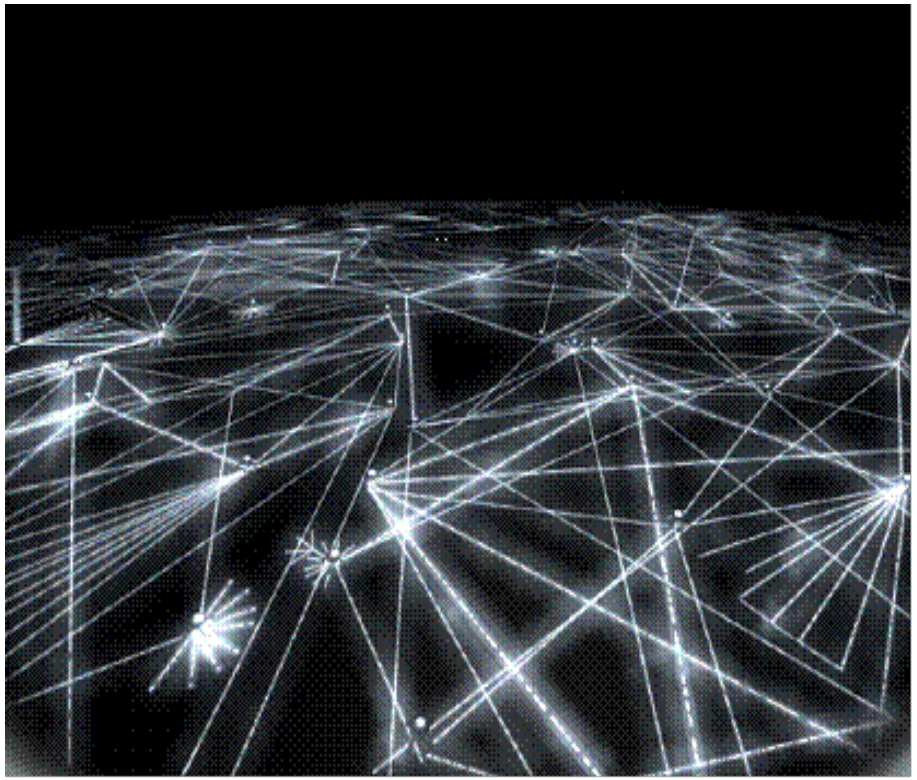
16th ICCRTS – 21st-23rd June 2011

Track 4: Paper 085

Information design for synchronization and co-ordination of modern, complex, multi-national operations



Geoff Markham

QinetiQ, St Andrew's Road, Malvern
Worcestershire WR14 3PS
United Kingdom

gmarkham@qinetiq.com

Paper presented by Andrew Fletcher, UK MOD

QinetiQ

0.1 Outline of this presentation

Information is generally understood as ‘data plus context’.

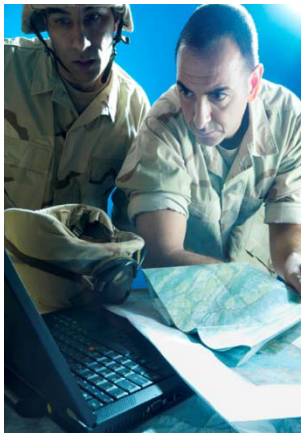
Organizations conducting modern, complex, multi-national operations, with both military and non-military involvement, need to manage contexts in ways which are efficient, supportive of federation, and agile.

This requires that information needs to be *designed*, not merely found or catalogued, to achieve synchronizations and co-ordinations in support of network-enabled behaviours.

The aim is safe use, a prescription for “right information, right people, right time” which guards against both misinterpretation (failures in context management) and mis-recognition (not appreciating, or not disseminating, pertinent information).

This paper explores ways in which *information schemata* can be implemented and supported through non-Equipment Lines of Development, and in particular the world of organization and work.

1. Overview



1.1 Context

Considerable effort has been expended by UK MOD over the last decade to overcome the limitations inherent in earlier CIS† support:

- focus on specific functional needs rather than inter-working across the enterprise
- technical and procedural barriers to interoperability

The primary focus of attention has been on alleviating the *technical* barriers, through:

- technical interoperability, e.g. through standards
- commonality of tools: rationalisation of functions and sharing of functionality in common tools
- commonality of information: common information models, common operating pictures, etc.
- technical networking, as a particular perspective on networking

† CIS = Computing and Information Systems

1.2 Purpose of this paper

The purpose of the current paper is:

- to look again at what it means to share *information*, as opposed to merely sharing data
- to remind us that:
  - this is not (just) a technical systems problem
  - the technical measures we have employed to date (e.g. pursuit of equipment standards, common pictures) will not 'scale up' to the demands of EBAO‡ and the Comprehensive Approach:
    - for organizations conducting modern, complex, multi-national operations, with both military and non-military involvement, the limited successes gained with purely technical measures will not be replicated
- to point to features of organizational design and practice which are pertinent to information sharing and which do have the potential to 'scale up'

‡ EBAO = Effects-Based Approach to Operations

1.3 The core problem

Information is generally understood as ‘data plus context’

Whilst recognising that some forms of context are enterprise-wide or universal, so a ‘simplistic’ definition of information – common to all actors – will suffice …

… *context* is (more generally) a function of the circumstances of generation (of information) and the use to which it is put. So:

- Information is relative to usage
- Two actors can see the same data and can potentially derive different information from it, because they each add their own context

Fitchett, McConnell and Sowray (11th ICCRTS) assert that:

- “Failures in shared understanding are an important contributory factor to disastrous outcomes.”
- “The development of shared understanding requires some degree of shared context, and that this is also a necessary feature for the achievement of synchronised effect.”

