15th ICCRTS
The Evolution of C2

Leveraging the Coalitions' Cloud for Collective Endeavours

I-008

Topics:
Information Sharing, Collaboration Processes, Behaviours
Concepts, Theory and Policy
C2 Architecture and Technologies

Authors:

Margarete C. Donovang-Kuhlisch
IBM Deutschland GmbH
EU Government CTO
Gorch-Fock-Str. 4
D-53229 Bonn
+49-228-881-435 / fax: -301
mdk@de.ibm.com
(primary point of contact)

Michael K. Small
IBM Software Group
Business Development Government
Meudon House, Meudon Ave
Farnborough Hants GU14 7NB, UK
+44-1252-558409
mike.small@uk.ibm.com

Abstract

Collective endeavours require the interaction and coherent cooperation between military, governmental, non-governmental and commercial organizations. They rely on the implementation of an underpinning "digital coalition platform" which unites and governs the policy, information and technology layers of the enterprise architecture. Not only does the platform need to provide interdisciplinary and coordinating services, it must do so flexibly across multiple security domains and classification levels.

The value proposition of information and computing clouds is to provide functional services and information for smart decisions from a virtualized infrastructure transparent to the service consumer – with negotiated and bounded service levels. A cloud consists of both a converged network and various hybrid transformational IT resources formed from and leveraging re-usable mature hardware and software components. The cloud management layer assures separation of concerns and provides guaranteed levels of security and service quality.

This paper illustrates how the dynamic infrastructure delivered by a private cloud can deliver decision superiority in environments where organizational structures, goals and objectives are developing at a much faster rate than traditional IT infrastructures can support. It develops the concept of cloud computing in the context of collective endeavours and demonstrates the expected capability gain reachable through the adoption of the cloud paradigm.

Problemspace

A generally trend is that complex and collective endeavours are supported by and take place in a "flat value network" where governance lies on common intent goal and purpose, and where hierarchical structures have or are replaced with spontaneous interaction and cooperation between peers in military, government, non-government and commercial organizations.

In order to support the envisioned coherent cooperation of a large number of heterogeneous partners in the value network in a secure and assured manner, the underpinning information and communication technologies (ICT) must be both pervasive and highly virtualized.

As the world continues to moves towards a digital society and economy which is smart (instrumented, interconnected and intelligent) and which is powered by the internet of the future, ICT must reach out to a new era of capability. Whereas interconnectivity, collaboration and information management issues were the focus research and ICT development, advanced data analytics and the generation of secure, assured, heterogeneous and virtualized networks are now priority issues. The internet of the future will have to enable new services in all areas of public and personal life and must bridge all service provider and service consumer perspectives. Dynamic and hybrid IT infrastructures based on converged networks are the foundation for such service excellence.

In this paper, we evaluate the transferability of such technologies and methodologies from the fields of smarter citizen services in education, healthcare, public safety and transportation to the demanding area of military operations.

A Coalition as an Enterprise of the Future

In 2008, IBM conducted the latest Global CEO Study (/1/) with 1130 chief executive officers, general managers and senior public sector and business leaders around the globe. In summary, it was found that in any market there is the need to change, and importantly to have an organizational infrastructure able to deal with demands from clients and with the inherent ability to adapt to new threats. This leads to the comprehensive definition of an agile organization depicted in Table 1.

Hungry for change	The enterprise of the future is capable of changing quickly and successfully. Instead of merely responding to trends, it shapes and leads them. Market and industry shifts are a chance to move ahead of the competition.
Innovative beyond customer imagination	The organization surpasses the expectations of increasingly demanding customers. Deep collaborative relationships allow it to surprise customers with innovations that make both its customers and its own business more successful.
Globally integrated	The enterprise of the future is integrating to take advantage of today's global economy. Its business is strategically designed to access the best capabilities, knowledge and assets from wherever they reside in the world and apply them wherever required in the world.
Disruptive by nature	The enterprise of the future radically challenges its business model, disrupting the basis of competition. It shifts the value proposition, overturns traditional delivery approaches and, as soon as opportunities arise, reinvents itself and its entire industry.
Genuine, not just generous	The enterprise of the future goes beyond philanthropy and compliance and reflects genuine concern for society in all actions and decisions.

Table 1: The Enterprise of the Future

The NATO Network Enabled Capabilities – Feasibility Study (/2/) defines the maturity levels for any coalition transformation as:

- Deconflicted
- Integrated
- Collaborative
- Coherent.

With this in mind, the same definition can be applied to the Coalition of the future (Table 2).

Hungry for change	The coalition of the future is capable of changing quickly and successfully. Instead of merely responding, the global defence community proactively predicts upcoming threats and adapts coalitions for prevention, risk mitigation and sustainability.
Innovative beyond	The coalition of the future respects the fact that safety and security cannot be achieved and maintained as a sole value. Locally and globally safety and

customer imagination	security can only exist in a stable balance of justice and liberty in society. The Coalition of the future does not exist in isolation but acts through deep collaborative relationships with other stakeholders in the societies in which is operates, delivering a combined effect which is significantly different from traditional coalition capabilities.
Globally integrated	The coalition of the future is integrating its members to face today's global risks and threats in society, economy and environment. Its operation is strategically designed to access the best capabilities, knowledge and assets from wherever they reside in coalition partners and apply them to deliver the best overall effect.
Disruptive by nature	The coalition of the future radically challenges its operational and tactical model, disrupting the basis of vulnerabilities that adversaries seek. Pre-emptive intelligence and the ability to make more informed decisions and the right time (Decision Superiority) enable it to take advantage of emerging opportunities, to prevent, deter and mitigate risks.
Genuine, not just generous	Founded on an effects-based approach to operations (EBAO, /3/), the coalition of the future can be seen to reflect genuine concern for society in all actions and decisions. It is in this context that the Coalition delivers balanced justice, liberty and safety (JLS): geography – politics – military – economy – social – infrastructure – information (GPMESII).

Table 2: The Coalition of the Future

Coalition Cloud Computing Strategy

The concept of cloud computing is not new: grid computing, utility computing or on demand computing have all described the concept of computing services delivered over the internet, on demand, and from a remote location rather than residing on the service consumer's own desktop, laptop, mobile devices or even within the consumer's organization's data centre. Based on a contract with a provider to deliver applications, computing power and storage via the pervasive web as a service, cloud computing can be considered the logical next step in virtualisation and service orientation:

- Data as a Service (DaaS)
- Software as a Service (SaaS)
- Infrastructure as a Service (IaaS)

With the emphasis on sharing and re-use of common resources, Cloud Computing offers a wide range of potential benefits (/4/) which include:

- Rapid scalability and deployment capabilities – providing just-in-time computing power and infrastructure
- Decreased maintenance and need for upgrades
- Improved resource utilization – elasticity, flexibility, efficiency
- Improved economics of scale
- Improved collaboration capabilities
- Ability to engage in usage-based pricing, making computing a variable expense, rather than a fixed capital cost with high overhead
- Reduced IT infrastructure needs – both up-front and support costs

- Capacity for on demand infrastructure and computational power
- Reduced environmental footprint – green-friendly
- Improved disaster recovery capabilities.

On the other hand, in order to integrate cloud offerings into the coalition's IT strategy, ten challenges must be addressed:

- Need for scalability – how do military operations guarantee the capacity is available given that their requirements are contingent in nature – but high priority once invoked.
- Need for high reliability – traditional military ICT is specified for the worst case. How do we ensure a common infrastructure is built to withstand the worst case and not the "common denominator".
- Need for securing data in the cloud – how can we maintain data ownership.
- Need for open standards and interoperability – 'net rules' for joining, consuming services from and providing services in a coalition cloud.
- Need to revise procurement practices – interoperability starts with the acquisition process, and how to buy shared services.
- Need to resolve potential legal issues – decision making is based on assured information, how will a cloud provide the same level of assurance.
- Need to regulate the "cloud market" – access to public and private cloud services.
- Need to redefine the roles of the IT workforce – delivering the benefits of the cloud to the military implies the implementation of a coordinated and concerted change programs.
- Need to assess the return of investment of cloud computing – how to articulate the business case for cloud computing.
- Need for cloud coordination – what is the governance framework for 'the cloud' and how do we integrate it into, or modify current military ICT governance processes.

