Coalition Interoperability Measurement Frameworks Literature Survey

Philip Bury, BEng, MBA, CMC, PTSC, PLFCSC
HDP Group Inc.
Contractor

DRDC CORA CR 2011-132
August 2011

Defence R&D Canada
Centre for Operational Research & Analysis

National Defence Défense nationale

Canada

Coalition Interoperability Measurement Frameworks Literature Survey

Philip Bury, BEng, MBA, CMC, PTSC, PLFCSC

Prepared By:
Philip Bury
151 Slater St., Suite 807
Ottawa, ON K1P 5H3
HDP Group Inc.
Contractor's Document Number: DND 1010
Contract Project Manager: Philip Bury, 613-658-3360
PWGSC Contract Number: Standing offer EN578-060502/055/ZT
CSA: Fred Ma, Defence Scientist, 613-992-4550

Defence R&D Canada – CORA

Contract Report
DRDC CORA CR 2011-132
August 2011

Principal Author

Original signed by Philip Bury

Philip Bury

Contractor

Approved by

Original signed by Ben Taylor

Ben Taylor

Acting Section Head, Joint Systems Analysis Section

Approved for release by

Original signed by Paul Comeau

Paul Comeau

Chief Scientist, DRDC CORA

This work was sponsored by Assistant Deputy Minister (Information Management) [ADM(IM)] as part of Collaborative Planning and Management Environment (CPME) Work Breakdown Element (WBE) 15BZ14, entitled "Framework for Measuring Progress in Coalition Interoperability (Five-Eyes)".

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

This paper is the report of a review of selected works that were referred to in a 2007 survey of methods to measure interoperability between military forces. It forms part of an effort to develop a framework for assessing interoperability in command, control, computers, and communications. The framework is being developed by the Joint Studies Operational Research Team, and is sponsored by Assistant Deputy Minister (Information Management). For the framework, the context of interest for interoperability was 5-Eyes (Australia, Canada, New Zealand, United Kingdom, and United States), at the strategic/operational level. The aim of this survey is to identify and describe any content of those papers that potentially contributes to the framework. The review was a limited success. The findings and recommendations are described in the Executive Summary.

It was found that many of the papers concentrated on the *Technical* aspect of interoperability, some directly technical, some very abstract. A few addressed human, organisational and policy matters. Since the papers were all published no later than 2007, it seems likely that useful work has been done since. The field is complicated by a plethora of definitions of interoperability. The four aspects of interoperability defined for this study (technical, human, doctrinal, and legislative) are too restrictive and exclude some important factors. Strong recommendations of the reviewer are: that future work focus on the human, organisational and policy aspects of interoperability; that it include preparations for unforeseen operation with allied or partner forces that do not have the technical capability or cultural assumptions of the 5-Eyes nations' militaries, and also with other governmental, non-military international, non-governmental organisations and other potential actors in the contemporary battlespace / mission space; and that empirical and field research be undertaken as soon as possible, to take advantage of current operations whilst they are still current.

Résumé

Le présent document est un rapport faisant suite à l'examen de travaux choisis cités en référence dans une enquête de 2007 sur les méthodes de mesure de l'interopérabilité entre les forces militaires. Ce document constitue une partie des efforts déployés pour concevoir un cadre d'évaluation de l'interopérabilité en ce qui a trait au commandement, au contrôle, à l'informatique et aux communications. L'Équipe de recherche opérationnelle et d'études interarmées élabore actuellement ce cadre et les travaux sont parrainés par le Groupe du Sous-ministre adjoint (Gestion de l'information). L'intérêt exprimé pour ce cadre par les Cinq pays (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) se situe au niveau interopérabilité stratégique/opérationnelle. Le but de la présente enquête est d'inventorier et de décrire tout élément de contenu des documents qui pourrait possiblement contribuer à l'élaboration de ce cadre. Cette étude a eu un succès limité. Les résultats et les recommandations sont présentés dans le sommaire.

On a découvert qu'une grande partie des documents portait sur l'aspect technique de l'interopérabilité; certains d'entre eux se présentaient comme technique alors que d'autres étaient

très abstraits. Quelques-uns portaient quant à eux sur des aspects humains, organisationnels et de politique. Étant donné que les documents ont tous été publiés en 2007 ou avant, il semble probable que les travaux utiles ont été faits depuis. Dans ce domaine, le grand nombre de définitions d'interopérabilité vient compliquer les choses. Les quatre aspects de l'interopérabilité définis pour cette étude (technique, humain, doctrinal et législatif) sont trop restrictifs et ne tiennent pas compte de certains facteurs importants. L'auteur de l'étude fait les importantes recommandations suivantes : que les travaux à venir se concentrent sur les aspects humain, organisationnel et de politique de l'interopérabilité; qu'ils incluent la préparations aux opérations imprévues avec les forces - alliés ou celles de partenaires - qui ne possèdent pas la capacité technique ou les acquis culturels dont disposent les forces militaires des Cinq pays ou avec toutes autres organisations gouvernementales, internationales non militaires ou non gouvernementales et autres intervenants pouvant être présents sur l'espace contemporain de bataille et de mission; que des recherches empiriques et sur le terrain soient entreprises aussitôt que possible afin de tirer parti des opérations actuelles alors qu'elles sont encore en cours.

Executive summary

Coalition Interoperability Measurement Frameworks Literature Survey:

Philip Bury; DRDC CORA CR 2011-132; Defence R&D Canada – CORA; August 2011.

Aim and Scope:

The aim of this literature review is to identify and describe any content of papers in a 2007 survey of measurement methods for military interoperability that can contribute to the interoperability assessment framework being developed by the Joint Studies Operational Research Team for the Assistant Deputy Minister (Information Management). The interoperability of interest is:

1. between 5-Eyes nations (Australia, Canada, New Zealand, United Kingdom, and United States),

2. in command, control, computers, and communications (C4), and

3. at the strategic/operational level, with emphasis on planning.

4. to be organized along the following four "C4[1] interoperability aspects": *Technical*, *Human* (to human), *Doctrinal*, and *Legislative*.

Findings:

1. The papers reviewed took a variety of analytical approaches to the questions and challenges of military C4 interoperability, some of them potentially useful. In general, with minor exceptions, US-based analysts considered the problems of operations involving US forces, while those from Australia and the UK considered multi-national operations, and the Australian papers also considered domestic operations, and in both domestic and expeditionary operations considered interoperability with non-military actors. These latter were found to be potentially helpful, and this broader perspective is considered by the reviewer to be important in the contemporary operating environment.

2. It was found that many of the papers concentrated on the *Technical* aspect of interoperability, some directly technical, some very abstract. A few addressed human, organisational and policy matters.

3. Since the papers were all published no later than 2007, it seems likely that useful work has been done since.

4. For the most part the analyses reviewed cited little or no empirical data, either from experiments or from operational and exercise experience. There was only one report of an

[1] C4 = Command, control, communications, and computers.

experiment, and only one (the same) with measurements, although two other writers cited historical examples. The lack of empirical data is a serious shortcoming in the study of interoperability.

5. A number of the papers reviewed examined issues which were outside this study's four agreed aspects of interoperability, which were an object of this review. They were found to be too restrictive and thus excluded some important factors. Also, the stated definitions of the four aspects were found to be vague and in need of clarification. Therefore, this review adopted two additional aspects, and posited more extensive definitions of the existing four. They are all found in section 2.1.1 below. Some others are also suggested in section 4.3 below.

6. Papers reviewed proposed some ways to assess interoperability, and to aggregate measures, but with only two exceptions, these proposals were entirely conceptual and did not provide methods of aggregating measurements. They also proposed a number of measures of performance, but almost without exception they were not truly measures, as the authors did not propose any scale or way of measuring them.. Empirical study might help both identify these and apply them to research. Although measures (things to be measured) were proposed, measurement (ways of measuring), that would produce results, were absent, with the sole exception of the experimental paper mentioned above, which had little applicability. That is to say, not only were there almost no empirical results, there were almost no ideas about how to get them or apply them.

7. A variety of definitions of interoperability were used, and these determined, or more likely were chosen in order to permit, the various paradigms offered.

8. Canadian appearances in the literature are rare, and this might be given some thought.

Recommendations:

1. If the study of interoperability is to be useful, it must be extended to interoperations with a larger variety of actors than the military forces of close allies, such as other governmental, non-military international, non-governmental organisations and other potential actors in the contemporary battlespace / mission space.

2. A key element of such an extended view of interoperability would be the organisational agility to play well in unforeseen situations with new friends who may not have the technical capability or cultural assumptions of the 5-Eyes nations' militaries.

3. As seen through the limited sample of papers reviewed, empirical and field research are required. These could include the observation of operations (In the opinion of this reviewer, the ISAF Kandahar experience is precious, about to disappear, and should not be wasted), exercises, commissioned experiments, questioning of Canadian Forces members with operational experience and historical research.

4. Potential collaborators are Defence Research and Development Canada -- Toronto and the Canadian Forces Experimentation Centre[2].

[2] Abbreviated "CFEC". CFEC is being changed into the Canadian Forces Warfare Centre at the time of writing.

Sommaire

Coalition Interoperability Measurement Frameworks Literature Survey:

Philip Bury; DRDC CORA CR 2011-132; R & D pour la défense Canada – CORA; Août 2011.

But et portée

Le but de cette étude de la documentation est de trouver et de décrire tout contenu provenant d'articles cités dans une enquête de 2007 sur les méthodes de mesure de l'interopérabilité militaire qui pouvant contribuer à élaborer le cadre d'évaluation de l'interopérabilité actuellement mis au point par l'Équipe de recherche opérationnelle et d'études interarmées pour le compte du Groupe du Sous-ministre adjoint (Gestion de l'information). Le type d'interopérabilité qui nous intéresse :

1. touche les Cinq pays (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis),
2. porte sur le commandement, le contrôle, l'informatique et les communications (C4);
3. se déroule au niveau stratégique/opérationnel, en mettant l'accent sur la planification;
4. doit être organisé en fonction des quatre « aspects de l'interopérabilité du C4 », c'est-à-dire les aspects *technique*, *humain* (à humain), d*octrinal*, et *législatif*.

Résultats

1. Les articles examinés empruntaient différentes approches analytiques relativement aux questions et aux défis liés à l'interopérabilité militaire du C4, certaines d'entre elles pouvant être utiles. En général, à quelques petites exceptions près, les analystes basés aux États-Unis examinaient les problèmes des opérations n'impliquant que les forces américaines, alors que les travaux des analystes australiens et du R.-U. portaient sur les opérations multinationales. Les articles australiens examinaient aussi les opérations nationales et, dans le cadre des opérations nationales et expéditionnaires, ils tenaient compte de l'interopérabilité avec des intervenants non militaires. Il a été déterminé que ces derniers pouvaient être utiles et l'auteur jugeait cette approche plus vaste est importante dans l'environnement opérationnel actuel.
2. On a découvert qu'un grand nombre d'articles portait principalement sur l'aspect *technique* de l'interopérabilité, certains articles étant technique, d'autres très abstraits. Quelques-uns portaient sur les aspects humains, organisationnels et de politique.
3. Étant donné que tous les articles ont été publiés en 2007 ou avant, il semble vraisemblable que des travaux utiles aient été faits depuis ce temps.
4. Dans l'ensemble, les analyses examinées ne donnaient que peu ou pas de données empiriques, qu'elles soient tirées d'essais ou d'expériences opérationnelles et d'exercices. Un

seul rapport faisait état d'un essai et un seul (le même) présentait des mesures, bien que deux autres auteurs citaient des exemple historiques. Le manque de données empiriques est défaut important dans l'étude de l'interopérabilité.

5. Quelques articles s'intéressaient à des problèmes qui ne sont pas liés aux quatre aspects de l'interopérabilité qui font l'objet de la présente étude. Ces articles se sont révélés trop restrictifs et excluaient de ce fait certains facteurs importants. De plus, les définitions énoncées des quatre aspects se sont révélées vagues et avaient besoin d'éclaircissements. En conséquence, la présente étude a adopté deux aspects supplémentaires et a proposé des définitions plus complètes des quatre définitions existantes. Elles peuvent toutes être trouvées à la section 2.1.1 ci-dessous. D'autres définitions sont aussi proposées à la section 4.3 ci-dessous elle aussi.

6. Les articles étudiés proposaient quelques façons d'évaluer l'interopérabilité et de recueillir des mesures, mais avec seulement deux exceptions, ces propositions étaient totalement conceptuelles et ne fournissaient pas de méthodes permettant de recueillir des mesures. Ces articles proposaient aussi un certain nombre de mesures du rendement, mais presque sans exception elles ne produisaient pas de véritables mesures étant donné que les auteurs ne proposaient aucune échelle ou de façons de mesurer. Une étude empirique pourrait aider à la fois à trouver une échelle ou une façon de mesurer et de s'en servir dans le cadre d'une recherche. Bien que les mesures (les choses devant être mesurées) étaient proposées, il n'y avait pas de méthodes de mesure pouvant produire des résultats, à la seule exception de l'article portant sur un essai mentionné plus tôt et qui avait peu de possibilités d'application. C'est donc dire que non seulement il n'y avait presque pas de résultats empiriques, mais qu'il n'y avait presque pas de propositions sur la façon de les obtenir ou de s'en servir.

7. Différentes définitions de l'interopérabilité étaient utilisées et celles-ci déterminaient les différents paradigmes offerts (ou plus vraisemblablement ces définitions ont été choisies afin de créer ces paradigmes).

8. Il était rare que ces articles fassent mention des Canadiens et il faudrait peut-être réfléchir à la raison de cette situation.

Recommandations

1. Pour que l'étude sur l'interopérabilité soit utile, elle doit être étendue aux interopérations avec un plus grand nombre d'intervenants plutôt que de la restreindre aux forces militaires de nos proches alliés. Elle doit porter aussi sur les autres organisations gouvernementales, internationales non militaires ainsi que les organisations non gouvernementales et les autres intervenants potentiels dans l'espace de bataille et de mission.

2. Lors d'événements imprévus, l'agilité organisationnelle à bien interagir avec nos nouveaux amis qui ne disposent pas des capacités techniques ou les acquis culturels des forces militaires des Cinq pays est l'élément clé d'une vision plus large de l'interopérabilité.

3. Tel qu'on peut le constater en raison du nombre limité d'articles étudiés, des recherches empiriques et sur le terrain sont nécessaires. Elles comprendraient l'observation des opérations (selon l'auteur de la présente étude, l'expérience acquise par la FIAS à Kandahar

est précieuse, mais pourrait bientôt se perdre), des exercices, des essais commandés, la consultation de membres des Forces canadiennes possédant de l'expérience opérationnelle et de recherche de type historique.

4. Recherche et développement pour la défense Canada – Ottawa et le Centre d'expérimentation des Forces canadiennes sont des collaborateurs éventuels.

This page intentionally left blank.

Table of contents

This page intentionally left blank.

1 Introduction

"The Combined Communications-Electronics Board[3] (CCEB) is a five nation joint military communications-electronics (C-E) organisation whose mission is the coordination of any military C-E matter that is referred to it by a member nation. The member nations of the CCEB [hereafter referred to collectively as 5-Eyes] are Australia [AU], Canada [CA], New Zealand [NZ], the United Kingdom [UK] and the United States of America [US]. The CCEB Board consists of a senior Command, Control, Communications and Computer (C4) representative from each of the member nations" [1].

In August 2010, the Centre for Operational Research and Analysis's (CORA's) Joint Studies Operational Research Team (JSORT)[4] met with the Canadian representatives to the CCEB in order to plan the development of a framework for assessing 5-Eyes interoperability. The Principal is Information Management (IM) Force Development (FD) 5, under the Assistant Deputy Minister (Information Management) [ADM(IM)]. The framework needed to be scoped so that it covered interoperability aspects that were deemed to be important and lacking (next paragraph). Part of the work plan was to contract a study of existing methods and approaches to assessing interoperability and extract those elements that could contribute to the framework. As a starting point, the study was to use one of the most comprehensive surveys on interoperability available: a 2007 survey [2] of measurement methods for military interoperability over the past three decades. A limited effort was to be devoted to identifying relevant new works as they were encountered. In particular, the same author as survey [2] refers to a few additional approaches in a later work [3], which an attempt is made to cover in this study as well.

This document reports on the study of the methods surveyed in reference [2] and mentioned in reference [3]. The aim is to identify, describe and organize ideas, methods, and metrics that can contribute to the interoperability framework. For the framework, the interoperability of interest is:

1. between 5-Eyes nations (Australia, Canada, New Zealand, United Kingdom, and United States),

2. in command, control, computers, and communications (C4), and

3. at the strategic/operational level, expeditionary and external to theatre, with emphasis on planning as opposed to intelligence.

