Information Interoperability and Information Standardisation for NATO C2 – A Practical Approach

Eddie Lasschuyt, MSc
Marcel van Hekken, MSc
TNO Physics and Electronics Laboratory
P.O. Box 96864
2509 JG The Hague
The Netherlands
Lasschuyt@fel.tno.nl / VanHekken@fel.tno.nl

1. Introduction

1.1. Rationale

Interoperability between information systems is usually 'achieved' by enabling connection at network level. Making systems really interoperable, by letting them understand and manipulate the exchanged information, requires a lot more. Above all, *information standards* are needed in order to gain common understanding about what will be exchanged. Besides that, information standardisation should be considered from a *global* point of view, taking into account the whole range of systems that will potentially exchange information for a certain purpose. The importance and complexity of information standards are often underestimated. Gaining efficient and effective interoperability starts with thinking about information standardisation in its totality first.

1.2. Context

Coalition operations within NATO require extensive co-operation between military units and organisations of the participating nations. This means that interaction is needed at the Command and Control (C2) level in the first place. Information has to be disseminated in order to achieve optimal 'situational awareness' among all parties involved in an operation. For this purpose they require what is called a "common operational picture" (COP), being the same view on the battlefield.
The changed nature of military operations, producing increasing amounts of information, as well as recent developments in technology, have led to the widespread use of C2-supporting information systems. They are usually called "Consultation, Command, Control, Communications and Intelligence systems", in short "C4I" systems. Although many of the current systems are still under development and not fully integrated in the operational decision making process, nations are more and more dependent on these systems as backbone for their C2 information distribution and processing.
Combining these two facts, i.e. the importance of NATO-wide C2 information dissemination to obtain a COP and the increasing use of C4I systems, results in the need for C4I systems that are able to *co-operate*. This means that different systems, with different functionality, using different natural languages and made by different manufacturers, should be able to participate in an overall C4I network and seamlessly interchange operational information. We refer to this as *interoperable* C4I systems.

1.3. Overview

This article discusses a general and practical approach to reach interoperability among a *large* number of information systems of *different* nature. It is focussed on the subject of *information standardisation*, for the purpose of gaining interoperable *systems*. Based upon this approach, a number of considerations and recommendations are given for interoperability within the NATO C2 domain, i.e. between NATO C4I systems[1]. The article is primarily intended to give an overview of this problem area and to make the reader aware of its significance and difficulty. It could make him/her realise that information standards deserve more attention in his/her community (e.g. a policy division, Defence research lab or C4I-related working group) and it may trigger him/her to give more thoughts on the matter. We must emphasise, though, that some issues in

[1] When we say "NATO C4I system" this includes national systems that are potentially used in a NATO context.

Paper presented at the RTO IST Symposium on "Information Management Challenges in Achieving Coalition Interoperability", held in Quebec, Canada, 28-30 May 2001, and published in RTO MP-064.

this article are not (yet) fully crystallised or haven't proven their value in practice (yet). Further discussion on these issues in international forums is strongly suggested.

In chapter 2 we start with a general introduction to interoperability, hereby setting the technical scope for this article. Chapter 3 defines the problem we want to solve. It does so in terms of possible interoperability architectures and factors that influence the choice. The theory of chapter 3 is applied in practice, on the NATO C2 domain, in chapter 4. Suggestions are given for improving the NATO standardisation efforts. Finally, chapter 5 summarises the conclusions made in the other chapters.

2. Information interoperability

2.1. Introduction

This chapter briefly explains what we mean by information interoperability, how an information standard fits in and why the latter is so important in establishing interoperability.

2.2. Types of interoperability

Interoperability is the degree to which entities are able to co-operate in achieving a common goal. There are many interpretations of the concept of interoperability between computer systems[2]. It varies from having a network connection and being able to transfer files or (a bit more sophisticated) send and receive e-mail, to using exactly the same applications at all systems and completely sharing the information they process.

In this paper we address *information interoperability*, achieved by the *automated exchange and interpretation of structured information* between/by systems. With minimum user intervention, systems must be able to *automatically* interchange certain information and utilise that for further processing. Especially important is the prerequisite that the information is *structured*, because this enables functionality such as distribution by subscription on certain topics, presentation of information on a map, fast search & retrieval facilities and filtering by specific selection criteria. The emphasis here lies on the exchange of *information* (rather than data), hereby preserving its meaning, integrity and context. Another precondition is that the exchange may not depend on proprietary products, such as database management systems and communication systems. In support of all these requirements, the information is often exchanged in a clustered manner, via some form of 'messages'. Summarised, this kind of interoperability offers an optimal connectivity between systems while preserving maximum independence of these systems.

Our definition of information interoperability is similar to what is called "level 4, 5 or 6 of interoperability" in NATO terminology [1]. This implies a physical connection between computer systems and (depending on the level) user-controlled accessibility restrictions. ATCCIS Replication [2] and automated ADatP-3 message exchange [3] are typical examples of this kind of interoperability.

2.3. Standardisation

The key notion for information interoperability is *standardisation*. By having common agreement on which information is exchanged, in what format, how this is done and under what conditions, it becomes easier to allow systems of different type to interoperate. Paragraph 3.2 explains about possible approaches of reaching interoperability, which depend on the degree of standardisation. We name the total set of agreements that make systems co-operate by exchanging information, an *interoperability standard.*

An important characteristic of an interoperability standard is its *scope*, which defines the objective of the standard, or, in other words, for what organisations, scenarios, systems, functions, etc. the standard is applicable. The scope must be clearly defined, so that it is absolutely unmistakable whether certain information under certain circumstances is part of the standard or not. An ambiguous scope will undoubtedly lead to confusion and possibly wrong use of the standard (for purposes it was not intended for).

---

[2] We deliberately do not consider interoperability in another context, for example between organisations. This article is focussed on system interoperability.

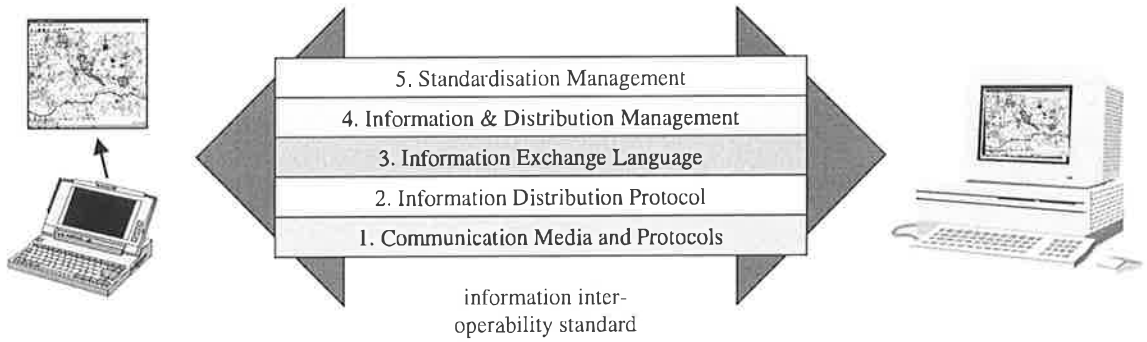


Figure 1 — Layered view on an interoperability standard

2.4. Interoperability layers

An information interoperability standard is composed of five layers (see figure 1), for each of which overall agreement is required:

1. Communication media and protocols.
   This layer provides basic data communication. Mostly existing (commercial or military) standards are used for this. Examples of such standards: TCP/IP, X.400, e-mail (SMTP), Combat Net Radio, CRONOS.

2. Information distribution protocol.
   Automated distribution of information (not: data) requires additional (higher-level) protocol standards in order to preserve meaning, integrity and context of the information. Concepts such as assured/confirmed delivery, transactional interaction, sequencing, queuing, forwarding, content-based routing, prioritisation, compression and encryption affect the way information is disseminated and must therefore be standardised. Examples of information distribution protocols: database replication, publish/subscribe.

3. Information exchange language.
   An unambiguous and structured description of the information to be exchanged within a certain scope is needed. Without a common understanding of the information, systems will never be able to interpret it in the same way. When a French C4I system reports a hostile unit to a German C4I system, both should have equal comprehension on the unit's size, location, etc. They must, so to say, 'speak the same language'. A *common exchange language*, or 'Esperanto', defines the semantics (what it means), the syntax (how it is structured) and the lexicography (how it is represented) of the information. Examples of exchange languages (see also par. 4.2): "Land C2 Information Exchange Data Model", AdatP-3.