We will come back to each of these issues in the technical solutions chapter "Cloud Core Services" on page 7.

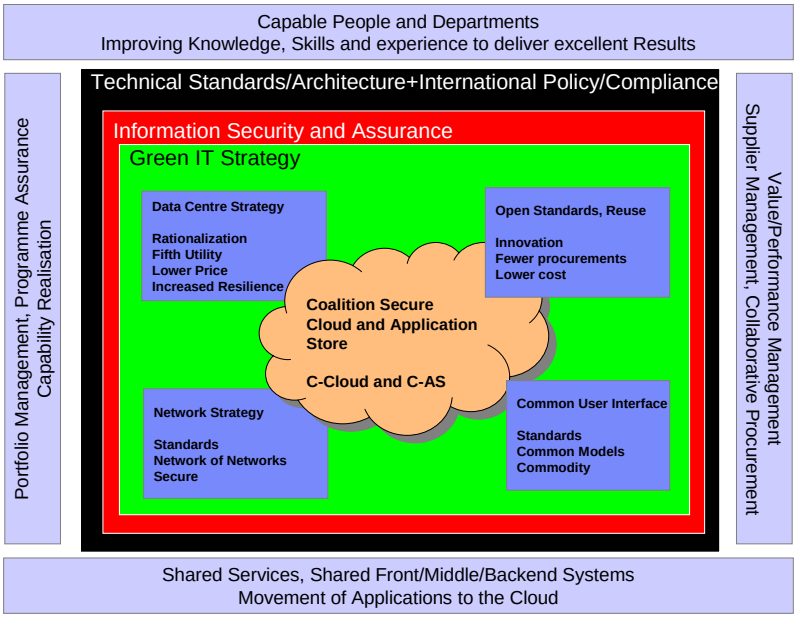

Figure 1: Architecture Blueprint of the Coalition Cloud

In October 2009, the UK Cabinet Office published the first draft of the Government 2020 ICT Strategy in which the government cloud is to be implemented (/5/). Figure 1 gives a pictorial view of this strategy – adapted to the domain of coalitions for collective endeavours.

The most important prerequisite for such a service delivery model is interoperability on all levels – as defined for example in the European Interoperability Framework (EIF, /6/):

- network integration – technical interoperability (addressed by service oriented architecture, SOA)
- semantic interoperability (information standards – metadata models)
- organizational interoperability (interaction standards – process coherence)
- political interoperability (harmonisation of policy).

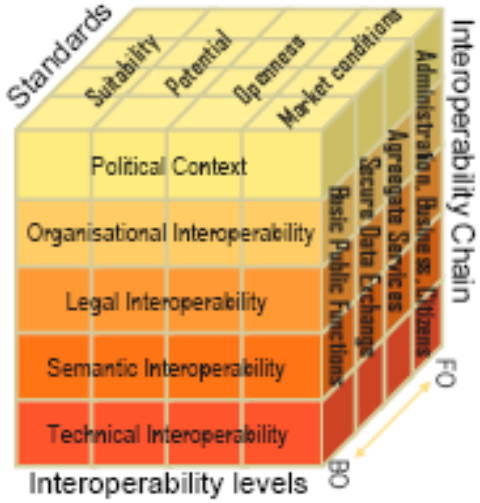

Figure 2: Aspects of Interoperability (EIF)

Figure 2 illustrates the different dimensions of interoperability and emphasizes the importance of standardisation in order to achieve and maintain suitability, potential/value proposition, openness and optimal operational conditions.

Coalition Collaboration Pattern

If we assume interoperability interactions as illustrated above, the various interaction and collaboration patterns as shown in Figure 3. Typically, multiple countries are involved (combined operations) and more than one military organisation per country (joint operations). In addition, interaction with non-military governmental organisations (GO) and non-governmental organizations (NGO) will occur within both national and multinational force structures.

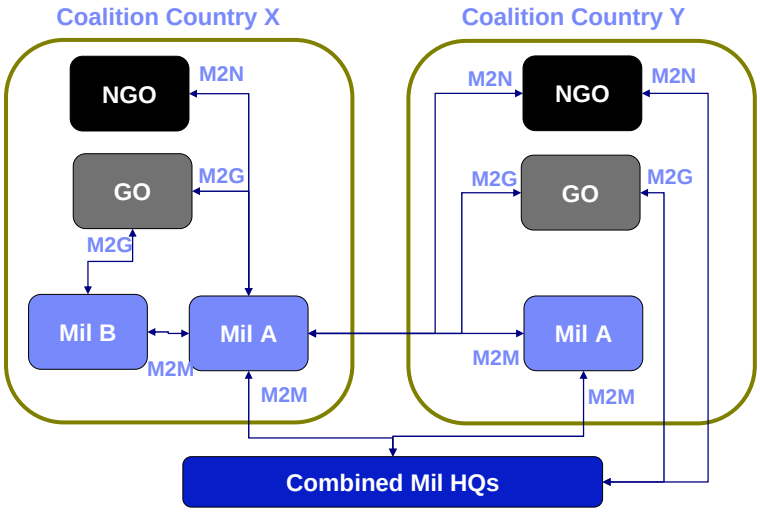

Figure 3: Communication Relationships in a Coalition[1]

Figure 4 and Figure 5 reflect that central governance by a single multinational headquarter is not always possible or preferable and is not required for effective coalition operations. An example for the first pattern could be a humanitarian relief operation, for the second the coalition internal intelligence exchange acting on an intelligence report from outside the military coalition.

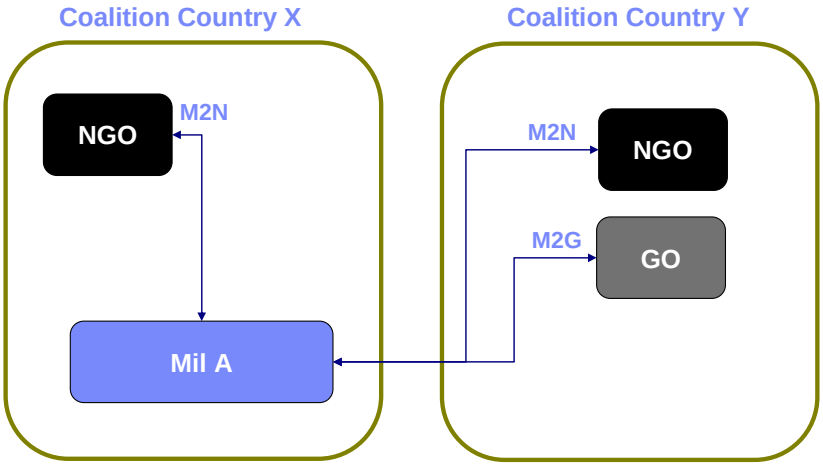

Figure 4: Direct Interaction with "foreign" Military

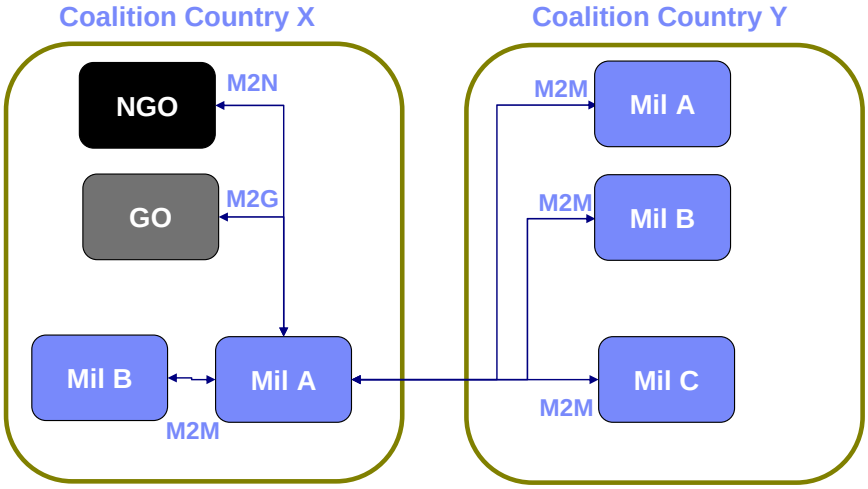

Figure 5: Internal Knowledge Management

In contrast, there will be cases, where exactly that type of coordination and governance will be necessary e.g. communication of shared situational awareness to non-military partners, as illustrated in Figure 6.