4. to be organized along the following four "C4 interoperability aspects": *Technical*, *Human* (to human), *Doctrinal*, and *Legislative*.

Findings in Chapter 4 and recommendations in Chapter 7 refer (among other things) to the scope of study described above. The initial focus of this study on survey [2] was meant to constrain the

[3] This organization is also often referred to as The Combined Communications Electronics Board i.e. with no dash in the name.
[4] JSORT has since been split into the Information Management (IM) Operational Research Team (ORT) and the Intelligence, Surveillance, & Reconnaissance ORT, both of which are continuing this work.

scope and have a reasonably thorough analysis while respecting the contract resourcing limit. This study was not meant to be the sole source of input into the framework formulation process.

The contract for this literature review had a time limit. To meet this limit, the thoroughness of the review was selectively de-emphasized on certain papers. Therefore, some of the papers were more completely reviewed than others, based on the reviewer's judgement.

1.1 Terminology

The following terms are used throughout this paper:

1. "Interoperability" generally means C4 interoperability, except where the context indicates otherwise.

2. "Coalition" means the set of all the participants in an activity which requires a form of interoperability, and is the set of interest; and

3. "Partner" refers to each member of that coalition and possibly others with whom some form of coordination is desired.

4. Since the framework is being developed by Canada under its role as a member of the Combined Communications Electronics Board (CCEB), the above four C4 interoperability aspects are also referred to as CCEB aspects (of interoperability) in this report.

These terms as used here carry no political, policy, organisational, or doctrinal baggage other than the above, unless it is explicitly mentioned.

2 Review of Interoperability Assessment Papers

The papers in survey [2] and reference [3] (Table 1) are referred to as Ford papers, after the author of the survey of those works. This chapter presents an overview of Ford's survey, reviews and analyses each the aforementioned papers, and reviews/analyzes a few additional papers of potential relevance to the interoperability framework. As mentioned, the primary objective is to extract those elements that could contribute to the framework, as scoped out in the Introduction.

Ford's survey covers models and methodologies for measuring interoperability from the past three decades. He encountered many definitions and assessment approaches for interoperability, and noted the deep and longstanding deficiencies in interoperability, even between the U.S. Services. The survey identifies organizations that contributed significantly to interoperability research, most pertaining to the U.S. Department of Defense. It critiques fourteen approaches. Ford himself favours models that permit quantitative analysis and mathematical optimization. He found that interoperability assessment approaches have had limited adoption because most of the measurements are at low (system) levels, while the models dealing with high (social, organizational, procedural) need further development before they are suitable for widespread use.

2.1 Conduct of the Review

2.1.1 Additional Aspects

Many, or most, of the papers reviewed introduce factors, attributes, components or aspects that are logically the counterparts of the CCEB aspects but are not included in the working definition. It is the opinion of this reviewer that they need to be included in any consideration of interoperability among groups. Therefore the following two are proposed (they are explained in section 4.3 below and are used in the reviews that follow):

1. *Human Factors*, distinct from the working definition of the *Human* CCEB aspect

2. *Organisational* (factors)

Some others are suggested in the discussion in section 4.3 below, but have not been used in the review for fear of overcomplicating the analysis.

This review's index	Ford 2007 index	Ford 2009 index	Framework acronym	Year	Full name	Comment
1	1	1	SoIM	1980	Spectrum of interoperability	•Interoperability in Defense Communications, IEEE Trans. Comm., 1980 •Gilbert E. LaVean
2	2	2	QoIM	1989	Quantification of Interoperability	•The Quantification of Interoperability, Naval Engineers Journal, 1989 •Dennis R. Mensh, Robert S. Kite, & Paul H. Darby
3	4	3	MCISI	1996	Military Communications & Information Systems Interoperability	•Military Communications & Information Systems Interoperability, MILCOM, 1996 •Col. Marek Manaowicz & Col. Piotr Gajewski
4	3	4	LISI	1998	Levels of Information Systems Interoperability	•Levels of Information Systems Interoperability, C4ISR AWG, 1998 •C4ISR Architecture Working Group co-chaired by J6 and ASD(C3I)/CISA
5	5	5	IAM	1998	Interoperability Assessment	•Interoperability Assessment, Proc. 66th MORS, 1998 (revised Aug 2003) •Michael J. Leite
6	6	6	OIM	1999	Organisational Interoperability Maturity Model for C2	•Organisational Interoperability Maturity Model for C2, Proc. 3rd CCRTS, 1999 •Thea Clark & Richard Jones
7	11	10	NMI	2003	NATO C3 Technical Architecture Reference Model for Interoperability	•NATO C3 Technical Architecture Reference Model for Interoperability, 1999, 2003 •NATO Consultation, Command, and Control Agency (NC3A)
8	9	8	LCI	2003	Interoperability Roadmap for C4ISR Legacy Systems	•Beyond Technical Interoperability—Introducing a Reference Model for Measures of Merit for Coalition Interoperability, Proc. 8th ICCRTS,2003 •Andreas Tolk
9	10	9	LCIM	2003	Levels of Conceptual Interoperability Model	•The Levels of Conceptual Interoperability Model, Proc. 2003, Fall SIW, 2003 •Andreas Tolk & James Muguira
10	12		SoSI	2004	System of Systems	•System of Systems (SoSI): Final Report, CMU Tech. Report,2004 •Edwin Morris, Linda Levine, Craig Meyers, Pat Place, & Dan PlakoshSoSI
11	13	12	NTI	2004	Non-technical Interoperability	•Non-technical Interoperability in Multinational Forces, Proc. 9th ICCRTS, 2004 •K. Stewart, H. Clarke, P. Goillau, N. Varrall, and M. Widdowson
12	7	13	OIAM	2005	Organisational Interoperability Agility Model	•An Organisational Interoperability Agility Model, Proc. 10th ICCRTS,2004 •Gina Kingston, Suzanne Fewell, & Warren Richer
13		11	NCW	2003	Network Centric Warfare	Incorporated into Schades's
14		14	NID	2005	NATI (C3 System) Interoperability Directive	Ford tagged Schades's 2005 conceptual delineation of levels of abstraction as NID
15	8	7	Stoplight	2002	Stoplight	•An Interoperability Roadmap for C4ISR Legacy Systems, Acq. Rev. Qtrly., 2002 •John Hamilton, Jerome Rosen, & Paul Summers
16	14	15	i-Score	2007, 2008	Interoperability Score	•The Interoperability Score, Proc. 2007 CSER, 2007 •Thomas Ford, John Colombi, Scott Graham, & David Jacques

Table 1. Summary of Ford papers[3]. The first column is the ordinal index assigned to each work in this report. The second and third columns represents the order in which the works appear in Ford's tabulation of surveyed works (Table 1 in each of references [2] and [3] respectively).

2.1.2 Definitions of the Current CCEB aspects

Some of the brief definitions available are not entirely clear, and assumptions need to be made. The assumptions made here may not be the intent of the originators, and should be reviewed. The following assumptions are made in the present review:

1. Legal matters are included in the *Legislative* aspect.

2. Government policy and strategic direction are included in the *Legislative* aspect.

3. Technical (C4) standards and conventions are included in the *Technical* aspect.

4. Orders, direction and guidance given by a commander within a mission, whether or not they have the force of law, are considered to be *Doctrinal*. For one thing, they may be issued to allies, coalition partners, or others with whom command relationships are not absolute. However, Rules of Engagement (ROE) are almost always set by strategic HQ with legal advice, and would be considered part of the *Legislative* aspect, as they usually have the force of law.

2.1.3 Attribution of Aspects

In a few instances, this review finds opportunities where an interoperability factor or component mentioned in a paper could be interpreted as connecting to a CCEB attribute, although the connection is not made explicit in the paper and may not have been intended by the author. An effort has been made to identify these inferences, but some may have been missed.

2.1.4 Scoring the Mappings to CCEB Aspects

The review of each paper includes two sections on scoring:

1. C4 interoperability aspects addressed

2. Analysis behind the mapping to the C4 interoperability aspects

Each paper is addressed in its own section 2.*x* in this chapter (*x*=2,3,...,20). The values attributed to the mappings in the 2.*x*.3 subsections are the opinion and judgement of the contractor conducting this review, generally without benefit of any quantitative data. Therefore the numbers are estimates, necessarily imprecise. The aggregated values in 2.*x*.4 sections are a crude combination of the former, with no analytic basis, and without pretence of rigour or precision. The appearance of decimal fractions is therefore false precision and should not delude the reader. They are there only to illustrate the process, not to claim exactitude.

2.2 Ford Survey Paper #1: SoIM – Spectrum of Interoperability

2.2.1 Document Sourcing Details

1. LeVean G. (1980), "Interoperability in Defense Communications"*, IEEE Transactions on Communications*, vol.28, no.9, pp.1445-1455.

2. Found at http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1094832 (not accessed -- accessible only with subscription).

2.2.2 Overarching Comments/Description

1. Scope:

    a. This paper gives a good survey of the US communications systems interoperability situation as of 1980, largely from the technical aspect. It introduces by implication the notion of a complex system, although that paradigm did not become fashionable until later.

    b. The paper is concerned almost exclusively with interoperability amongst US military communication systems; the mentions of NATO and US civil systems really refer to possible outside users or to the use in emergency by the US military of these systems.

    c. Since the paper was written in 1980, it is set in the context of the Cold War, and some of the interoperability issues are driven by the possible transition from confrontation to conflict. Some theorists hold that the distinction is now obsolete, and that the world is in a constant state of confrontation, in which limited conflicts are nested. The situation and scenarios depicted in the paper apply well to such a context.

    d. The paper mentions that the US Defense Communications Agency is to adopt a definition of a spectrum of interoperability, yet to be developed at the time of the paper's writing. In section III, p1448, the author goes on to posit a seven-level spectrum or range, based on two factors.

        i. Technical interface possibilities

        ii. Management / control possibilities

        While the examples are dated, the notion seems sound and might be developed. The spectrum is not depicted graphically, probably for the good reason that it's not quantified.

2. Sections I and II describe the perceived need, in 1980, for communications interoperability. This is based on US defence policy at the time, the complexity of the US command structure, the need to shift from one connection to another according to the international situation, and many different communications systems with diverse ownership. Section III at p1448 introduces management / control possibilities on six levels, again not quantified. These

contribute to the spectrum combining technical and management / control possibilities, which, as noted above, cannot be considered a metric. The ensuing discussion is mostly about technical issues, but makes clear that these are complicated by the doctrinal issues mentioned.

3. Levels. Section III at p 1448 describes technical possibilities on a scale of four levels, by example. The examples are dated but could inform a contemporary description. The scale does not pretend to be metric or quantified, and therefore the spectrum based on it cannot be considered a metric. The paper deals in some depth with technical obstacles and approaches to interoperability.

4. Potential measures: Technology issues include:

   a. differing radio frequency bands

      i. Do radios use the same frequency bands?

      ii. Do shared electronic operating instructions (EOI) provide for agreed bands?

   b. differing protocols for digitisation of radio signals

      i. Is there an agreed standard for compatibility of (good) or common (better) digitisation protocols (e.g. a STANAG), shared EOI

      ii. Is there an agreed standard for compatibility of (good) or common (better) digitisation equipment (e.g. a STANAG) ,

   e. bandwidth

      - Is there agreement on bandwidth loads / service levels (STANAG),(EOI)

   f. uncontrolled, therefore divergent upgrades of originally compatible systems (this could be considered a management issue)

      - Is there standardisation in equipment (e.g. STANAG)

   g. differing secure voice protocols. This discussion addresses the technical problem of different systems designed for differing sets of protocols.

      - Is there a pre-existing agreement, like a STANAG, or one made for the mission, an EOI?

   However, the different problem of different security levels is not addressed. This could properly belong under the management / control (*Doctrinal* or *Technical*) box.

   Much of the technology is dated, but the approach seems to provide ideas for a similar approach now.

5. Amongst other things the author suggests that for practical reasons,

a. different communities should not be required to acquire identical systems, merely to make them compatible; and

b. The number of nodes required to be interoperable should be kept to a minimum.

The world has changed since the paper was written. Suggestion (a) is understandable, but should be accepted only if necessary and with great caution, as it is a potential source of trouble; "compatibility" is a fuzzy word. Suggestion (b) **should be avoided if at all possible**, since in the fluid situation of the contemporary operating environment, entities of which it was never expected can find themselves required to interoperate.

6. Goals proposed in section IV p1449 include

   a. development of (quantifiable) measures of interoperability

   b. early consideration of interoperability in the design stage of systems, bolstered by these measures

   c. configuration control to ensure that compatible systems do not become incompatible

   d. discipline and measurability in the setting of interoperability requirements, since they are design constraints which would hamper other performance needs.

2.2.3 C4 Interoperability Aspects Addressed

1. *Technical* 7

2. *Doctrinal* 3

2.2.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

1. As discussed above, most of this paper examines technical obstacles to interoperability, and possible solutions. Therefore the *Technical* aspect is allocated 7/10 of the weight of this paper. *Technical* 7.

2. The discussion of what the author calls management / control possibilities is useful, and while limited, underlies the more extensive discussion of technical issues. This factor might be considered part of the *Human* aspect, but could also be connected to *Doctrinal* or *Legislative*. On balance, *Doctrinal* seems to be a more appropriate box and is therefore allotted 3/10 of the weight of this paper. However, this carries the caveat that the management / control discussion concerns mainly the management / control of communications systems, so this weight might be reconsidered. *Doctrinal* 3

2.2.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

1. Political. See section 4.3 below.

2. Security. See section 4.3 below.

3. Interagency. See section 4.3 below.

2.3 Ford Survey Paper #2: QoIM – Quantification of Interoperability

2.3.1 Document Sourcing Details

Mensh et al. (1989), "The Quantification of Interoperability"*, Naval Engineers Journal*, vol.101, no.3, pp.251-259.

2.3.2 Overarching Comments/Description

1. The study reported here posits seven components of interoperability, and then attempts to measure their validity and importance to overall performance of a wide-area multi-subsystem C2 system. Regrettably, it was difficult to understand the paper due to assumptions by the authors about the familiarity of the reader with the environment. It is doubtful that even readers with that familiarity would fully understand the report. As nearly as it can be understood the concept mixed intra-system performance components with externalities, and allowed both to overlap. The logic of the argument and the design of the experiment were difficult to follow.

2. The study was interesting in that it used a computer simulation to generate experimental inputs, and human observers to assess the outcomes, an approach that seems to have potential.

3. The study examined the overall performance of a simulated wide-area communications-computation-human system, and may have had some success in doing so.

4. The assumptions in the experiment are questionable, as are the logic and experimental technique. There are some interesting concepts, including an adaptation of the Boyd loop, thought it is not clear that this is intentional. The components listed in 2.3.4 below seem to confuse characteristics on the one hand and inputs / externalities on the other.

5. However, this effort had two significant and all-too rare virtues: it produced data, and it proposed a reality-based method to integrate the data to develop a way of assessing interoperability as a whole

    a. The QOIM effort was an experiment in the laboratory sense; it posited a set of measurables, and measured them, in a trial with real people, suitable test subjects and a plausible scenario.

    b. The authors then propose gathering data over a number of iterations, plotting them against success and failure, and finding correlations. This logic is sound, although it leaves open the question of how to identify overall mission interoperation success

and failure, and doesn't seem to suggest a programme to test and validate in realistic exercises and real operations, which is vital.

2.3.3 C4 Interoperability Aspects Addressed

1. *Technical* 4.2
2. *Doctrinal* 0
3. *Human* 0
4. *Legislative* 0
5. *Human Factors* 2.6
6. *Organisational* 3.2

2.3.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The study posits seven components of interoperability:

1. media
2. languages
3. standards
4. requirements
5. environment
6. procedures
7. human factors

These are explained as follows.