4. Information & distribution management.
   In support of setting up and maintaining the exchange of information within an operational environment, certain additional rules and procedures must be agreed upon. They depend on requirements imposed by the environment. Examples relevant for the NATO C2 domain: security measures (e.g. an information classification scheme or a Public Key Infrastructure), rules on ownership of information, features that enable selectivity of information (e.g. filtering), a procedure to establish and manage information exchange contracts between organisations, rules that guarantee the use of world-wide unique information element identifiers.

5. Standardisation management.
   Finally, an interoperability standard cannot exist without proper agreement upon how to support the development and maintenance of the standard as a whole. This includes management organisations, procedures (e.g. for handling change proposals) and tools (e.g. for data modelling).

The lower layers have a more technical nature, while the upper layers consider more organisational matters. In our opinion, the *exchange language*, the middle (third) layer involving both technical and organisational issues, is the most challenging and important interoperability layer to be standardised. Therefore, this part of an interoperability standard, also called the *information standard*, will be the subject of the rest of this paper. (Many statements, however, also apply to the interoperability standard as a whole.)

2.5. Information standard

Standardising information as part of an interoperability strategy is an often-underestimated effort. A common exchange language is hard to obtain. We give three reasons. Firstly, unless the scope is very small, several organisations and/or nations will be involved. For that reason it will usually be very difficult to reach consensus on which information is relevant for exchange, how information elements relate to each other, what format is used for specific information items, etc. Every party has its own standards, habits, principles, technology and — above all — pride. Secondly, information analysis is a difficult process in which domain experts and information technologists need to co-operate closely. It takes a lot of patience and understanding to get a complete and unambiguous picture of a certain problem area. The information requirements may appear rather unclear and complex, which makes clarifying and structuring this an intensive and time-consuming effort. Thirdly, recording the results of an information analysis, for instance in a data model, requires special skills. The modeller must take into account many conditions in order to obtain an information structure that is broadly usable. It must be understandable for users, compact enough to implement, flexible so it can cope with future requirements (without radical changes), etc. In conclusion, making an information standard involves many players and many kinds of issues, varying from politics to technology, and is therefore a complex matter.

Besides being the most difficult one, the common exchange language (information standard) is also the most *important* interoperability layer in our view. Not that the other layers are unessential for achieving interoperability, but (in theory, in order to minimise the effort) they could be simplified very much by using commercial products and/or minimising the quality of distribution. The information standard, however, cannot be bought 'off the shelf' and cannot be reduced without narrowing the interoperability scope. More than the other interoperability aspects, the information standard affects the functionality that systems, by operating together, offer.

An information standard for exchange can be specified in several formats. Within the NATO context, the most widely used formats are relational data models, formatted messages and glossaries. We consider a *relational data model* as the best way to specify an information standard. Among other reasons this is because data models are commonly used and supported by methods and tools, represent a very unambiguous and structured definition of information (unlike glossaries), offer maximum flexibility in selecting information subsets to be exchanged (unlike formatted messages) and are both easy to be communicated with users and to be implemented in a database. Therefore this article assumes future exchange languages to be expressed in relational data models[3].

The next chapter outlines how information standards can be used to obtain interoperability between systems.

3. Interoperability architectures

3.1. Introduction

This chapter defines the problem of integral information interoperability at *large scale*. It does so by describing architectural aspects of interoperability and their effect on the efficiency of information distribution. We hereby concentrate on information exchange between *systems*, although in most cases we could also have spoken about organisations instead, because both represent a node in an information exchange network (technical versus operational view)[4]. Although the theory of this chapter is applicable in general, we mainly use examples out of the NATO C2 context.

---

[3] A rapidly rising specification technique is the eXtensible Mark-up Language (XML). It is in particular useful to define a standardised syntax for documents and messages. However, some kind of data model is still required to describe the meaning and context of the information. XML offers schema techniques for that, but these are less mature (regarding method, tools, etc.) than relational data models. Hence, we think that XML is a valuable instrument to pack information (in a message) for exchange between systems, but it should be applied in combination with relational data models that define the total set of available information.

[4] An (information) system is a local set of computers, databases, applications, etc. interconnected by a Local Area Network. An organisation utilises such a system. It supports the information supply that facilitates the business processes. When organisations are interoperable, in this article we mean their systems exchange information, usually over a Wide Area Network.

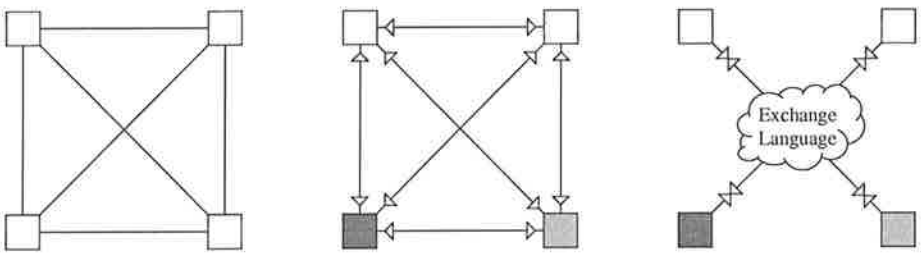
3.2. Basic architectures

As said before, information interoperability between computer systems is the ability to exchange and interpret information. In order to do so, systems must be able to 'talk' to each other and to 'understand' each other. The interaction is not necessarily directly. Instead, it may take place through one or more 'interpreters' or 'translators' ('interfaces' in computer terminology) that translate between information languages. There are three basic architectures for interoperable systems (see figure 2):

a. Standardisation of systems.
The internal architecture of each system is identical, including the information structure. One could say the interoperability standard is integrated within the systems. Information exchange is feasible without additional interfaces. This situation may occur when a distributed organisation is able to set up new systems for all its offices and base them on a single (standardised) architecture. A 'corporate' information standard is part of that. In most cases, however, this approach does not work, because the organisation will have to deal with different types of systems, often also legacy systems, with dissimilar internal architectures and information structures.

b. Bilateral exchange.
Every *type* of system[5] has its own internal architecture and uses a specific information structure. To exchange information, dedicated interfaces between each pair of interconnected systems are needed. The interfaces transform information from one format to another. For n systems connected to each other, this results in n(n-1) one-way interfaces in total. This solution is preferred when only two or three different types of systems are involved (and this will not change in the future). In case of more system types and more than a few interconnections, this architecture becomes highly undesirable, as it imposes numerous interfaces then.

c. Standardisation of the exchange language.
Every type of system has its own internal architecture and uses a specific information structure. Via an interface to a common exchange standard, information can be exchanged between all systems. In this case, n systems require only 2n one-way (or n two-way) interfaces in total. This third option is commonly seen as the most practical solution for integral information interoperability. The number of interfaces is minimal and proportionate to the number of system types. Besides that, the architecture offers flexibility in the sense that new systems can be added without having to adapt the other systems (by adding new interfaces).



a) systems of the same type, sharing an equal information structure, thus no interfaces

b) systems of different type, no information standardisation, resulting in 12 one-way interfaces

c) systems of different type, one common information standard, 4 two-way interfaces

Figure 2 — Basic architectures for information interoperability

Notice that an 'arrow' in figure 2 represents the translator on top of a system that transforms incoming (or outgoing) information from an external to an internal format (or vice versa).

Despite the advantages of the preferred basic architecture for interoperability (c), this solution in itself is not feasible for the whole 'universe' of systems, even if we restrict that to C4I systems within NATO. The ideal solution for NATO-wide interoperability would be a *single* standard for all information exchange between

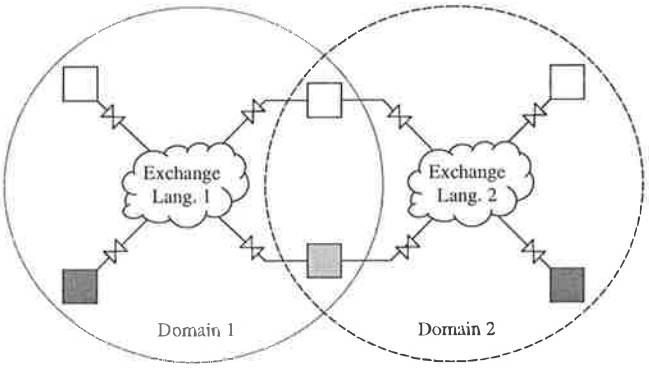
[5] Be aware of the difference between systems and system *types*: systems of the same type have an equal architecture and use exactly the same type of information.