[1] NGO = non-governmental organization
GO = governmental organization
M2N = military-to-NGO
M2M = military-to-military
M2G = military-to-GO
HQ = headquarter

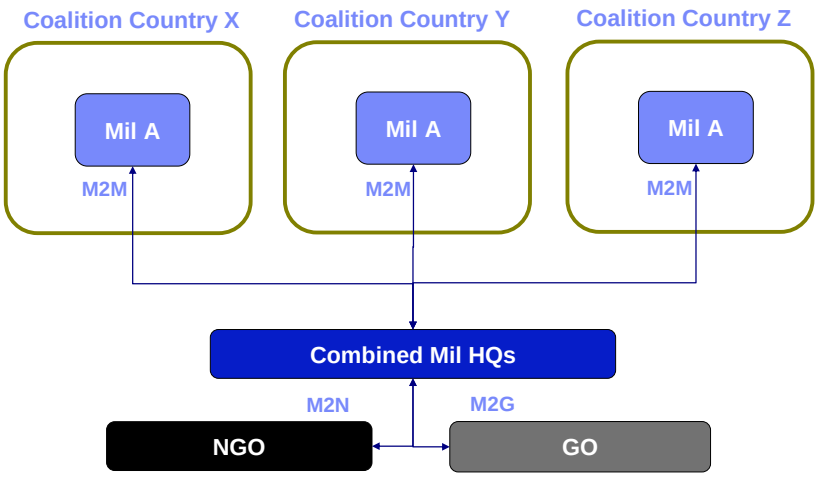

Figure 6: Coalition as a Point of Single Contact

The cloud has to be able to accommodate these different communication patterns, their respective policies and the complex business rules that govern a coalition (such as the rules of engagement (RoE) for example).

Cloud Core Services

Conceptual Model

The EIF defines a Generic Public Services Conceptual Model (GPSCM) and can be used to describe the organizing principles which underpin the construction and operation of the interoperability chains, such as those within a coalition mission structure and to detail the interaction patterns. The GPSCM promotes the reuse of information, concepts, patterns, solutions and standards in the coalition member states and at the combined level; specifically, it:

- it takes into account the reality that information can exist at several levels of forces in the member states
- it takes into account key aspects of the coalition services context: significant cross-border and cross-domain data exchanges are involved which will have a fundamental impact on the design and implementation of IT systems across the coalition – by defining interconnectivity.

Through each of these mechanisms, the model highlights the need for modular, loosely coupled infrastructure components cooperating in the delivery of services. The basic elements of the model are depicted in Figure 7:

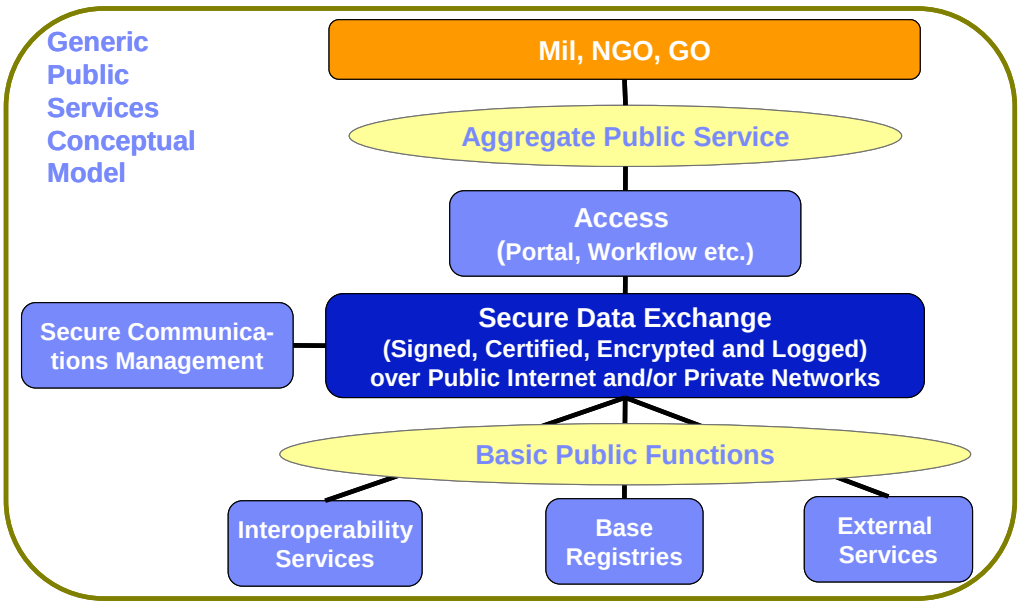

Figure 7: Generic Public Services Conceptual Model (GPSCM)

The model explicitly posits the coalition-wide adoption of service orientation for system conception, development and delivery, as well as an application landscape designed with consistent service components. Service orientation is an architectural style for creating and using business processes, packaged as services, throughout their lifecycle.

The GPSCM implies that a common component model can be developed at the national and system levels to align with the global GPSCM and provides an opportunity for coalition partners to reconfigure their systems and applications to increase reusability. Modularity and reusability are improved by coalition members incorporating service-level agreements and operational policies at the component level. Service consumption based on the model can be organized in several different ways as described below in chapter "Services Consumption Designs".

Services Consumption Designs

The most straight-forward, yet hardest to implement method is to define aggregate services which can be negotiated and thus configured by all coalition partners. The aggregation of a potentially large number of basic components in several member countries and systems using several base registries is orchestrated and governed by the cloud core services and therefore is transparent to the service consumer, as depicted in Figure 8.

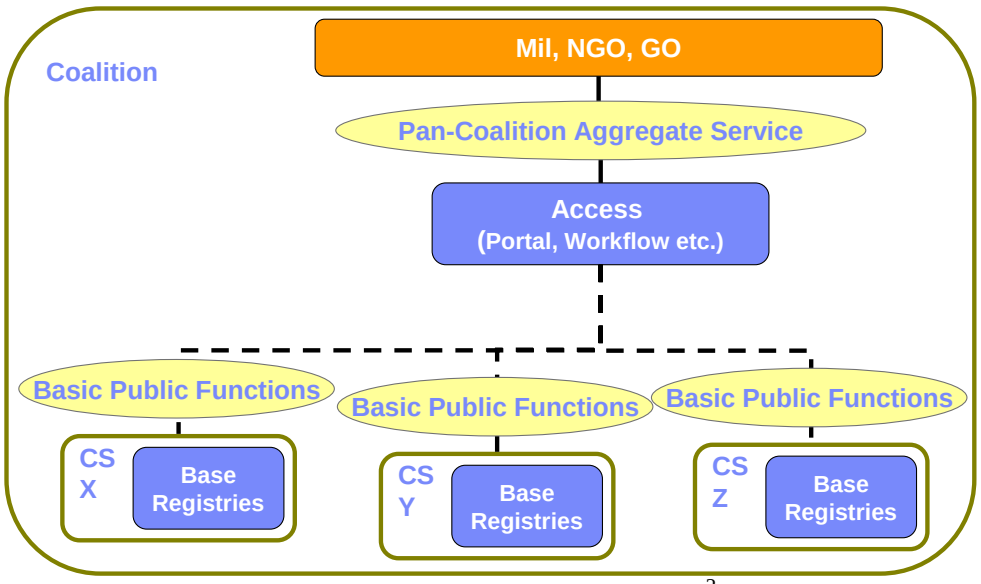

Figure 8: Integrated Access Portal[2]

The next level of complexity is introduced when some of the basic functions to be aggregated in a service are not implemented within a given instantiation of the GPSCM, but are part of another instance. This can be achieved by the inter-registry interaction shown in Figure 9.