1.4 Resolving the core problem

If (some classes of) information have to be defined relative to its usage

- … rather than having a ‘universal meaning’ …

We can employ a ‘complicated’ definition of information

- which essentially localises its meaning to a particular set of actors and uses

This enables us to exercise proper discrimination in our IM/IX† procedures …

… but it leaves us without a definition of *information in transit*:

  - How do we describe information being passed from one group of actors to another?

† IM/IX = Information Management / Information Exploitation

1.5 Structure of the paper

What is meant by ‘information’?

- Ideas from the literature
- A general schema

The concept of *safe use:*

- a prescription for “right information, right people, right time”
- two-sided: guards against both misinterpretation (failures in context management) and mis-recognition (not appreciating, or not disseminating, pertinent information)
- challenges to safe use – informatic distance

‘Simplistic’, ‘complicated’ and ‘complex’ models – why we need them all

- Models of organization
- Models of IM/IX

The information entity and information schema approach

- Fitchett, McConnell and Sowray – 11th ICCRTS

Understanding ‘information in transit’:

- What is ‘context’?
- How is context ‘exchanged’ and ‘acted upon’?

Credible implementation mechanisms

- and why it’s not all about meta-data!

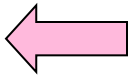
1.6 What this presentation focusses on

What is meant by 'information'?

- Ideas from the literature
- A general schema

The concept of *safe use:*

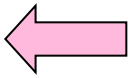
- a prescription for "right information, right people, right time"
- two-sided: guards against both misinterpretation (failures in context management) and mis-recognition (not appreciating, or not disseminating, pertinent information)
- challenges to safe use – informatic distance



Some examples

'Simplistic', 'complicated' and 'complex' models – why we need them all

- Models of organization
- Models of IM/IX



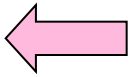
Some illustrations of different IM/IX approaches

The information entity and information schema approach

- Fitchett, McConnell and Sowray – 11th ICCRTS

Understanding 'information in transit':

- What is 'context'?
- How is context 'exchanged' and 'acted upon'?

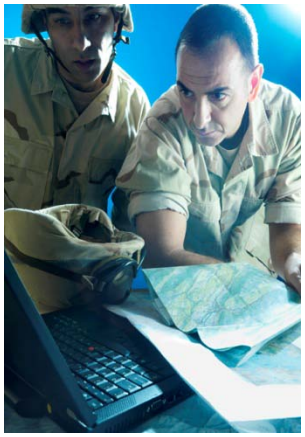


An overview of the analysis, with highlights and implications

Credible implementation mechanisms

- and why it's not all about meta-data!

2. Safe use – and the challenges to it



2.1 What is ‘safe use’?

Safe use is a prescription for “right information, right people, right time” which guards against mis-interpretation (failures in context management) and mis-recognition (not appreciating, or not disseminating, pertinent information)

- N.B. two-sided - we need to avoid both the wrong use of information and the failure to make the right use of it
- The scope is that of Information Assurance, encompassing:
  - Security (protective marking and ‘need to know’)
  - Safety (i.e. safety-related – can also contribute to safety-critical systems)
  - IM/IX concerns – organizational effectiveness, optimal use of human and technological resources

Safe use is:

- an aspiration or headmark
- a set of criteria for Information Assurance

2.2 Examples of challenges to ‘safe use’ (1)

Missing information:

- A database of blue force locations contains a number of entities in area X and no entities in area Y. But we cannot infer that there is no risk of fratricide from friendly fire in area Y without an appreciation of both the procedural conditions of blue force data collection (e.g. that the currency of the information is no better than 30 minutes latency with respect to reality) and the contingent conditions (e.g. that some friendly assets are currently not transmitting blue force locations, perhaps because of network problems).

Sampling effects:

- It is hypothesised that recent developments will be reflected in a shift in adversarial tactics, for which a number of indicators can be set up (e.g. size and frequency of events of a certain type). A trawl of an event database shows up a distribution which is similar to that which might now be expected. However, we cannot interpret this as confirmatory without knowing how that events database has been created (e.g. whether there are collection biases in operation, either independently of or driven specifically by the original hypothesis).