1. **Media** was defined, in effect, as carrier and connection quality. The associated Measure of Effectiveness was Completeness = Exchange AND Utilisation (of information regarding exercise events), the two latter being Measures of Performance (MoP). Exchange seems to mean that if a message were originated, it was received, which would be principally a *Technical* matter. Utilisation would mean that if a message were received, it was acted upon, which would appear to be a *Human Factors* effect. Both of these factors could have occurred exclusively within a single electronic-human system, without regard to Interoperability, and the report does not discriminate. The most interesting result seems to be that when a message got though, it was acted upon 4/5 times. *Technical* 6, *Human Factors* 4

2. **Languages** was defined as the means by which service or data is exchanged over one or more media, including receipt, intelligibility, processing means, time to process, and error rate and type. This would mix our *Technical* and *Human Factors* aspects, in proportions difficult to judge. The MoE and MoP were Message Correctness = Intelligibility AND Manual intervention and Error, both of which latter could be attributed to *Technical* or *Human Factors* effects. The report correctly acknowledges that since the events and outcomes were simulator-generated, the Language component did not apply in this experiment. *Technical* 5, *Human Factors* 5.

3. **Standards** were defined as criteria to direct operational commonality among equipment or systems. These are *Technical*, but cannot be applied to existing systems, which must be assessed on reality, not aspiration. MoE and MoP were Messages Correctly Translated = Messages Processed AND Translation Errors. These MoP appear to be peculiar to single components of a system or sub-system, cannot be considered measures or components of interoperability and can't be considered useful to our study. Again, the report correctly acknowledges that since the events and outcomes were simulator-generated, the Standards component did not apply. *Technical* 10.

4. **Requirements** was defined as the set of operational needs and fiscal realities. These might drive design and acquisition, and would serve as standards for assessment, but are not elements of interoperability. MoE and MoP were Tactical Picture Consistency = Correlation Data AND Timeliness Data. This is hard to understand, but in any case was not measured.

5. **Environment** was defined as the set of identifiable instances, operational needs and mixtures of systems, units or forces, including weather, electromagnetic interference. It seems that these things are externalities outside the control of the maker or the user, and would be issues only as factors in design. They therefore cannot be connected to any of our Aspects. The MoE and MoP were Target Valid Detection = Target Opportunities AND Target Classification. These don't seem to correspond to the definition. The events counted as successes seem to be those in which targets were detected and reported, and interoperability then must include sensor performance. Since the experiment was simulation-based, it is difficult to see what these outcomes show.

6. **Procedures** were defined as rules of conduct that guide the man (sic) in his interaction with other men or with non-human systems. These would include Standard Operating Procedures (SOP), operational plans (OPLANS) and doctrine. This is the CCEB *Doctrinal* component. MoE was based on a variation of Boyd's OODA loop, and given the acronym TEMPO. MoP were TEMPO=Procedures Followed AND Message Processing Delay and Mission Impact. Effectively TEMPO was to determine, given existing procedures (*Doctrinal*) if and how well the procedures were effectively executed, and the impact resulting if they were not well followed. This was, in effect, a measure of internal staff performance, so it does not appear to have measured the component as defined or to have been related to interoperability as we understand it. As measured, it would be the *Organisational* aspect 10.

7. **Human Factors** were defined as the set of factors that cannot generally be described by predictable behaviour, and the generally intangible elements of interoperability in a man-machine interface. They could include human error, improper training, procrastination, stress etc. This would seem to apply both to intra-subsystem performance and to inter-subsystem

interoperation. The MoE and MoP were Processing Timeliness = Human Errors AND Manual Correlation AND Decision Making Delays. There is no indication of whether events were inter-subsystem transactions or local, and so no measure of interoperation seems to have been possible. One interesting result is that only one of seven outcomes was successful, which certainly indicates the importance of the *Human Factors* considered. *Human Factors* 4, *Organisational* 6.

Simple arithmetic then gives the attribution in section 2.3.3 above.

2.3.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

The content of the report and the discussion above cover elements in both the *Human Factors* and *Organisational* aspects proposed.

2.4 Ford Survey Paper #3: MCISI – Military CIS Interoperability

2.4.1 Document Sourcing Details

1. Amanowicz et al. (1996), "Military Communications and Information Systems Interoperability", *Proceedings of the IEEE Military Communications Conference,* vol. 1.

2. Found at http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D568629&authDecision=-203 (21 October 2010 accessible only by IEEE subscription).

2.4.2 Overarching Comments/Description

This paper describes a method for determining the interoperability of pairs of systems given quantitative criteria, treated as the distance between pair members in interoperability space. The paper does not name, describe or attempt to assess any such criteria. It would be an interesting model to pursue if these criteria (probably subsets of the CCEB aspects) were available and suitably quantified. The paper does not appear to consider the weighting of the criteria once defined and measured.

2.4.3 C4 Interoperability Aspects Addressed

None.

2.4.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

None.

2.4.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None.

2.5 Ford Survey Paper #4: LISI – Levels of Information Systems Interoperability

2.5.1 Document Sourcing Details

1. Description found in Appendix D of: C4ISR Architecture Working Group (1997), *C4ISR Architecture Framework Version 2.0*, 18 December 1997, http://www.fas.org/irp/program/core/fw.pdf (accessed 21 October 2010).

2. The more extensive LISI source document is *Levels of Information Systems Interoperability (LISI)*, C4ISR Architecture Working Group 139 pp, 30 March 1998. It has not yet been studied, but a very quick and cursory scan of section 2.18 (LISI 2) suggests that the document that was studied is a fair representation.

2.5.2 Overarching Comments/Description

1. The study is focussed principally on the *Technical* aspect but the form of the discussion could easily be transferred to other aspects. It refers to exchange between nodes, not systems, so would (?) address intra-system interoperability (maybe not). Perhaps the view being taken (This is important in the review of other studies) regards the system being considered as the set of the various entities, be they simple systems or simple nodes, as the target of the examination. The study appears to address US, and US Department of Defense (DoD) needs, not international or interagency.

2. The Procedures, Applications, Infrastructure, Data (PAID) attributes could be seen as conceptually similar to the CCEB components. However, with the exception of the Procedures attribute, which considers doctrine etc, the study addresses hardware and software almost exclusively.

3. The Levels portion of this model is out of the scope of the present study, but might be useful in the overall CCEB exploration of interoperability.

4. The LISI model is widely cited, at least at the time of the Ford papers, and appears to have been taken into use in the defence industry and perhaps the IT systems industry generally. It appears to provide a useful framework for considering some aspects of interoperability.

5. Similarly, the overall system architecture, as described in the C4ISR AWG Report referred to above, of which the LISI model is Appendix D, invites study of the other aspects. See for example section 3 of that report, in particular discussion of the Operational Architecture View.

6. Note that section 3 of the LISI 1998 source document mentioned in section 2.18 includes an Assessment Model, with profiles, metrics, and questionnaires.

2.5.3 C4 Interoperability Aspects Addressed

1. *Technical* 7.5

2. *Doctrinal* 2.5

2.5.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The closest this paper comes to addressing the CCEB aspects is the PAID paradigm:

1. "***P***rocedures focus on the many forms of guidance that impact on system interoperability, including doctrine, mission, architectures, and standards." *Doctrinal* 10;

2. "***A***pplications represent the functional aspects of the system. These functions are manifest in the system's software components, from single processes to integrated applications suites." *Technical* 10

3. "***I***nfrastructure defines the range of components that enable interactions between systems, including hardware, communications, system services, and security. For example, infrastructure considers the protocols, enabling software services, and supporting data structures for information flow between applications and data." *Technical* 10

4. "***D***ata includes the data formats and standards that support interoperability at all levels. It embodies the entire range of styles and formats from simple text to enterprise data models." *Technical* 10

Simple arithmetic then gives the attribution in section 2.5.3 above

2.5.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

1. The LISI Levels of Interoperability model, concerned mostly with system technical matters, is not intended to correspond to the four-aspect view. However, any study of the interoperability must take the notion of progressive levels into account, difficult though they may be to assess and measure.

2. Similarly, as mentioned section 2.5.2 paragraph 5 above, there would be useful elements in the Report of which LISI forms a part, if it has not been studied before.

2.6 Ford Survey Paper #5: IAM – Interoperability Assessment Model

2.6.1 Document Sourcing Details

1. Leite, Michael J. (1998), "Interoperability Assessment", *66th MORS Symposium*, Naval Post Graduate School, Monterey, CA , 23-25 June.

2. Found at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA350577&Location=U2&doc=GetTRDoc.pdf (accessed 21 October 2010)

2.6.2 Overarching Comments/Description

This paper develops a framework for assessing the technical interoperability of – principally within – a communications and processing system, that is, a system providing the last two Cs of C4. It gives a set of levels or "Degrees of Interconnection", ascending, Connectivity, Availability, Interpretation, Understanding, Execution, Feedback. It then gives a set of nine Interoperability Components: Requirements, Standards, Data elements, Node connectivity, Protocols, Information flow, Data latency, Interpretation, Understanding, and Information utilisation.

2.6.3 C4 Interoperability Aspects Addressed

1. *Technical* 8

2. *Doctrinal* 1

3. *Human Factors* 1

2.6.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The paper addresses almost exclusively the *Technical* aspect of C4 Interoperability. The Interoperability Components given in the paper can be mapped to the CCEB aspects as follows:

1. Requirements. *Technical* 10;

2. Standards. *Technical* 10;

3. Data elements. *Technical* 10;

4. Node connectivity. *Technical* 10;

5. Protocols. *Technical* 10;

6. Information flow. *Technical* 10;

7. Data latency. *Technical* 10;

8. Interpretation. *Technical* 10;

9. Understanding. *Technical* 10; and

10. Information utilisation. *Technical* 10

11. Therefore the mapping is simple: The paper is all *Technical*. However, with imagination, we are reminded of some other possibilities. The paper:

    a. under Standards discusses standardisation, which could remind the reader of the *Doctrinal* aspect,

    b. under Data suggests (without using the term) a common data dictionary, which could be standardisation and again *Doctrinal*,

    c. under Interpretation mentions individual processors, which here imply the *Technical* aspect but could equally well be *Human Factors* ,

    d. under Information Utilisation verification and validation which again are intended to be technical but could be *Human Factors*, or *Organisational*, or *Doctrinal*.

These interpretations are almost certainly unintended by the author, but they serve as reminders and even inform the reader of other aspects, which are accordingly attributed above.

Therefore, quite arbitrarily, the mapping in section 2.6.3 above was determined.

2.6.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None observed.

2.7 Ford Survey Paper #6: OIM – Organisational Interoperability Maturity Model

2.7.1 Document Sourcing Details

1. Clark, T. et al. (1999), "Organisational Interoperability Maturity Model for C2", *3rd International Command and Control Research and Technology Symposium*, Newport, Rhode Island, June.

2. Found at http://www.dodccrp.org/events/1999_CCRTS/pdf_files/track_5/049clark.pdf (accessed 21 October 2010).

2.7.2 Overarching Comments/Description

1. This paper introduces the idea of organisational interoperability, and finds that the LISI Reference Model is "principally technological". It proposes the Organisational Interoperability Model, based on a definition of interoperability as "the need of one group to interact in some way with another group". This is understood herein to mean that the remainder of the paper then addresses the ability of one group to interoperate with another, rather than the capability of the larger set or system of interactors. The paper sees "compatibility" as the degree with which one electronic system can operate with another. This illustrates that much of the current discussion of interoperability focuses on the interaction or compatibility of (or more properly, between and among) electronic information systems, and overlooks the human and organisational dimensions, for which the paper proposes a model, that could serve as an extension of the LISI model.

2. For the organisational approach to interoperability the paper asserts that the large variety of situations in which one organisation might need to operate with another makes fully planned (prescriptive) interoperability impractical and that flexible interoperability is required. That is, a participating organisation must be prepared to interoperate in a way that cannot be prepared in advance. This relates to suggestions in other papers reviewed, and in the reviewer's comments in Chapters 4 and 7.

3. The paper then proposes levels of organisational interoperability, in descending order: unified; combined; collaborative; ad hoc; and independent. It then proposes that each of these levels demands a corresponding level of system compatibility as given in the LISI model. It refers to the LISI model of exchange levels of information systems (LISI p D-4) and proposes the model of Organisational Interoperability Maturity (OIM). The levels of Organisational Maturity (sic – but evidently the levels of Organisational Interoperability Maturity) are given in descending order

   a. unified,

   b. combined,

   c. collaborative,

   d. ad hoc, and

   e. independent.

   A correspondence between these levels and the LISI levels is made.

4. To support this argument, the paper posits attributes of Organisational Interoperability, which correspond in a logical sense to the CCEB aspects. They are preparedness, understanding, command style and ethos, and are discussed below.

5. Pursued by Fewell and Clark (2004), "Evaluation of Organisational Interoperability in a Network Centric Warfare Environment", *9th International Command and Control Research*

and Technology Symposium, Copenhagen: The Command and Control Research Program, http://www.dodccrp.org/events/9th_ICCRTS/papers/010.pdf

2.7.3 C4 Interoperability Aspects Addressed

The organisational approach described in this paper can be mapped broadly to the following CCEB aspects:

1. *Doctrinal* 1.75
2. *Human* 1.75
3. *Human Factors* 3
4. *Organisational* 3.5

2.7.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The argument in this paper can best be mapped to the CCEB aspects by reviewing the attributes of organisational interoperability that it describes. With the paper's definitions, and a discussion of how they might be mapped, they are:

1. **Preparedness:** "This attribute describes the preparedness of the organisation to interoperate. It is made up of doctrine, experience and training." Doctrine, as used here, is pretty well the *Doctrinal* aspect, which also includes joint training. The training required is not only joint, that is inter-organisation training, but collective training within the various organisations, and individual training. Experience builds relationships and trust, the *Human* aspect, but also individual skills, which would be *Human Factors*, and group skills, an *Organisational* aspect. Experience also reinforces the cohesion that enables a group to function, and thus to interoperate coherently with other groups. Therefore this attribute would map to the *Human Factors* aspect and to an *Organisational* quality, as suggested in section 4.3 below. Somewhat arbitrarily, let us say *Doctrinal* 3, *Human* 1, *Human Factors* 3, *Organisational* 3.

2. **Understanding:** "The understanding attribute measures the amount of communication and sharing of knowledge and information within the organisation and how the information is used." This is partly organisational structure, which can be mapped to the *Doctrinal* aspect. It will be affected by relationships and trust, which is the *Human* aspect. Understanding will also be affected by pre-existing individual *Human* Factors, and *Organisational* experience and culture. Say *Doctrinal* 2, *Human* 2, *Human Factors* 3, *Organisational* 3.

3. **Command Style:** "This is the attribute that describes the management and command style of the organisation – how decisions are made and how roles and responsibilities are allocated/delegated." This attribute will in part be related to the *Doctrinal* aspect and also relationships and trust and thus the *Human* aspect. However, it is also very much based on the command presence of each individual commander, and the acceptance of command by individuals, human elements not captured by the latter aspect, and also by the tradition or

4. **Ethos:** "The ethos attribute is concerned with the culture and value systems of the organisation and the goals and aspiration of the organisation. The level of trust within the organisation is also included." Although the trust relationships of the *Human* aspect are included, the writers make it clear here that this is an attribute belonging to the group, and could be described as organisational culture and cohesion. *Human* 2, *Human Factors* 3, *Organisational* 5.

Now if as a first approximation we assign each of the above attributes equal weight, arithmetic gives us the mapping in section 2.7.3 above. That calculation is far from scientific, but may give an idea of the direction of this paper.

2.7.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

Described in Chapter 4 below.

1. *Human Factors*.

2. *Organisational*.

The discussion above indicates that the authors of the OIM paper have in mind some qualities of an organisation, making it capable of interoperation with others that are not captured by the four CCEB aspects of interoperability as stated. These could include both an expanded definition of the *Human* and, *Human Factors*, aspects and an additional aspect covering non-doctrinal elements of organisation, such as cohesion and organisational culture (*Organisational*).

2.8 Ford Survey Paper #7: NMI – NATO Tech Architecture

2.8.1 Document Sourcing Details

The Ford reference, the NATO C3 Technical Architecture (NC3TA) Model, as Major Ford then observed, is still not easy to find on the NATO website. The furnished substitute, ADatP-34(D) 2010, NATO Interoperability Standards and Profiles, is hard to find on the web. Note, however, that both the Ford Paper and the SOSI paper discuss the NC3TA. **It is worth finding**.

2.8.2 Overarching Comments/Description

ADatP-34(D) is, like many NATO publications, very difficult to read. It addresses standards and protocols. Profiles are described in terms of the standards achieved and the protocols effectively adopted. It was very difficult to find any reference to any interoperability component other than strictly *Technical*.

2.8.3 C4 Interoperability Aspects Addressed

Only the *Technical* aspect is addressed, and this is limited to data and protocol compatibility, and agreed service levels. It is no doubt an important element of NATO C4 interoperability, but it is of little value in measuring overall interoperability except in supporting effective data transfer.

2.8.4 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None.