NATO C4I systems (see figure 3). However, a number of political, organisational, operational and technical issues (see further) make this solution unlikely to be ever achieved. Therefore, a subdivision in multiple exchange languages — each with a specific scope — will be necessary. Finding an optimal partition is the real challenge here. In support of this, the next paragraphs exploit the concept of "interoperability domains".

Figure 3 — The perfect (but impossible) solution

3.3. Interoperability domains

As we have seen, a number of systems can be made interoperable at information level by defining a common information standard (exchange language) which describes the information these systems want to share with each other. We define an *interoperability domain* as the total set of systems (or system types) that exchange information by means of the same exchange language. A system is said to be part of a domain when it interacts with other systems by making use of the domain's exchange language. A system can belong to more than one domain in case it 'talks' *multiple* languages (see figure 4).



Example of two systems that are part of two interoperability domains, i.e. using two languages to exchange information with other systems.

Figure 4 — Multiple exchange languages

The size or *scope* of an interoperability domain determines *how many and what kinds of systems* belong to that domain. According to paragraph 2.3 the scope must be unambiguously defined. Because a domain represents an information standard, its scope can also be specified by means of the *kind of information* that is exchanged between systems within the domain. Two basic preconditions are valid when establishing the information scope:

1. Exchangeability.
   For the purpose of interoperability, only information which will (or can) be *exchanged* between systems is part of the standard. Thus, given a system, information that is not meant to be exchanged with other

systems, but just used internally, does *not* belong to a standardised exchange language. Notice that this also applies to (distributed) systems of the *same* type.

2. Commonality.
The exchanged information is *shared* by the systems that require being interoperable, but not necessarily by *all* systems. Instead, the information part of the standard must be in common by *at least two* types of systems. This results in a range of possible scopes for the standard, limited by two 'extremes' (see figure 5a): the 'highest common denominator' (HCD, dark and shaded parts) versus the 'lowest common multiple' (LCM, only dark portion) of exchangeable information. Exactly which of the common information will be part of the standard depends on several factors (see further). Relevant in this is the ratio between HCD and LCM. For example, if the latter is only small compared to the former (see figure 5b), then a small part of the exchanged information is common for *all* systems.

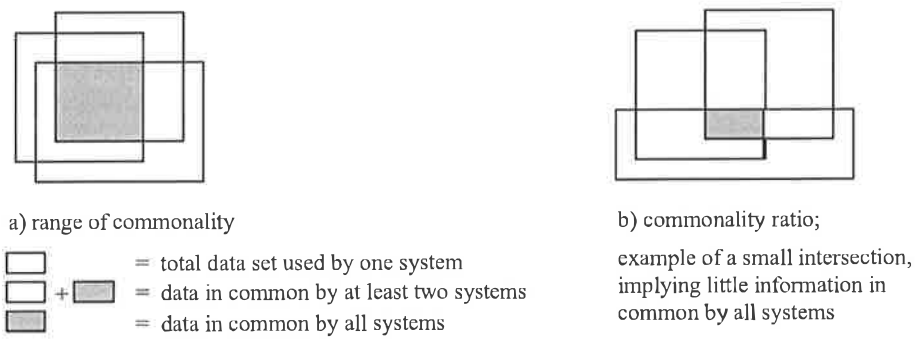


Figure 5 — Common information

Taking these two prerequisites as a starting point, the scope of an interoperability domain will primarily be based upon the operational requirements with respect to interoperability. Naturally, there will always be a drive for fitting all systems into a single domain (as in figure 3). But how large a domain eventually can become, depends on several things, such as:

- the number of different system types that must be included in the domain;
- the diversity in functionality of these system types;
- the amount of information to be exchanged between the systems;
- the degree of commonality of that information;
- the number, contents and change ability of 'legacy' information standards;
- the number of organisations using the systems within the domain;
- the number of additional parties involved in the standardisation process.

The more system types, functional diversity and exchangeable information, the more different types of information (subjects) have to be covered by the domain. This makes it harder to reach agreement on a common information standard. Also, which information is common for which systems affects the ease of agreement (e.g. because more bilateral than multilateral negotiation is necessary). Already existing standards may interfere as well, depending on their scope and whether their 'survival' or invariability is a precondition. And, of course, the number of actors in the standardisation effort, either representing one of the systems or involved for other reasons, highly influences the outcome of the standard. In general, when much information has to be harmonised between many players, the chances of success become smaller and the final result will cost more effort and time.

3.4. Domain structures

The previous analysis reveals that when a large number of systems needs to become interoperable, dealing with *multiple* domains is usually unavoidable. Of course, aiming at a single information standard is a good starting point, because it will result in the simplest (and cheapest and fastest) technical solution. But in practice this will often not be realistic. Therefore, making systems interoperable generally means *connecting different interoperability domains*.

We start with a relatively simple situation. We have three domains, for instance the C2 domain of the Army, Airforce and Navy of some nation. Due to reasons mentioned above, the national Ministry of Defence has chosen for this split-up. How can interoperability be achieved between C4I systems belonging to these different domains? There are two options (see figure 6): using direct links (a) or using an additional information standard (b). This corresponds to basic architectures 'b' and 'c' of paragraph 3.2, but one level higher. For figure 6b this results in a 'second level' exchange language. Regarding the usefulness of both options, the same reasoning (as in par. 3.2) applies over here: the second approach is better in case of more than two or three domains, because of the huge number of interfaces required otherwise. Only severe differences in information exchange requirements between pairs of domains, meaning little information in common for all three domains, makes the first option more suitable.

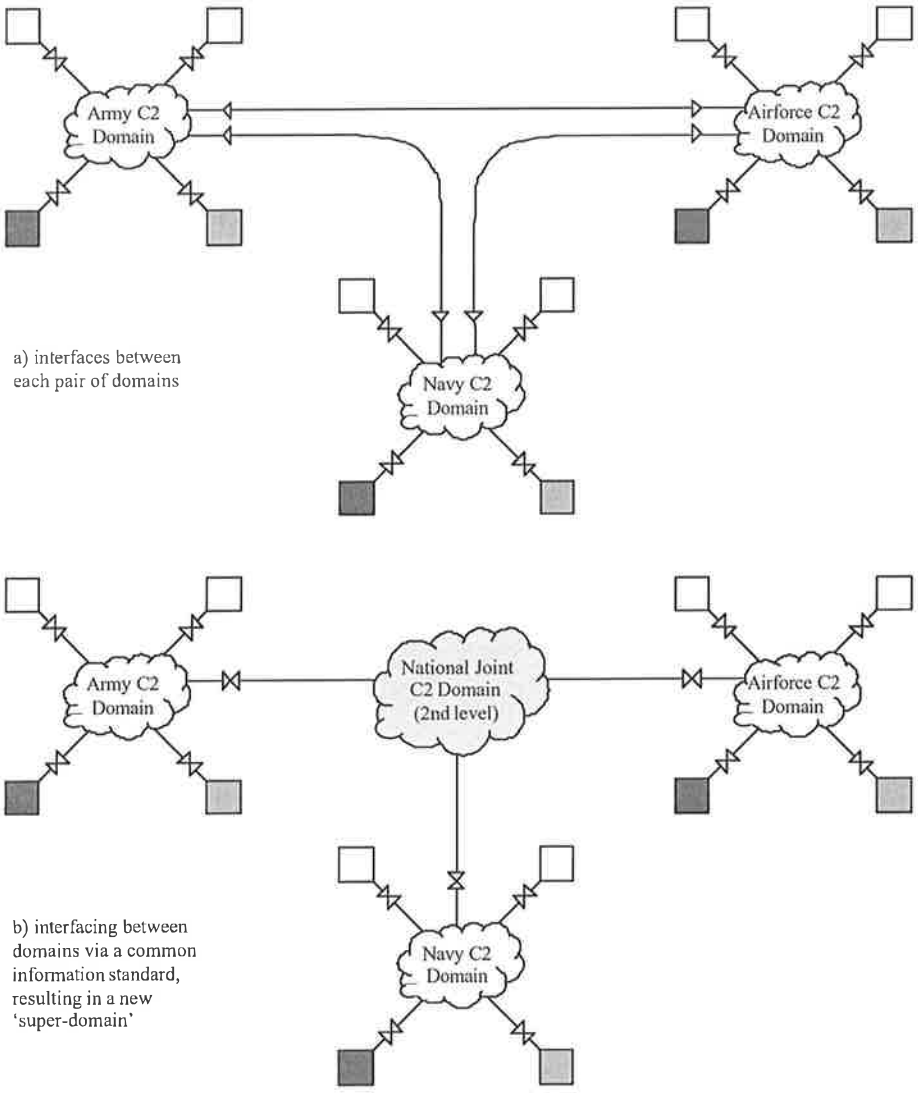


Figure 6 — Two options for interoperability between multiple domains

The connected domains in figure 6 are actually an abstraction of systems connected to multiple domains, as shown in figure 7. In option 'a' all systems are part of the three 'force' domains; in option 'b' each system belongs to one of the 'force' domains as well as to the 'joint' domain. Although both figures represent equal architectures, drawing systems as linked to only *one* domain (as in figure 6) may express the fact that this particular exchange language comes closest to (or is even equal to) the 'natural' language of these systems, i.e.

