Towards Multi-national Capability Development in Cyber Defence

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 NCI Agency Cyber Defence scientific and technical projects. He is also the Project Manager for the Bi-SC AIS IDS acquisition project which provides the NATO Military Command sub-structure with Host based Intrusion Detection capability.

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 NCI 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.

Agata Szydelko

Received Master's degree in Management and Marketing at Wroclaw University of Economics. As Principal Business Manager she is responsible for the strategic planning, cooperation development and business assurance of Multinational cooperation with the Nations and Organizations in the area of C4ISR. Her professional experience as NCIA Senior Contracting Officer includes the execution of high-volume NATO C4ISR acquisitions, also in support of NATO operations in Afghanistan and the Balkans. Moreover, as International Business Manager for national industry she was in charge of the supply of IT systems to commercial and military customers.

Resumo

Para o Desenvolvimento de uma Capacidade Multinacional de Ciberdefesa

Este artigo apresenta uma abordagem de desenvolvimento de uma capacidade multinacional de ciberdefesa que tem sido discutida entre vários países da NATO e a NATO Communications and Information Agency, inserida no contexto da NATO Smart Defence. Existem ganhos potenciais se se alavancarem requisitos e recursos comuns, quando as capacidades existentes entre os vários países são variáveis e o financiamento destinado os desenvolvimento das mesmas é escasso, sendo que se apontam alguns dos fundamentos justificativos para esta cooperação multinacional.

Abstract

This article presents a multi-national cyber defence capability development approach discussed between several NATO Nations and the NATO Communications and Information Agency in the context of NATO Smart Defence. There is potential gain from leveraging common requirements and resources when the levels of nation capabilities in this area vary and funding to develop the capabilities is scarce. The article will address some of the fundamentals for multi-national cooperation.

Introduction[1]

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 requires 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 currently being discussed between an open group of NATO Nations and the NATO Communications and Information Agency (NCI Agency). 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.

1 This article is an update of the one published in the special issue of the *Information & Security* journal on C4ISR support to the Comprehensive Approach. Frederic Jordan and Geir Hallingstad (2011). "Towards Multi-National Capability Development in Cyber Defence". *Information & Security* n. º 27, pp. 81-90. Available at http://www.procon.bg/node/2469.

Background

The analysis and recommendations of the group of experts on a new strategic concept for NATO (Albright, 2010) 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 (NATO, 2010), 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.

A major element of the NATO Cyber Defence is the NATO Computer Incident Response Capability (NCIRC) Full Operational Capability (FOC) project, which will provide not only a technology refresh of the existing NCIRC IOC capability but will also introduce new technologies to improve cyber defence situational awareness and enhance NATO's ability to respond to evolving cyber-threats.

Once the NATO CIRC FOC capability is in place the NCI Agency will establish the appropriate mechanisms to enable the nations to acquire the associated tools and services for national use.

The NATO Secretary General's original call for Smart Defence in February 2011 (Rasmussen, 2011) at the Munich Security Conference has been repeatedly reiterated in numerous addressees and forums. The Chicago Summit declaration of 20 May 2012 – "Toward NATO Forces 2020" (NATO, 2012) – clearly confirmed that Smart Defence is at the heart of the new approach towards NATO retaining and developing the capabilities necessary to perform its essential core tasks of collective defence, crisis management, and cooperative security. 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 is to facilitate the development of cyber defence capabilities in the nations and NATO 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.

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.

NATO already facilitates coordinated research through the Science and Technology Organisation (S&TO), 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 S&TO 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 S&TO 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.

Collaboration Climate

While the advantages argued for any multinational efforts remain nearly the same for any multinational project – interoperability, economies of scale, optimized collaboration and more efficient use of the resources it is remarkable that in an area considered to be of great sensitivity and with significant security concerns the nations are willing to open up and work together, seeing more pros than cons for joining up the collaborative environment. Economic crisis? Maybe, although if this was the case the multinational collaboration projects would have been flourishing all over the place, which does not seem to be the case. What then? The most likely explanation is that the overwhelming pressure coming from around the globe and the cross-borders nature of computer networks pushed the nations to reconsider the limits of their own sovereignty for the benefit of enhancing the collaborative security, probably marking a new era in multinational collaboration and once again in human history pushing the limits of sharing.