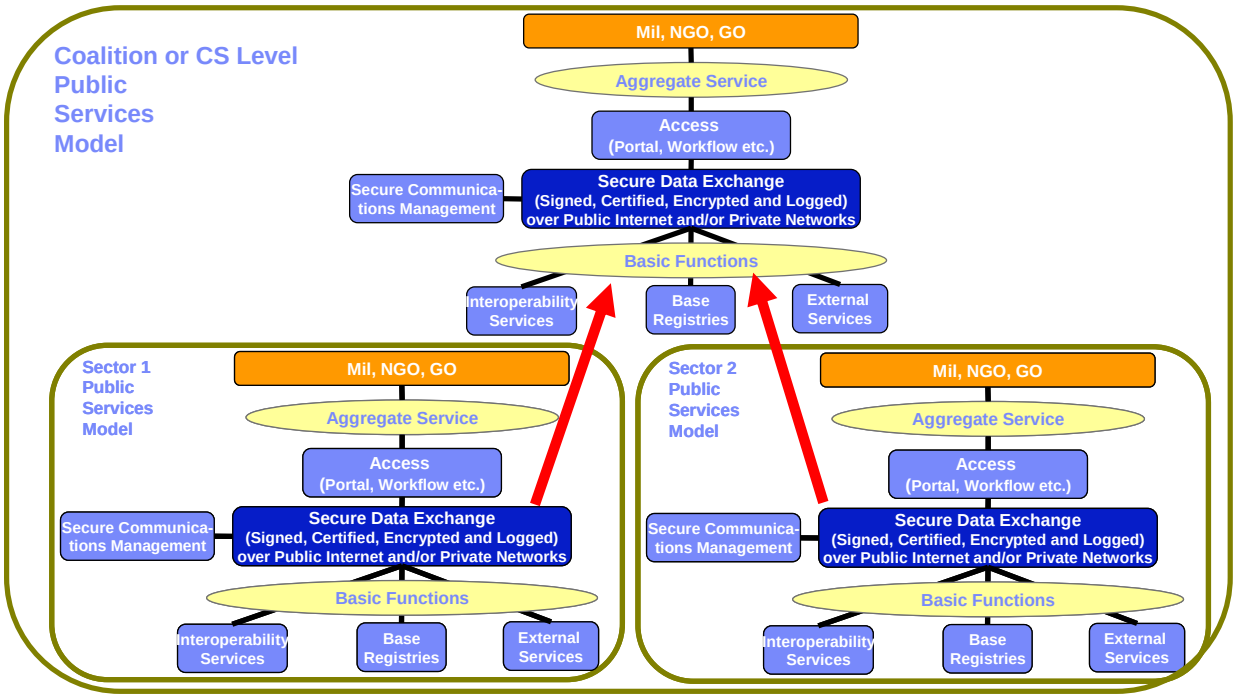

Figure 9: Remote Service Invocation

[2] CS = coalition state/country

Finally, the model allows for a comprehensive "coalition federated enterprise service bus" (ESB) because it builds only on open standard specifications only. Figure 10 gives an impression of the granular and hierarchical structure of such an ESB.

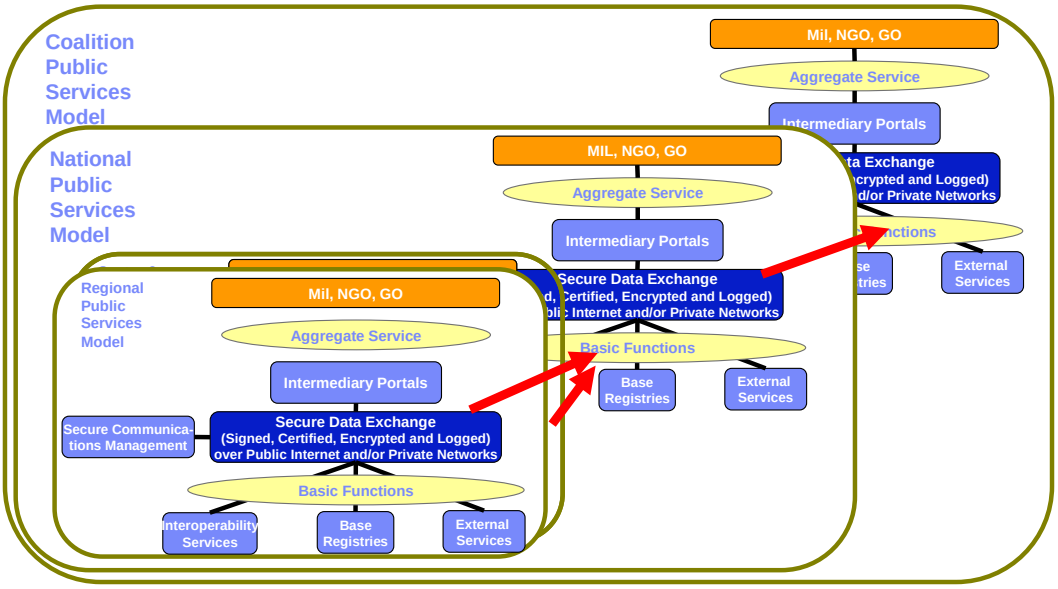

Figure 10: Federated Enterprise Service Bus

Open standard base core cloud services can help to address the most crucial implementation issues:

Trust: the cross-border and cross-system application of the GPSCM involves allowing controlled external access to national data. Building trust in the "control" mechanism is a significant challenge to overcome.
Efforts by the coalition members guided by the mandate should be undertaken to produce a clear, detailed and systematic definition of the roles, rights and responsibilities of data owners, data custodians and data users, including the cross-border dimension in these definitions. This requires technical, organisational and legal support.

Service levels and pan-coalition service dependence on lower-level services: as the aggregated service depends on the basic public functions, the level of service provided by the aggregated one depends on the levels of services provided by third parties.
The establishment of negotiated, appropriate SLAs will be needed and is crucial for successful coalition service implementation. As all such services face the same principal problem, a standardized approach to provisions and other content of such SLA's is strongly recommended.

Common interface standards for basic functions: are needed, because these basics are developed by different parties, possibly in different member countries and must be bundled to provide coalition services. An example where this has been done well in the past is the common formal messaging service where coalition militaries already provide a messaging service to each other; however, to make use of the rich information available, this concept must be taken forward, much further if the kind of interactions described in chapter "Collaboration" on page 12 are to be made available efficiently and effectively in a coalition context.
There is the need for a common taxonomy of such basic functions – at both technical and semantic levels.

Data Protection: as there is likely to be an exchange of national data across border taking place, there will be national data protection requirements to respect. The intermediary layers,

„consumer access" and „secure document exchange", are intended to enforce these security requirements. For example, a difficulty might be that data originating from different nations may have attached different legal requirements with respect to data protection.
The challenge is two-fold: as differences will persist, the intermediary layers will have to continue to cope with a heterogeneous environment of persisting national data protection restrictions; however, conflicts in requirements affecting feasibility have to be eliminated via definition of minimum common requirements as codified in common agreements.

Hidden conceptual mismatch: each of the elements of the model contains many assumptions that could result in situations where incompatible mismatches in conceptual framework and enterprise architecture elements such as „roles" lead to unworkable situations – e.g. the decision making responsibilities and standard operations procedures in two different countries may be quite different – in this case "role" cannot be defined in sufficient granularity.
The challenge then is to define a common approach and conceptual framework at the next level of detail, so as to ensure interoperability of the resulting conforming systems.