2.3 Examples of challenges to ‘safe use’ (2)

Information incest:

- Stripping out data duplicates does not necessarily mean that information incest has been prevented, if insufficient context comes back to strip out the real underlying duplication. Information may be reflected in quite diverse data representations and yet derive from a common military activity and/or group of events. An inability to identify the underlying correlations can lead to a misleading impression of frequencies and priorities.

Procedural gaps:

- Information holdings can refer to one facet of reality but its structure might lead us to think it refers to another. For example, a medical records database may show a particular individual as a casualty currently receiving care from a Medical Unit, but that does not necessarily mean he or she is physically located at the Medical Post or Field Hospital which appears as the nominal location of that Medical Unit.

2.4 What could contribute to ‘context’?

Context is anything that relativises some information (so the only information for which explicit context need not be provided is that with universal, or enterprise-wide, meaning).

Generally, the context required in particular cases may have components in respect of some, or all, of the following dimensions:

- Ontological (e.g. domain-specific ontologies):
  - Organizational (e.g. functional communities); Ideologies; Unobtrusive controls; Activities; Stories
- Standpoint (e.g. strategic, operational, tactical):
  - Shared definitions of the environment
  - Theories of action (associating interpretations of the environment with response actions)
- Systems of interest:
  - ~ Granularity of interest
  - Timescale of interest
  - Filters on environmental cues
  - Purpose (e.g. intervention type)
  - Security classification

2.5 Measures of difference in context

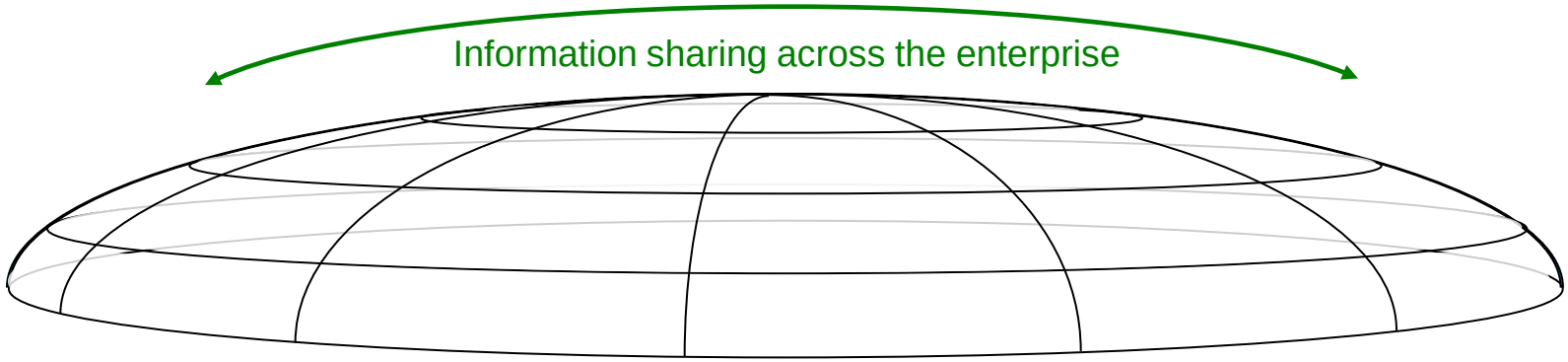
There is a potential for ‘loss of context’ wherever producers and consumers of information are at different points along any of the dimensions of context, e.g.:

- members of different organizations (e.g. different functional communities);
- having different standpoints (e.g. strategic v. tactical).

=> *Informatic distance*:

- a measure of the separation between producer and consumer, taking all of the dimensions of context (above) into consideration

We can use *curvature* as a pictorial metaphor for informatic distance:

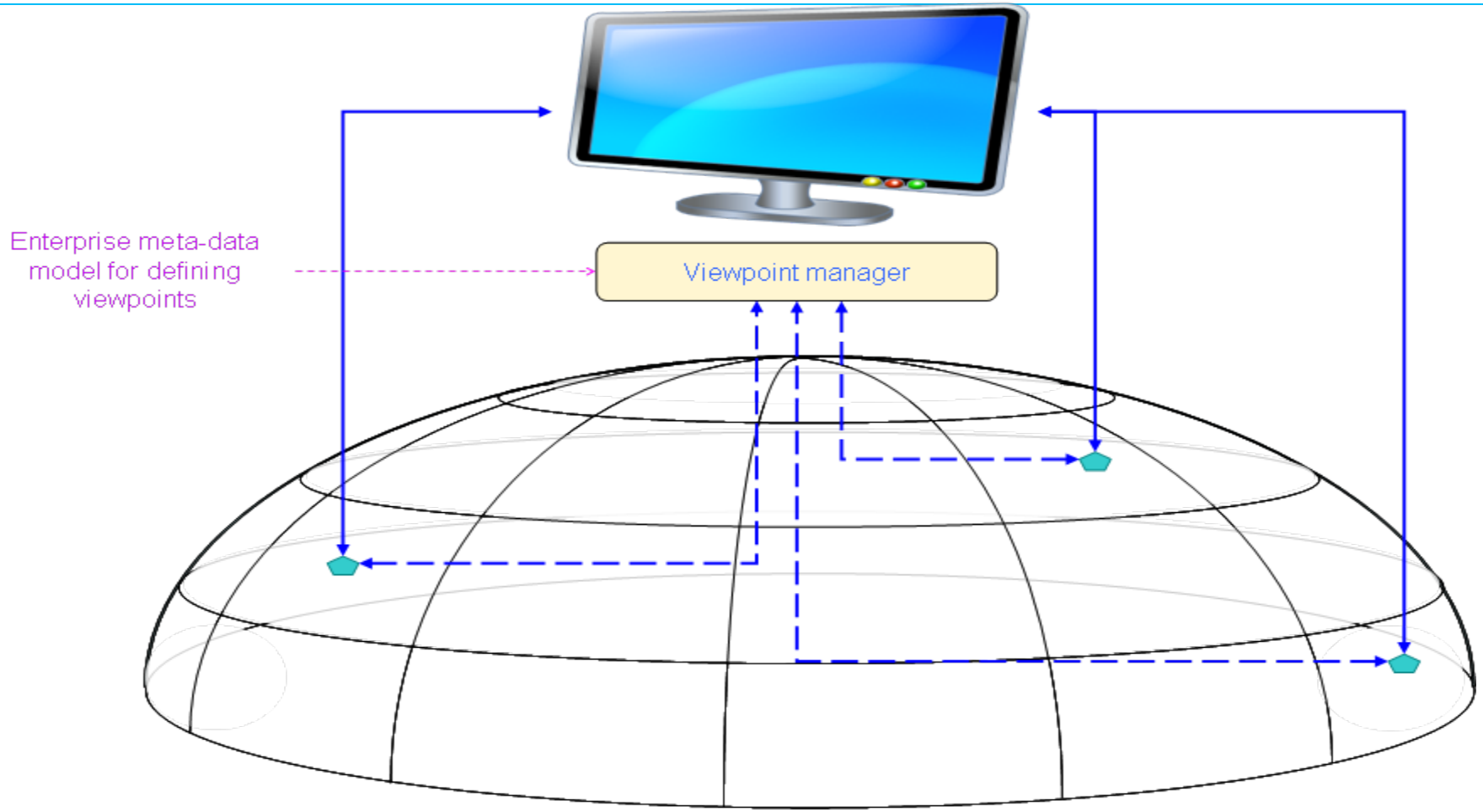


3. Enterprise IM/IX approaches

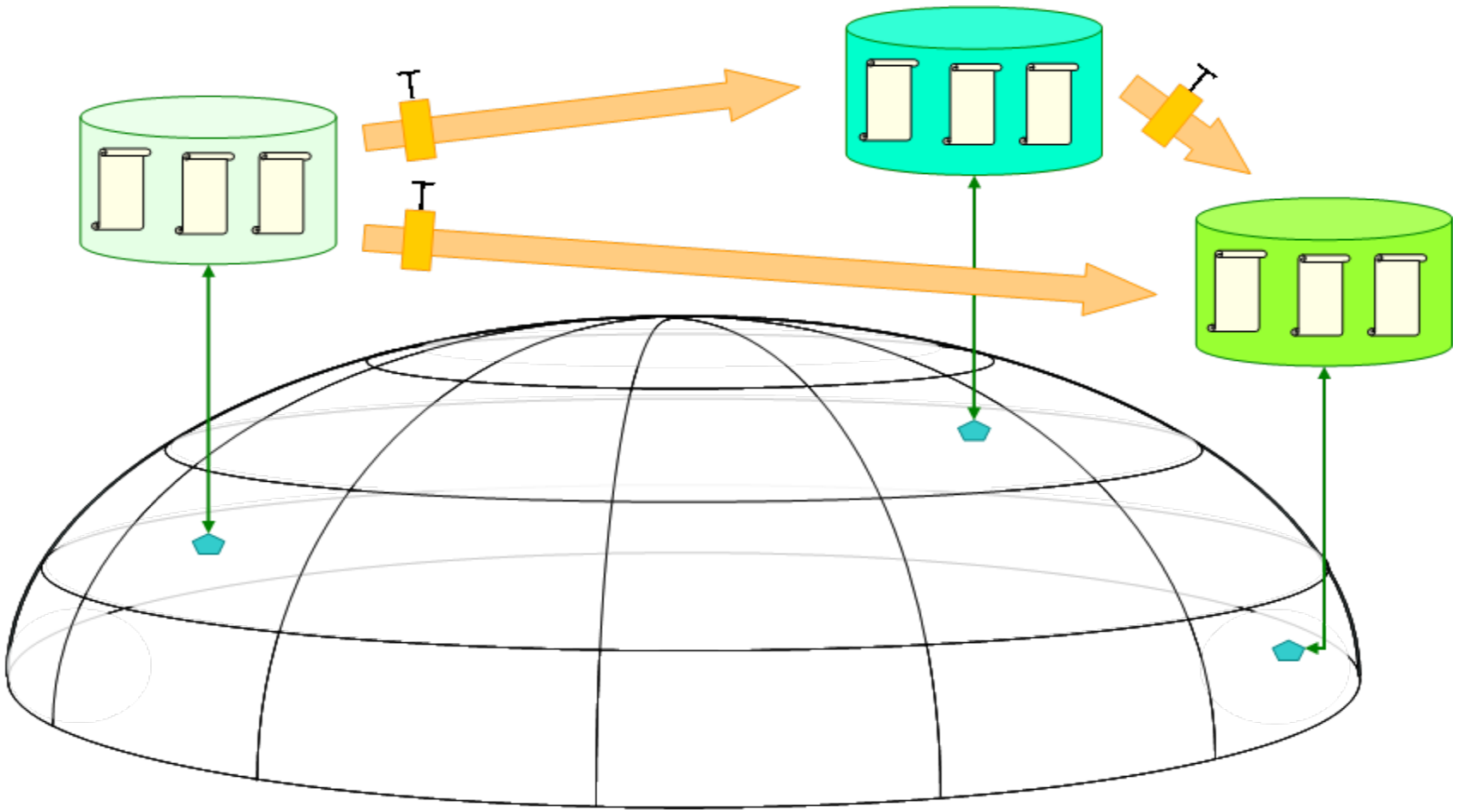
Two classes of approach:

- Unified:
  - seeks to ‘flatten’ the curvature
  - OK for purely factual information, e.g. geo-location of assets [discuss!]
- Federated
  - negotiates the curvature
  - copes with non-factual / conditional / subjective information

3.1 A unified approach: common operational picture



3.2 A federated model: multiple repositories with controlled flow between them



4. Information in transit

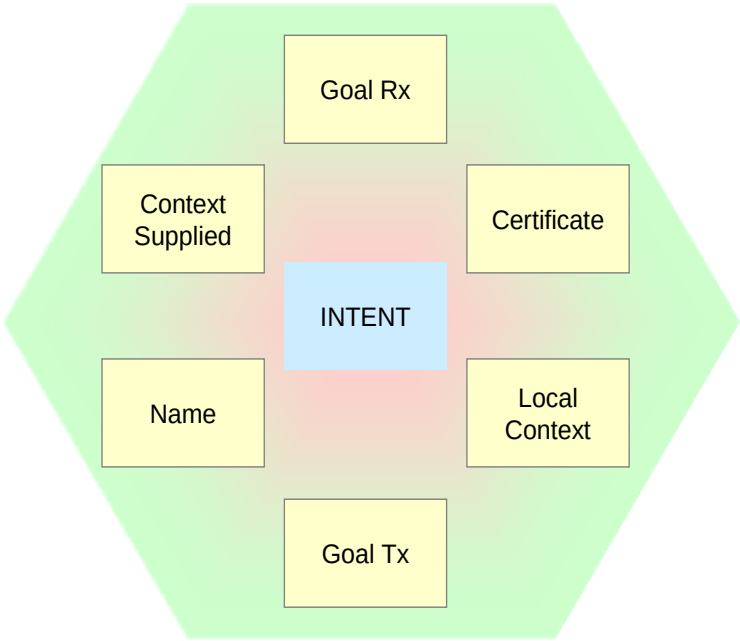
If ‘information generated’ is now different from ‘information received’ …

What happens ‘in transit’?

- What context-defining information needs to be passed?
- How is context acted on and transformed en route?

4.1 Using the idea of the ‘information entity’

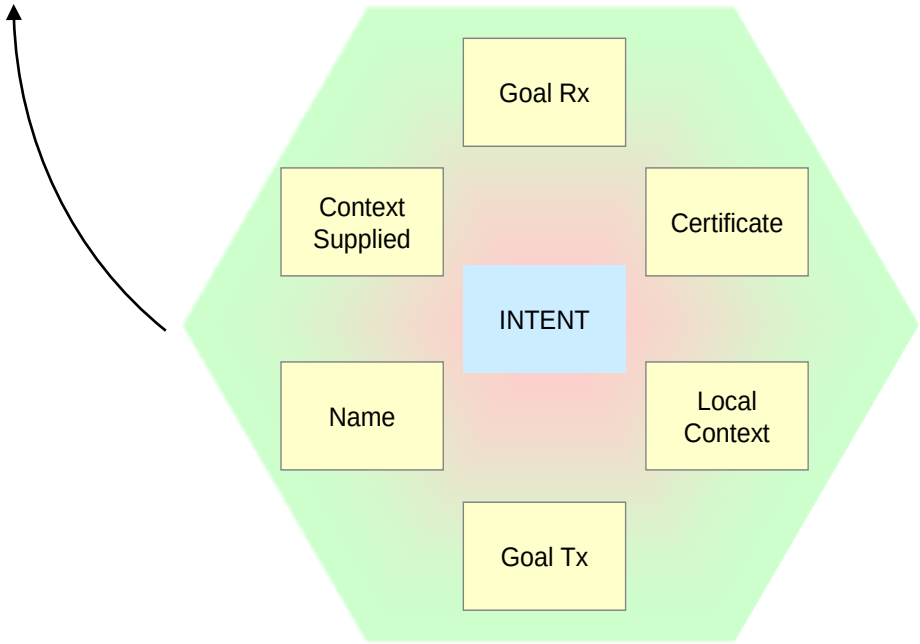
- Fitchett, McConnell and Sowray (11th ICCRTS) propose that the provision of a form of *schema* – used to construct a temporal and spatial context for relevant information - would enable the provision [i.e. exchange / shared use] of appropriate information to all entities within a System of Interest
- This schema is based on an information entity with elements as shown:
  - Intent, which is an internally generated information object derived as a result of external influences
  - Goal received (a specific and privileged external influence)
  - Context supplied (which is global)
  - Local context
  - Goal transmitted (through which other entities can be influenced)
  - Name (own identity)
  - Certificate (recognition mechanism for authentication purposes)



