MULTINATIONAL

MN CD2 - Cyber Defence Capability Development

Supported by

NCI AGENCY

The establishment of the Multinational Cyber Defence Capability Development project (MN CD2) by five founding Nations - Canada, Denmark, Netherlands, Norway and Romania, marks an important step in the support provided by the NCI Agency to the development of NATO and national Cyber Defence capabilities. Upon the establishment of the project, further Nations are also welcome to join in accordance with the MN CD2 Memorandum of Understanding (MoU).

Through this multinational project the Nations have an opportunity to work together to develop new Cyber Defence capabilities. Capability development activities will be conducted as specific work packages organized under a yearly Programme of Work (PoW). Nations can decide what work package they want to be part of and can also recommend new work packages for inclusion into the MN CD2 PoW. Each work package will only be governed by the decisions of its participants.

MN CD2 is fully aligned with the Allied Command Transformation (ACT) Cyber Defence Programme of Work and leverages the experience the NCI Agency has developed as the Host Nation for the NATO Computer Incident Response Capability (NCIRC) Initial Operational Capability (IOC) and Full Operational Capability (FOC) projects. MN CD2 is also in line with NATO Smart Defence efforts as a Tier 1 project in the Smart Defence Proposal Database, with the C3 Board as the Sponsor Committee.

What are the objectives of the Multinational Cyber Defence Capability Development Initiative?

The overall objective of the MN CD2 project is to facilitate the development of national Cyber Defence capabilities through a collaborative effort. It provides a vehicle for the Nations to focus their efforts in areas of their choice, and within any monetary constraints, while maintaining an overall approach and achieving a well-balanced Cyber Defence capability.

There are several benefits from a multinational effort in developing Cyber Defence capabilities. First, there is a potential for cost-savings through joint research, development, and specification of a given capability. In addition to cost savings, the quality of the result will likely be better since the effort receives more diverse exposure. Furthermore, there is potential cost savings in joint procurement due to economies of scale, and even with individual procurement in a nation, the cost is reduced due to the ability to use the common procurement requirements. Finally, a capability developed in this way is, by default, "born interoperable" and potentially saving significant investments in the long term, rather than the often used ad-hoc and most of the time costly solutions that provide limited functionality.

Cyber Defence – Today's critical capability to address 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." - November 2010 - Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization adopted by Heads of State and Government at the NATO Summit in Lisbon – Active Engagement, Modern Defence.

"Smart Defence is at the heart of this new approach. The development and deployment of defence capabilities is first and foremost a national responsibility. But as technology grows more expensive, and defence budgets are under pressure, there are key capabilities which many Allies can only obtain if they work together to develop and acquire them. We therefore welcome the decisions of Allies to take forward specific multinational projects, including for better protection of our forces, better surveillance and better training. These projects will deliver improved operational effectiveness, economies of scale, and closer connections between our forces. They will also provide experience for more such Smart Defence projects in future" – May 2012 - Chicago Summit Declaration on Defence Capabilities: Toward NATO Forces 2020.

Cyber Defence is the application of security measures to protect and react to cyber-attacks against Communication and Information Systems (CIS) infrastructure. It requires capabilities to prepare, prevent, detect, respond, recover, and learn lessons from attacks that could affect the confidentiality, integrity and availability of information as well as supporting system services and resources. Developing a new cyber defence capability in a financially constrained time is challenging, and requires a smart and efficient approach to quickly realize the necessary ability across NATO and NATO Nations. Cooperation, coordination and sharing of effort using an established collaboration platform ensures a rapid and interoperable capability development.

What services can Nations get through the MN CD2 Initiative?

Governance

This programme is established with a management structure executing the primary coordination and interface activities required to align the various national and NATO efforts. This includes coordination of all facets of capability development including research, design and engineering, testing and experimentation, verification, procurement preparation, and procurement. In addition, the programme ensures interoperability through validation and/or certification of the capabilities and in particular the interoperability interfaces. One of the main objectives is to maintain flexibility and agility in the MN CD2 project.

