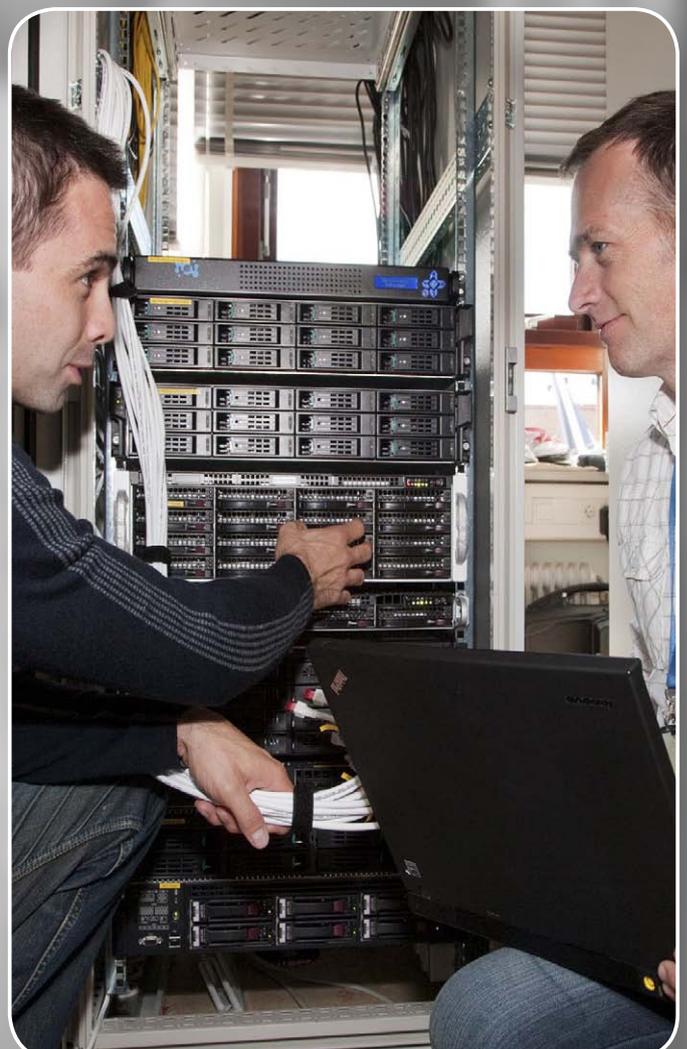


MN CD2

Multinational Cyber Defence Capability Development Initiative



CYBER DEFENCE – TODAY’S CRITICAL CAPABILITY TO ADDRESS THE EMERGING SECURITY CHALLENGES

“We will ensure that NATO has the full range of capabilities necessary to deter and defend against any threat to the safety and security of our populations. Therefore, we will (...) develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations.”

- Strategic Concept for the Defence and Security of The Members of the NATO adopted by Heads of State and Government in Lisbon – Active Engagement, Modern Defence

“Cyber threats are rapidly increasing and evolving in sophistication. In order to ensure NATO’s permanent and unfettered access to cyberspace and integrity of its critical systems, we will take into account the cyber dimension of modern conflicts in NATO’s doctrine and improve its capabilities to detect, assess, prevent, defend and recover in case of a cyber attack against systems of critical importance to the Alli-

work closely with other actors, such as the UN and the EU, as agreed. We have tasked the Council to develop, drawing notably on existing international structures and on the basis of a review of our current policy, a NATO in-depth cyber defence policy by June 2011 and to prepare an action plan for its implementation.”

- LISBON SUMMIT DECLARATION Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon on 20 November 2010

Cyber defence is the application of security measures to protect against and react to cyber attacks against Communication and Information Systems (CIS) infrastructure. It requires the capability to prepare for, prevent, detect, respond to, recover from, and learn lessons from attacks that could affect the confidentiality, integrity and availability of information and supporting system services and resources.

Developing new cyber defence capabilities in a financially constrained time is challenging

Control, Intelligence, Surveillance and Reconnaissance (C4ISR) also through other Multinational (MN) Project Initiatives, such as: MN Integrated Command and Control, MN Alliance Defence Analysis and Planning for Transformation, MN NATO Exercise Tool (including the development of JPECT as an ICC tool), MN Counter-Improvised Explosive Devices and MN Civil Military Interaction.

WHAT IS NC3A?