2.9 Ford Survey Paper #8: LCI – Layers of Coalition Interoperability

2.9.1 Document Sourcing Details

1. Tolk, A. (2003), "Beyond Technical Interoperability -- Introducing a Reference Model for Measures of Merit for Coalition Interoperability", *8th International Command and Control Research and Technology Symposium*.

2. A slide presentation was provided and is found at http://www.dodccrp.org/events/8th_ICCRTS/Pres/track_1/2_1530tolk.pdf (accessed 26 October 2010)

3. The supporting paper was found with some difficulty at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.79.6784&rep=rep1&type=pdf. Time limitations permitted only brief review of the paper. This indicated that the slide set reviewed here is an accurate representation of the paper.

2.9.2 Overarching Comments/Description

This is a slide presentation. Dr. Tolk, evidently a systems engineer, uses that potentially very powerful approach and goes well beyond the technical focus of his earlier LCIM paper, using the Net-Centric Warfare paradigm as a frame of reference. The work refers to "networking humans, organizations, institutions, services, nations, etc" and suggests that the "Social and Organizational Component may superimpose [sic] the Technical Interoperability". It quotes the elusive NATO C3 TA Reference Model for Interoperability as giving the highest level of interoperability as "(4) Seamless Sharing of Info: •Common Information Exchange; and •Distributed Applications". The author quotes with approval the NATO Code of Best Practice for Command and Control Assessment at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA422189&Location=U2&doc=GetTRDoc.pdf, which proposes a hierarchy of measures:

1. Measures of Policy Effectiveness (MoPE), which focus on policy and societal outcomes;

2. Measures of Force Effectiveness (MoFE), which focus on how a force performs its mission or the degree to which it meets its objectives;

3. Measures of C2 Effectiveness (MoCE), which focus on the impact of C2 systems within the operational context;

4. Measures of Performance (MoP), which focus on internal system structure, characteristics and behaviour; and

5. Dimensional Parameters (DP), which focus on the properties or characteristics inherent in the physical C2 systems.

These have the virtue of focussing on desired outcomes, and giving adequate attention to political, doctrinal, social and human factors. That document, the NATO Code of Best Practice (NCOBP), **is worthy of further study**. Tolk goes on to propose a structure of metrics, and a series of layers of coalition interoperability. A valuable contribution of this work is that the author emphasises a number of non-technical factors in effective interoperability, and proposes metrics that give them adequate attention. Regrettably, of course, the proposed metrics do not provide detail that would result in quantified values. The author describes his set of measures as a "core / hub" (a framework, one might say) that can then be filled with what he calls "real" measures for real systems. Dr. Tolk makes an important point when he cites the top level of interoperability from the NCOBP as "Measures of Policy Effectiveness" and in his own proposed hierarchy for net-centric warfare, puts at the top "Measures of Military Utility". In each case, the very important message is that, in the end, the value of interoperability lies in its contribution to political / policy and military objectives.

2.9.3 C4 Interoperability Aspects Addressed

1. Technical 4.22

2. Doctrinal 3

3. Human 0.11

4. Legislative 1.56

5. Human Factors 0.78

6. Organisational 0.33

2.9.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The most convenient hook for mapping is the set of Layers of Coalition Interoperability. The layers, and corresponding CCEB aspects, are;

1. Political Objectives *Legislative* 10

2.	Harmonized Strategy/Doctrines	*Doctrinal* 6, *Legislative* 4
3.	Aligned Operations	*Doctrinal* 3, *Human* 1, *Human Factors* 3, *Organisational* 3
4.	Aligned Procedures	*Doctrinal* 10
5.	Knowledge/Awareness	*Technical* 3, *Doctrinal* 3, *Human Factors* 4
6.	Information Interoperability	*Technical* 5, *Doctrinal* 5
7.	Data/Object Model Interoperability	*Technical*
8.	Protocol Interoperability	*Technical* 10
9.	Physical Interoperability	*Technical* 10

A very arbitrary summation gives the weighting in section 2.9.3 above.

2.9.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

Human Factors, *Organisational*. See Chapter 4 below.

2.10 Ford Survey Paper #9: LCIM – Levels of Conceptual Interoperability Model

2.10.1 Document Sourcing Details

1. Tolk, A. & Maguira, J. (2003), "The Levels of Conceptual Interoperability Model", *2003 Fall Simulation Workshop,* Orlando, FL, September.

2. Found with some difficulty at http://www.sisostds.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=24721&PortalId=0&TabId=105 (accessed 26 October 2010)

2.10.2 Overarching Comments/Description

This paper is concerned with data compatibility, data models and data protocols. It proposes a series of levels of compatibility based on the degree to which data standards lend themselves to mutual understanding. It argues that even with a high degree of data standardisation, data sets

cannot be mutually recognisable and understandable between user systems without very specific data models. The paper proposes a series of levels of conceptual (data) interoperability.

2.10.3 C4 Interoperability Aspects Addressed

1. *Technical* 10

2.10.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

With quite a stretch, the discussion of the need for conceptual data interoperability could be connected to Doctrinal standards and Human intervention. This paper is concerned entirely with data dictionaries, standards and protocols, and is therefore entirely *Technical*.

2.10.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None discovered.

2.11 Ford Survey Paper #10: SoSI – System of Systems Interoperability

2.11.1 Document Sourcing Details

1. Morris, E. et al. (2004), System of Systems Interoperability (SOSI): Final Report, April 2004, Carnegie Mellon University, Systems Engineering Institute, CMU/SEI-2004-TR-004 / ESC-TR-2004-004.

2. Found at http://www.sei.cmu.edu/reports/04tr004.pdf (accessed 30 October 2010).

2.11.2 Overarching Comments /Description.

This paper is the report of a research effort funded by DoD in order to identify problems in interoperability and find solutions. It identifies six DoD and Institute of Electrical and Electronic Engineers (IEEE) definitions and despairs of ever finding a definition satisfactory to all. It then gives the working definition used throughout the study: The ability of a set of communicating entities to (1) exchange specified state data and (2) operate on that state data according to specified, agreed-upon, operational semantics. The discussion proceeds with a review of the LISI, OIM, LCIM, and LCI models, generally consistent with those herein, and the still-elusive NC3TA, which it describes as “intended to categorize how operational effectiveness could be enhanced by structuring and automating the exchange and interpretation of data”. The paper then posits the System of Systems (SOSI) model, which is intended to address the features of the other models but also to address “programmatic concerns between organizations building and maintaining interoperable systems” with a consistently applied set of management, constructive, and operational practices that support the interoperability web. “Improvements in technology alone (whether XML or any other) will not be sufficient. There must be parallel improvements in

the ways that current and future interoperability needs are identified, and how organizations pursue interoperability." So the SOSI study acknowledges the organisational and human dimensions as being important and under-studied, but goes little further in addressing them.

"The SOSI model extends the existing models by adding a focus on programmatics (e.g., activities performed to manage the acquisition of a system). In the SOSI model, programmatic, constructive, and operational issues must be managed across the life cycle." That is, the SOSI model addresses the many challenges of developing systems that are interoperable. It gives little detail concerning any of these issues. What is needed is a set of compatible models that collectively address all of the dimensions of interoperability."

2.11.3 C4 Interoperability Aspects Addressed

A full score of interoperability as envisaged by this review can't be attributed to this paper, as it is concerned with so much that is outside the scope. By implication only:

1. *Technical* 2
2. *Human Factors* 0.5
3. *Organisational* 1

2.11.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The paper acknowledges the requirement to address the *Human Factors* and *Organisational* aspects, but no more than that. It deals with *Technical* matters only slightly more. Its principal contribution is to recommend measures to develop and acquire US DoD systems that are mutually interoperable (programmatics). There is so much emphasis on this matter that it seems unreasonable to give the aspects mentioned in section 2.11.3 any more than the low scores shown above.

2.11.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

See Chapter 4 below.

The matter principally addressed in this paper is "programmatic", which is the whole business of acquiring mutually interoperable systems for the US DoD. That factor does not appear to be an aspect of interoperability within the intent of this review.

2.12 Ford Survey Paper #11: NTI – Non-Technical Interoperability

2.12.1 Document Sourcing Details

1. Stewart, K. et al. (2004), "Non - technical Interoperability in Multinational Forces", *9th International Command and Control Research and Technology Symposium*, Copenhagen, 14-16 September.

2. Found at http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/130.pdf (accessed 30 October 2010).

2.12.2 Overarching Comments/Description

This paper is part of a series by the UK Defence Scientific and Technical Laboratory (DSTL) and QinetiQ PLC, relating to 'command in the network enabled era'. As the title makes clear, it is intended to address the non-technical aspects of interoperability. It does so by identifying "sources of incompatibility" through interviews with British military officers with multinational operational experience. The paper then acknowledges the OIM model, and presents the non-technical interoperability framework (NTI) which amends and expands it as follows:

a. Preparedness

   i. Organisational Preparedness.

   ii. Preparedness of Personnel.

b. Understanding

   i. Communication.

   ii. Coordination Between Contingents

c. Command

   i. Command Style

   ii. Command Structure

d. Ethos

   i. Level of Trust (between contingents)

   ii. Shared Goals and Purpose

   iii. Cultures and Values

The paper goes on to propose the Multinational forces Co-operability Index (MCI) which proposes a matrix for assessing interorganisational interoperability, based on suggesting degrees or levels (or measures) for each of a number of implied components of the components of the four attributes listed above

The paper then proposes a number of possible areas of interoperability that have the potential to undermine it, and would be candidates for intervention. Unfortunately, they are not mapped to the attributes, but this should not be difficult.

This paper is probably the best of any reviewed herein in its treatment of non-technical aspects or attributes of interoperability. It is significant in using empirical data: interviews with officers with operational experience.

2.12.3 C4 Interoperability Aspects Addressed

See Chapter 4 below.

1. *Doctrinal* 7.17
2. *Human* 9
3. *Legislative* 0.67
4. *Human Factors* 9.67
5. *Organisational* 13.5

2.12.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The NTI models maps as follows[5]:

a. Preparedness

   i. Organisational Preparedness. Doctrine 4, *Organisational* 6

   ii. Preparedness of Personnel. *Human* 3, *Human Factors* 7;

b. Understanding

   i. Communication. *Human* 5, *Human Factors* 5

   ii. Coordination Between Contingents. *Doctrinal* 4, *Human* 2, *Organisational* 4;

c. Command

[5] With more time, the reviewer could have gone into greater detail.

i. Command Style. *Doctrinal* 2, *Human* 2, 2, *Human Factors* 3, *Organisational* 3;

ii. Command Structure. *Doctrinal* 3, *Human* 2, *Human Factors* 3, *Organisational* 2;

d. Ethos

i. Level of Trust (between contingents) *Human* 6, *Organisational* 4

ii. Shared Goals and Purpose. *Legislative* 2, *Organisational* 8

iii. Cultures and Values. *Doctrinal* 2, *Human Factors* 2, *Organisational* 6.

If each sub-attribute within an attribute is arbitrarily weighted equally, and then each attribute likewise, the result is the scoring in section 2.12.3 above.

2.12.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

See section 4.3 below.

1. *Human Factors*.
2. Political.
3. *Organisational*.

2.13 Ford Survey Paper #12: OIAM – Organisational Interoperability Agility Model

2.13.1 Document Sourcing Details

1. Kingston G. et al. (2005), "An Organisational Interoperability Agility Model", *10th International Command and Control Research and Technology Symposium* submission 158, June.
2. Found at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA463924&Location=U2&doc=GetTRDoc.pdf (accessed 31 October 2010).

2.13.2 Overarching Comments/Description

This paper studies Organisational Interoperability Agility, an organisation's *potential* to have agile interfaces in future coalition operations. It emphasises the variety and unpredictability of potential interoperability partners and challenges. Building on the OIM, it analyses the attributes that extend that model to interoperability agility maturity. Though questionable, the authors

subsume Understanding into Preparation on the grounds that the former is a component, or a result, of the latter. They expand Command to include Command and Coordination, and add to all three resulting attributes the factors seen as necessary for agility in interoperability. Thus they give three attributes:

1. Preparation;

2. Command and Coordination; and

3. Ethos.

The authors also propose levels of interoperability maturity. In descending order: Dynamic, Open, Accommodating and Static. They also identify the areas of scope required to develop organisational (interoperability) agility: the *organisations* with which interoperation may be required, the *activities* that may be involved, and the *environment* in which this is to occur. Comment: this paradigm relates to discussions in section 4.3 paragraph 7 and section 4.5.1 below concerning the scope of the present study.

2.13.3 C4 Interoperability Aspects Addressed

1. *Doctrinal* 10.5

2. *Human* 1.25

3. *Human Factors* 3

4. *Organisational* 7.75

2.13.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

While the attributes listed correspond broadly to those in the OIM model, they give slightly differing emphasis to each (slightly abridged below):

1. Preparation.

    a. Compatible doctrine and the ability to rapidly achieve this with a broad variety of organisations. Doctrinal 4, Organisational 6

    b. Wide variety of relevant collective experience working with a variety of organisations. Organisational 10

    c. The ability to rapidly plan and train to achieve interoperability. Doctrinal 4, Human Factors 2, Organisational 4

    d. Mechanisms to work together and share information already in place and practiced with other organisations Doctrinal 5, Organisational 5;

2. Command and Coordination.

a. Mechanism for interacting with management / C2 styles. Doctrinal 10

b. Practice in timely change of C2 styles and to adjust and exploit C2 styles. Organisational 10

c. Ability to staff C2 structures from the whole organisation (should include building joint C2 structures with partner organisations). Doctrinal 5, Organisational 5; and

3. Ethos.

a. Willingness to operate with any partner in the context, including those with no formal doctrine, and to share information as necessary. Doctrinal 2, Human 2, Human Factors 3, Organisational 3

b. Willingness to recognise and act on common purpose. Doctrinal 2, Human 3, Human Factors 3, Organisational 2

c. Experience in adapting to changes in doctrine. Human Factors 4, Organisational 6

d. Willingness to accommodate differences in goals and values and recognise a common purpose, while working with organisations with multiple and conflicting goals (e.g. Afghanistan today). Doctrinal 2 Human 2, Human Factors 3, Organisational 3.

This breakdown subjectively yields the scores in section 2.13.3 above.

2.13.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

1. *Human Factors*.

2. *Organisational*.

These suggested aspects are described in section 4.3 and mapped in section 4.2, below.

2.14 Ford Survey Paper #13: NCW Power to the Edge

2.14.1 Document Sourcing Details

1. Alberts, D. and Hayes, R. (2003), *Power to the Edge: Command...Control...in the Information Age,* Command and Control Research Program (US DoD).

2. Found at http://www.dodccrp.org/files/Alberts_Power.pdf (accessed 31 October 2010).

3. Chapter 7 pp. 107-122 addresses interoperability.

2.14.2 Overarching Comments/Description

1. Chapter 7 discusses concepts of information interoperability. It introduces four domains of interoperability, based on four domains of warfare:

   a. Physical. Devices, media and connectors;

   b. Information. A signal gets to its intended destination, with content intact;

   c. Cognitive. The signal makes sense; and

   d. Social. Ability and willingness to create a shared understanding.

5. Chapter 7 also discusses the relative complexity of a system of interoperable systems. It proposes as one solution a regime of *post and smart pull* which requires only that one participant be able to map another's data to one's own. It seems that this could be considered a smart hub system, or a loose federation.

6. In the current strategic and operational environment, net-centric warfare (NCW) is seen by many as an obsolete buzzword. Nevertheless, there is much in this chapter, the rest of the paper, and the whole of Alberts and Hayes's work, and the work of others, on NCW that could be of interest to an analyst or designer of interoperability. For example, at page 27, the assumptions for self-synchronization are:

   a. Clear and consistent understanding of command intent;

   b. High quality information and shared situational awareness;

   c. Competence at all levels of the force; and

   d. Trust in the information, subordinates, superiors, peers, and equipment.

   These factors (assumptions) have been taken into account in the analysis in section 2.14.4 below. However, that portion of the book was not studied in the present review. **The whole book warrants reading in the context of the sponsor's interoperability study.**

2.14.3 C4 Interoperability Aspects Addressed

1. *Technical* 3

2. *Doctrinal* 2.25

3. *Human* 0.75

4. *Human Factors* 1.75

5. *Organisational* 2.25

It should be kept in mind that, due to the subjective nature of the analysis, extra decimal places do not imply greater accuracy.