their internal data structure. It may also indicate that translation between languages takes place in sequence instead of directly. For instance, according to option 'b' the following transformations could take place when two systems exchange information:

- sequential: Army System X ↔ Army C2 Language ↔ Joint C2 Language ↔ Airforce C2 Language ↔ Airforce System Y
- directly: Army System X ↔ Joint C2 Language ↔ Airforce System Y

It is true the sequential translation seems less efficient, because it takes more steps. The advantage, however, is that less different types of translators are needed, due to reuse (e.g. the same "Army C2 / Joint C2" translator can be used by all Army systems!). This reduces costs, development time and system maintenance. Finally, hooking up systems to a single domain more or less imposes the environment in which the information standard of this domain is managed. Generally, the same organisations that are responsible for the directly linked systems are also involved in developing and managing the standard.
In conclusion, although it does not affect the architecture, drawing domains as linked to each other and systems as linked to a single domain, is often better. So a *hierarchy* of domains (with systems as 'leafs') is preferred over a 'flat' domain structure.

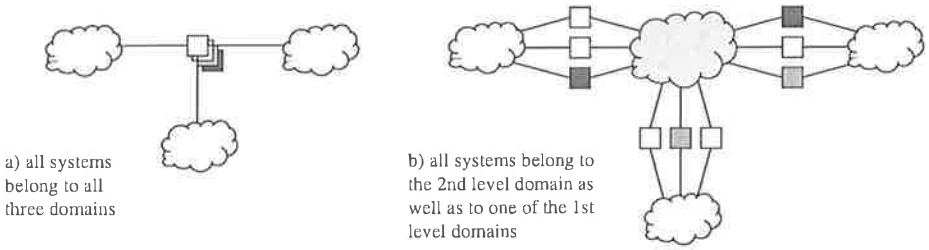


Figure 7 — Same two options as in figure 6, but drawn less abstractly

It is possible to connect systems to a *second* level interoperability domain. This indicates these systems use the exchange language underneath that domain to interact with each other. For them, this is the lowest-level domain to which they belong. In the example of figure 6b one could add a couple of joint C4I systems, as boxes directly linked to the National Joint C2 Domain. We call these systems 'internal' to that domain.

Here it may become rather difficult to fully understand the matter and realise the implications. We attempt to explain it as clearly as possible by exactly defining what it means when domains have different *levels* and when domains are *linked* to each other. Figure 8 could help to envisage things.

Domain levels. For $n \geq 2$, an n-th level interoperability domain connects two or more (n-1)-th level domains (as well as zero or more internal systems). This means that systems belonging to different (n-1)-th level domains (as well as internal systems) are able to exchange information by means of the common exchange language inherent to the *n-th* level domain. That these systems also use the (n-1)-th level language to *mutually* exchange information is irrelevant at this abstraction level.
With respect to the information *scope* of an n-th level domain, the same two preconditions apply as for first level domains (exchangeability and commonality, see par. 3.3). Hence, the 'super-domain' contains (1) only information that is also encompassed by the connected domains (exchanged by systems over there) and (2) only information in common by at least two of the connected domains. However, since an n-th level domain can also have 'internal' systems, these rules also apply to these systems (as if the domain was first level). This makes that, on top of the subset of information out of the 'subdomains', the n-th level domain may contain additional information types as well.

Domain linkage. If we look again at figure 6, we see two kinds of connections. Firstly, a link between two domains of the same level (6a). This implies (1) that a system of one domain can exchange information with a system of the other domain and (2) that this is done by 'talking' the language of either his own domain or the other domain. Secondly, a link between two domains of different levels (6b). This implies again (1) that a

system of one domain can exchange information with a system of the other domain, but in this case (2) that it must take place by using the language of the *highest-level* domain. For instance, an Army system and a Joint C4I system will interact via the National Joint C2 Language.
Connecting more than two domains in a *row* only makes sense when there are higher-level domains in between. Suppose we have a 'chain' of three domains of the same level. The systems at both ends *cannot* exchange information with each other, because their 'own' domains are not directly linked. (They would only be able to interact indirectly, if a system of the middle domain would forward the information.) Now imagine a chain of five domains with levels 1 - 2 - 3 - 2 - 1. Between systems of the first and of the third, fourth or fifth domain the 3rd level Esperanto is used, while between systems of the first and of the second domain the 2nd level language is spoken. Summarised, an interoperability domain can only act as 'intermediate' domain when it is defined at a higher level than the domains it must connect. Being of a higher level implies mandatory usage of its information standard for exchange.

To conclude this paragraph about domain structures, one should notice that an information environment that is large enough might contain numerous interoperability domains at several levels. Figure 8 illustrates how a large number of systems (or organisations) may be interconnected by means of several information standards at three different levels. Yet, to obtain such a structure is far from easy. The next paragraph explains the factors that play a role in finding an optimal domain structure and shows what real-life factors disturb the theory.

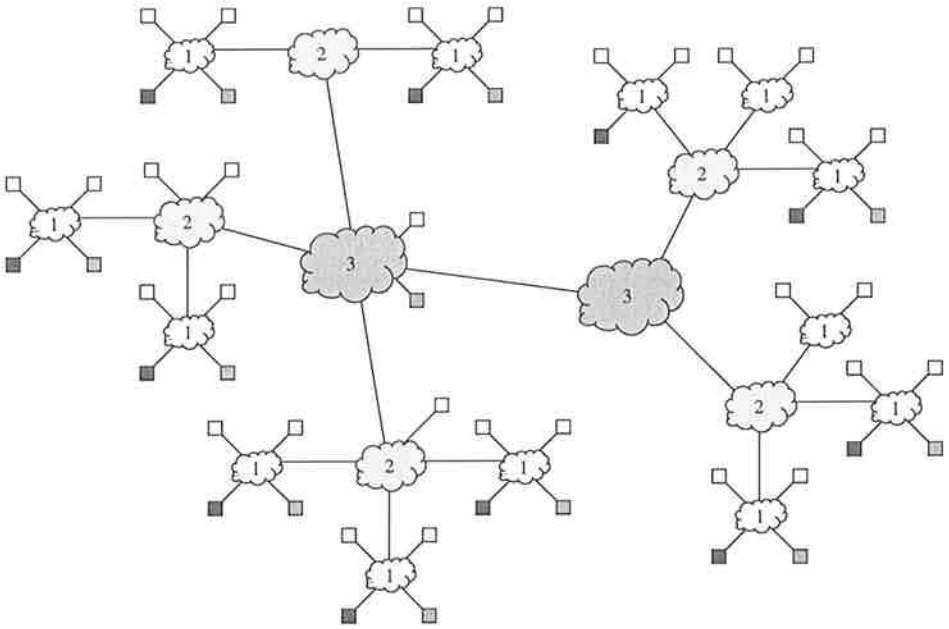


Figure 8 — Interoperability domains at different levels

3.5. Domain factors

Given a context for interoperability, what domains at what levels should be defined in order to obtain an optimal solution? By optimal we mean that the domain structure is such that a minimum standardisation effort will result in an efficiently working information exchange. This paragraph investigates several relevant factors and offers some guidelines.

We firstly consider the optimal size of a single domain. Scoping an interoperability domain affects a number of factors in positive or negative manner. The *larger* the scope of a domain:

- \- the more difficult it will be to reach common agreement on that domain;
- \- the more difficult it will be to maintain the information standard;
- \+ the more systems can interact via the same standard;
- \+ the fewer domains are needed to cover the whole problem area;

+ the less information transition between domains is required;
- the more overlap there will be with other domains;
- the higher the possibility that there is overlap with legacy domains;
- the more complex the information standard will be (to understand and implement);
+/- the more generic the information standard will be[6].

For *smaller* domains these factors are affected in opposite direction.