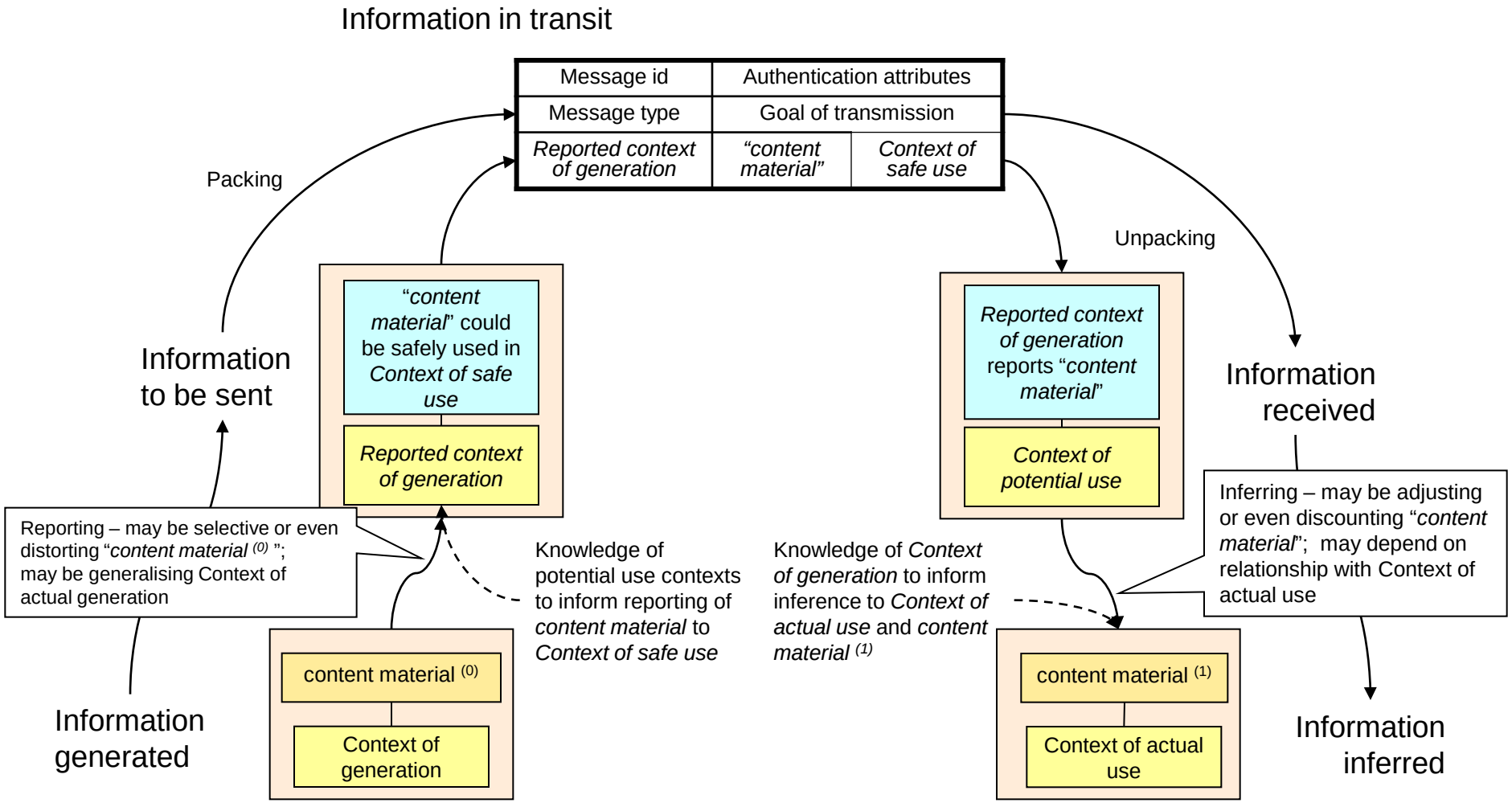
4.2 Interpreting the ‘entity’ as a ‘message’