In the cloud, these challenges can be addressed with a "4-corner-model" which is for example already adopted in the European program "pan-European Procurement On Line" (PEPPOL, /7/) and illustrated in Figure 11:

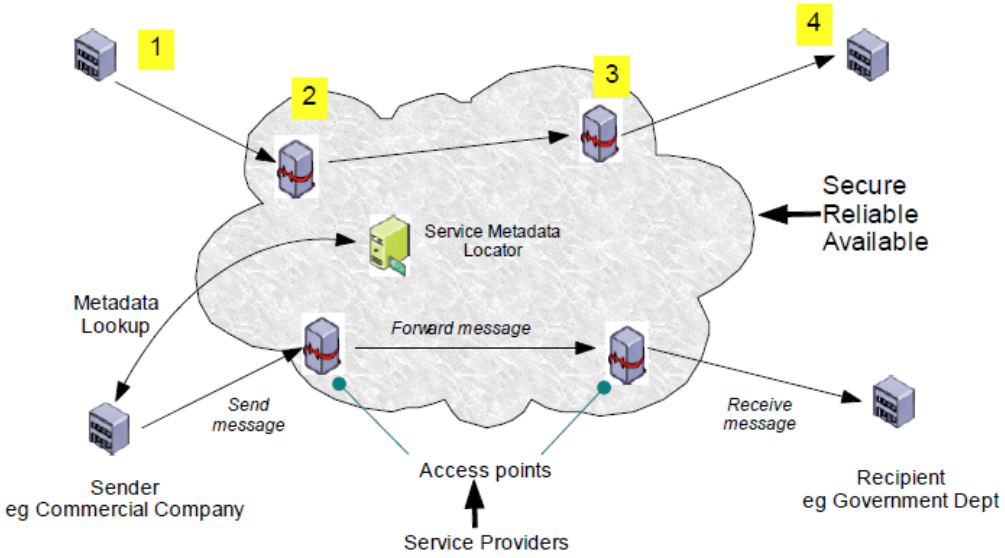

Figure 11: Coalition Cloud Access Points

Core cloud services are the access points for service consumers and providers. Message mediation is governed by the GPSCM. An innovative approach is taken regarding the metadata location and management. A domain name server (DNS) is placed within the cloud infrastructure to resolve the location names for the sites where the coalition partner maintain their respective metadata e.g. the catalogue of their intelligence products. This way, data ownership and sovereignty is assured. Part of the access point functionality is identity assurance using any of the following techniques to generate trust:

- Certificate Authority (CA)
- Trusted Service List / Transport Layer Security (TLS)
- Security Token Service (STS)

Common and Functional Area Services

The NATO C3 Technical Architecture (/8/) defines both common and functional (restricted to communities of interest) services on top of standardized hardware and operating software – for which we have just introduced the coalition cloud. Therefore, these functionalities need to be implemented using the web and web technologies. In the following paragraphs, we give an overview about the state of the art.

Collaboration

A finding of the IBM CEO Study was: "***71% of CEOs plan to place greater focus on external partnerships and collaboration that extends beyond the traditional walls of the enterprise***". Smart collaboration in the cloud is about:

- Globally **connecting** employees, clients, providers and partners to build strong relationships that drive results
- **Collaborating** from anywhere to become a more agile, adaptable organization
- **Innovating** to leverage the power of participation and generation of new ideas and concepts
- **Optimizing** the cost of enabling people.

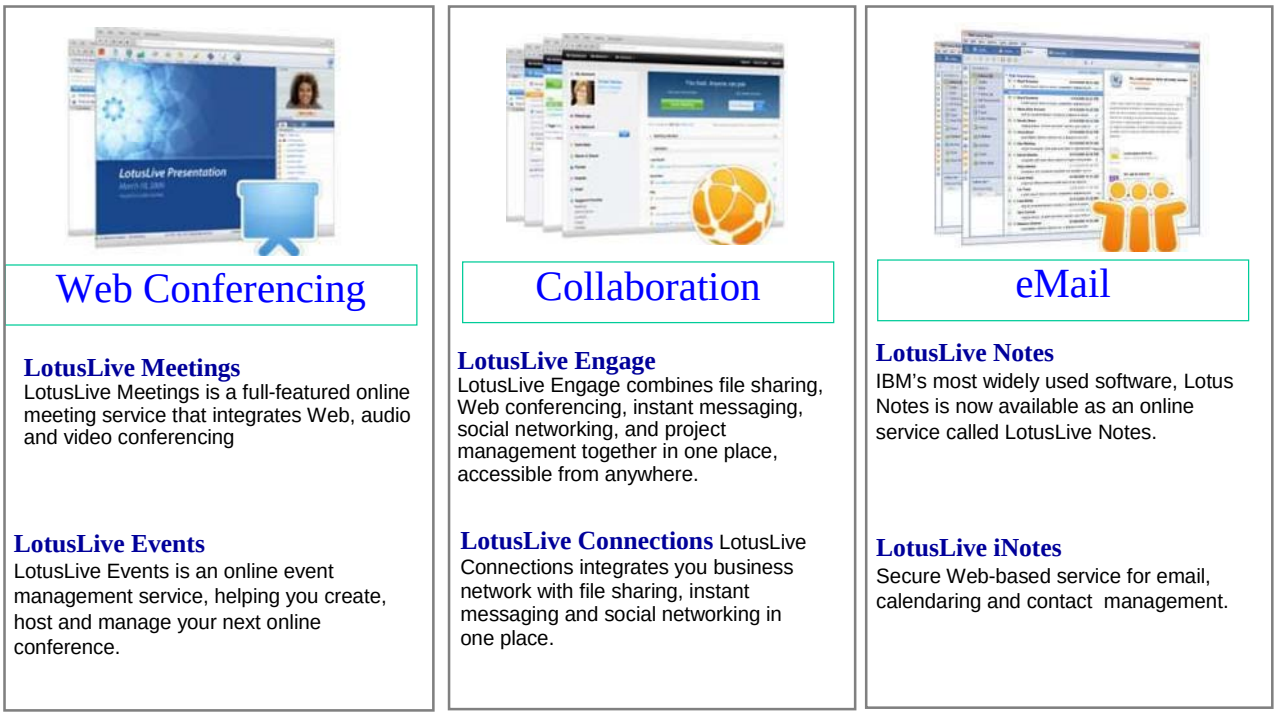

Figure 12: www.LotusLive.com (/9/)

This comprehensive collaboration in the cloud portfolio shown in Figure 12 seamlessly fits into any GPSCM implementation. Figure 13 extends the value proposition into the cloud partner ecosystem – which also is a potential intelligence source for any coalition.

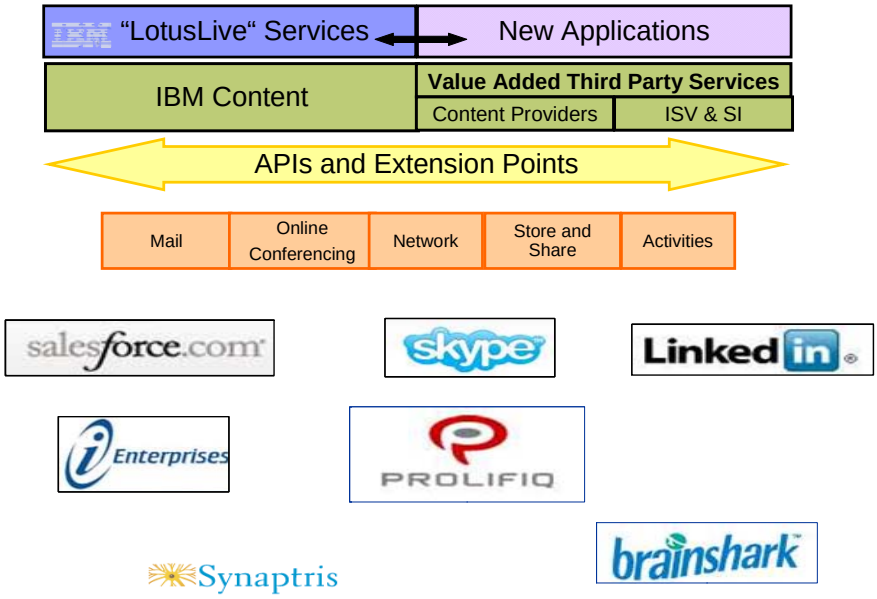

Figure 13: Collaboration Partner Ecosystem[3]

Information Sharing and Document Management

Content of the coalition's information domain is governed by the intelligence lifecycle

- Ingestion
- Dissemination
- Collaborative Analysis
- Visualisation and Exploitation and
- Optimization.

