TOWARDS MULTI-NATIONAL CAPABILITY DEVELOPMENT IN CYBER DEFENCE

Frederic JORDAN and Geir HALLINGSTAD

Abstract: With NATO and the NATO Nations being heavily dependent on their communication and information systems, ensuring their proper operation is a critical task. Establishing appropriate cyber defence capabilities is a major endeavour and one which a lot of nations are currently putting increased focus on. The multi-national approach to cyber defence capability development presented in this paper is an approach to leverage the common interest nations have in this area to efficiently develop high-quality capabilities through cooperation and coordination. The paper goes on to present initial topics where the approach could be immediately leveraged, including information sharing, situational awareness, and distributed sensor collection and coordination capabilities. The paper concludes that this way forward could significantly improve our cyber defence capabilities and contribute to the overall security of the Alliance.

Keywords: Situational awareness, information sharing, distributed sensor networks, correlation infrastructure, CERT, NATO Computer Incident Response Capability, NCIRC, experimentation, validation.

Introduction

NATO and NATO Nations are heavily dependent on communication and information systems (CIS), which, to varying degrees, are vulnerable to threats from different adversaries through their network connections and also from access by authorized and/or unauthorized insiders. A disruption or an intrusion into a CIS could seriously harm the functions of the Alliance, especially if it affects NATO or the NATO Nations' classified networks. Even if unauthorized access to the secure networks is successfully denied, cyber-attacks on critical infrastructure could degrade the functioning of national security, law and order, and lead to disturbances and losses in economic systems.

Cyber defence is the application of security measures to protect against, and react to cyber-attacks against communications and command systems infrastructure. It re-

quires capabilities to prepare for, prevent, detect, respond to, recover from, and learn lessons from attacks that could affect the confidentiality, integrity and availability of information as well as supporting system services and resources.

However, establishing an effective cyber defence capability is a new and major endeavour. Many nations have just started to consider cyber defence as a significant defence capability. Building a cyber defence capability also represents a high level of technical complexity, many procedural challenges, as well as an urgent requirement which makes the implementation even more challenging.

This article presents a multi-national cyber defence capability development approach. The potential gain from leveraging common requirements and resources is high, as NATO and the NATO Nations have varying levels of capabilities in this area and limited funding to develop the capabilities. The article will address some of the fundamentals for multi-national cooperation, as well as some of the cyber defence topics with high probability for immediate success.

Background

The analysis and recommendations of the group of experts on a new strategic concept for NATO [1] highlighted that "NATO must accelerate efforts to respond to the danger of cyber-attacks by protecting its own communications and command systems, helping Allies to improve their ability to prevent and recover from attacks, and developing an array of cyber defence capabilities aimed at effective detection and deterrence." The new strategic concept,[2] approved by the heads of state at the Lisbon summit in November 2010, highlights the new threats and emerging security challenges as one of the key aspects to address in order to keep the Alliance effective. The further development of the cyber defence capability is listed as necessary to ensure the safety and security of the population. Furthermore, it is stated that cyber defence shall be included in the NATO defence planning process to enhance and coordinate NATO and national cyber defence capabilities. Another section of the strategic concept recognizes the need to "develop and operate capabilities jointly for reasons of cost effectiveness and as a manifestation of solidarity", pointing to the need for multi-national cooperation.

Following this direction, the Defence Ministers adopted in June 2011 the revised NATO Policy on Cyber Defence which sets out a clear vision on NATO's efforts in cyber defence throughout the Alliance and also establishes the principles for NATO's cyber defence cooperation with partner countries, international organizations, the private sector, and academia. Allies are also encouraged to work more closely with their national defence industrial leaders to pursue collaborative and multinational projects

wherever possible, and to seek out opportunities for consolidations and mergers to develop cyber defence capabilities.

The political direction is clear both with respect to the significance of establishing a solid, comprehensive cyber defence capability, and to the importance of cooperation between nations to be cost-effective and efficient in order to be able to quickly share information about cyber incidents, to rapidly react to cyber threats and attacks against Alliance CIS.

Establishing multi-national capability development

The objective of a multinational cyber defence capability development (MNCD2) programme will be to facilitate the development of cyber defence capabilities in the nations and NATO through a collaborative effort. It will thus provide 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.