2.14.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

The four domains of interoperability in this paper could be mapped to the CCEB aspects, although they are conceptually somewhat different. The mapping would be inexact, as the domains are based on concepts different from the CCEB aspects, but if attempted it would be as follows:

1. Physical. In the paper, Physical is used both to describe the physical environment of warfare, that is, the movement of soldiers and ships etc and the application of force, or effects, but also applied to network interoperability to mean the means of transmission. In this latter sense it is *Technical* 10;

2. Information is the creation, manipulation and sharing of information, and could be *Technical* 2, *Doctrinal* 3, *Human Factors* 2, *Organisational* 3;

3. Cognitive contains perceptions, awareness, beliefs, values, sense-making and decisions. Say *Doctrinal* 3, *Human* 1, *Human Factors* 3, *Organisational* 3; and

4. Social means the set of interactions between and among force entities. *Doctrinal* 3, *Human* 2, *Human Factors* 2, *Organisational* 3.

Simple arithmetic provides the scoring in section 2.14.3 above.

2.15 Ford Survey Paper #14: NID – NATO Interoperability Directive

2.15.1 Document Sourcing Details

1. Schade, U. (2005), "Towards the Edge and Beyond: The Role of Interoperability", *10th International Command and Control Research and Technology Symposium*, 13-16 June.

2. Found at http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/091.pdf (accessed 3 November 2010)

Note: Schade refers to and quotes a document called the NATO Interoperability Directive (NID) AC322-SC/2-WG/4 WP(2003)0015-REV-2. Ideally, given more time, this document would also be reviewed.

2.15.2 Overarching Comments/Description

Even though Ford refers to this work as NID, Schade actually draws heavily upon NID and other works to articulate his own perspective of interoperability. This paper argues that in discussion of interoperability, at the time of writing, there was (perhaps is) a disconnect between system and

force views, and seeks to converge them. The author maintains that the important thing is that forces be interoperable. He then proposes levels of force interoperability, in ascending order:

1. Missing interoperability, where forces cannot exchange any data;

2. Physical interoperability, where forces can exchange data but there is no guarantee that it can be interpreted. It is then necessary for the human intellect to interpret it;

3. Syntactic interoperability, in which information can be exchanged and shared, but not necessarily knowledge, and human intellect must be applied at a higher level, still subject to misunderstanding and potentially great attendant consequence;

4. Semantic interoperability, where information is interpreted identically by all. Common situational awareness emerges; however, this is not sufficient for self-synchronisation; and

5. Pragmatic interoperability, where the receiver of a message recognises the intent behind it. Schade acknowledges Alberts & Hayes, supra, also requiring competence at all levels, and trust in the information, subordinates, superiors, peers and equipment.

Schade emphasises the importance of first, data transfer and, second, common language; all else can be achieved by humans. He wanders into the territory of edge organisations, NCW etc, quoting Alberts & Hayes, explaining that such organisations are outside hierarchy, and it is not sufficient that they receive and understand orders or understand superior's intent, but that they share it. **This observation is important** when the study of interoperability is extended to non-military organisations, and allies whose commitment may not be absolute.

2.15.3 C4 Interoperability Aspects Addressed

1. *Technical* 1.4

2. *Doctrinal* 2.2

3. *Human* 1.2

4. *Human Factors* 2

5. *Organisational* 2.8

2.15.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

Schade is discussing interoperability from a different perspective than in the present project. He gives levels, but does not explicitly mention aspects, factors or attributes. However, some may be inferred:

1. Information transfer. *Technical* 7, *Doctrinal* 3

2. Common understanding. *Doctrinal* 4, *Organisational* 6

3. Shared intent. *Doctrinal* 2, *Human* 2, *Legislative* 2 based on widely understood political direction, *Human Factors* (Command style), 2 *Organisational* 2;

4. Trust. *Human* , 4, *Human Factors* 3, *Organisational* 3; and

5. Competence. *Doctrinal* 2, *Human Factors* 5, *Organisational* 3.

2.16 Ford Survey Paper #15: Stoplight

2.16.1 Document Sourcing Details

1. Hamilton J. et al. (2002), "An Interoperability Road Map For C4ISR Legacy Systems", *Acquisition Review Quarterly* (Winter).

2. Found at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA487874&Location=U2&doc=GetTRDoc.pdf (accessed 4 November 2010)

2.16.2 Overarching Comments/Description

This paper proposes a colour code based on:

1. operational requirements;

2. acquisition requirements;

3. interface effectiveness; and

4. rates of readiness based on the above.

However, the paper does not provide any suggested requirements or interface standards. It provides a very basic aggregation method only.

2.16.3 C4 Interoperability Aspects Addressed

The paper describes *Technical* factors only, in a very general way, not warranting a score.

2.16.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

Mapping is of no value.

2.16.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None found.

2.17 Ford Survey Paper #16: i-Score – Interoperability Score

2.17.1 Document Sourcing Details

1. Ford et al. (2007), "The Interoperability Score", *Proceedings of the 5th Annual Conference on Systems Engineering Research,* Hoboken, NJ, 14–16 March.

2. Found at http://www.stevens-tech.edu/ses/seem/fileadmin/seem/Proceedings_PDF/27 (accessed 4 November 2010).

2.17.2 Overarching Comments/Description

This paper proposes a method for assessing interoperability. A mathematical model is based on the level of human intervention (taken to be the need for translation, human or machine, between members of a pair of systems. The discussion sets aside physical / technical issues such as the quality of physical (electronic digital) communication and adopts a very broad meaning for translation, seeming to extend to all means necessary to make an exchange mutually beneficial in enhancing the knowledge (or perhaps any performance) intended by the exchange. No attempt is made herein to follow the mathematics of the aggregation, but it seems plausible. This approach assumes a numerical measure in each pair case, of the degree (and, presumably, type) of translation or intervention required, but seems to have potential as an aggregation and assessment tool.

2.17.3 C4 Interoperability Aspects Addressed

This assessment model could address any interoperability aspect as long as it could be quantified.

2.17.4 Analysis Behind the Mapping to the C4 Interoperability Aspects

None.

2.17.5 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None

2.18 Ford Survey Paper #17: LISI 2

2.18.1 Document Sourcing Details

C4ISR Architecture Working Group (1998), C4ISR Architecture Working Group *Final Report -- Levels of Information Systems Interoperability (LISI)*, 30 March.

2.18.2 Overarching Comments/Description

This is a more extensive LISI source document than that originally reviewed (section 2.5 above). It is a later LISI model and contains an Assessment model which proposes a number of metrics which are conceptual and do not contain quantifiable (numeric) measures. The metrics are based on the Capabilities Model, Fig 3-7 therein. It proposes a rollup to successive levels of interoperability which is depicted graphically and verbally but not numerically. It has not been studied in this review, but a very quick and cursory scan suggests that the LISI document that was studied in section 2.5 above is a fair representation, in the PAID paradigm, for mapping to the CCEB aspects. The "LISI 2" paper is referred to here, in this section, because it is probably the real Ford 2007 reference and probably warrants further study.

2.19 NATO C3 System Interoperability Directive (NID)

2.19.1 Document Sourcing Details

AC/322-D(2004)0040 and associated documents.

2.19.2 Overarching Comments/Description

Caveat: These documents were skimmed only very briefly

The NID is concerned mainly with processes, approvals and controls. It emphasises the importance of Interoperability Requirements (IOR), because in the view presented by the documents, C4 interoperability need and should only be pursued in directions justified by the importance of the supporting IOR. It describes the NATO Interoperability Environment (NIE) which is to include a number of required elements. Noticeable were the Gateways between respective C3 systems, whose function is to facilitate information flow, and the Boundary Protection Devices, whose function is to control it. There seems to be little attention to the nature, concept or technology of C3 / C4 Interoperability

2.19.3 C4 Interoperability Aspects Addressed

Very rough estimate:

1. Technical 3
2. Doctrinal 3
3. Legislative 4

2.19.4 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

None

2.20 ForceNet

2.20.1 Document Sourcing Details

The Technical Cooperation Program's (TTCP's) Technical Report ForceNet Implications For Coalitions Study TR-MAR-23-2006 March 2008 and associated documents.

2.20.2 Overarching Comments/Description

Caveat: These documents were skimmed only very briefly

ForceNet is described (as of the time the report was written) as a proposed architecture for net-centric maritime warfare (NCMW) in the US Navy and among allied (TTCP) navies; an

> "operational construct and architecture framework for naval warfare in the information age, which integrates warriors, sensors, network, command and control, platforms and weapons into a networked, distributed combat force, scalable across the spectrum of conflict from seabed to space and sea to land."

The collection and the report document a study into the benefits and costs to each partner of implementing the ForceNet architecture in the TTCP navies. A number of maritime scenarios were gamed, and the benefits to each, of successive levels of ForceNet development were assessed. Then the steps required to implement in each navy were discussed. Since this was a collaborative document, no overall decision was proposed. The report includes the following:

> "…access to a capable network is necessary but not sufficient to fully reap the military benefit of sharing information in the battlespace. Determining networked systems value must include processes that explore the manner in which the system could or should be used. There is a need for concurrent development of technical systems and coalition operational concepts that inform on hybrid systems utility and accommodate legacy and emerging warfare concepts of operation (CONOPS). The complexity introduced by networking will mean that a priori identification of optimal system utility is very difficult… *An a priori system-of-systems design for NCMW is impractical. Complex behaviour and usage of networked systems cannot be anticipated* (emphasis reviewer's). Coherent design of coalition systems of systems is unmanageable due to the misalignment of national equipment programmes. The concept of "compose-ability" or "plugability" to rapidly assemble tailored force packages suggests a practical way forward."

2.20.3 C4 Interoperability Aspects Addressed

Very rough estimate:

1. Technical 3
2. Doctrinal 4
3. Organisational 3

2.20.4 C4 Interoperability Factors Covered Other Than the Four Predetermined C4 Interoperability Aspects

Programmatic: Very broadly, the steps each navy (including Canada's) must take, largely in capital acquisition, to implement various stages of ForceNet in different platforms. Anyone such as Director of Maritime Requirements (Sea) interested in acquisition of ForceNet should study it.

3 New Papers (not Reviewed in this Literature Study)

There has been little opportunity during this review to search for additional papers on interoperability. The following is merely a list of accidental finds and the reviewer's ideas.

1. Huynh and Osmundson A Model for Assessing the Performance of Interoperable, Complex Systems, http://sse.stevens.edu/fileadmin/cser/2006/papers/127-Huynh-Performance%20Assessment%20Model.pdf (accessed 6 November 2010)

2. The OIM model has been pursued by Fewell and Clark, http://www.dodccrp.org/events/9th_ICCRTS/papers/010.pdf

3. Real NID, NATO Interoperability Directive (NID) AC322-SC/2-WG/4 WP(2003)0015-REV-2 as referred to in section 2.15 above.

4. NATO Code of Best Practice for Command and Control Assessment at http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA422189&Location=U2&doc=GetTRDoc.pdf

5. Remainder of NCW book, and related works by Alberts & Hayes and others under DODCCRP, on NCW etc at dodccrp.org.

6. Atkinson et al., "The Agile Organisation", http://www.dodccrp.org/files/Atkinson_Agile.pdf
   - Reviewer's note: It's a while since this reviewer has read it, but it is worth a look.

7. Hamilton et al., *Developing Interoperability Metrics,* Chapter 6 of the SPAWAR Interoperability IA Research Project (see item 8 below), 4 Dec 2002, http://www.eng.auburn.edu/users/hamilton/security/spawar/6_Developing_Interoperability_Metrics.pdf (accessed 9 Nov 2010)

8. Hamilton et al. ed, *SPAWAR Interoperability IA Research Project,* Auburn University, apparently sponsored by (US Navy) Space And Naval Warfare Systems Command (SPAWAR), http://www.eng.auburn.edu/users/hamilton/security/spawar (accessed 9 Nov 2010)

9. Clarke, H., Goillau, P., and Stewart, K. G. (in preparation). Development of a framework for soft interoperability in multinational forces. Referred to in the NTI paper as a more thorough treatment of the subject, as an unpublished QinetiQ Report. Not found with a cursory search.

10. Briscombe et al., *D3C: a coherent, socio-technical framework for identifying, modelling and managing risks in coalition C2,* http://www.dodccrp.org/events/11th_ICCRTS/html/presentations/137.pdf (accessed 9 November 2010). May be the paper mentioned in item 9 above.

11. Pigeau R. (ed) and McCann C. (ed) The Human in Command ISBN 978-0306463662

4 Perspective on the Coverage of Reviewed Papers

4.1 Balance

1. Many of the papers reviewed are principally concerned with the *Technical* aspect in one way or another, although this term has to include some broad high-level conceptual views.

2. In most but not all cases, unsurprisingly, papers originated by US agencies are concerned with interoperability within US, generally military, systems, most often from a technical perspective; while those originating outside the US, such as Australia (several) or the UK, take a multinational and often interagency view and most often cover non-technical perspectives. These latter, non-technical interagency and domestic, were found to be potentially helpful, and this broader perspective is considered by the reviewer to be important in the contemporary operating environment.

3. Almost all of the papers reviewed were theoretical, and there were very few with any empirical content. This is a weakness of the literature reviewed.

4.2 Potential Measures From Ford Papers by Interoperability Aspect

The following is a list, by interoperability aspect (the CCEB four plus two used by the reviewer) of each of the papers reviewed, with some potential measures taken *or inferred, sometimes liberally,* from them.

Papers reviewed proposed some ways to assess interoperability, and sometimes to aggregate measures, but with only two exceptions, these proposals were entirely conceptual. They proposed a number of measures of performance, but almost without exception these were not truly measures, as the authors did not propose any scale or way of measuring them and did not provide methods of aggregating measurements. Although measures (things to be measured) were proposed, measurement (ways of measuring), that would produce results, were absent, with the sole exception of one experimental paper, which had little applicability. That is to say, not only were there almost no empirical results, there were almost no ideas about how to get them or apply them. *Empirical study is necessary for successful study of this field.*

Caveat: Many of the following suggested measures are a result of interpretation and extrapolation, often generous, by the reviewer, that may or may not have been intended by the respective author.

4.2.1 *Technical*

1. SOIM.

    a. Matching radio frequencies (Y/N)

b. Compatible radio digitisation protocols

c. Agreed bandwidth loads (service level)

d. Coordination of system upgrades

e. Common (best) or compatible (good) secure voice protocols

2. QOIM

a. Media

i. Carrier quality

ii. Connection quality

b. Languages (computer)

i. Intelligibility

ii. Error rate

c. Standards

i. Message processing

ii. Translation (machine) errors

d. Requirements

i. Common (strategic, operational, tactical) picture consistency

ii. Common (strategic, operational, tactical) picture timeliness

e. Environment (sensor data interpretation?)

i. Target detection

ii. Target identification

f. Procedures Not technical

g. Human Factors Not technical

3. MCISI

This paper describes a mathematical method for aggregating measures of interoperability given quantitative measures, but contains no potential measures. See section 4.4 paragraph 2 below.

4. LISI

   Using the PAID attributes:

   a. Procedures

      i. Compatible or interoperable system architectures

      ii. Common standards

   b. Applications

      - Compatible software, from processes to application suites.

   c. Infrastructure

      i. Communications and processing equipment

      ii. Standard system services

      iii. Compatible protocols

      iv. Compatible data structures

   d. Data

      - Standardised data formats and styles

5. IAM

   Quality attributes

   a. Common agreed acquisition (design) requirements for data, information exchange and intersystem controls

   b. Standard definitions of nodes, content and media (carriers)

   c. Agreed data elements and dictionary

   d. Agreed service and quality levels for node connectivity, that is, carrier quality

   e. Agreed protocols for access to each data stream (this might address the automated elements of security)

   f. Agreed standards for automated tracking of information according to format, originator, subject etc (the automated version of human tracking of messages in and out, and action taken)

   g. Agreed standards for information flow capacity and reliability

h. Agreed standards for data latency or timeliness

i. Agreed standards for (automated) message interpretation,

j. Agreed standards for (automated) utilisation (tracking, losses, misclassification, fratricide (of messages) duplication),

k. Agreed standards for system quality control and feedback.

6. OIM

The *Technical* aspect is not covered in this paper.