Rules for finding the optimal scope are hard to give. Fact is that the first factor, the exertion to agree on a standard, has the most impact on the final result. And, as we have seen in paragraph 3.3, this depends on several aspects such as the diversity of the information and the number of organisations involved. In general, an interoperability domain should have a scope of *maximum size*, under the condition that the information standard is still *manageable* with regard to overall approval, maintenance and implementation.

Another guideline is that the information inside a domain should always be related to a particular *subject* (that is, information should be of a specific *type*). This subject is often associated with certain functions and/or organisations as well. An information standard should not cover a variety of hardly related subjects; instead, it should have a *strong internal correlation* [10].
Similar to the subject, the information *owners*[7] should be correlated. The total set of information enclosed by a standard must be owned and exploited by a *limited* number of *related* organisations. This keeps the standard manageable. This is not the case when there are too many potential owners for a certain type of information and these owners are not organised such that only a few representatives are involved in the standardisation process.
So, subject and ownership usually determine the contents and scope of an information standard. A subject/ownership area can be very wide, but also rather specific. Example areas in our context are NATO C2, NATO Air C2, NATO Intelligence, NL Army C2 and NL Airforce Ground Operations.

We now consider the possible divisions of a complete context area into interoperability domains. Similar to the previous statements about separate domains, a domain *division* should also be based upon the *subject (type)* and *owner* of the information. This makes that each domain is an information standard for a *particular* subject and/or owner. Diversity in information types and owners exists along many dimensions, for example:

- topic or function of the information (e.g. personnel, materiel);
- purposes or activities for which specific information is used (e.g. viewing the current situation vs. supporting the planning process);
- the required quality of the information (e.g. real-time vs. non-real-time data);
- organisations that are formally responsible for specific information (e.g. nations, NATO).

Paragraph 4.3 contains a more extensive list of dimensions, aimed at the NATO C2 area.

This approach forms the basis for obtaining relatively autonomous (loosely coupled) domains. The functional relation (subject) and organisational influence (ownership) between domains should be weak and well defined [10]. In other words, domains should have *minimum overlap*. In the first place, this minimises the co-ordination between the developers of different interoperability domains. More synchronisation increases the complexity and the implementation costs of standards. Furthermore, minimum overlap can reduce the total number of domains and/or information translations. Also, it prevents multiple 'paths' — that is a choice between information standards — for exchanging information between two arbitrary systems. For instance

---

[6] Large information standards (data models) tend to have a generic nature, which means that specific information elements are represented in a non-specific manner. For instance, geographical demarcations such as no-fly zones, air corridors and unit sectors may be expressed as 'control features'. This increases the flexibility of the standard, because similar new information elements can be included without (or with little) changes to the model. A serious drawback is the loss of semantics, which makes the standard more difficult to comprehend and less clearly scoped. Also, implementing applications on a generic data model is more complex.

[7] An information owner (in our context) is a (military) organisation responsible for certain information. The owner creates and manages that information. For example, a Spanish regiment that has observed some incident and reports it via a C4I system, will be the owner of the information representing this event. Although information may be copied and sent to other organisations, only the owner is allowed to modify or delete the 'master copy'. Each piece of information has exactly *one* owner. These basic rules of ownership are generally accepted as foundation for distribution of information.

(see figure 9), enemy data between national Army C4I systems could be exchanged via a Land C2 standard or an Intelligence standard. Finally, with non-overlapping domains unambiguous information is avoided. Two or more standards that (partly) cover the same type of information rarely use exactly the same structure and format for that information. This causes conflicts — systems may understand certain information differently — and the "degree of standardisation" diminishes.

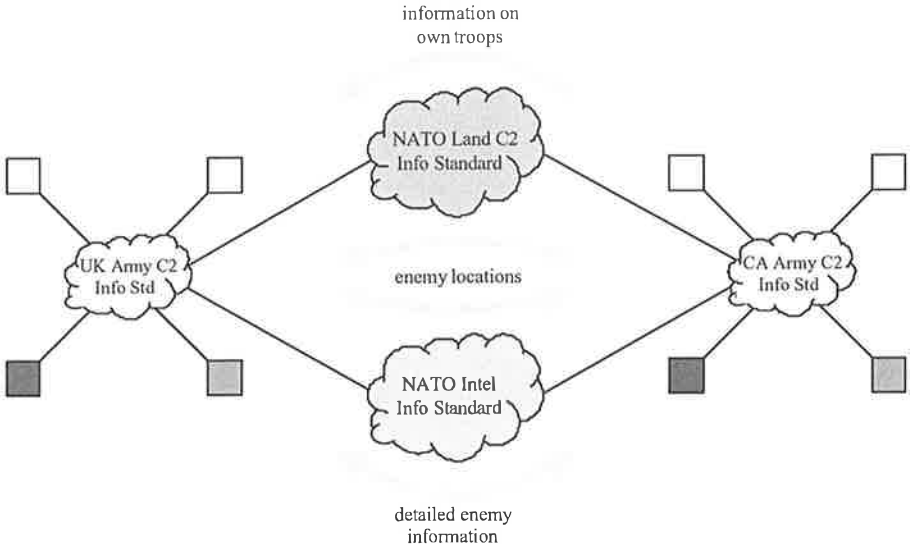


Figure 9 — Example of multiple paths due to overlapping information standards

The *level*, at which domains should be defined, depends on their role as common language for certain systems within the interoperability context. When an information area is subdivided into separate domains, systems that must be interoperable are usually grouped accordingly. A higher-level domain often origins from the requirement to enable systems of different domains to be interoperable as well. Such a domain will contain a subset of information in common by the lower-level domains. In case there are also systems that make use of the super-domain as their first level domain, it may contain additional information. This does imply, however, that the same criteria for scoping and subdividing domains (as described above) must be taken into account again.

As stated before, the domain structure should be founded on the type of information and/or ownership, hereby aiming for a minimum overlap between domains. However, this reflects an ideal situation. In reality, there are several factors that distress the ultimate domain structure, such as:

- sizeable subjects with many details and many complex relationships between data elements;
- a large number of separate information owners for a particular subject;
- already existing information standards that are not permitted to be substituted;
- involved organisations not able to agree on a logical subdivision;
- unfinished information standards due to long-lasting development.

How these (and possibly other) factors exactly will have an effect on the eventual domain structure, cannot be predicted; this depends on the situation. One should accept as a fact that the perfect solution is difficult to obtain and influenced by many factors. Chapter 4 will continue with a practical insight on this matter, aiming at the best reachable solution for NATO C2 interoperability.
Before that, the next paragraph briefly describes some technical consequences of having a domain structure.

3.6. Technical implications

Up to this point the discussion about interoperability has been concentrated on the aspects 'information' and 'management'. But making systems part of *multiple* interoperability domains, one of our recommendations above, has some significant *technical* implications as well. Without going into detail, we give the most

important requirements to be fulfilled in order to make systems interoperable according to the approach explained before:

- Multiple translators are part of a system. Along the lines of figures 6, 7 and 8, each system needs to be able to 'talk' multiple exchange languages. The system has to transform its internal information structure into the exchange languages and vice versa. When information is being exchanged, one or more translators are run, depending on the domain to which the source or destination system belongs. If the concept of 'sequential' translation (see par. 3.4) is applied, there are also translators in use that convert between different exchange languages.
- The translation process between two information structures may be quite complex, especially if one is more generic than the other is. This is caused by, among other things, different sets of valid information element values ("attribute domains") without a one-to-one mapping. Loss of information may even occur due to severe differences. A translator is surely not a trivial component of a system.
- The difficulty of translation between two information standards highly depends on their *compatibility*. Standards that consist of similar information elements and structures are easier to convert into each other than standards that differ completely. In terms of data models this means the models should at least have an (almost) equal *core* structure, i.e. a common '*framework*'. This contains the fundamental and central parts of the data models. Thus, in order to 'ease' interoperability, exchange languages should be as compatible as possible, by basing them on the same framework.
  This requirement is not always feasible. A system's internal information structure is usually primarily influenced by system requirements, such as performance and application functionality, often resulting in structures unlike the framework. And for legacy systems it will be virtually impossible to change the internal database towards that framework structure.
- Besides compatible, exchange languages should also be *extendable*. Information standards tend to be never complete and finished; regular upgrades are inevitable. This is due to a long development time, the quickly changing military environment, evolving information requirements, new systems, etc. The information standard must therefore be *flexible*, meaning that new information types can be added without (or with minimally) changing the existing structure. This also ensures *backward compatibility*, the ability of systems to keep working with old versions of the standard. Flexibility can be achieved by specifying the basic information elements in the underlying data model (i.e. the framework) in a *generic* way.