Ingestion typically takes place in a single node of the coalition network, but immediately after that the cloud management services take over. In particular, they support different subject matter experts in constructing a comprehensive operational picture out of single intelligence pieces by collaborating over an intelligence dossier. Figure 14 shows a few such analysis steps exploiting the cloud-inherent unstructured information management architecture (UIMA, /10/).

Key is that the use of ontologies derived from adversaries' business process (in the case of intelligence domains) or of the force deployment planning process (in the case of planning departments) can provide tailored "views" of the body of knowledge which represents the coalition's combined "view of the situation".

[3] API = application programming interface
ISV = independent software vendor
SI = system integrator

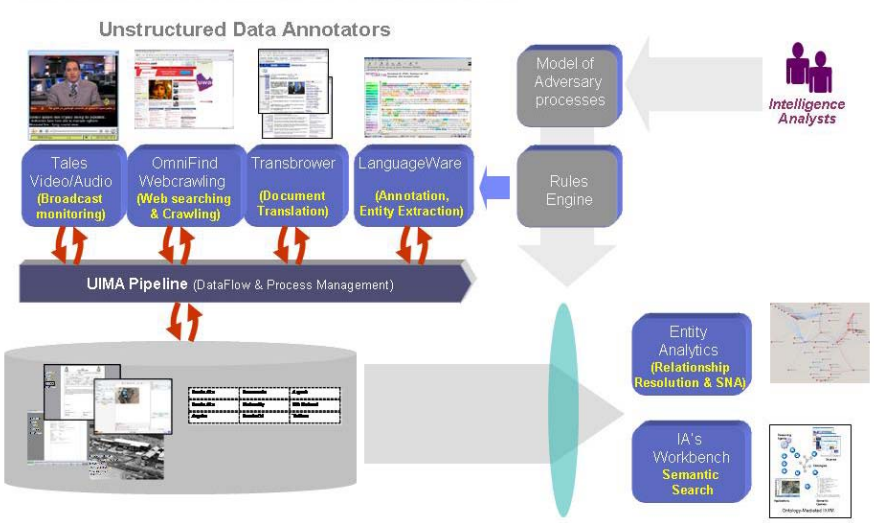

Figure 14: Analyst's Workbench[4]

It is important to note that trust in identity is crucial for this process to be supported by the cloud. e-Identity and e-Signature are two mandatory core cloud services to be provided. If metadata augmentation of an intelligence product is performed e.g. a satellite picture is tagged, then this new data has to be signed by the analyst – the signature becomes part of the metadata.

Location based search

In a globalized, "flat" world, it is important not only to gain insight from unstructured data e.g. through the use of ontologies depicted in Figure 14, but also to derive spatial context from unstructured web resources. In /11/, Dirk Ahlers and Susanne Boll have introduced a focused crawler that applies heuristics to crawl and analyze web pages that have a high probability of carrying a spatial relation to a region or place. Figure 15 shows the architecture of this spatial search engine.

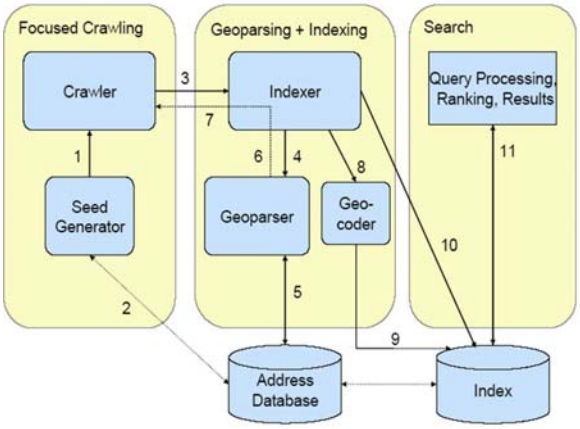

Figure 15: Location-based Web Search

[4] UIMA = Unstructured Information Management Architecture
IA = Intelligence Analyst

This architecture consists of the typical components of a search engine – with special additions for the geographical and geospatial focus:

- A *crawler* discovers and downloads web pages. It takes a URL (universal resource locator), downloads the page, analyses the content (the tools of the analyst's workbench could be integrated) and repeats this procedure by following outgoing links
- An *indexer* tokenizes the page, identifies relevant tokens and makes them accessible to search by storing them in an index
- A *front end* allow the user to search the index with a submitted query. It handles query processing and presentation – and can be integrated in the workbench mentioned beforehand.

LanguageWare Miner for Socio-Semantic Networks

The IBM® LanguageWare Miner for Multidimensional Socio-Semantic Networks (/12/) provides a unified API that helps in creating solutions for these types of multidimensional networks (people, documents, tasks, etc.) and provides an integrated platform for combining social computing, semantic processing, and activity-centred computing for enhanced user experience. Key features include the following:

- a unified and flexible API that allows applications to quickly adapt to changing needs and provides a high degree of personalization
- customization for clustering and fuzzy inference of information on the network through specialized techniques (activation spread on networks)
- semantic processing for both ontology- and instance-based information. This might be used for automatic generation of meta-tags for use in semantic Web applications or in socio-semantic desktop applications such as NEPOMUK (Networked Environment for Personal Ontology-based Management of Unified Knowledge, /13/).

The technology contains an Eclipse application that provides a graphical interface to the basic features of the libraries. This distribution also comes with a small data set and some sample texts. The data set describes information about a fictional organization, including management structures, products, locations, company terminology, etc. Using this application, you can build data into lexico-semantic dictionaries, explore the underlying multidimensional network, perform analysis on text, and perform some basic investigation into the additional information that can be inferred from the underlying network.

The technology is used in several security and law enforcement project following the value proposition of an extension of NEPOMUK towards an ontological network miner (/14/).

Stream and event processing

Stream computing (/15/) is a new paradigm for ultra low latency and high throughput in-motion analytics – needed e.g. at the stock exchange, in intelligent traffic management, but also to achieve a coalition's shared situational awareness.

Continuously, data is flowing in and, while in motion, being processed by analytic components, sent along to other analytics – continuously flowing, needing to be processed on the fly, without going to disk (see Figure 16).

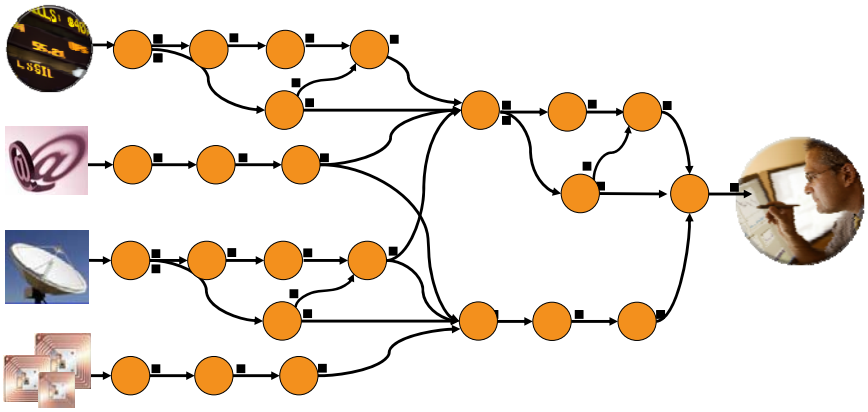

Figure 16: Stream Processing

The stream computing model as illustrated in Figure 17 can be implemented in appliances in the cloud infrastructure and therefore, stream processing of various data sources/sensors can be considered a functional area service in the coalition's cloud.