7. NMI

- Promulgates common technical and system architecture

8. LCI

a. Physical connections are compatible

b. Communication protocols are compatible

c. Data elements and standards are compatible

d. Communication interfaces are compatible

e. Documentation of system functionality is commonly understood (good) and compatible (better) or common (best)

f. Modelling language (this applies even beyond simulators) is unified (UML proposed)

g. Common operating picture is in place and available to all

h. A common model of the operation (one step up from a common operating picture)

9. LCIM

- Data models are fully documented and compatible from the structural to the semantic level

10. SOSI

a. Programmatic interoperability

- Coordination of system requirements in acquisition

b. Constructive e interoperability

- Coordinated and informed design and project management

c. Operational interoperability

   i. Intuitive (user friendly) interfaces

   ii. Opportunistic users who find workarounds (kluges) to interoperability problems

11. NTI

    No technical aspects mentioned.

12. OIAM

    No technical measures in this paper.

13. NCW

    - Common standards in the creation, manipulation and sharing of information

14. NID. Liberal interpretation.

    a. Information transfer

       i. Quality

       ii. Timeliness

       iii. capacity

    b. Common understanding

       - Common operational picture

15. Stoplight

    - None

16. i-Score

    - Seamlessly intelligible exchange of information

4.2.2 *Doctrinal*

1. SOIM

   The *Doctrinal* aspect is covered in this paper only by implication. The only possible measure that suggests itself is the adoption and maintenance of compatible standards. A STANAG or QSTAG type of document concerning communication compatibility could be considered either technical or doctrinal. An EOI could be considered doctrine, and adherence to standards to which these are held might be an opportunity for a measure.

2. QOIM

   - Procedures. Doctrine is mentioned in passing, so a measure might be: consistent doctrine for interoperation in handling and responding to incoming traffic.

3. MCISI

   - None

4. LISI

   - Procedures

     i. Standard doctrine including

     ii. Standard mission statement formats and content

5. IAM

   To map IAM to the *Doctrinal* aspect is a generous extrapolation of this paper, which is mainly technical.

   a. Agreed protocols for access to information (this might also address elements of security),

   b. Agreed standards for response and execution (time, format, content etc)

   c. Agreed standards for (human) message interpretation,

   d. Agreed standards for (human) utilisation of messages, of whatever form (message control, tracking of information, actions etc) etc),

6. OIM

   a. Preparedness

      i. Previously agreed common (best) or compatible (good) doctrine

      ii. joint training

      iii. Agreement, implemented, for collective training by partners in adapting to a common, or each others', doctrine

      iv. Agreement, implemented, for individual training standards in operating with coalition partners

   b. Understanding

      - Common or partner doctrine is universally accepted and understood

   c. Command style

- Command style doctrine is universally homogenous across the coalition, or is adaptable to the styles of others

7. NMI
   - No doctrinal measures
8. LCI
   a. Harmonised doctrine
   b. Aligned operations
   c. Aligned procedures
   d. Common knowledge awareness
   e. Information interoperability
9. LCIM
   - No doctrinal measures
10. SOSI
    - No doctrinal measures identified
11. NTI
    a. Preparedness
       i. Availability of doctrine for interoperation, at all levels
       ii. Compatible structures and processes across the coalition
    b. Understanding
       i. Agreed common standards for spoken and written language (best) or language proficiency among personnel (good)
       ii. Agreed procedures and willingness to exchange information
       iii. Procedures for routine exchange of liaison officers
    c. Command style
       - Doctrinal basis for assuring compatibility and adaptability of command styles
    d. Command structure
       i. Compatible structures

ii. Compatibility of formal command relationships

iii. Doctrine assuring unity of effort

e. Ethos

i. Doctrine fostering mutual trust and understanding

ii. Doctrine fostering development and support of shared goals and purpose

iii. Doctrine fostering learning and harmonising of culture and values

12. OIAM

a. Preparation.

i. Compatible doctrine

ii. Established procedure to rapidly harmonise doctrine with a broad variety of organisations.

iii. Procedures established and practiced to rapidly plan and train to achieve interoperability.

iv. Mechanisms to work together and share information already in place and practiced with other organisations

b. Command and Coordination.

i. Mechanism for interacting with different management / C2 styles.

ii. Process for timely change of C2 styles and to adjust and exploit C2 styles.

iii. Procedure to staff C2 structures from the whole organisation (should include building joint C2 structures with partner organisations).

c. Ethos.

i. Doctrine fostering willingness to operate with any partner in the context, including those with no formal doctrine, and to share information as necessary.

ii. Doctrine fostering willingness to recognise and act on common purpose.

iii. Doctrine fostering practice in adapting to changes in doctrine.

iv. Doctrine to accommodate differences in goals and values and recognise a common purpose, while working with organisations with multiple and conflicting goals (e.g. Afghanistan today). **Comment**: This is a strategic issue which needs a lot of work.

13. NCW

    a. Clear and consistent understanding of command intent

    b. Common standards in the creation, manipulation and sharing of information

14. NID. Liberal interpretation.

    a. Procedures for information transfer

    b. Procedures for common understanding

    c. Doctrine for shared intent among partners

15. Stoplight

    - None

16. i-Score

    - Seamlessly intelligible exchange of information

4.2.3 *Human*

1. SOIM.

   None.

2. QOIM

   None.

3. MCISI

   None

4. LISI

   None

5. IAM (probably unintended)

   - Information Utilisation. Verification and validation

     i. Validated high level of confidence in information from counterparts

     ii. Validated high level of confidence that information will be put to use

     iii. Willingness to accept and share verification measures of counterparts

6. OIM

    a. Preparedness

        - Individuals in partner organisations are familiar to each other through visits, meetings and joint exercises and training

    b. Understanding

        - Individuals are accustomed to sharing knowledge and understanding with members of other partners

    c. Command style

        - Commanders are familiar with and trust each other

    d. Ethos

        - Organisational goals, value systems and culture are shared (best) or understood and accepted (good) across the coalition

7. NMI

    - No *Human* measures

8. LCI

    - *Human* aspect not covered in this paper

9. LCIM

    - *Human* aspect not covered in this paper

10. SOSI

    - *Human* aspect not covered in this paper

11. NTI

    a. Preparedness

        i. Prior training and education in interoperation

        ii. Prior personal contact by meetings, exercises etc

    b. Understanding

        - Relationships developed to ensure mutual understanding

    c. Command style

        i. Development and maintenance of mutual trust among commanders through education, joint exercises and personal contact

ii. Development and maintenance of comfortable relations and understanding among commanders through education, joint exercises and personal contact

iii. Experience and understanding in development of unity of effort

d. Compatible structures

- Familiarity and trust in the command relationships of other partners

e. Ethos

i. Development and maintenance of mutual trust and understanding of the values, cultures, goals and aspirations of partners

ii. Shared goals and purpose

iii. Prior ability through training, education and practice to learn and harmonise values, cultures, goals and aspirations of partners

12. OIAM

a. Preparation.

i. Wide variety of relevant individual experience working with a variety of organisations.

ii. Familiarity with members of partner organisations through joint exercises and training, meetings and visits

iii. Experience and skill in working with members of partner organisations and developing and validating relationships on the fly

iv. Established habits of working together and sharing information with other organisations

b. Command and Coordination

i. Commander experience and skill with partner command counterparts and diverse management / C2 styles.

ii. Practice in timely change of C2 styles, structures and relationships

c. Ethos.

i. Willingness to accept any partner in the context,

ii. Willingness to recognise and act on common purpose.

iii. Willingness to work and collaborate with those of unfamiliar organisations and cultures

iv. Willingness to accommodate differences in goals and values and recognise a common purpose, while working with organisations with multiple and conflicting goals (e.g. Afghanistan today, and no doubt on future missions).

13. NCW

a. Shared beliefs and values

b. Trust in partner information, individuals, organisations and equipment.

14. NID. Liberal interpretation.

- Trust

15. Stoplight

- None

16. i-Score

- Seamlessly intelligible exchange of information

4.2.4 *Legislative*

1. SOIM.

- None.

2. QOIM

- None.

3. MCISI

None

4. LISI

- Agreed common mission

5. IAM

- Interpretation. (Implied)

i. Consistent high standard in sending easily understood traffic

ii. Consistent ability to understand incoming traffic

6. OIM

a. Preparedness
   - Political authorities and agreements are in place to enable all aspects of interoperability.

b. Understanding
   - Individuals are authorised to share knowledge and understanding with members of other partners

c. Command style

   i. Commanders are authorised to conduct joint training

   ii. Commanders are authorised to transfer and accept appropriate command authority, are aware of this authority, and have practised it jointly

d. Ethos

   i. Authority has been granted to adapt organisational goals to the needs of interoperability

   ii. Commanders are granted authority to adapt organisational goals, value systems and culture to the needs of the coalition

7. NMI
   - Requires formal adoption by all parties

8. LCI

   a. Common (best) or compatible (good) political objectives

   b. Harmonised strategy

   c. Shared knowledge and awareness

9. LCIM
   - *Legislative* aspect not covered in this paper

10. SOSI
   - *Legislative* aspect not covered in this paper

11. NTI

   a. Preparedness

      i. Government authorisation for interoperation, and preparation and training for interoperability, all levels

ii. Government authorisation of compatible structures and processes across the coalition

b. Understanding

i. Government adoption of common spoken and written language (best) or

ii. Government resourcing of language proficiency among personnel (good)

iii. Government authority and willingness to exchange information

iv. Government direction and resources for routine exchange of liaison officers

c. Command style

- Policy basis for assuring compatibility and adaptability of command styles

d. Command structure

i. Policy basis for compatible structures

ii. Policy basis for compatibility of command relationships

iii. Policy assuring unity of effort

e. Ethos

i. Policy support for developing and assuring mutual trust and understanding

ii. Policy support for developing and assuring shard goals and purpose

iii. Policy support for learning and harmonising culture and values

12. OIAM

a. Preparation.

i. Prior authority to interoperate and prepare for interoperability

ii. Authority and resourcing for working with a variety of organisations.

iii. Authority and resourcing to rapidly plan and train to achieve interoperability.

iv. Prior authority to work together and share information with other organisations

b. Command and Coordination.

i. Prior authority to adapt command structures and relationships to the requirements of interoperability as they arise

ii. Authority to staff C2 structures from the whole organisation (should include building joint C2 structures with partner organisations).

c. Ethos.

- Authority, prior or with a quick response, to adapt goals and objectives to harmonise with partners

13. NCW

- No measures identified in the chapter reviewed

14. NID

a. Authority for information transfer.

b. Shared (strategic) intent

15. Stoplight

- None

16. i-Score

- Seamlessly intelligible exchange of information

4.2.5 *Human Factors*

1. SOIM.

- None.

2. QOIM

a. Media. Consistent prompt and effective response (handling and action) to incoming traffic

b. Languages.

i. Consistent preparation of traffic intelligible to partners

ii. Consistent ability to interpret and understand incoming traffic from partners

c. Human Factors.

- Training and skill in dealing with information in an interoperability environment

3. MCISI

4. LISI

- None

5. IAM

   This is a generous extrapolation of this paper, which is mainly technical:

   - Agreed training and skill standards

6. OIM

   a. Preparedness

      i. Individuals are trained and accustomed to working in an interoperability situation with expected partners

      ii. Individuals are culturally and socially prepared for working in an interoperability situation with expected (Comment: and unexpected) partners

   b. Understanding

      i. Individuals are trained for and accustomed to sharing knowledge and understanding with members of other partners

      ii. Individuals are trained and prepared to understand, and share understanding of, procedures, styles and customs / culture of other partner organisations

   c. Command style

      i. Commanders understand and adapt to the command styles of others partners

      ii. Commanders are able to adapt command style to the needs of other partners

   d. Ethos

      i. Organisational goals, value systems and culture are shared among organisations across the coalition

      ii. Organisational goals, value systems and culture are shared among individuals across the coalition

7. NMI

   - No human factors measures

8. LCI

   - Shared knowledge and understanding

9. LCIM

   - No human factors measures

10. SOSI

- Operational interoperability
  - Opportunistic users who find workarounds (kluges) to interoperability problems

11. NTI

    a. Preparedness

        i. Skill and experience in interoperation, at all levels

        ii. Compatible training and skills across the coalition

    b. Understanding

        i. Common spoken and written language (best) or language proficiency among personnel (good)

        ii. Knowledge of the organisation, doctrine, structure and culture of partner organisations

        iii. Authority, facility and willingness to exchange information

        iv. Routine exchange of liaison officers as a source of the above

    c. Command style
        - Willingness for and experience in assuring compatibility and adaptability of command styles

    d. Command structure

        i. Familiarity with differing command structures and relations of partners, and willingness to adapt to them

        ii. Experience and skill in developing and maintaining unity of effort

    e. Ethos

        i. Experience, willingness and skill in developing and assuring mutual trust and understanding

        ii. Experience, willingness and skill in developing and assuring shared goals and purpose

        iii. Experience, willingness and skill in learning and harmonising culture and values

12. OIAM

    a. Preparation.

i. Individual skill and experience in operating with a broad variety of organisations.

ii. Individual skill and experience in rapidly planning, train and achieving interoperability

iii. Individual skill and experience working together and sharing with other organisations

b. Command and Coordination.

i. Skill and experience interacting with different management / C2 styles

ii. Skill and experience in timely change of C2 styles and formal command relationships and to adjust and exploit C2 styles

iii. Ability to build and staff C2 structures from the whole organisation (should include building joint C2 structures with partner organisations)

c. Ethos.

i. Willingness and judgement to operate with any partner in the context, including unfamiliar ones,

ii. Willingness to work together with other partners to arrive at a common purpose.

iii. Readiness to adapt to changes in doctrine

iv. Willingness to accommodate differences in goals and values and recognise a common purpose, while working with organisations with multiple and conflicting goals (e.g. Afghanistan today)

13. NCW

a. Clear and consistent understanding of command intent;

b. Competence at all levels

c. Effective interactions between and among force entities

14. NID. Liberal interpretation.

- Competence

15. Stoplight

- None

16. i-Score

- Seamlessly intelligible exchange of information

4.2.6 *Organisational* Factors

1. SOIM
   - None
2. QOIM
   a. Procedures
      i. Consistent and effective use of standard procedures, doctrine etc
      ii. Ability to respond well to failures in, or failures to follow, procedures
   b. Human Factors
      i. Collective training and skill in operating in a complex interoperability environment
      ii. Operating environment that minimises stress, and the impact of stress
3. MCISI
   - None
4. LISI
   - Agreed common mission
5. IAM
   - None
6. OIM
   a. Preparedness
      i. Organisations are trained and accustomed to working in an interoperability situation with expected partner organisations
      ii. Organisations have adopted, or are prepared to adopt, structures and procedures to a common standard (best) or to each other (good)
      iii. Organisations are culturally and socially prepared for working in an interoperability situation with expected partners
   b. Understanding
      i. Organisations are trained for and accustomed to sharing knowledge and understanding with members of other partners

ii. Organisations are trained and prepared to understand, and share understanding of, procedures, styles and customs / culture of other partners

c. Command style

i. Commanders throughout the organisation are trained and prepared to understand and adapt to the command styles of others partners

ii. Commanders throughout the organisation are trained and prepared to adapt command style to the needs of other partners

d. Ethos

i. Organisational goals, value systems and culture are shared among organisations across the coalition

ii. Organisational goals, value systems and culture are shared among individuals across the coalition

7. NMI
   - No organisational factors measures

8. LCI

   a. Aligned operations

   b. Aligned procedures

9. LCIM
   - No organisational factors measures

10. SOSI
    - No organisational factors measures

11. NTI

    a. Preparedness

    i. Collective skill, openness and experience in interoperation, at all levels

    ii. Organisational culture of welcoming interoperation and willingness to take the steps to enable it

    iii. Organisational culture encouraging individual and group efforts to enable interoperability

iv. Compatible and mutually understood structures and processes across the coalition

b. Understanding

i. Collective knowledge and understanding of partners

ii. Authority and cultural willingness to exchange information

iii. Routine exchange of liaison officers and encouragement in terms of career and other rewards, of exchange postings

c. Command style

i. Organisational experience in and willingness for assuring compatibility, acceptance and adaptability of command styles

ii. Familiarity with partner command styles

d. Command structure

i. Compatible structures

ii. Culture of versatile command relationships

iii. Culture of developing and maintaining unity of effort

e. Ethos

i. Culture of encouraging and developing mutual trust and understanding

ii. Culture of developing and assuring shard goals and purpose

iii. Culture fostering learning and harmonising culture and values

12. OIAM

a. Preparation.

i. Compatible doctrine *and* the ability to rapidly achieve this with a broad variety of organisations

ii. Compatible organisational culture

iii. Organisational culture fostering collaboration with partners

iv. Organisational culture robust enough to adapt to that of other partners

v. Wide variety of relevant collective experience working with a variety of organisations

vi. The ability to rapidly plan and train to achieve interoperability

vii. Mechanisms to work together and share information already in place and practiced with other organisations

b. Command and Coordination.

i. Mechanism for, and skill and experience in interacting with differing management / C2 styles

ii. Collective skill and experience in timely change of C2 styles and in adjusting and exploiting C2 styles.

iii. Collective ability to reorganise C2 structures and the ability to staff them from the whole organisation (should include building joint C2 structures with partner organisations)

c. Ethos.

i. Collective willingness to operate with any partner in the context, including those with different organisational cultures and structures, and to share information as necessary

ii. Collective willingness to recognise and act on common purpose

iii. Collective skill and experience in adapting to changes in doctrine

iv. Collective willingness to accommodate differences in goals and values and recognise a common purpose, while working with organisations with multiple and conflicting goals (e.g. Afghanistan today)

13. NCW

a. Clear and consistent understanding of command intent;

b. Collective competence at all levels

c. Effective interactions between and among force entities

14. NID. Liberal interpretation.

a. Common understanding

b. Shared intent.

c. Mutual trust within and among organisations

d. Organisational competence

15. Stoplight
    - None

16. i-Score
    - Seamlessly intelligible exchange of information

4.2.7 Other Factors

1. Elements of interoperability performance might include:

   a. Performance of interfaces;

   b. Performance of connectors; and

   c. Performance of nodes.