4. NATO C2 interoperability

4.1. Introduction

The previous two chapters have revealed some theoretic aspects of information interoperability and information standards. In this chapter we will apply the theory to the NATO C2 environment and come up with a possible practical approach for achieving interoperability at information level. Guidelines are given for obtaining an optimal domain structure with usable information standards, enabling interoperable C4I systems.

We must stress the fact that the presented approach is an *example* of how it could work. Our view on the current NATO interoperability and standardisation developments and on NATO long-term policy is not complete and accurate enough, simply because it is very difficult to oversee this whole field. So, there may be relevant factors we have not taken into account. Nevertheless, being an example the method may still very well serve as a first step in the right direction.

4.2. Current NATO developments

Table 1 gives an overview of some of the most important C4I developments within NATO [4,8,9], varying from specifications to real systems. All developments are concerned with interoperability and standardisation in some way, if only to facilitate the (system) internal distribution of information. Per development we cite the scope of the information to be exchanged and how the corresponding "information standard" is called (and/or looks like). Notice that we only consider the information *contents* here; quality aspects like security and actuality of information are not included in the scope.

System or Specification	Meaning	Information Scope	Information Standard — Name and/or Appearance
ADatP-3	Allied Data Publication 3	C2	ADatP-3 formatted messages
NCDM	NATO Corporate Data Model	C2	NATO Reference Model + functional views
Bi-SC AIS	Bi- Strategic Command Automated Information System	C2	(none yet, to be integration of ACE-ACCIS and MCCIS)
ACE-ACCIS[8]	Allied Command Europe - Automated Command and Control Information System	C2 (SC Europe)	(none yet, to be integration of i.a. BICES, JOIS, LOGFAS[9])
AIntP-3	Allied Intelligence Publication 3	C2 Intel	AIntP-3 data model
BICES/BICC	Battlefield Info. Collection and Exploitation System / BICES Initial Core Capability	C2 Intel (Land)	ACE Intelligence Data Model
PAIS	Prototype ACE Intelligence System	C2 Intel	PAIS database
JOIIS	Joint Operational Intelligence Info. System	C2 Ops/Intel	JOIIS database
ADAMS[9]	Allied Deployment and Movement System	C2 Logistics	Logistic Database
ACROSS[9]	ACE Resource Optimisation Software Sys.	C2 Logistics	Logistic Database
ATCCIS	Army Tactical C2 Interoperability Spec.	C2 Land	Land C2 Info. Exchange DM
MIP	Multilateral Interoperability Programme	C2 Land	Land C2 Info. Exchange DM
ACCS	Air Command and Control System	C2 Air	ACCS Conceptual DM
ICC	Initial CAOC Capability	C2 Air	ICC database
MCCIS	Maritime Command and Control Information System	C2 Sea (SC Atlantic)	MCCIS databases + ADatP-3 and "OTH-Gold" form. msg.'s
Link 11/16/22	Tactical Data Links 11/16/22	C2 Air/Sea	Link 11/16/22 form. messages

Table 1 — Some relevant C4I developments within NATO context

Most information standards mentioned here cover both the operational and tactical levels (and sometimes more), although the exact scope with regard to the operation level is unclear for the majority. Some standards seem to support particularly higher-level information. For example, ACE-ACCIS supports the consultative process between senior commanders and agencies. Other standards mainly comprise low-level information, such as the Tactical Data Links that incorporate things like tracks and engagement orders. Nevertheless, in all cases at least some (but often much) 'generic' information at operational/tactical level is included in the standard. The status of an Army Battalion inside the operation area, for instance, is surely of interest for many users and will be supported by many C4I systems. This fact, together with the similarities in information scope between much of the systems and specifications (as shown the table's third column), causes considerable overlap among the existing (or emerging) information standards. As explained in paragraph 3.5, this situation is undesirable. The question now is: how can we improve this? In the next paragraph we first outline a potential ideal collection of C2 information standards for NATO, followed by a paragraph that suggests a practical way to apply this, while taking into account the current developments.

4.3. Optimal NATO domain structure

Taking NATO C2 as our context for interoperability and assuming no standards exist yet (or all existing ones can be replaced), what domains at what levels should be defined in order to obtain an optimal solution? Using the guidelines of paragraph 3.5 we attempt to find the best possible subdivision of the NATO C2 area into separate interoperability domains (information standards). Various kinds of partitions could be employed; each determines how domains are created based upon a *specific* categorisation of information. Eleven possible dimensions for subdivision have been identified:

a. functional area (data about C2, politics, administration, law, sensor & weapon systems, etc.);
b. operation level (strategic, operational, tactical or technical data);
c. command level (e.g. data for Division/Brigade vs. Battalion and lower);
d. operation type (e.g. data required for Article-V or Crisis Response Operations);
e. operational context (data for an operation, exercise, test, simulation, etc.);

[8] Due to the Bi-SC AIS developments, ACE-ACCIS might never become a sole system, because it may have been integrated before it is finished. In this article we still assume it is a separate system under development.
[9] ADAMS and ACROSS are part of the Logistics Functional Area Services (LOGFAS), a part of ACE-ACCIS. Both systems use the same database, the Logistic Database (LOGBASE).

f. region (e.g. data used in the regions Europe and Atlantic);
g. responsibility, i.e. nations and multinational organisations (NL, AFNORTH, etc.);
h. operational theatre, matching the military forces (Land, Air or Sea data);
i. subfunctional area (for C2: data about Intelligence, Operations, Logistics, NBC, etc.);
j. time and dynamics (current situation, plans, historical events, encyclopaedic data, etc.);
k. function regarding interoperability (operational info, security info, distribution info, etc.).

Of course, not all of these subdivisions are suitable. We now explain which are feasible as a basis for a NATO C2 interoperability domain structure.
(a) Due to our scope, i.e. NATO C2, the functional area will be pure C2. Though C2 information is related with other kinds of information, for instance of administrative nature (personnel, economics, finances, etc.), we still think the boundary is quite sharp. Looking at the global information requirements for primary operational/military tasks (e.g. obtaining situational awareness of the battle space), there is *no significant* overlap with other functional areas. In addition, including other functional areas will result in a C2 domain too big to handle, above all because of the huge amount of organisations and systems that will be involved. So, C2 interoperability domains should exist apart from other functional domains[10]; this article does not address the latter.
(b) The operation level will be limited to operational and tactical, because the levels above and below are not the primary context for Command and Control. As already said, most C4I systems are intended for the operational and tactical levels. Making distinction between the two levels is not relevant, because there is severe overlap with respect to the type of information involved and because several C4I systems cover both levels anyway[11].
(c) Although the command level is linked to the operation level, in principle our scope reaches from Corps down to the smallest unit sizes. Modern operations with multinational and flexible forces require potential C2 information exchange with any unit regardless of its size. Dividing information according to command level is therefore not useful.
(d) Considering the present diversity in operation types, we may presume that more new types will probably emerge in future and that most kinds of operational information are applicable for most types. Therefore, it is of no use to define a separate interoperability domain per operation type.
(e) Our operational context includes operations and exercises. The information needed in both cases is equal ("train as you fight"), so domain partitioning is undesirable. Other settings, for instance a military simulation environment, fall outside our scope.
(f) Regions are no base for domains, because the type of information required for C2 hardly depends on a region. Operations should be conducted in the same manner everywhere.
(g) Mapping interoperability domains on NATO nations and NATO organisations, possible owners of specific information, may be useful from the point of view of minimising the number of parties concerned with the standardisation process. Also, the type of information used within those often dissimilar 'worlds' could differ considerably. In the case of *nations* a domain separation is valid: national rules and feelings (politics) make all-enclosing information standards on C2 virtually impossible. Hence, nations could act as boundaries for interoperability domains. For *NATO organisations*, on the other hand, it is different. The organisational structure of NATO is big and complex; many associations exist and many organisations have common responsibilities. Thus splitting up information according to the NATO structure is not obvious. Besides that, NATO itself endeavours enterprise-wide systems and standards.
(h) Historically, military forces have different doctrines and thus different information requirements derived from that. Subdivision of interoperability domains founded on Army, Navy and Airforce seems convenient.
(i) Subfunctional areas of C2, such as Intelligence and Logistics, cover diverse subjects. This implies much information of different type, especially regarding the details. A division in domains based upon subfunctional areas seems logical. However, there are two problems. Firstly, the areas also *share* much information, namely

[10] Nevertheless, there are tendencies which strive for integration of all functional areas around C2. Examples are: the inclusion of 'in-depth' sensor and weapon data according to the philosophy of Network Centric Warfare; the (Dutch) effort to integrate the national Defence 'green' and 'white' domains (C2 and administrative/management data respectively).
[11] What *is* relevant is this context is the 'quality' of information, such as its timeliness and accuracy. Tactical information usually requires to be more real-time and more precise than operational information. However, this article only concerns about information *types*, not qualities. On the other hand, quality aspects could have been used as dimensions to divide information. For example, one could distinguish between real-time, near real-time and non-real-time data. We did not consider such categorisations, because they seem to be not very useful.