Framework for Cyber Defence Capabilities

In order to aid in cyber defence capability development, Allied Command Transformation (ACT) and the NCI Agency have initiated the development of a cyber defence capability framework (Hallingstad and Dandurand, n.d). 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;
- Situational awareness visualization;
- 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.

Topics for MNCD2

Through an analysis of existing capabilities and needs, the following three areas have been identified as 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.

Cyber Defence Information Sharing Capability

The first topic, the development of a *cyber defence information sharing* capability, will 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 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 specification, 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 will 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 S&TO working group (IST-081-RTG-039).

For the infrastructure design, the communication infrastructure requirements will 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 NATO 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.

Once this initial Cyber Defence information sharing capability is in place, other issues of importance could be addressed. For example, there is currently no standard approach for the direct integration of data into Cyber Defence applications. As well, there is no agreed framework or standard to facilitate collaboration between Nations and NATO on the dynamic generation, refine-

ment and vetting of cyber security data. For these reasons, the NCI Agency has started investigating under the ACT cyber defence research and development programme (R&D POW) the concept and requirements for a Cyber Defence Collaboration and Exchange Infrastructure (CDXI). The CDXI addresses syntactic and semantic interoperability between different communities of interest that nevertheless wish to exchange Cyber Defence data, while avoiding the pitfall of supporting only a single ontology. In particular, it uses pure enumerations and independent topic ontologies as a mean to provide an agile and decentralized data model.

To understand the CDXI, it is best to see it primarily as a software library to be used in the development of Cyber Defence applications. While it will have its own set of user interfaces, these will be intended primarily for the management of the core infrastructure and its data. The exchange of information in operational scenarios and the automation of Cyber Defence will be through various applications developed by industry and organisations that use the "CDXI software library" to manipulate the required Cyber Defence data for those purposes. Whether or not these applications will expose the full range of services offered by the CDXI through their own user interfaces will depend on each application's purpose, their intended user community and the products' specific goals.

Cyber Situational Awareness

The second topic under consideration 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.

From a capability definition perspective, visualization represents activities in the CIS, as well as the CIS components, the objectives and their priorities, the threats, discovered vulnerabilities and reference security information from vari-

ous sources. In addition, the visualization needs to show projected actions based on the events and context and present these to the users with the potential impact. The visualization should address the needs of different user roles at different command or management levels, including the ability to alert, highlight, filter, and drill-down for additional detail as necessary, in a customizable fashion.

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 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).

Distributed Multi-sensor Collection and Correlation Infrastructure (DMCCI)

Attacks on CIS infrastructures are increasingly sophisticated and increasingly successful. In particular the Advanced Persistent Threats (APT) has grown in importance and can no longer be dismissed as marginal events. This has led to efforts to fundamentally rethink the defensive strategy. For example, DARPA has started several projects under its CRASH program (Clean-slate design of Resilient Adaptive Secure Hosts) that aim to fundamentally redesign CIS systems with security as a main requirement. The main aim of the Distributed Multi-source Collection and Correlation Infrastructure (DMCCI) investigated under the ACT R&D POW is to define an open architecture that overcomes the limitations of the current protection and detection mechanisms in order to increase network situational awareness and facilitate the detection of advanced and stealth attacks.

At its core the DMCCI capability provides 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.

In effect, DMCCI enables the rapid, seamless and continuous introduction of complex, multi-source detection algorithms that can correlate data from various sources not only newly arriving data but also on previously stored data, including events, network flows and metadata. It also supports and streamlines the post intrusion analysis and damage assessment processes while addressing constraints imposed by the geographic distribution of the components of a CIS as well as the bandwidth limitations of its communications links.