2. SOIM.

   The Goals suggested in section IV of the SOIM paper, in section 2.2.2 paragraph 6 above, are about (for countries, alliances or forces) how to get to and sustain (mainly technical) interoperability and are not about interoperability itself. They should be of interest to ADM(IM) staff and to CCEB in developing a programme.

4.3 Aspects of Interoperability

The CCEB aspects taxonomy must be revisited. For one thing, it is of limited value in the absence of a set of more thorough formal definitions of the aspects. For another, it seems (this may not be true, as the domain evolves) that the three aspects other than *Technical* will overlap and be hard to classify in the absence of very rigorous definition and inevitably some judgement. Some aspects or scope expansions that might be considered follow:

1. *Doctrinal* must include not only doctrine shared among partners, but each member organisation's doctrine concerning interoperability, and that doctrine's ability to adapt to changing circumstances and partners.

2. *Human* in its present CCEB definition is very restrictive, therefore see the proposed *Human Factors* below.

3. *Human Factors*. This aspect would cover interorganisational connections, a field much broader than only relationships and trust. It is also intended to cover individual training and experience, and the effects on an individual of organisational culture, such as command style, or a willingness to share information with colleagues, whether members of one's own organisation or of a partner. This is a characteristic of individuals, and a factor in

interoperability among organisations, but cannot be boxed into trust and relationships. It is a characteristic of each individual's skill and knowledge in interacting with individuals in the other group, and with the groups as a whole. It goes beyond the set of each trust and relationship link and includes qualities of the organisation (complex system) as a whole. Complex system theory insists that the system has attributes other than the sum of its nodes and links. Those qualities can be described as part of an organisational aspect, but some apply to the set of all humans in the organisation. For the purposes of the present review, these things are classified as *Human Factors*.

4. *Organisational*. The discussion above indicates that the authors of several papers have in mind some qualities of an organisation, making it capable of interoperation with others, which are not captured by the four CCEB aspects of interoperability as stated. These could include both an expanded definition of the *Human* aspect, and an additional aspect covering non-doctrinal elements of organisation, such as cohesion and organisational culture. This includes organisational culture as it governs the common behaviour of many individuals in an organisation in the circumstance, including the effects of collective training, and cohesion. Organisations learn and adapt. Complex system theory insists that the system has attributes other than the sum of its nodes and links.

5. *Legislative*. This aspect needs better definition. It would be useful to divide it into a. Policy or Political, and b. Legal. In the present review, this aspect is taken to include the effect of the broad political direction given to an organisation and its commander concerning the degree to which information can be shared, and members in general of another organisation (or nation) can be trusted and relied upon. It may not be a matter of legislation, but has the authority of government. Even if the concerns of Canada and CCEB in this matter are primarily military, military operations in the present and the predictable future will always have a strong political component, will be of a largely political nature, and will require close interoperation with political actors.

6. Security. This probably isn't an Aspect in the sense of the CCEB Four, but it is certainly in issue in interoperability. Security must be taken into consideration in any discussion of interoperability, since the sharing of information and intentions is still bound by many compartments, layers and caveats. Perhaps it is *Doctrinal* and *Legislative*, but it doesn't fit neatly. Maybe it's even subset of *Technical*, with elements of *Human* or *Human Factors,* since the decision to share is often made on the spot by an individual.

7. Interagency. Not so much aspect as scope. Current and future military operations involve not only the military forces of allies, but of many other players (personal anecdote available on request) domestic and foreign. In these situations, failure of interoperability may well be a showstopper. Operations outside Canada, which are the purview of CEFCOM, typically require close interaction with many military forces beyond CCEB, ABCA, Five-eyes or NATO. There are also many important actors who are not the military forces of allies or coalition partners. These include international agencies of other nations, international agencies such as the UN, the EU, the AU etc, and NGOs. The Canadian Army Force Employment Concept (FEC) of Adaptive Dispersed Operations (ADO) insists throughout on the Joint Interagency Multilateral and Public (JIMP) model, and this is reflected in current and evolving doctrine, training and organisation. Furthermore, while the present study seems to be directed to the needs of CEFCOM, it would be useful to take the needs of Canada

2.7 above uses domestic examples to good effect. In the opinion of the reviewer, today's interoperability requires adaptation to the needs of forces with less sophisticated technology and unfamiliar cultures, and other more ambiguous actors in the mission space.

4.4 Assessment and Levels

1. SOIM, in section 2.2 above, under Goals proposes amongst other things, that levels and standards ought not to be set too high, nor applied where they are not needed, since they become a design constraint (this might apply in non-technical aspects as well). This might be described as a minimalist, economical or disciplined approach.

2. MCISI, see section 2.4 above, proposes a wholly mathematical model, based on aggregation of distances in n-space in system pairs, where the n-space is various dimensions of interoperability. The model depends utterly on numerical measures, but doesn't suggest any. Within these limitations, it might have some use if measures can be found that can be expressed in such a way.

3. LISI, that is, "LISI 2" the paper mentioned in section 2.18 above, should be reviewed closely. In sections 3 and 4 it proposes a structure and concepts, and graphic depictions, for assessing levels of interoperability.

4. i-Score, see section 2.17 above, proposes a mathematical model, using as a measure the degree of intervention required to ensure mutual comprehension, and proposes levels based on degrees of mutual comprehension. It is for the analyst and user to determine if such measures are an adequate description, and to develop the degrees of needed intervention.

5. NTI, section 2.12 above, proposes the Multi-national Forces Co-operability Index, a matrix described in section 2.12.2. To be useful it would require a lot of filling in, and doesn't give an easy roll-up, but could well be potentially useful for trying to make sense of levels of interoperability.

6. Many of the papers reviewed propose measures, (that is, things to measure, as opposed to scales to measure them by, which are generally absent) that are measures of performance, rather than measures of effect, In a topic such as this, the distinction is not always easy to make, but is important. Some try: the LISI model's top level is "advanced collaboration", which is certainly a desirable quality, and perhaps suggests successful performance, even success, of the electronic environment, but not of the coalition of organisations. NTI, OIM, and OIAM do much the same. The studies are none the less valuable, but not conclusive. Tolk in the LCI presentation (and citing the NCOBP) mentions objectives, policy effectiveness, and military utility, and shows a logical pathway to them, but goes no further. This suggests a further case for empirical study.

4.5 Observations

4.5.1 Scope

In the opinion of this reviewer, based on the papers reviewed, to limit the study of interoperability to that among allied military forces is to make it much too narrow, and greatly diminishes its usefulness. That issue may well be the first priority, but also (and see 4.3 paragraph 7 above):

1. Forces other than those of familiar high-tech partners are likely to be involved in any operations in the foreseeable future, and will not be able to conform to interoperability standards or aspirations of our usual allies. In planning for interoperability, provision must be made for them for political as well as operational reasons.

2. Interagency is important. Operations in the foreseeable future will involve other government departments, agencies of other governments, international organisations (IO) and non-governmental organisations (NGO). Interoperability with them will be as important as with other armies.

3. Close contact and cooperation with indigenous elements, such as host governments and others, will be vital, and while they may not be full partners, it will often be necessary to share information, and to plan with them.

In many of the above cases, electronic compatibility will be limited or unavailable, and more effort will need to given to more old-fashioned instruments of interoperability, and to social and cultural familiarity. The present attention being paid to non-technical interoperability is appropriate, and should be extended beyond traditional allies' military forces. The OIM and OIAM papers, both Australian, emphasise the importance of interoperation with a variety of non-military agencies at several levels of government, a perspective that applies to Canada, both in domestic operations (Canada Command) and expeditionary operations (Canadian Expeditionary Forces Command). OIAM, by emphasising agility in interoperability, develops the important concept of being prepared to interoperate with a variety of partners, often unexpected.

Because of time constraints, the papers reviewed were all published no later than 2007. It seems likely that useful work has been done since, and study of more recent material should be made as soon as feasible.

4.5.2 Familiarization with Other Nations' Militaries

These remarks are based, with the exception of the NTI reference at paragraph 6 below, on the reviewer's own experience, and in general will be well known to military readers.

1. Exchange officers (there's no reason this couldn't apply to Senior NCOs, but this is a convenient term) are, as the name implies, posted, typically in peacetime, to the forces of allied countries to serve in appointments as though they were members of the host service. They are not liaison officers, and their function is explicitly not to serve as a conduit for information, but to gain experience. In the Canadian Forces, this programme has been popular for many years, although it seems to have been damaged by budget cuts recently. It

is potentially useful for benchmarking and cross-pollination, and is no doubt useful in establishing relationships with foreign forces, but in the past seems to have been a bit hit-or-miss. It can apply at all officer ranks, and both Generals Hillier and Natynczyk have served as deputy commanding general of III US Corps Fort Hood, and in General Natynczyk's case in Iraq. The result is that they are known and trusted by the US.

2. Unit exchanges are temporary arrangements whereby a unit visits and participates in activities such as exercises with a foreign force. Generally these are distinct from planned international exercises.

3. Joint standing headquarters and formations. There are several international organisations such as NATO rapid response force headquarters and standing naval forces which train and operate together in peacetime, and occasionally in real operations. Examples are NATO's standing naval task forces, the coalition anti-smuggling naval force in the Indian Ocean, and several army corps HQ, such as the Allied Rapid Reaction Corps (ARRC) and 1 German-Netherlands Corps, in which members of several armies spend full-length postings. Another example was the Stand-By High Readiness Brigade (SHIRBRIG), a grouping of like-minded nations which cooperated to be ready to respond to a crisis.

4. Liaison officers (LO) in peacetime are sent, with cooperation, to live and work with foreign forces, but their function, as distinct from that of exchange officers, is to learn as much as they can about the host force, and to serve as a conduit for information.

5. Liaison officers during military operations or exercises have a function analogous to that in peacetime. They are the historically oldest method of improving interoperability, except that they are now more likely to use a radio or computer than a horse. Their function is to assist in mutual communications, awareness and understanding. In operations or exercises, an officer or senior NCO will be sent to superior, subordinate or flanking headquarters, especially if different nationalities are involved. A particular advantage of LO is that they are technology independent, except for their own communications, which means that they are useful in operations where some partners do not have the technical capability for seamless communications. If an LO is reasonably bright and well-informed, and can get on well with his hosts, he can overcome obstacles in most or all of the interoperability aspects.

6. The NTI paper (section 2.12 above) suggests, under Conclusions, some ideas for improving relationships that apply to the *Human* and *Human Factors aspects*, such as cultural awareness training.

4.5.3 What it's All About

In the LCI presentation the author, Dr. Tolk, makes an important point when he cites the top level of interoperability from the NCOBP as "Measures of Policy Effectiveness" and in his own proposed hierarchy for net-centric warfare, puts at the top "Measures of Military Utility". In each case, the message is that, in the end, the value of interoperability lies in its contribution to political / policy and military objectives.

4.5.4 Definitions of Interoperability

Although there are a number of definitions of interoperability, and most writers take care to state their choice, there is no unanimity on how to approach it. Some attempt to frame and assess interoperability of a single military system, others of a collection of systems in one country (typically the US), others of an international grouping.

4.5.5 Experiments for Exploration and Validation

1. No reports of real experiments or tests were found, with the exception of NTI (paragraph 2 below) and SOIM (paragraph 3 below). There needs to be more field research done. At present, there are few, other than the JWID / CWID series, which are about demonstrating technical tools, and an ambitious exercise project in DLR 4 a few years ago. The latter was mostly about intra-Canadian interoperability, no trivial matter, but it may have had non-Canadian input. This reviewer visited that experiment, and it seemed to be eminently sensible and practical, and must have yielded interesting results.

2. A partial exception was the NTI study reviewed in section 2.12 above, which interviewed soldiers with operational experience.

3. Another was SOIM, reviewed in section 2.2 above. This was salient among the papers reviewed because it was a report of an experiment, and it suggested a way to put the results to use.

4. A partial exception to the lack of data, and an interesting one, is the references by Alberts & Hayes in the NCW book, and by Schade in the NID paper, to historical examples. Unfortunately, although illustrative, and food for insight, these examples are anecdotal, and therefore can hardly be assessed as data. However, they suggest the possibility of more extensive historical research (which those writers may have done) which could be worthwhile.

5. The best test bed available, or likely to be available for some time, is ISAF. It won't be available, or a Canadian perspective won't be available, for long. The recently proposed new Canadian training mission in Kabul would not be a substitute.

4.5.6 Practicalities

In SOIM, amongst other things, the author suggests that for practical reasons,

1. different communities should not be required to acquire identical systems, merely to make them compatible; and

2. the number of nodes required to be interoperable should be kept to a minimum.

The world has changed since the paper was written. Suggestion (1) is understandable, but should be accepted only if necessary, as it is a potential source of trouble; "compatibility" is a fuzzy word. Suggestion (2) should be avoided if at all possible, since in the fluid situation of the

contemporary operating environment, diverse entities, of which it was never expected, can find themselves required to interoperate at levels and with links that were not foreseen.

4.5.7 Best Technical and Non-Technical Papers

1. The full 1998 LISI paper, called "LISI 2" in section 2.18 above is probably the most comprehensive, with the important caveat that it was not fully reviewed here. At the time the reference papers reviewed here were written, it was generally treated as the reference model, as was intended. One limitation is that for the most part it focuses on US systems, although it mentions NATO, but this limitation doesn't seem to detract from its generality. It is a relatively long read. The runner-up would be the shorter paper reviewed as LISI in section 2.5 above.

2. The Non-Technical Interoperability (NTI) paper reviewed in section 2.12 above is the best overall treatment of the non-technical / non-electronic aspects of interoperability, and has an impressively military bibliography. Runners-up would be OIM in section 2.7 above, and OIAM in section 2.13. The LCI presentation (section 2.9) has some good ideas and makes the important point that it is all about political and military effect. These papers should initiate some useful lines of inquiry.

4.5.8 Other Observations

1. In SOIM, goals proposed at section IV page 1449 include

   a. development of (quantifiable) measures of interoperability

   b. early consideration of interoperability in the design stage of systems, bolstered by these measures

   c. configuration control to ensure that compatible systems do not become incompatible

   d. discipline and measurability in the setting of interoperability requirements, since they are design constraints which would hamper other performance needs.

   These make sense. With a little imagination, they could be turned into goals for the non-technical aspects as well.

2. Very few research papers by Canadians were found – in fact the only related paper was the Keith Stewart DRDC paper to the International Command and Control Research and Technology Symposium. Does Canada usually go to that forum?

4.6 Judgements, Insights, Ideas

1. Interoperability cannot be attributed to a single system, only to a set of family of systems or sub-systems or at least to a pair. Whatever the system or subsystem characteristics, interoperability is conditional on a number of factors such as the requirement, the threat, the physical and electronic environments, and no doubt others. These cannot be controlled by the

user and their variability must be predicted and included in the design requirements, and the subject system tested against them. Lack of clarity in these ideas leads to confusion in the interpretation of a number of the papers reviewed. It leads, inter alia, to confusion among the components of interoperability and the factors governing performance.