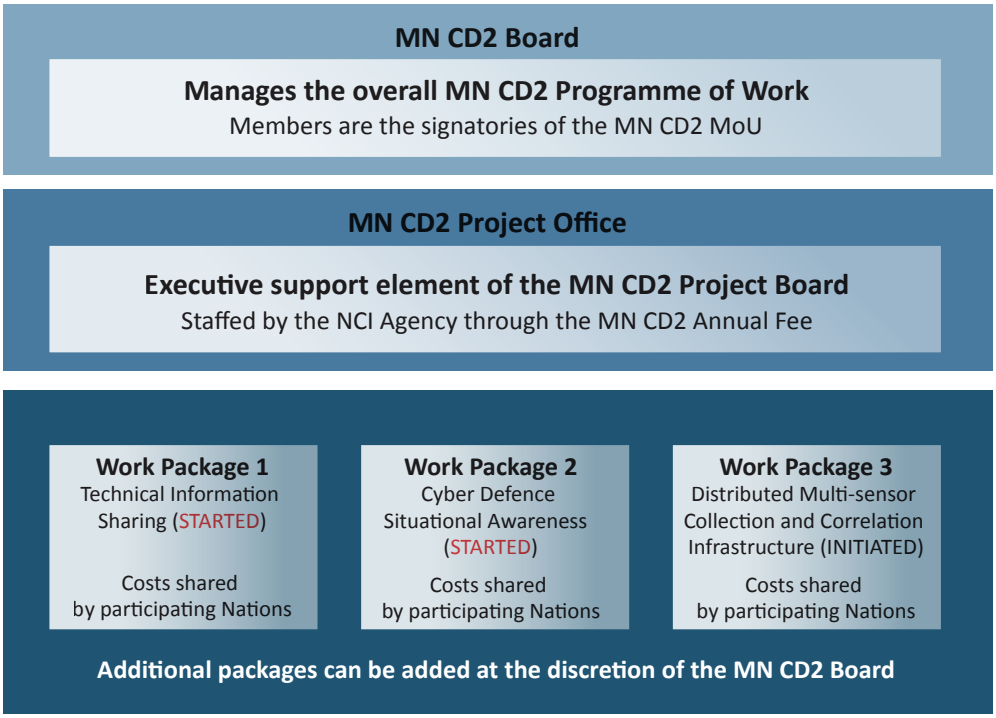
Coordination and Joint Execution

The MN CD2 Initiative allows a coalition of willing Nations to leverage common interests and national activities to:

- Conduct joint development and acquisition of interoperable Cyber Defence capabilities;
- Coordinate national Cyber Defence scientific and technical activities;
- Promote multilateral collaboration and information sharing.

In order to support Cyber Defence capability development, ACT and the NCI Agency have developed a Cyber Defence capability framework which provides a clear overview of the Cyber Defence technical capabilities. This framework provides a structured way for the MN CD2 participants to assess the possible capability gaps in their Nations and come up with joint development plans.

MN CD2 Governance and Management Model



Technical and Engineering forum

The MN CD2 Initiative will 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;
- Liaise with Cyber Defence civil entities and national industries.

Test & Experimentation

A key element of joint capability development is an experimentation and validation infrastructure that ensures that new Cyber Defence capabilities are validated and interoperable as required.

From experience gained in other technical areas, the vision is to establish a federated and shared experimentation and validation infrastructure which would possibly borrow concepts from other federated capabilities like the Distributed Networked Battle Labs (DNBL) Framework.

Legal Framework

The primary focus of the MN CD2 MoU is to establish the multinational project governance and management framework as well as to facilitate the execution of the multi-year PoW. The MoU will be supplemented by Task Orders detailing the exact scope and execution of the respective Work Packages. The MN CD2 MoU is a very flexible legal tool which allows any NATO Nation to join the MN CD2 initiative at any time. It also includes the possibility for participating Nations to offer Contributions in support of the execution of any work package.

Management Model

The MN CD2 Governance and Management model is presented above. The MN CD2 Board is a group composed of the Work Package Participants and the NCI Agency. The MN CD2 Project Office is the executive staff of the MN CD2 Board responsible for carrying out the work related to the MN CD2 coordination, fund management, administration, and organization of the work packages into a 3-year Rolling Plan, as well as providing secretarial support to the MN CD2 Board, including preparation of the MN CD2 Board meetings. The work packages are services/deliverables and/or equipment to be delivered at the request of one or more participants, in the MN CD2 framework.

Current topics for MN CD2

Through an analysis of existing capabilities and needs, the following three work packages have been identified as initial targets for MN CD2:

- WP1: Technical Information Sharing Interfaces;
- WP2: Situational Awareness;
- WP3: Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI).