Information in transit

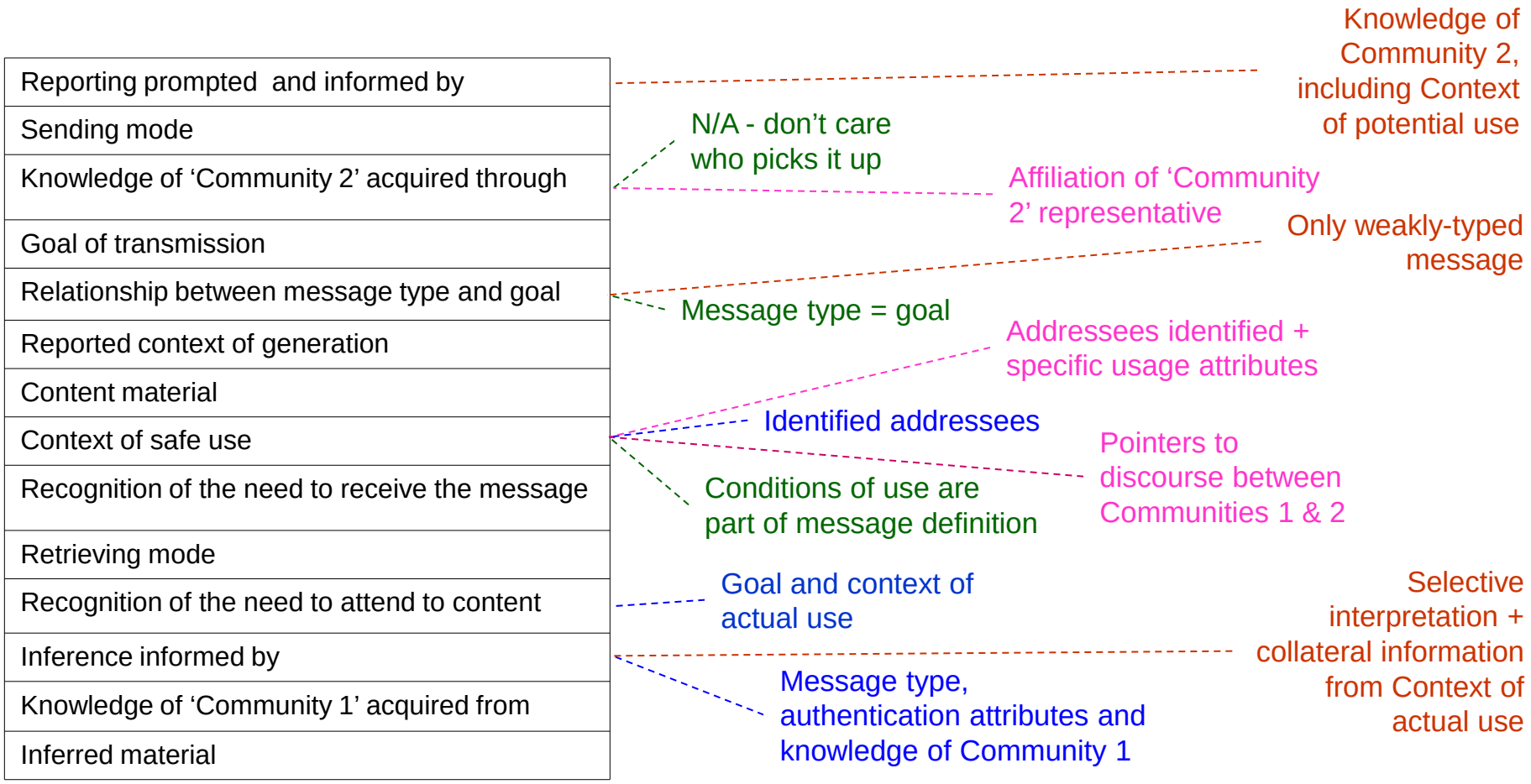
Message id	Authentication attributes	
Message type	Goal of transmission	
Reported context of generation	*“content material”*	*Context of safe use*