2. Hub vs. federation. Given a choice between hub and federation, CCEB might be wise to adopt a federation approach, simply to establish a shared set of methods and characteristics required for interoperability, but to include in it the capability for members and for the federation / coalition to accept and connect to other partners. This approach might have the virtue of establishing aspirational objectives. The CCEB partners are ideally suited for the interoperability effort, and have apparently, even the non-NATO partners, been working together on it since early in the cold war. However, in the contemporary operating environment, often the partners will be non-CCEB and non-NATO, and will have a hard time not only with the *Technical* aspect, but with the others. The CCEB partners would be well advised to build in hooks for a hubbish arrangement, since that's what we're likely to get[6], and the hooks should be not only technical.

3. Probably, *Technical* interoperability is the easiest aspect to measure and to build standards for, but not necessarily easy to implement.

4. What's being studied here is a constellation of complex (probably adaptive) systems. That field of study might provide useful clues. See Atkinson *The Agile Organisation* (Chapter 3), and many others.

5. Interoperability depends above all else on the commitment of the partners to the coalition. In NID (section 2.15 above), Schade emphasises the importance of first, data transfer and, second, common language; all else can be achieved by humans[7]. He wanders into the territory of edge organisations, NCW etc, quoting Alberts & Hayes, explaining that such organisations are outside hierarchy, and **it is not sufficient that they receive and understand orders or understand superior's intent, but that they share it. This observation is important when (comment: as it should be) the study of interoperability is extended to non-military organisations, and allies whose commitment may not be absolute.**

6. The systems engineering approach with several different views or perspectives or layers, often depicted by a network diagram, could be useful. An example is LISI's ("LISI 2" the 1998 paper) use of the terms Operational Architecture View, the System Architecture View and the *Technical* Architecture View. This approach could perhaps be applied to the four or more CCEB aspects: what does the network look like in the e.g. *Doctrinal* view, what are its

[6] Rumsfeld: "You go to war with the army you've got" (a remark that probably contributed to his eventual resignation). The (humble) reviewer: "You go to war with the war you've got" or "You go to war with the allies you've got". In other words, first, we don't choose the conflict or other situation that we find ourselves in. Therefore we must be prepared for a variety of missions, force structures and environments. Second, we don't choose our partners. Therefore we must be prepared for partners who don't have the technology, the culture or the preparation that we (CCEB) have, and for which we are optimising. Therefore we must be adaptable in our interoperation, just as in our tactics.

[7] "God created the integers; all else is the work of man." Attribution apocryphal, usually Kronecker, but sometimes Aristotle.

strengths, weaknesses, strong and weak links and nodes, key variables etc. Each node must be linked to the others in a given view, but perhaps not, or more weakly, in others.

7. Have we considered the body of work that DRDC Toronto has done on Command, and on C2? For example Pigeau and McCann, who have devoted much to the study[8].

8. Is it possible that the Keith Stewart, Defence Scientist, DSTL UK, who was an author of the NTI paper in 2004, might be the Keith Stewart who is now at DRDC Toronto (See e.g. Command approach: Problem bounding versus Problem solving in Mission Command, paper 176 at the 14th International Command and Control Research and Technology Symposium (2009), http://www.dodccrp.org/events/14th_iccrts_2009/papers/176.pdf)? Their works bear a certain resemblance.

9. There needs to be more field research done. Where possible, it should be done in a real operational, in addition to, and more urgently than, an experimental or exercise setting. At the risk of belabouring a point made elsewhere in this report, that is our present operation in Kandahar, which will not be available for long.

[8] See e.g. The Human in Command through Amazon, or Google the names, or check DRDKIM(?). Ms McCann has retired, but it's believed she works as a consultant. Dr. Pigeau was, at last report, in a senior position in DRDC.

5 Challenges in Conducting this Study and Proposed Solutions

For good reasons of practicality, this review took as a first priority references made in a 2007 study, the Ford Paper. In the event, that is all that was reviewed. There were by 2007 probably some useful sources not mentioned by Ford, and much has probably been done since. As soon as feasible, they should form part of any study of the interoperability problem.

6 Concluding Comments

1. The papers reviewed were, almost without exception, theoretical, with no empirical data.

2. Papers reviewed proposed a number of sensible theoretical measures of performance, but almost without exception no real measurables; ways of measuring or aggregating these things. Empirical study is necessary to both identify these and apply them to research.

3. The present study of which this review is a part is concerned almost exclusively with interoperability with partner military forces in expeditionary operations. However, several of the papers reviewed make the important point that interoperability with non-military actors is of increasing importance in today's world, and also interoperability in domestic operations, implying inter-service, inter-agency and inter-(levels of) government is an important challenge. Also, any interoperability regime, to be useful in today's world, must allow for operation with unplanned partners having less modern technology and different ways of doing things.

4. The CCEB aspects need to be enlarged to include factors that are not now included, and the definitions need to be made much more thorough and complete.

5. There are, at least among the papers reviewed, a number of ways of expressing components, or factors, or aspects of interoperability, and from these some ideas of potential measures can be taken. However, there were no hard measurables found: no ruler or scale with numbers.

6. There are several definitions of interoperability available, and the choice of definition naturally influences subsequent analysis.

7. Perhaps one desirable standard would be a set of definitions of interoperability for researchers. The same could be said for aspects / factors / components, but of course that is part of the present study.

8. Seemingly rigorous models for assessing interoperability were found, but they need to be tried with some sort of data that can enable testing against the real world.

9. There needs to be more field research done: experiments, observation of exercises, and observation of real operations. The best possible opportunity, ISAF, won't be there long.

10. Historical research might be useful, if it can be translated into digestible data.

11. Interviews and questionnaires with Canadian Forces (CF) members with experience of multinational operations, as in the NTI paper, would be useful.

12. Potential collaborators are DRDC Toronto and the CF Experimentation Centre, now called the CF Warfare Centre.

13. Canadian appearances in the literature are rare, and this lacuna should be given some thought.

7 Recommendations

7.1 Observation, Experiments, Validation and Data Collection

Based on the limited sample of the papers reviewed, there is a surprising dearth of experimental or field research. It seems to make no sense to construct an elaborate body of theory without the insight and validation of reality, or at least a semblance thereof. If this subject is taken seriously, the following should be pursued:

1. Field research on operations. This is opportunistic, which means don't wait until it fits the programme, do it when real operations are available, and if necessary, figure out what to do with the data later. Exercises and experiments are always with us, and the real thing is more realistic than any exercise, and no one can argue with its validity. Observation of operations or exercises is less costly than commissioned experiments, because the test bed is already in place. The problem is access, but this should be possible, as researchers are typically deployed now. The ideal would be our operation in Afghanistan, which won't last long.

2. Field research on realistic field exercises. This is almost as good. But if a real operation is the opportunity, do that. Again, observation of an exercise is less costly than a commissioned experiment, but access would have to be arranged.

3. Field research on simulation exercises or hybrids. These are in some ways less realistic than field exercises, but in some ways more so, since some unrealisms can be programmed out, and a wider variety of scenarios can be explored. Again this avenue is less costly than a commissioned experiment, but access would have to be arranged. Data collection and recording might be aided by the digital environment.

4. Commissioned experiments. These might be in the field, in a simulation environment, or a hybrid, which is not uncommon these days. In some ways these are less realistic than exercises, in some ways more, for the same reason as in points 2 and 3 above.

5. Historical research, and the experience of CF members, might be fruitful fields.

7.2 Scope

See the remarks in section 4.3 paragraph 7 and section 4.5.1 above. Future work should address interoperability with actors other than our closest allies, other than military forces, and even with those who are not allies. *(Personal anecdote available from the reviewer on request)*. This means the *Human*, *Human Factors*, and *Organisational* aspects, and that will have to extend to social and cultural training, education and doctrine. It also means that forces will need to have the built-in organisational ability to interoperate with unexpected partners.

CCEB's four aspects of interoperability, as now defined, do not describe the field, are insufficient to study this topic, and if used alone and unmodified will lead to unhelpful or misleading results. The four aspects must be expanded, and / or new ones added, as described in section 4.3 above.

References

[1] Combined Communications-Electronics Board (CCEB) (U) (online at Intellipedia, the U.S. Government's Unclassified wiki), https://www.intelink.gov/wiki/CCEB (Access date 5 August 2011).

[2] Ford, T.C. (2007), A Survey on Interoperability Measurement, In *12th International Command and Control Research and Technology Symposium* (online), The Command and Control Research Program, http://www.dodccrp.org/events/12th_ICCRTS/CD/html/presentations/096.pdf (presentation), http://www.dodccrp.org/events/12th_ICCRTS/CD/html/papers/096.pdf (paper).

[3] Ford, T.C., Colombi, J.M., Jacques, D.R, and Graham, S.R. (2009), A General Method of Measuring Interoperability and Describing Its Impact on Operational Effectiveness, In *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology* 6(1), 17-32, London (UK): Sage Publications.

This page intentionally left blank.

List of symbols/abbreviations/acronyms/initialisms

ABCA	America, Britain, Canada, Australia
ADatP	Allied Data Publication
ADM	Assistant Deputy Minister
ADO	Adaptive Dispersed Operations
ARRC	Allied Rapid Reaction Corps
AU	Australia
AWG	Architecture Working Group
C2	command and control
C3	command, control and communication
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
C4ISTAR	C4 (command, control, communications, computers), intelligence, and STAR (surveillance, target acquisition, and reconnaissance)
CCEB	Combined Communications Electronics Board
CEFCOM	Canadian Expeditionary Force Command
CF	Canadian Forces
CFEC	Canadian Forces Experimentation Centre
CIS	communications and information systems
CONOPS	concept(s) of operations
CORA	Centre for Operational Research and Analysis
CWID	Coalition Warrior Interoperability Demonstration
DLR	Director Land Requirements
DND	Department of National Defence
DOD	Department of Defense
DODCCRP	Department of Defense Command and Control Research Program
DP	Dimensional Parameters
DRDC	Defence Research and Development Canada
DSTL	Defence Scientific and Technical Laboratory
EOI	electronic operating instructions
FEC	Force Employment Concept
HQ	headquarters

i-Score	Interoperability Score
IAM	Interoperability Assessment Model
IEEE	Institute of Electrical and Electronics Engineers
IM	Information Management
IO	international organisations
IOR	Interoperability Requirements
ISAF	International Security Assistance Force
IT	Information Technology
JIMP	Joint Interagency Multilateral and Public
JWID	Joint Warrior Interoperability Demonstration
LCI	Layers of Coalition Interoperability
LCIM	Levels of Conceptual Interoperability Model
LISI	Levels of Information Systems Interoperability
LO	Liaison officers
MCI	Multinational forces Co-operability Index
MCISI	Military CIS Interoperability
MoCE	Measures of C2 Effectiveness
MoFE	Measures of Force Effectiveness
MoPE	Measures of Policy Effectiveness
NATO	North Atlantic Treaty Organization
NC3TA	NATO C3 Technical Architecture
NCMW	net-centric maritime warfare
NCO	non-commissioned officer
NCOBP	NATO Code of Best Practice
NCW	net-centric warfare
NGO	non-governmental organisations
NID	NATO [C3 System] Interoperability Directive
NIE	NATO Interoperability Environment
NMI	NATO Tech Architecture
NTI	Non-Technical Interoperability
OIAM	Organisational Interoperability Agility Model
OIM	Organisational Interoperability Maturity Model
OODA	observe, orient, decide, and act
OPLANS	operational plans

PAID	Procedures, Applications, Infrastructure, Data
QoIM	Quantification of Interoperability
QSTAG	[NATO] quadripartite standardization agreement
ROE	Rules of Engagement
SHIRBRIG	Stand-By High Readiness Brigade
SoIM	Spectrum of Interoperability
SOP	Standard Operating Procedures
SoSI	System of Systems Interoperability
SPAWAR	Space And Naval Warfare Systems Command
STANAG	[NATO] standardization agreement
TA	Technical Architecture
TTCP	The Technical Cooperation Program
UK	United Kingdom
UML	Unified Modeling Language
UN	United Nations
US	United States
XML	Extensible Markup Language

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)

HDP Group Inc.
151 Slater St., Suite 807
Ottawa, ON K1P 5H3

2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)

UNCLASSIFIED
(NON-CONTROLLED GOODS)
DMC A
REVIEW: GCEC December 2013

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Coalition Interoperability Measurement Frameworks Literature Survey

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Bury, P.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
August 2011	100	3

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Contract Report

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Assistant Deputy Minister (Information Management) [ADM(IM)]
National Defence Headquarters
MGen Pearkes building
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
WBE 15BZ14	THS-1775111, standing offer EN578-060502/055/ZT

10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DND 1010	DRDC CORA CR 2011-132

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

This paper is the report of a review of selected works that were referred to in a 2007 survey of methods to measure interoperability between military forces. It forms part of an effort to develop a framework for assessing interoperability in command, control, computers, and communications. The framework is being developed by the Joint Studies Operational Research Team, and is sponsored by Assistant Deputy Minister (Information Management). For the framework, the context of interest for interoperability was 5-Eyes (Australia, Canada, New Zealand, United Kingdom, and United States), at the strategic/operational level. The aim of this survey is to identify and describe any content of those papers that potentially contributes to the framework. The review was a limited success. The findings and recommendations are described in the Executive Summary.

It was found that many of the papers concentrated on the Technical aspect of interoperability, some directly technical, some very abstract. A few addressed human, organisational and policy matters. Since the papers were all published no later than 2007, it seems likely that useful work has been done since. The field is complicated by a plethora of definitions of interoperability. The Four Aspects of interoperability as agreed by the CCEB are too restrictive and exclude some important factors. Strong recommendations of the reviewer are: that future work focus on the human, organisational and policy aspects of interoperability; that it include preparations for unforeseen operation with allied or partner forces that do not have the technical capability or cultural assumptions of the CCEB family, and also with other governmental, non-military international, non-governmental organisations and other potential actors in the contemporary battlespace / mission space; and that empirical and field research be undertaken as soon as possible, to take advantage of current operations whilst they are still current.

Le présent document est un rapport faisant suite à l'examen de travaux choisis cités en référence dans une enquête de 2007 sur les méthodes de mesure de l'interopérabilité entre les forces militaires. Ce document constitue une partie des efforts déployés pour concevoir un cadre d'évaluation de l'interopérabilité en ce qui a trait au commandement, au contrôle, à l'informatique et aux communications. L'Équipe de recherche opérationnelle et d'études interarmées élabore actuellement ce cadre et les travaux sont parrainés par le Groupe du Sous-ministre adjoint (Gestion de l'information). L'intérêt exprimé pour ce cadre par les Cinq pays (Australie, Canada, Nouvelle-Zélande, Royaume-Uni et États-Unis) se situe au niveau interopérabilité stratégique/opérationnelle. Le but de la présente enquête est d'inventorier et de décrire tout élément de contenu des documents qui pourrait possiblement contribuer à l'élaboration de ce cadre. Cette étude a eu un succès limité. Les résultats et les recommandations sont présentés dans le sommaire. On a découvert qu'une grande partie des documents portait sur l'aspect technique de l'interopérabilité; certains d'entre eux se présentaient comme technique alors que d'autres étaient très abstraits.

Quelques-uns portaient quant à eux sur des aspects humains, organisationnels et de politique. Étant donné que les documents ont tous été publiés en 2007 ou avant, il semble probable que les travaux utiles ont été faits depuis. Dans ce domaine, le grand nombre de définitions d'interopérabilité vient compliquer les choses. Les quatre aspects de l'interopérabilité définis pour cette étude (technique, humain, doctrinal et législatif) sont trop restrictifs et ne tiennent pas compte de certains facteurs importants. L'auteur de l'étude fait les importantes recommandations suivantes : que les travaux à venir se concentrent sur les aspects humain, organisationnel et de politique de l'interopérabilité; qu'ils incluent la préparations aux opérations imprévues avec les forces - alliés ou celles de partenaires - qui ne possèdent pas la capacité technique ou les acquis culturels dont disposent les forces militaires des Cinq pays ou avec toutes autres organisations gouvernementales, internationales non militaires ou non gouvernementales et autres intervenants pouvant être présents sur l'espace contemporain de bataille et de mission; que des recherches empiriques et sur le terrain soient entreprises aussitôt que possible afin de tirer parti des opérations actuelles alors qu'elles sont encore en cours.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

CCEB; Combined Communications Electronics Board; 5-eyes; five-eyes; interoperability; multinational; questionnaire; survey; framework

Defence R&D Canada

Canada's Leader in Defence
and National Security
Science and Technology

R & D pour la défense Canada

Chef de file au Canada en matière
de science et de technologie pour
la défense et la sécurité nationale

www.drdc-rddc.gc.ca