This programme will be established with a management structure executing the primary coordination and interface activities required to align the various national and NATO efforts. This will include coordination of all facets of capability development including research, design and engineering, testing and experimentation, verification, procurement preparation, and procurement. In addition, the programme will ensure interoperability through validation and/or certification of the capabilities and in particular the interoperability interfaces.

NATO already facilitates coordinated research through the Research and Technology Organisation (RTO), which covers a wide spectrum of activities. Each nation usually participates in technical activities based on own funding in already established national projects. This structure, therefore, primarily helps to coordinate on-going projects. This is sometimes problematic as nations may have different objectives, and when participating in activities over time, the individual national objectives may change and make cooperation and coordination more difficult. Furthermore, the RTO activities are limited to research and do not include any other components of capability development.

Within NATO, there is currently no programme for Nations to establish a viable cyber defence capability. The defence planning process is there to help establish the capability requirements across the nations, and the RTO can facilitate research coordination. However, there is no multi-national approach in NATO that will ensure pull-through from requirements analysis, over prioritization and research, to acquisition and final implementation.

To reap full benefit of the common interests in achieving cyber defence capabilities, a greater effort is required to align national activities in addition to coordination. This requires a dedicated structure to continually monitor national requirements and efforts and to coordinate and strategize on the way forward so as to ensure that there is no dispersion of efforts and that the tempo of research and development activities is in line with the assessment of the risks against NATO and national CIS. Establishing this structure and facilitating the coordinated development of cyber defence capabilities is the purpose of the MNCD2 programme.

However, joint plans are often difficult to establish due to the lack of a common reference framework and terminology that one can use as a foundation for coordinated capability development. Likewise, there are no metrics defined so as to assess how much of a given specific cyber defence capability is needed within NATO (or nationally), which could potentially lead to inefficient use of scarce resources.

Advantages of Multinational Effort

There are several benefits from a multi-national 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 has 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,

Framework for Cyber Defence Capabilities

In order to aid in cyber defence capability development, Allied Command Transformation (ACT) and the NATO C3 Agency (NC3A) have initiated the development of a cyber defence capability framework.[3] This document aims to clarify the scope of cyber defence, establish a common taxonomy, provide a foundation for multi-national capability development, and identify interoperability interfaces for cyber defence to enable federated cyber defence.

The capability framework contains a hierarchical breakdown of the cyber defence capability, meaning that each capability is broken down into manageable components and gives a structured way to determine what NATO and the nations are working on, and which capabilities need to be addressed further. The first level cyber defence capabilities identified in the capability framework are:

- Malicious activity detection;
- Attack termination/prevention/mitigation;
- Dynamic risk, damage and attack assessment;
- Cyber-attack recovery;
- Timely decision making;
- Cyber defence information management.

While many of the capabilities listed above have been a subject of research over the last few decades, others are immature. In order to efficiently progress towards these capabilities, the various NATO and national efforts must be coordinated. The capability breakdown is central in this effort with its terminology and structured breakdown.

The framework currently consists of capability definitions only. However, one can achieve a capability in several different ways, and the same capability can vary in its efficiency and ability. Therefore, a natural extension to the capability definition would be a maturity model that would describe levels of a capability. For example, the ability to detect a malicious cyber attack can take days or seconds while still being the same capability. However, the ability to detect in real-time is clearly a more mature capability and needs to be expressed.

A natural accompaniment to a maturity model is measurements and metrics to evaluate the capability. This is important to define in order to evaluate the overall capability, both to establish that the desired effect is being achieved, and to establish the maturity level of the capability for the purpose of defence planning and interoperability in multi-national scenarios.

Potential topics for MNCD2

Through an informal analysis of existing capabilities and needs, the following three areas have been identified as possible initial targets for a multinational capability development initiative: 1) cyber defence information sharing, 2) cyber situational awareness, and 3) a distributed multi-sensor collection and correlation capability.

The first topic, the development of a *cyber defence information sharing* capability, would enable efficient exchange of cyber defence information such as incident information, attack signatures, and threat assessments, between national Computer Emergency Response Teams (CERTs) including the NATO Computer Incident Response Capability (NCIRC).