'generic' C2 information (about units, materiel, locations, plans, etc.). So, domains based upon them would have quite some overlap. Even worse, "Generic C2" is a subfunctional area in itself, because there are quite some C4I systems that mainly provide a global situational picture, leaving out details about logistics, etc. Secondly, the subfunctional area partitioning and the Land-Sea-Air partitioning (see item 'h') are diametrically opposed. Each force makes use of subfunctional areas, which could imply severe overlap between force-related and subfunctional information. Despite of these two problems, we still think it is useful to have interoperability domains projected on subfunctional areas of C2 (in parallell with the force-based domains). For certain subfunctional areas much of the information is very specific and independent of the other areas; a relatively small part is generic. This argues in favour of separation. Another reason is that such information tends to be applicable for all forces. This is proven by the fact that some systems supporting a certain subfunctional area are indeed being built in a joint effort. If the force domains are limited to generic information, then the overlap with the subfunctional area domains is minimised. Summarised, distinct domains for C2 subfunctional areas are feasible and the mutual overlap is taken for granted. Logistics, Intelligence and Generic C2 appear to be the most obvious areas to create separate domains for. For now, we limit ourselves to these three areas, but some other areas (e.g. Personnel) may be a candidate as well. The remaining subfunctional areas should be included in the selected ones (e.g. Operations, NBC and CIMIC could be part of Generic C2, provided they encompass only little dedicated information).
(j) The subdivision of information in accordance with its timely and dynamical nature is particularly interesting for end users (and may result in a corresponding application set). In line with the C2 decision process they usually work in a way information about (for instance) current situation and planning is employed *separatly* (e.g. in different overlays). However, these kinds of information sets typically have a substantial part in common, so they are not applicable as domains.
(k) Finally, in the perspective of interoperability not only operational data is exchanged, but also all kinds of supporting data. This could be security information describing who owns a C2 data item and whether it is classified, or distribution information about who is subscribed to what C2 data. Such supporting information inherently belongs to the interoperability domain — it must be standardised as well — even though most of it is normally not contained in the operational information standard, but defined separately. Although essential for interoperability, we do not consider such information any further in this article.

In conclusion, NATO C2 information at operational and tactical level should be subdivided along the following dimensions:

1. owners: nations + NATO as a whole;
2. themes: Land, Air and Sea;
3. subfunctional areas: Generic C2, Intelligence and Logistics (for now).

This results in a possible interoperability domain structure as displayed in figure 10. Some explanation:

(i) The national domains are of national concern. Here we have taken the (probable future) Dutch situation as an example. Keep in mind that the top of the picture should have been 'multiplied', because (in principle) all NATO nations will be connected to the NATO domains; to keep the overview, only one nation is drawn.
(ii) The subfunctional area (NATO) Generic C2 has been integrated with the three themes (forces). This means that the NATO Land, Air and Sea domains contain *generic* Land/Air/Sea C2 information. (Notice that the NL domains are *not* generic, but include subfunctional areas as well.)
(iii) An additional "NATO Joint C2" domain covers what the three thematic domains have in common and require to exchange. This domain is limited to *generic* C2 too.
(iv) Besides the Joint C2 domain, the NATO Intelligence and Logistics domains are *joint*[12] as well. The three domains are thus supposed to cover the greater part of the whole area of joint NATO C2 information; possible additional subfunctional areas (see item 'i') may complete this.
(v) The systems (little boxes), some of which virtual (dotted), are examples that serve to explain the usage of the interoperability domains. Figure 10 shows that systems of any kind can potentially exchange information with each other by using one or more exchange languages[13].
(vi) Notice that most systems are directly linked to just one domain, in line with the guidelines about domain hierarchy in paragraph 3.4. There is one example system, ACE ACCIS, for which this is not possible, because that system is part of domains not connected to each other. This may illustrate the (unmanageable?, undesirable?) diversity in functionality of this (future) system.

[12] Evidently, all NATO interoperability domains contain information of *combined* nature.
[13] Provided that at least a network connection is available as well (interoperability layers 1 and 2, see par. 2.4).

(vii) The bar on the right side of the picture denotes the level at which the domains are defined, relative to the national force domains that got level 1. The five NATO force and subfunctional area domains are second level, because they are meant to connect the corresponding national information areas (which are *virtual* domains in this context, because it is of national concern how to organise the own information). These domains do *not* have different levels with regard to each other, since they cover (more or less) separate information areas. The NATO Joint C2 domain, on the other hand, is of the third level, because this domain acts as the common language for three other (second level) domains.

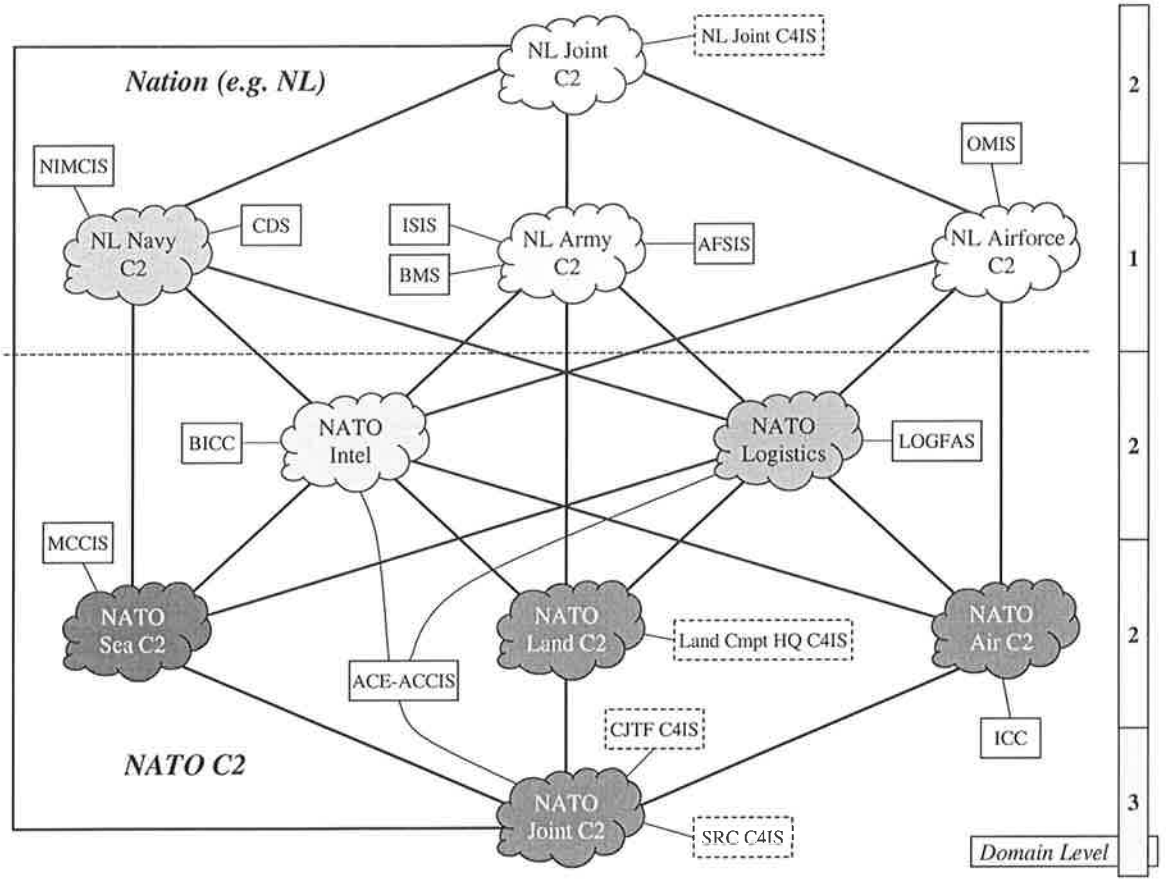


Figure 10 — Possible optimal interoperability domain structure for NATO C2

4.4. The optimal solution in practice

In our opinion, NATO should aim for a formation of information standards in line with what is shown in the previous paragraph. The final optimal NATO C2 interoperability domain structure may appear to look somewhat different, for instance due to additional subfunctional areas, but we think the general idea is feasible in reality.