The NATO Consultation, Command and Control Agency (NC3A) is a NATO agency that shares the legal personality of NATO. Our Charter was approved by the North Atlantic Council, and NC3A operates under a 100% customer funding regime. NC3A is part of the NATO C3 Organization, along with the NATO C3 Board and NATO Communication and Information Systems (CIS) Services Agency (NCSA).

The NC3A’s mission is to enable NATO’s success through the unbiased provision of comprehensive Consultation, Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) capabilities.

NC3A is the Host Nation for all Cyber Defence capability development in NATO and has developed over the years a recognized experience in the design and implementation of Cyber Defence solutions and Computer Incident Response Capabilities (CIRCs) through the NATO CIRC (NCIRC) initial operational capability, and more recently the NCIRC full operational capability and the Bi-strategic Commands Automated Information System Intrusion Detection Systems projects. NC3A plays a unique role in the NATO Cyber Defence community through capability delivery and scientific support (Fig 1).

WHY THE MN CYBER DEFENCE CAPABILITY DEVELOPMENT INITIATIVE?

The overall objective of the initiative is to facilitate the success of member Nations (with support from national industries) in producing capabilities for an effective operational response to the threat of cyber attacks while promoting multilateral collaboration.

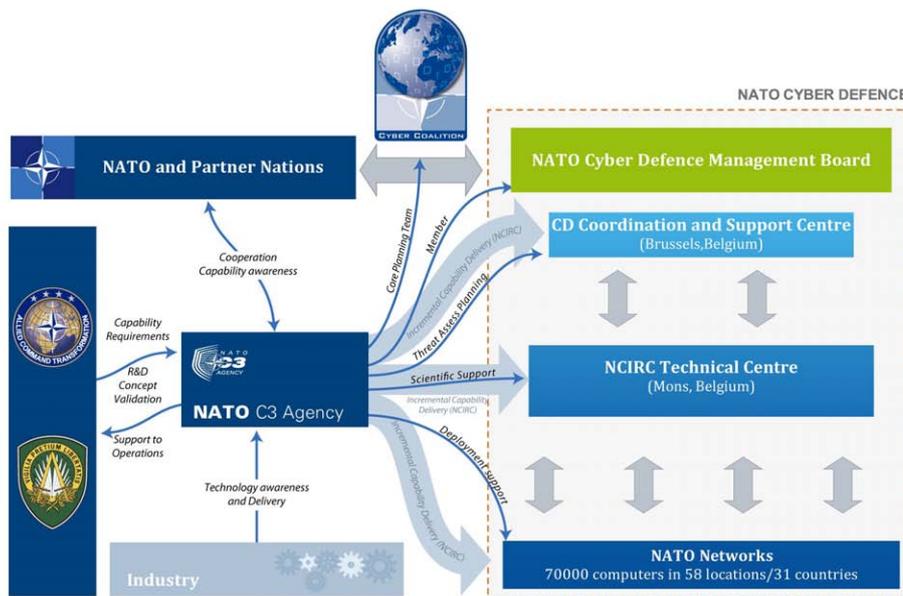


Figure 1 NC3A’s role in NATO Cyber Defence

ance. We will strive in particular to accelerate NATO Computer Incident Response Capability (NCIRC) to Full Operational Capability (FOC) by 2012 and the bringing of all NATO bodies under centralised cyber protection. We will use NATO’s defence planning processes in order to promote the development of Allies’ cyber defence capabilities, to assist individual Allies upon request, and to optimise information sharing, collaboration and interoperability. To address the security risks emanating from cyberspace, we will

and requires a smart and efficient approach to quickly achieve the necessary ability across both NATO and NATO Nations. Cooperation, coordination and sharing of effort could ensure a rapid and interoperable capability development.

NC3A proposes to address the multiple areas of Consultation, Command,

The initiative aims to leverage common interests and national activities from a coalition of willing Nations to:

- jointly research and develop an agreed subset of interoperable Cyber Defence capabilities; and
- deliver an assured capability for interoperability of Cyber Defence information to support multinational and federated operations.

WHAT SERVICES WOULD NATIONS GET THROUGH THE INITIATIVE?

Coordination in Capability Development

The MN CD2 is presented to the Cyber Defence Management Board (CDMB) to seek overall coordination with Cyber Defence Action Plan. The initiative would allow a coalition of willing Nations to leverage common interests and national activities to:

- coordinate their national Cyber Defence scientific and technical activities;
- promote multilateral collaboration and technical information sharing;
- develop interoperable Cyber Defence capability; and

- enable joint acquisition schemes.