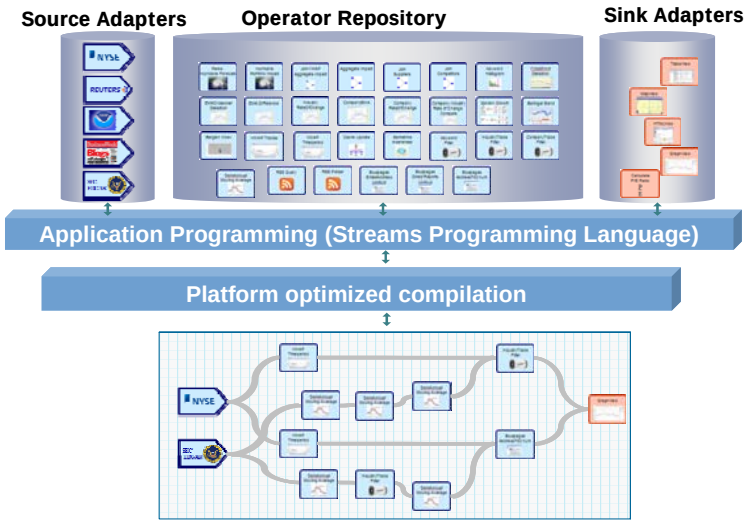

Figure 17: Stream Processing Model for Sensors and Actuators

Figure 18 refers to a maritime research project in Ireland, where stream processing is used to perform large volume, complex acoustic characteristic matching and correlation.

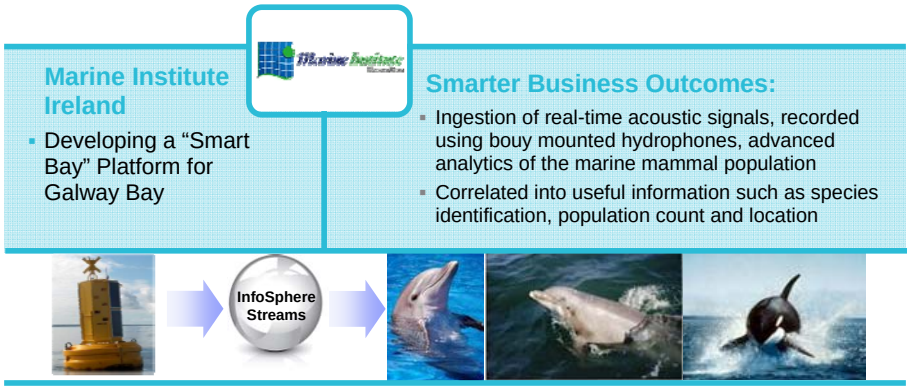

Figure 18: Detection of Events in a Smart Bay

The analysis results give insight about the behaviour of maritime mammals and will allow for more harmonic coexistence between economics (e.g. harbor activities, fishing) and nature by

being able to detect events in real-time and even anticipate upcoming events through pattern analysis and recognition.

Recognition of Common Intent

As regions like Europe develop towards a politically and economically integrated body, agencies, organisations and enterprises from various nations – like coalitions - face the challenge of having to collaborate and provide services to achieve common goals and create prior negotiated, intended outcomes. While European and national legislations set context and rules for such business conduct in multi-national service-oriented ecosystems, agile business process management needs more than an underpinning ontology to ensure semantic interoperability. It requires a complete business process management language (BPML) based on a formal grammar to support inter-nation administrative business processes automatically. In a case study (/16/), the collaborative exploitation of common intent in the context of pan-European e-Government services for a typical life-event of a citizen has been evaluated – in this case, moving residence from Germany to Belgium.

This approach is sufficiently robust and generic that it can be immediately applied to any scenario a coalition is faced with a collective endeavour e.g.

- humanitarian aid
- rescue
- relocation of troops
- disruption of drug production.

The business benefits are the same as those in the more intuitive e-business or e-government environment. They enable policies to be adopted, or modified quickly, and provide the enable for putting agile mission structures in place – able to adapt quickly to new mission priorities or to take advantage of the new services provided by a newly joining unit or organization.

Agile Policy Adaptation

Counter insurgency, peace keeping and peace support operations require flexibility, efficiency and effectiveness at all levels of command. As examples of the complex endeavours that today's commanders are confronted with, these operations are characterized by the need for coalitions to act as a value network: a heterogeneous set of mutually supporting governmental and non-governmental organisations committed to a common purpose. Doctrine, policy, ways of working and the Rules of Engagement (RoE), form the "business rules" which characterise the environment of such a value network. The people, organizations, processes and systems which are 'configured' to deliver services according to these business rules must be continuously adaptable to ensure the most effective response to the threats, risks and opportunities that confront commanders. Discovery – definition – enforcement describes the business-rules lifecycle of any value network. In /17/, we have described the business architecture and the existing and emerging technologies which enable effect-oriented adaptation, as well as the benefits to coalition operations of a structured approach to discovering, modelling, implementing and monitoring the business rules which drive coalition operations

Anticipated Capability Benefits

The component business model (CBM) of coalition operations is defined by the following capability matrix (Figure 19, adapted from /18/).

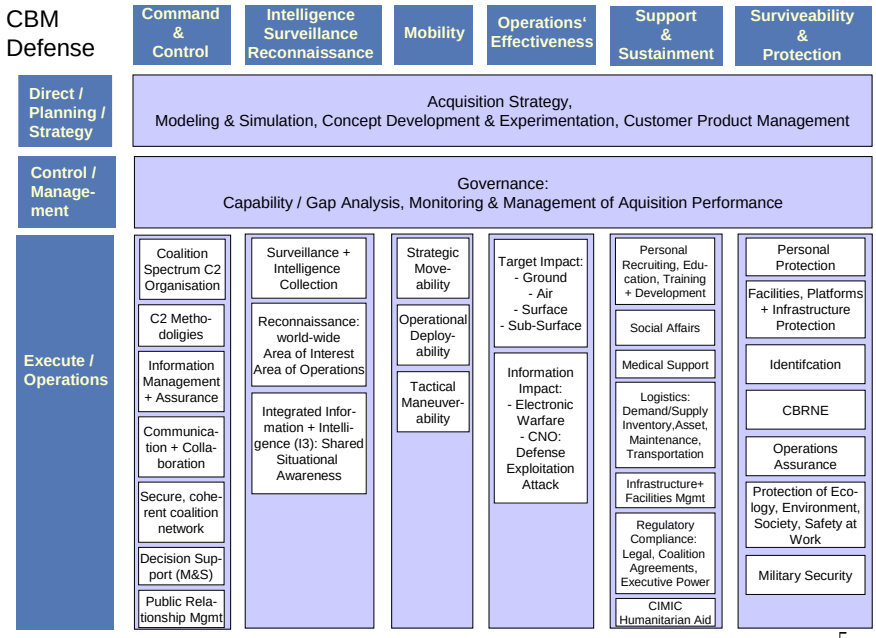

Figure 19: Capabilities Matrix and Component Business Model[5]

Adapting the cloud paradigm and implementing the coalition cloud (C-Cloud) can lead to the following capability gains (compared to Figure 19) – this list does not claim to be complete:

- **C2-Organisation:**
  knowledge about the interactions and dependencies of the decision makers (the awareness about mutual intent) can provide more flexibility in the command structure and thus make the organisation more agile.
- **Information Management and Assurance:**
  the cloud management infrastructure provides trustworthy metadata management and provisioning while maintaining the sovereignty of the data and information owners and suppliers.
- **C2-Support:**
  based on integrated intelligence exploiting hybrid data sources, commanders will be given higher quality and more timely shared situational awareness to enable more predictive and effective operations planning and execution.
- **Intelligence-Surveillance-Reconnaissance (ISR):**
  complex analysis tools such as web mining, semantic and location-based search, complex event and stream processing and collaboration means to gain business insight will allow for better exploitation of ISR capabilities.