How can this optimal long-term objective be achieved? The current developments (see table 1) are a 'fact of life' and can probably not be altered too much. Instead, the policy should be to 'divert' these programmes such that they will grow towards the intended structure. This implies certain developments will have to integrate (see further).

Recent developments within NATO reveal that NATO is indeed working in a similar direction. This is especially valid for the "Bi-SC AIS" programme [4,5,6], that aims to converge ACE and ACLANT systems. This must result in a single system consisting of a "Core Capability" (common services) and several "Functional Area Services" (specific applications). It illustrates that NATO has the intention to integrate

things. However, it appears the emphasis currently lies on the integration of *systems*, not information in particular. Moreover, NATO aims at a *single* all-enclosing system, a 'Utopia' which we think is unreachable. It is technically complex, requires consensus among many players and is unmanageable (while operating) due to its magnitude.
Instead on systems, it might be better and easier for NATO to focus on *interoperability standards*, including information standards. Enabling many different systems to exchange and understand the same information is already hard enough. Integrating these systems is even more difficult and, in fact, unnecessary. The main goal behind this integration into the Bi-SC AIS is to gain *interoperable* NATO C4I systems[14], for which an interoperability standard is sufficient. (NATO comes closer to this approach in another of its integration efforts, namely the planned migration of the Tactical Data Links [7]).

Suppose the approach described above appears to be feasible — also politically — in reality. Then the information standards mentioned in table 1 might be directed towards figure 10 in the following way:

- The MCCIS databases and the ADatP-3/OTH-Gold formatted messages for MCCIS are the basis for a Maritime Data Model, which covers the NATO Sea C2 domain.
- Given its maturity, the Land C2 Information Exchange Data Model (ATCCIS) is the most likely candidate for the NATO Land C2 domain.
- The ACCS Conceptual Data Model should develop into the NATO Air C2 information standard (possibly by also integrating the ICC database).
- The Tactical Data Link messages should be integrated with the ACCS data model and the MCCIS formatted messages.
- The AIntP-3 and ACE Intelligence data models (possibly together with the PAIS/JOIIS databases) must result in a single NATO Intel information standard.
- The Logistic Database forms the obvious basis for the NATO Logistics domain.
- Finally, the NATO Reference Model (part of the NCDM) can be the basic framework (see par. 3.6) for all NATO information standards. It induces a core structure in order to ensure compatible and flexible data models.

Important is that these developments are closely monitored and co-ordinated from a central point of view. Their scope should be clearly specified and communicated, so that no overlap or blind spots can occur and the aimed interoperability domains are indeed obtained.

In general, if NATO should decide to follow the above-mentioned approach, it not only needs to define a policy that defines the global objectives (interoperability by means of information standards, etc.), but also a frame of reference on how these objectives should be realised. This includes, among other things, the intended overall interoperability domain structure (which can be considered as a NATO information exchange 'meta standard'), preconditions for developing the independent information standards (such as the data model framework), preconditions for other aspects of an interoperability standard (e.g. communications and security, see par. 2.4) and a migration path for 'redirection' of the current related C4I developments. This is what we normally call an "information architecture" [10], being a vision on how the NATO information requirements should be accomplished, hereby fulfilling prerequisites with respect to structure, components, flexibility, etc. Essential in this is the role of a central high-level NATO body, for instance the NATO Data Administration Organisation (NDAO), which must co-ordinate the different domain developments and make sure the NATO information architecture is indeed adopted.

One of the major problems here is, and will always be, the existence of (legacy) standards and systems already in use. But this is not different from the Bi-SC AIS approach, where this problem occurs just the same. Prescribing NATO-wide interoperability standards may even be less problematic in our approach, because existing systems can remain and would 'only' need an interface on top.

---

[14] Some other general objectives of system integration are re-use of software and common user interfaces. It seems in NATO context these goals are less important than achieving interoperability (or not valid at all).

Another problem has to do with the scope of the proposed information standards. They contain much information and involve many players and systems. This implies laborious consensus and a long development time. But again, a similar issue must be solved for Bi-SC AIS as well.

If people can be convinced of the importance of information standardisation for the purpose of interoperability and if the quality of the approach presented in this paper is proven, then the problems will be overcome and an interoperability domain structure such as introduced here, may become reality.

5. Conclusions

Below, the conclusions drawn in this article are summarised.

- Current and future military operations within NATO require extensive co-operation (information exchange) between participating military units, organisations and nations and, as a consequence, interoperability between their supporting C4I systems.
- The interoperability concept has many interpretations, but a commonly used form is information interoperability, because it offers optimal connectivity between systems, while preserving maximum independence. Information interoperability is defined as the ability of systems to automatically exchange and interpret information that is common to those systems.
- In the (mostly occurring) case that more than a few systems have to exchange information, standardisation of the 'interface' is a key factor to achieve information interoperability. Otherwise, dedicated interfaces are needed between every pair of interconnected systems, leading to an exponential grow of the number of interfaces required.
- Information interoperability requires the standardisation of several aspects. One is the exchange language or information standard, in our view the most challenging and important, but also most difficult, aspect. The difficulties in defining such an information standard are a consequence of technical, operational, organisational and political matters.
- One single information standard for all information exchange between systems is a solution that is unlikely to be ever achieved, even if we restrict the 'universe' to NATO C4I systems. Therefore, a subdivision in multiple information standards — each with a specific scope — will be necessary. The set of systems that exchange information by means of the same 'scoped' information standard is called an interoperability domain.
- We assume the following preconditions for information standards that support interoperability. Firstly, only information which will (or can) be exchanged is part of the standard. Secondly, the information within the standard is used (and exchanged) by more than one system within the domain, but not necessarily by all systems.
- For interoperability domains the same argument with respect to standardisation is valid as for individual systems. When the number of domains increases, it is better to standardise the exchange between them by defining an information standard (domain) at a higher level. This line of reasoning may continue for a number of hierarchic levels.
- The scope of an interoperability domain (information standard) can depend on several factors. In general, a domain should be of maximum size and should have minimum overlap with other domains, under the condition that the information standard is still manageable with regard to overall approval, maintenance and implementation. This requires a co-ordinated interoperability domain division strategy, as part of an overall information architecture.
- The division into interoperability domains should be based upon the subject or type of the information. Diversity in information types may exist along many dimensions. For NATO C2, the following dimensions seem the most preferable ones: owners (nations, NATO), themes (Land, Air, Sea) and subfunctional areas (Generic C2, Intelligence, Logistics). Based on these dimensions, we have defined a possible optimal interoperability domain structure for NATO C2.

- In reality, several factors distress this optimal domain structure. Already existing information standards, lack of (political) agreement on a logical structure, and unfinished information standards (due to long-lasting development) are the most obvious ones. Looking at the various C4I (information standardisation) developments within NATO, compared to the optimal interoperability domain structure, leads to the following conclusions. The objective to gain a single integrated system ("Bi-SC AIS") may be too ambitious; in order to obtain NATO-wide interoperability an interoperability standard will be sufficient (and hard enough to achieve). The C4I developments could be 'directed' towards this optimal domain structure.
- Concerning interoperability within the NATO C2 area in general, we conclude that information standards and their scoping and subdivision are still very much underestimated aspects of interoperability and that more attention for these aspects is needed in the future.

References

1. NATO Interoperability Planning Document (NIPD)
2. Army Tactical Command and Control Interoperability Specifications (ATCCIS), Working Papers 14-X series (2000)
3. Allied Data Publication 3 (ADatP-3), STANAG 5500
4. "NATO signals an all change", Jane's International Defense Review (February 2000)
5. Bi-SC AIS Implementation Strategy (March 2000)
6. Bi-SC NATO Common Operational Picture - Operational Requirements (July 2000)
7. Bi-SC Data Link Migration Strategy (December 2000)
8. (Mobile) C2 in Crisis Management Operations, NL Ministry of Defence (October 1998, in Dutch)
9. Policy for Operational Information Supply, NL Ministry of Defence (April 2001, concept, in Dutch)
10. Information Architecture, Van der Sanden / Sturm (2000, in Dutch)