4.3 A general model of information exchange

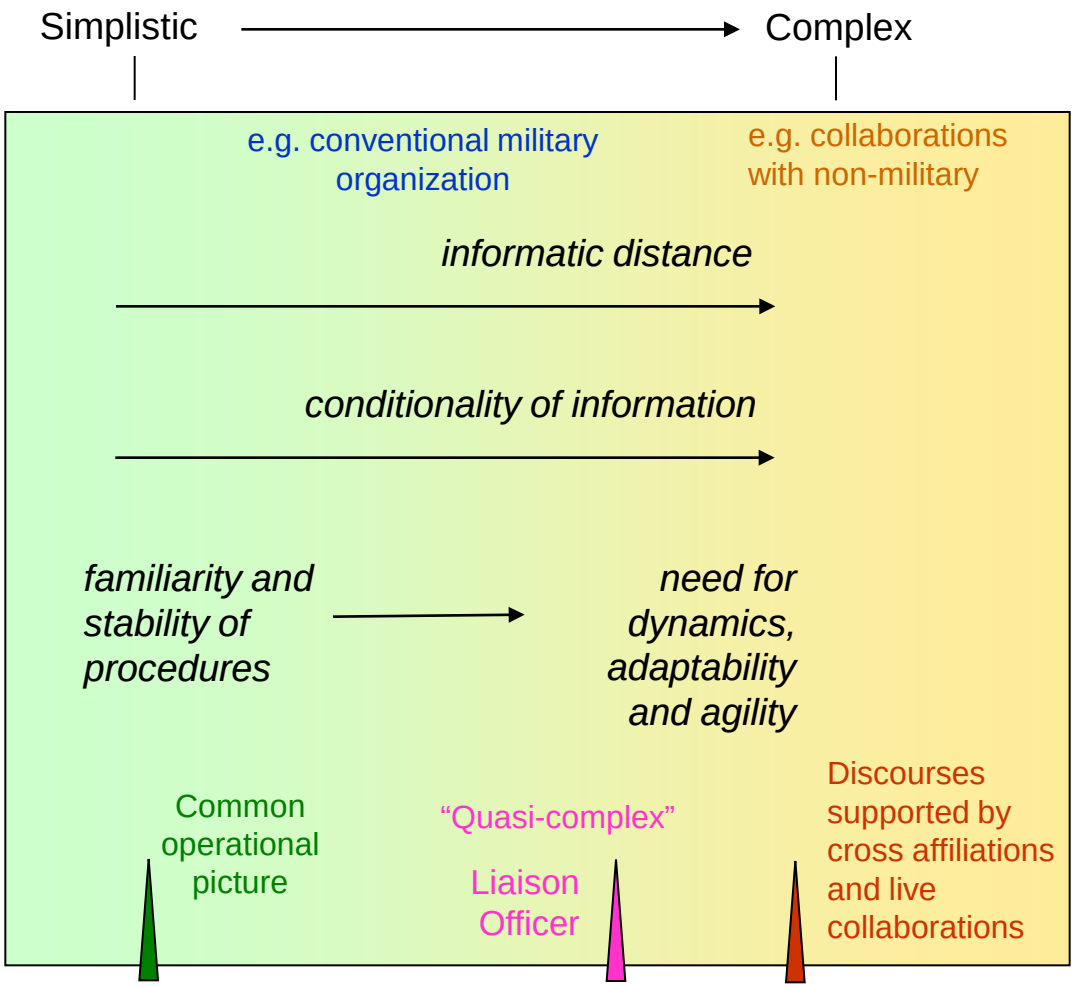


4.4 Mechanisms and their dependence on conditions

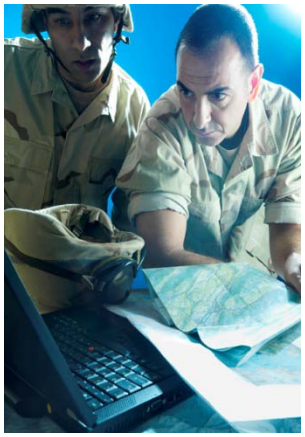


4.5 Analysis of mechanisms and their dependence on conditions

Reporting prompted and informed by
Sending mode
Knowledge of ‘Community 2’ acquired through
Goal of transmission
Relationship between message type and goal
Reported context of generation
Content material
Context of safe use
Recognition of the need to receive the message
Retrieving mode
Recognition of the need to attend to content
Inference informed by
Knowledge of ‘Community 1’ acquired from
Inferred material



5. Conclusions



5.1 Conclusions

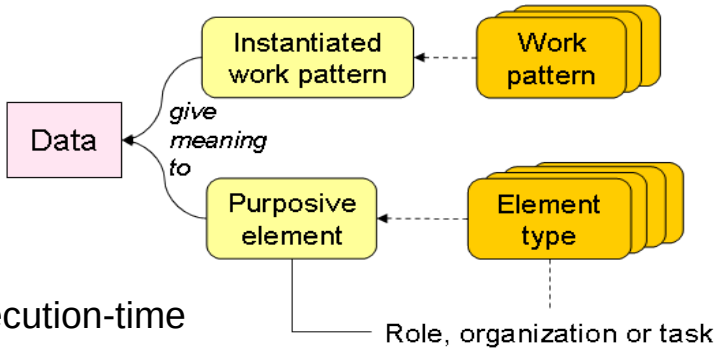
We cannot do this all with meta-data

- As we move towards quasi-complex and complex, we need information whose codification is simply not possible
  - Certainly not at ‘design-time’ – and in some cases not even at ‘run-time’

We need to recognise the role played in informatics by social and organizational components

- E.g. Liaison Officers, collaborations

For ‘complex’ operations and ‘complex organizations’ – e.g. with military / non-military participation – information is relative not only to the community which produces it but also to the work patterns they are employing



- Organization becomes a way of ‘building language’ at execution-time

www.QinetiQ.com