To support this coordination, the Cyber Defence capability breakdown currently being developed by NC3A on behalf of ACT is provided at Fig 2. The capability breakdown gives a clear picture of the operational aspects of cyber defence and divides the effort into manageable pieces that can be addressed independently. Development of maturity levels for the capabilities will further support the development of coherent capabilities.

Governance

The MN CD2 initiative would be established with a management structure executing the primary coordination and interface activities required to align the various national and NATO efforts. One of the main objectives would be to maintain flexibility and agility in the programme.

As a minimum, the MN CD2 management structure should provide:

- executive guidance;
- strategic vision for the MN CD2 programme and related projects; and
- policy for programme controls.

Technical & Engineering forum

The initiative would provide a forum to:

- consolidate requirements from the Cyber Defence operational community;
- provide recommendations and guidance on the implementation roadmap of interoperable cyber defence capabilities; and
- liaise with Cyber Defence civil entities and national industries.

Test & Experimentation

The MN CD2 initiative could employ the Distributed Networked Battle Labs* (DNBL) framework to support Test & Experimentation activities so as to enable collaborative experimentation, testing, verification and validation to achieve interoperable Cyber Defence capabilities in advance of operational testing. Within this capacity, the MN CD2 initiative could also provide support to training as well as to the cyber coalition exercises.

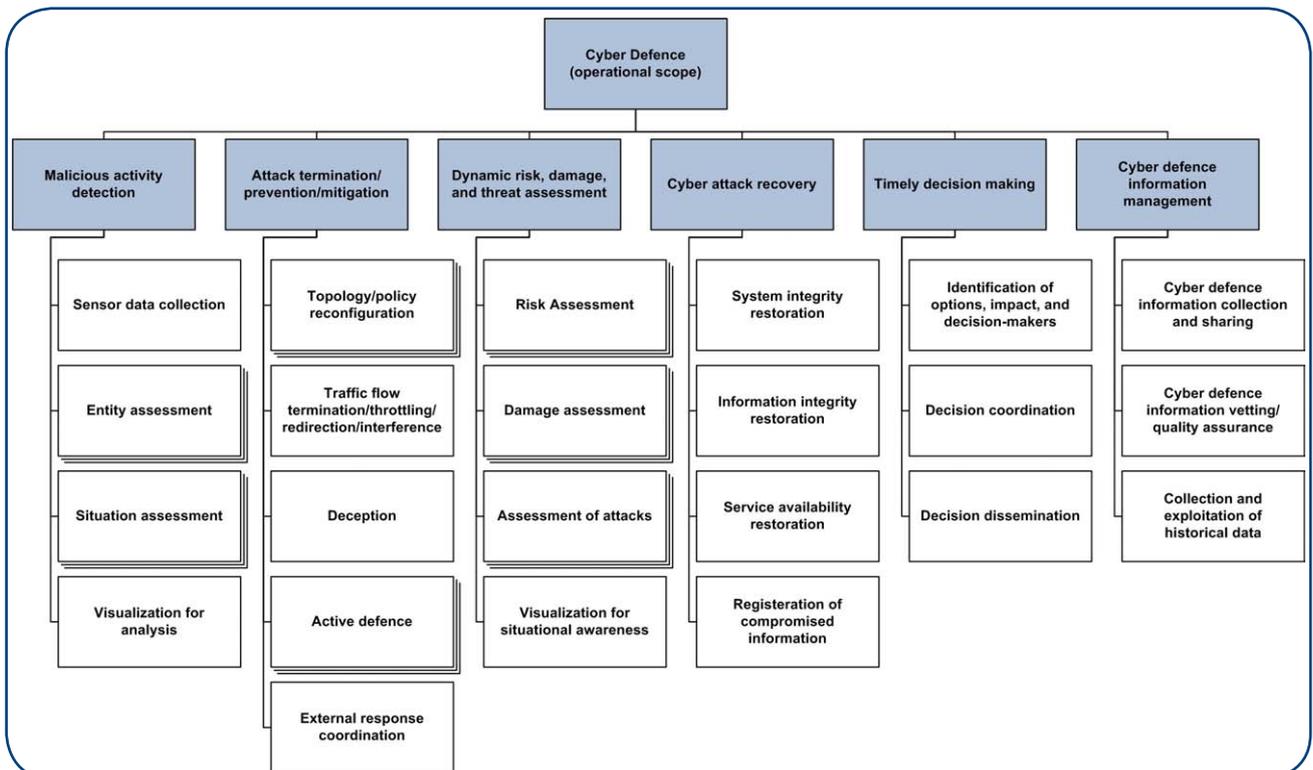


Figure 2 Cyber Defence Capabilities

* Distributed Networked Battle Labs* (DNBL) is a value network developed to host communities of interest, as for interoperability testing, modelling and simulation, training, cyber defence, etc

HOW CAN NC3A HELP?