One use case of how DMCCI could facilitate post intrusion analysis and damage assessment is when malicious software and malicious network traffic is detected in an organization's CIS. The organization then usually generates or exploits a security bulletin which contains the signatures or traces of the attack. The signatures are then deployed through-out NATO networks allowing anti-virus software to detect *new* compromises using this malware. However, attackers are likely to remove these traces on machines that have already been compromised. An analysis of different APT attacks shows that attackers often use the initial malicious software only to exploit a software vulnerability on a host and then install a different piece of malicious software to remotely control the machine. So the question is now, which hosts in the organization's network have *in the past* received any of the signatures associated to the attack. Anti-virus software cannot answer this question as it did not previously have the signatures of the newly discovered files. All these hosts need to be analysed for signs of compromise. And the follow up question is, with which hosts have these potentially compromised hosts communicated, as the attackers may have used the compromised hosts as a pivoting point (stepping stone) to move laterally to other parts of the organization's networks.

DMCCI would allow an analyst to answer these questions by running queries over correlated data from collected from network, DNS servers and proxy servers, without the need of a manual investigation of each of these systems. The analyst can then focus the manual effort on forensic investigation of affected hosts. In addition, DMCCI will allow the analyst to use findings from his investigations to write advanced algorithms that will detect similar attacks and shorten the delay between the time of attack and time of detection. The goal is to be able to apply new rule sets and detection algorithms not only upon new flows and events but also upon past flows and events. DMCCI 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 C&I Agency Role in Multinational Development

The NCI Agency is part of the NATO Communications and Information Organisation (NCIO), along with the Agency Supervisory Board and supports the mission of the NCIO through unbiased and independent advice in the C4ISR area. The NCI Agency consists primarily of NATO employed personnel in order to be independent of industry and national bias, including among others scientists as well as procurements specialists. The NCI Agency is authorized by its Charter to provide technical advice and support to customers who are either NATO bodies or Nations.

The legal framework to be used for the establishment of the MN CD2 is a multilateral Memorandum of Understanding (MOU). 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 programme of work across the three proposed Work Packages. The MOU will be supplemented by Task Orders detailing the exact scope and execution of the respective Work Packages. One of the advanced features of this MOU is the opportunity for inclusions of Contributions in Kind offered by any of the participating nations in the execution of the project. Currently the MN CD2 is open for participation to all the NATO nations.

Under the MN CD2 legal umbrella the NCI Agency will act as a multi-national executive coordination agent in support of capability development in cyber defence, from running project office to any area covered under the technical framework. The support will span from research contributions and correlation to procedure design and engineering and procurement. In this role, the NCI Agency will 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.

MN CD2 and Smart Defence

A big step forward in the establishment of the MN CD2 project was the decision by Canada in June 2012 to take on the Lead Nation role for this project as well as its inclusion in the NATO Smart Defence Multinational Projects database. This further reconfirms the nations' will for the project establishment and provides greater project visibility and alignment with the NATO Defence Planning Process.

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 NCI 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 the NCI Agency 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. Finally, it's coming right on time for the nations to take advantage of collaborative rather than individual efforts in one of the most crucial areas for the stability and prosperity of our world.

References

Albright, Madeleine K. (2010). *NATO 2020: Assured Security, Dynamic Engagement – Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*. Brussels, 17 May.

Hallingstad, Geir, Luc Dandurand (n.d.). Cyber Defence Capability Framework – Revision 3"(NATO C3 Agency Reference Document RD-3060). The Hague.

Jordan, Frederic, Geir Hallingstad (2011). "Towards Multi-National Capability Development in Cyber Defence", *Information & Security* n.º 27, pp. 81-90. http://www.procon.bg/node/2469

NATO (North Atlantic Council) (2010). "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation". Lisbon, November.

NATO (2012). "Chicago Summit Declaration on Defence Capabilities: Toward NATO Forces 2020". 20 May. Available at http://www.nato.int/cps/en/SID-EE03881B-D6E19CED/natolive/official_texts_87594.htm

Rasmussen, Anders Fogh (2011). "Building Security in an Age of Austerity". Keynote speech by NATO Secretary General Anders Fogh Rasmussen at the 2011 Munich Security Conference. Available at http://www.nato.int/cps/en/natolive/opinions_70400.htm.