[5] CBM = Component Business Model
CNO = Computer Network Operations
M&S = Modelling and Simulation
CIMIC = Civil – Military - Collaboration
CBRNE = chemical/biological/radioactive/nuclear/explosive

- **Information Impact:**
  the cloud infrastructure can also be used for information operations and the governed dissemination of operation information into society.
- **Sustainment:**
  the cloud as the holistic, virtual and pervasive infrastructure allows, for example, immersive training with innovative technologies. It also integrates the entire supplier ecosystem enabling more innovative logistics support. And by definition, the core concept includes the whole area of CIMIC, since the cloud paradigm is pervasive by its nature. Importantly, this enables a more seamless transition between operational phases as new groups and organizations can be incorporated and leave the mission structures to adapt as needed using the flexibility of the cloud paradigm.
- **Protection:**
  the advanced information exploitation tools inherent in the cloud management infrastructure together with risk management policies and fraud models can lead to earlier risk detection and initiation of the counter measures needed to protect the cloud and the mission structures.

Summary

In this paper, we have defined a smart coalition cloud with the characteristics:

- Instrumented:
  trust and confidence are achieved by deploying a wide range of sensors to measure operation-critical performance indicators. Many of the sensors are IT-related, but they also include the important sensors which can contribute to situation, context and history awareness.
- Interconnected:
  classic information and stream processing techniques are combined to ingest relevant information in real-time and build a virtual data warehouse on which data analytics can be applied.
- Intelligent:
  advanced analytics contribute to the creation of situational awareness for all coalition partners; collaboration tools allow for the intelligent sharing of those and for the exploitation of the underlying common intent.

In conclusion, we have applied the concept of the cloud to the domain specific environment of complex endeavours to illustrate how the internet of the future will deliver the adaptable, versatile and secure information, application and service infrastructure needed to underpin coalition mission structures of the future.

A. Appendices

A.1 Figures

Figure 1: Architecture Blueprint of the Coalition Cloud 4
Figure 2: Aspects of Interoperability (EIF)....5
Figure 3: Communication Relationships in a Coalition....6
Figure 4: Direct Interaction with "foreign" Military 6
Figure 5: Internal Knowledge Management 6
Figure 6: Coalition as a Point of Single Contact....7
Figure 7: Generic Public Services Conceptual Model (GPSCM)....8
Figure 8: Integrated Access Portal 9
Figure 9: Remote Service Invocation....9
Figure 10: Federated Enterprise Service Bus....10
Figure 11: Coalition Cloud Access Points 11
Figure 12: www.LotusLive.com (/9/) 12
Figure 13: Collaboration Partner Ecosystem 13
Figure 14: Analyst's Workbench 14
Figure 15: Location-based Web Search 14
Figure 16: Stream Processing 16
Figure 17: Stream Processing Model for Sensors and Actuators....16
Figure 18: Detection of Events in a Smart Bay 16
Figure 19: Capabilities Matrix and Component Business Model 18

A.2 Tables

Table 1: The Enterprise of the Future 2
Table 2: The Coalition of the Future....3

A.3 References

/1/ The Enterprise of the Future, IBM Global CEO Study, 2008, GBE03035-USEN-00.
/2/ NC3A: NATO Network Enabled Capabilities – Feasibility Study V.2, 2006.
/3/ NATO Allied Command Transformation, NATO Concepts for Alliance Future Joint Operations (CAFJO) Draft, January 2006.
/4/ Wyld, D., Moving to the Cloud: An Introduction to Cloud Computing in Government, e-Government Series, IBM Center for The Business of Government, 2009.
/5/ Government ICT Strategy – New World, New Challenges, New Opportunities, UK Cabinet Office, October 2009.
/6/ European Interoperability Framework, Draft Version 2, December 2008.
/7/ www.peppol.eu , January 2010.
/8/ NATO C3 Technical Architecture (NC3TA), Version 1.0., July 1999, Brussels, Belgium
/9/ www.lotuslive.com, January 2010.
/10/ www.alphaworks.ibm.com/tech/**uima**, January 2010.
/11/ Ahlers, D. & Boll, S., Location-based Web Search, Page Proofs ©, Springer, 2007.
/12/ http://www.alphaworks.ibm.com/tech/galaxy, January 2010.
/13/ http://nepomuk.semanticdesktop.org/xwiki/bin/view/Main1/Project+Summary, January 2010.
/14/ http://www.dfki.uni-kl.de/~grimnes/2006/12/telco/IBM_OntologicalNetworkMiner_v1_2.pdf, January 2010.

/15/ http://www.youtube.com/watch?v=mri7cha8ziw, January 2010.
/16/ Donovang-Kuhlisch, M. & Schade, U. „Smart e-Government Services by Recognition of Common Intent", ICSOC submission, May 2009.
/17/ Donovang-Kuhlisch, M. & Small, M. Agile Policy Delivery through Smart Knowledge Discovery and Decision Support ", MCC 2009, Prague, September, June 2009.
/18/ Konzeption der Bundeswehr, MoD Germany, August 2004.

A.3 Abbreviations

API	Application Programming Interface
BPML	Business Process Management Language
C2	Command and Control
C3	Communication, Command and Control
CA	Certificate Authority
C-AS	Coalition Cloud Application Space
CBM	Component Business Model
CBRNE	Chemical – Biological – Radioactive – Nuclear – Explosive
C-Cloud	Coalition Secure Cloud
CCRP	Command and Control Research Program
CEO	Chief Executive Officer
CIMIC	Civil – Military – Communication
CNO	Computer Network Operations
CS	Coalition State
CTO	Chief Technology Officer
DaaS	Data as a Service
DNS	Domain Name Server
EBAO	Effects-based Approach to Operations
EIF	European Interoperability Framework
EU	European Union
GO	Governmental Organization
GPMESII	Geography – Politics – Military – Economy – Social – Information – Infrastructure
GPSCM	Generic Public Service Conceptual Model
IaaS	Infrastructure as a Service
ICCRTS	International Command and Control Research Technical Symposium
ICT	Information and Communication Technology
ISR	Intelligence – Surveillance – Reconnaissance
ISV	Independent Software Vendor
IT	Information Technology
JLS	Justice – Liberty – Safety
M&S	Modelling and Simulation
M2G	Military to Governmental Organization
M2M	Military to Military
M2N	Military to Non-Governmental Organization
Mil HQ	Military Headquarter
NATO	North Atlantic Treaty Organization
NEPOMUK	Networked Environment for Personal Ontology-based Management of Unified Knowledge
NGO	Non-Governmental Organization
PEPPOL	Pan-European Public Procurement On Line
RoE	Rules of Engagement

SaaS	Software as a Service
SI	System Integrator
SLA	Service Level Agreement
SOA	Service Oriented Architecture
STS	Security Token Service
TLS	Transport Layer Security
UIMA	Unstructured Information Management Architecture
UK	United Kingdom
URL	Universal Resource Locator

A.4 About the Authors

Margarete is a member of the IBM technical leadership team for the evolution of a smarter planet and executive IT specialist as well as technical leader and chief architect for the Government Industry in Europe, nourished by her experience as technical consultant for the German MoD and Armed Forces regarding the business transformation towards network-centric operations (NCO) and the effects-based approach to operations (EBAO). She has joined the IBM Defence team more than twenty-five years ago, after achieving her Master of Science Degree in Mathematics in 1981.

Mike has a twenty years experience in the Royal Air Force, during which he gained Masters Degrees in both Engineering and Economics. In active service he contributed to the development of Joint C2 capabilities and intelligence production and as well had an appointment in the MOD Equipment Capability Customer where he significantly shaped the UK MOD's concept of network-enabled capability (NEC). Joining IBM in 2006 as a Defence subject matter expert (SME), he has contributed to aligning C4ISTAR requirements with capability development within IBM and is now driving their integration into the IBM Government Industry Framework.