NC3A as an executive agency could play a facilitation and coordination role and act as an unbiased partner to:

- pool national scientific and technical resources; and
- interact with the existing Cyber-Defence entities within NATO on requirements for interoperability.

WHAT IS THE LEGAL CONSTRUCT OF COOPERATION WITH NC3A?

NC3A offers flexible legal solutions to respond quickly to the needs of Nations. Participation to the Multinational Cyber Defence is open both to Nations that have signed the NC3A C4ISR Memorandum of Agreement (MOA) and those that have not yet done so.

The MOA is a framework agreement covering full cooperation on C4ISR activities, which defines in advance the terms of the collaboration. Specific projects are defined in Technical/Implementing Arrangements which also set out the financial terms and which refer, for the rest, to the C4ISR MOA. Technical/Implementing Arrangements can be issued quickly since the general terms of the collaboration have already been defined in the C4ISR MOA. Multiple Technical/Implementing Agreements can be added to the C4ISR MOA, to cover both multinational and bilateral cooperation.

Currently NC3A has signed C4ISR MOAs with nine NATO nations and two PfP nations. NC3A is negotiating 14 additional MOAs with other Nations. Note that the C4ISR MOA is to be distinguished from the Memoranda of Understanding that the National Security Authorities (NSAs) are establishing with the Cyber Defence Management Authority (CDMA) at NATO, and which aim at enabling the conduct of information exchanges and cyber defence services and related activities between the NSAs and the NATO CDMA.

Nations that have not signed a C4ISR MOA with NC3A may also participate in the Multinational Cyber Defence initiative after putting in place a task-specific arrangement such as a letter of agreement. Depending on the scope of the project, this legal framework can be put in place in a short period of time.

WHAT IS THE COST FOR PARTICIPANTS?

Under the customer funding regime, NC3A is mandated to achieve financial break-even. This means that NC3A has to cover the cost of its resources (staff, equipment and facility use) allocated to the project as well as for any work contracted to industry.

The MN CD would be supported by contributions from members of the programme. Annual fees would cover the work of the Agency as executing agent which would facilitate and organize the programme on behalf of the members. The basic activities to be covered would include periodic reporting of activity, progress on annual POW for the programme, briefings, organising and facilitating meetings. Moreover, specific functional area Technical Agreements could be established with members to detail a specific scope of activities.

WHAT IS NEXT?

The MN CD2 Roadmap Planning includes:

7th Feb 2011	1st MN CD2 Workshop
Mar-Apr 2011	Receipt of the Statements of Interests (SOIs)
May-Jun 2011	Focused meetings with Nations 1st stage
Jul-Aug 2011	Focused meetings with Nations 2nd stage
Sep-Oct 2011	2nd MN CD2 Workshop
Oct-Nov 2011	Letters of Agreements signed, Programme of Work (POW) defined
Dec 2011	Initial MN CD2 Project Office established

Subsequently: Annual MN CD2 Project Meetings

All the aspects of MN Cooperation Development of C4ISR capabilities are presented in the Multinational Cooperation Development Brochure at:

<http://www.nc3a.nato.int/About/Pages/Publications.aspx>

For further information please contact:

Directorate Sponsor Account NATO&Nations
Mrs Agata SZYDELKO
 Principal Business Manager
 Tel: +32 2 707 8241
 e-mail: agata.szydelko@nc3a.nato.int

Mr Frederic JORDAN
 MN CD2 Project Manager
 Tel: +31 70 374 34 86
 e-mail: frederic.jordan@nc3a.nato.int

Mr Geir HALLINGSTAD
 MN CD2 Deputy Project Manager
 Tel: +31 70 374 37 42
 e-mail: geir.hallingstad@nc3a.nato.int



Location Brussels
 Boulevard Léopold III, B-1110 Brussels, Belgium
 Telephone +32 (0)2 707 4111

Location The Hague
 P.O. Box 174, 2501 CD The Hague, The Netherlands
 Telephone +31 (0)70 374 3000
www.nc3a.nato.int



NATO C3 Agency
 Sponsor Account NATO and Nations (DSA N&N)
 Telephone +32 (0)2 707 8547
 Fax +32(0)2 707 8770
 Email: DSANN@nc3a.nato.int
www.nc3a.nato.int/Opportunities