The activities needed to put this capability in place include a determination of the type and format of the information to be exchanged, completing an interface specifi-

cation, design of the infrastructure for sharing, writing procurement requirements, the actual procurement, and a test and validation of the delivered equipment. In addition, there may be a need for training and education of staff in the use of the system, and there will likely be a need to translate some formats from the existing CERTs' systems to meet the interface specification and allow interoperability with the other CERTs.

The determination of the requirements for information to be exchanged and the data format would leverage the lessons learned from the annual NATO Cyber Coalition exercise as well as the Coalition Network Defence Common Operational Picture work conducted in an RTO working group (IST-081-RTG-039).

For the infrastructure design, the communication infrastructure requirements would be thoroughly assessed so as to determine the elements required at the National CERTs, the elements required at the NCIRC as well the available transport networks, for, at least, each of the three main security domains (NATO Unclassified, NATO Restricted and NATO Secret).

Procurement could be done individually in a nation, jointly, or any combination of the two. In the case of multiple procurements in different nations, there would be a clear need for a testing and validation effort since different systems will need to interoperate.

The second topic is the development of a capability to improve *cyber situational awareness*. For most NATO Nations, operational cyber defence is performed using a variety of tools and products including Intrusion Detection System (IDS) and other sensors, Security Incident and Event Managers (SIEM), vulnerability databases, and network monitoring software. These tools typically operate individually and there is no overall view. Cyber defence situational awareness is, therefore, achieved by experts manually consulting and consolidating a variety of feeds. Significant competency and a lot of manual effort are required.

Due to the complexity and the vastness of information provided by these feeds, an efficient and accurate visualization capability is required to provide relevant and clear situation perception that supports a timely decision making process. It is necessary to generate specialized views for humans to be able to understand what is happening and derive knowledge from all this information. This includes views for the expert analysts to let them be more efficient in their investigations, as well as views for the commanders and managers in order to understand the current state of the CIS.

The joint development of this capability would simplify and enable quick decision making in the cyber domain, especially in a coalition environment, by providing a flexible set of visual interfaces (e.g. dashboards, dynamic views, and reporting features). It would leverage work conducted under the ACT cyber defence research and

development programme (R&D POW) on the Consolidated Information Assurance Picture (CIAP) which provides a set of specifications of various flexible views using information contained in the NATO Consolidated Security Information Repository (CSIR) and to be implemented by the NCIRC Full Operational Capability (FOC).

The third topic, the *distributed multi-sensor collection and correlation infrastructure* capability would provide the means to coherently collect and correlate data from multiple sensors in an efficient and distributed manner so as to enable flexible management of sensor data storage and run a variety of correlation algorithms against the collected data. This is necessary in order to increase the maturity level on malicious activity detection from being able to detect known attacks to being able to detect targeted attacks against the organization.

This capability is currently being investigated under the ACT cyber defence R&D POW and is based on a set of specifications that address the consolidation of the data generated by various sensors located within a CIS, forwarding selected portions of it to a central location, and making the rest available for processing and querying by analysts through a centralized management capability.

The specifications ensure that any analysis code can be executed in a distributed fashion, thus providing an open and flexible distributed processing and analysis infrastructure that can be used to extract key cyber defence information from the CIS being protected. It could also be used to address many of the capabilities related to situational awareness within the cyber defence capability framework.

Cyber Defence Experimentation and Validation Capability

A key element of joint capability development is an experimentation and validation infrastructure that would ensure that new cyber defence capabilities are validated and interoperable as required. For this reason, the NATO cyber defence capability framework has to be complemented by a structure that would allow NATO and NATO Nations to experiment new technologies, technical/operational concepts and procedures and to test cyber defence standards against a reference.

From experience gained in other technical areas, the vision would be 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.

By defining the necessary trust and technical environment allowing the federation of existing efforts, this capability would have the potential to contribute to a better and accelerated development of cyber defence and cyber security capabilities in a cost effective manner.