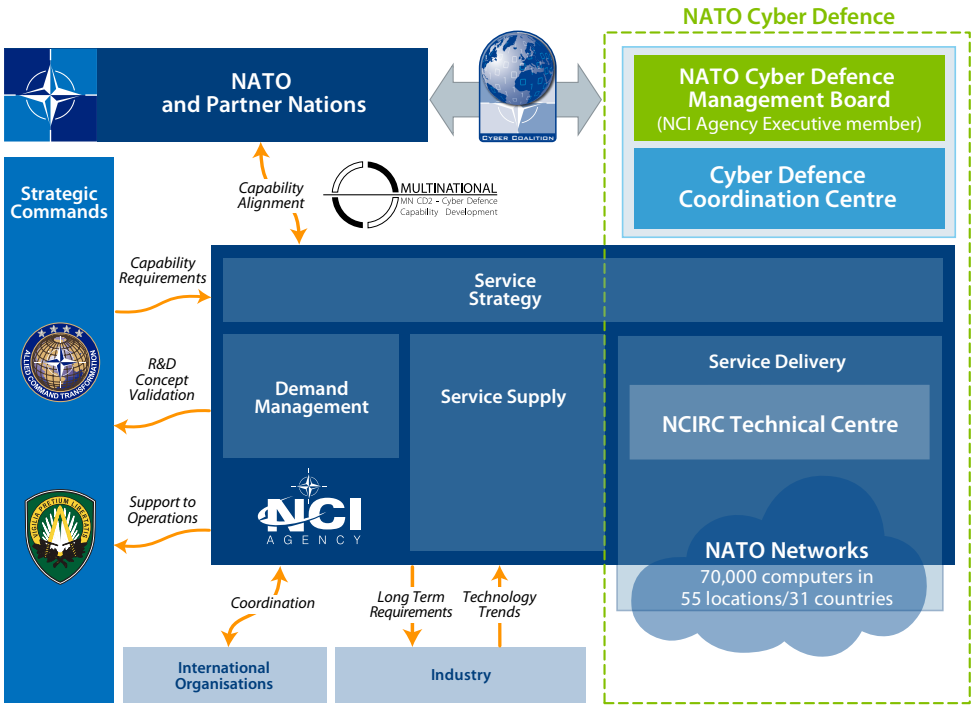
Additional work packages will be considered depending on Nation's priorities and strategic directions.

About the NCI Agency

The NATO Communications and Information (NCI) Agency connects forces, NATO and Nations, where and when required by providing interoperable Communications and Information Systems and services.

The NCI Agency is the provider of NATO-wide IT services and state-of-the-art C4ISR capabilities including Cyber and Missile Defence. In strengthening the Alliance, the Agency applies industry best practices and provides a full life-cycle approach: from analysis and concept development, through experimentation and Capability Development, to operations and maintenance for both missions and exercises. The NCI Agency is a key pillar of NATO Secretary General's Smart Defence and Connected Forces initiatives.

The Agency was established on 1 July 2012, as part of a broader NATO reform, through the merger of the NATO Consultation, Command and Control Agency (NC3A), the NATO Air Command and Control System Management Agency (NACMA), the NATO Communication and Information Systems Services Agency (NCSA - except Deployable CIS), the Active Layered Theatre Ballistic Missile Defence (ALTBMD) Programme Office and the elements of NATO Headquarters Information and Communication Technology Service.



NCI Agency support to MN CD2

Under the MN CD2 legal framework the NCI Agency acts as an enabler and a co-ordination agent and is fully committed to the success of the MN CD2 Initiative.

NCI Agency support will span from running the MN CD2 Project Office to providing project management, contracting, legal and technical support to any work package under execution.

The NCI Agency will also facilitate discussions between MN CD2 and the NATO Cyber Defence community and will strive to ensure that MN CD2 work packages leverage any relevant activity conducted under NATO common funding so as to avoid duplication or overlap of activities.

NCI Agency funding model for MN CD2

Under the customer funding regime, the NCI Agency is mandated to achieve financial breakeven. This means that the NCI Agency has to cover the cost of its resources (staff, equipment and facility use) allocated to the project as well as any work contracted to industry. The MN CD2 project is supported by contributions from projects participants. Annual fees cover the work of the Agency as executing agent, which facilitates and organizes the programme on behalf of the members. The basic activities to be covered include periodic reporting, progress on annual PoW, briefings, organising and facilitating meetings. The Task Orders are agreed to detail a specific scope of activities and address the execution of the MN CD2 PoW.

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

Bâtiment Z
Avenue du Bourget 140
1110 Brussels
Belgium
www.ncia.nato.int

NCI AGENCY

For further information please contact:

Ms Agata SZYDELKO
Demand Management
Principal Account Manager MN&ORG
Tel: +32 2 707 8241
e-mail: agata.szydelko@ncia.nato.int