW
  - Cooperative Cyber Defence Centre of Excellence (CCD COE) POW
NC3A Cyber Defence R&D Activities

Existing Management Systems

Orient

Decide

Observe

Act
NC3A Cyber Defence R&D Activities

- Data Collection and Aggregation
- Connections to external systems
- Normalization and Standardization

Existing Management Systems
NC3A Cyber Defence R&D Activities

- Advanced Detection
- Consolidated IA Picture
- Dynamic Risk Assessment
- Visualization

Processing, Analysis & Visualization
NC3A Cyber Defence R&D Activities

- Recommendation Engine
- Course of Action Analysis
- Decision Processes
NC3A Cyber Defence R&D Activities

- Authorization System
- Active Defence
- Automated Counter-measures

Defensive Response

Existing Management Systems
Challenges
Challenges : CIAP

- Proliferation of source of information that could be potentially useful to derive situational awareness.
Challenges: CIAP

A few examples:

- Network topology with vulnerable and compromised hosts
- Geographical view with cyber layer
- Treemaps to prioritize issues
Challenges : CIAP

- Displaying large computer networks is a challenge:
  - Scalability
    - Should handle hundreds of thousands of nodes and edges
  - Layout algorithm
    - Graph layout has to be automated, but part of the graph must be anchored, leading to stable or fixed layout after small changes
  - Dynamic views
    - Overview, pan & zoom are mandatory features.
    - Ability to click on objects to get more details or fold groups.
    - Ability to move objects manually.
Challenges: DRA

✦ Objective of the DRA capability:
✦ For the CIS users: give them an indication whether a CIS can be relied upon to perform its functions in the environment in which it is used.
✦ For the CIS operators: assist them in the prioritization of the issues related to a change in the risk assessment (e.g., newly discovered vulnerabilities, configuration changes, and active threats detected in the CIS), provide a measure of the urgency of each issue, and assist in determining the proper response.
✦ For other stakeholders: provide them with risk-related information captured throughout the operational lifecycle of a CIS to be used to improve CIS design and implementation, as well as risk management systems and processes for the specific CIS, other NATO CIS, and future CIS.
DRA-Hybrid prototype overview

1. System information
   Vulnerabilities
   Security events

2. Attack paths, Exposed hosts

3. Risk Assessment engine
   (PILAR)

4. Increased Risks
   Potential Responses

External tools

DRA-Hybrid prototype

Modified threats

Risks

DRA User

System description
DRA Market Survey (2009)

Criteria of evaluation grouped into 5 topics:

- Risk Model, value calculation and characterization
- Vulnerability and threats characterization
- Remediation and recommendation features
- Interfaces
- Other considerations

No product was found fully compliant.
Challenges: RDAC

- Limitations of the current (centralized) model;
- Requirement for an intermediate aggregation and filtering layer
- RDAC prototype developed in 2010 aims at demonstrating the concept by capturing and aggregating traffic and logs.
Collaboration with Industry
Workshop Objectives

✧ Continuous dialogue and collaboration through:

✧ Further development of the CD/IA framework
✧ Distributed Networked Battle Lab (DNBL) Testing activities
✧ Others?
Ideas!

Questions?

Next Steps...

Over To You
ACT

✧ Alex SCOTT
  ✧ alex.scott@act.nato.int
  ✧ +1(757)747-3239

✧ LTC Ross SNOW
  ✧ ross.snow@act.nato.int
  ✧ +1(757)747-3299

NC3A

✧ Frederic JORDAN
  ✧ frederic.jordan@nc3a.nato.int
  ✧ +31 703743486

✧ Luc Dandurand
  ✧ luc.dandurand@nc3a.nato.int
  ✧ +31 703743485