NATO C3 Agency Role in Multinational Development

NC3A is part of the NATO Consultation, Command and Control Organisation (NC3O), along with the C3 Board and the NATO CIS Services Agency (NCSA), and supports the mission of the NC3O through unbiased and independent advice in the C4ISR area. NC3A consists primarily of NATO employed personnel in order to be independent of industry and national bias, including both scientists and procurements specialists. NC3A is authorized by its Charter to provide technical advice and support to customers who are either NATO bodies or Nations.

As the potential legal framework of a multinational programme, NC3A has established C4ISR Memorandum of Agreement (MOA) with a number of nations. The MOA is a framework agreement covering full cooperation on C4ISR activities, with the collaboration terms defined in advance. For the execution of a specific scope of work, the C4ISR MOA can be complemented by Technical Agreements describing the work and financial terms.

NC3A can act as a multi-national executive coordination agent in support of capability development in cyber defence in any area covered under the technical framework. The support can span from research contributions and correlation to procedure design and engineering and procurement. In this role, NC3A can also facilitate the discussion with the cyber defence operational community about the definition and establishment of maturity levels for the technical elements under investigation so as to provide prioritization and guidance for implementation.

Finally, NC3A can support the setting up and maintain a framework for sharing information about NATO, national and coalition research activities. This can be based on centralized or synchronized databases holding the available information and allowing features like extensive searching and cross-reference capabilities.

Conclusion

The political guidance regarding cyber defence is to continue to develop the capability, and that the overall alliance cyber defence capability needs to be considered through the NATO defence planning process. In addition, technical capabilities should be developed jointly in order to be as efficient as possible.

Securing cyberspace is a complicated issue and, in particular, implementing effective interoperable cyber defence capabilities is a major endeavour with many technical, procedural and political challenges. NATO and NATO Nations are currently at various stages of implementation for such capabilities and are now challenged to develop the tools and mechanisms that will allow them to optimize their resources and exploit all possible synergies. A multi-national cyber defence capability development programme will help NATO and NATO Nations and deliver benefits to all participants

by providing support, coordination, and coherency in the area of cyber defence capability development.

The NATO C3 Agency is well positioned to support this effort through its charter and its mix of unbiased personnel including scientists and procurement specialists. In addition, the existing legal agreements between NC3A and a number of nations can be used to accelerate and ease the setup of such an initiative.

A multi-national cyber defence capability development will meet the political guidance as agreed in the new strategic concept and the subsequent cyber defence concept and policy. More importantly, it will contribute to a significant improvement in defence against the continually increasing threat of cyber attacks across the alliance and therefore contribute to the overall security of the alliance.

Notes:

[1] Madeleine K. Albright (Chair), *NATO 2020: Assured security; dynamic engagement – Analysis and recommendations of the group of experts on a new strategic concept for NATO* (Brussels, Belgium, 17 May 2010).

[2] *Active Engagement, Modern Defence*, Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation, adopted by Heads of State and Government in Lisbon, 19 November 2010, <www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf>.

[3] Geir Hallingstad and Luc Dandurand, *Cyber Defence Capability Framework - Revision 2*, Reference Document RD-3060 (The Hague: NATO C3 Agency, in press).

FREDERIC JORDAN started his career in 1996 with an Aerospace Engineer degree and a Master's degree in Computer Science. He then worked as an Information Security Engineer in the French Ministry of Defence before he joined the NATO C3 Agency in 2005. Since then his responsibilities have progressively evolved from scientific and technical activities to project and team management. He is now the Project Manager for most of the NC3A Cyber Defence scientific and technical projects. He is also the Project Manager for the Bi-SC AIS IDS acquisition project which will provide the NATO Military Command sub-structure with Network and Host based Intrusion Detection capability.
E-mail: Frederic.Jordan@nc3a.nato.int.

GEIR HALLINGSTAD received his B.Sc. and M.Sc. in computer engineering from Iowa State University in 1996 and 1997, respectively. He has over 10 years of experience working with information security in military systems and is currently working as a principal scientist at the NATO C3 Agency. His work area includes networked systems that provide both secure and flexible communications in support of an network enabled capability (NEC) operational environment, and the establishment of cyber defence and its various components as a fundamental capability in providing cyber security and information assurance.
E-mail: Geir.Hallingstad@nc3a.nato.int.