Adaptation of interoperability standards for cross domain usage

B. Essendorfer, Christian Kerth, Christian Zaschke
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB,
Fraunhofer Str. 1, 76131 Karlsruhe, Germany;

ABSTRACT

As globalization affects most aspects of modern life, challenges of quick and flexible data sharing apply to many different domains. To protect a nation's security for example, one has to look well beyond borders and understand economical, ecological, cultural as well as historical influences. Most of the time information is produced and stored digitally and one of the biggest challenges is to receive relevant readable information applicable to a specific problem out of a large data stock at the right time.

These challenges to enable data sharing across national, organizational and systems borders are known to other domains (e.g., ecology or medicine) as well. Solutions like specific standards have been worked on for the specific problems. The question is: what can the different domains learn from each other and do we have solutions when we need to interlink the information produced in these domains?

A known problem is to make civil security data available to the military domain and vice versa in collaborative operations. But what happens if an environmental crisis leads to the need to quickly cooperate with civil or military security in order to save lives? How can we achieve interoperability in such complex scenarios?

The paper introduces an approach to adapt standards from one domain to another and lines out problems that have to be overcome and limitations that may apply.

Keywords: Interoperability, Data Sharing, Data Dissemination, Standard, Cross Domain

1. INTRODUCTION

In an economic and political interdependent world the ability to share goods and information still is the key for success. Although borders between nations seem to become more important, again many scenarios involve cross border collaboration and the exchange of goods, services and people.

An obvious example for cross border collaboration is the protection of a nation's security. The threat nowadays in most settings does not come directly from across the border by another nation but from terrorist organizations that are connected all over the world and plan their attacks over long distances and sometimes long time periods. It is obvious that national secret services and police must collaborate here to be able to identify potential endangers and follow them across national borders. Data sharing is of interest and often time criticality is an important aspect as well as the ability to filter relevant information out of a large data stock.

Military missions for NATO and UNO also require the ability to share data and information to the right people at the right time.

The use cases of these two domains, the Military and the Civil Security Domain, are similar [1] and in case of cooperation it makes sense to share data. But also in other areas collaboration across borders and across organizations is necessary to draw the right conclusions.

Our climate, for example, is a complex task. To be able to understand how it changes throughout the time, measurements from weather stations all over the world have to be connected to get a detailed picture. To enable conclusions of why it changes those measurements have to be combined with data on specific events or with environmental data (e.g., [2]).

Also in medicine or in the Biodiversity Domain there is a need to collaborate to learn more about a specific problem or to understand how aspects interdepend and what might be a possible solution.

Common to all those examples is that the processes how to acquire and disseminate information as well as the technical means to share data most of the time were developed independently by the different actors making it difficult to directly share the information across domains.

Although most of the time the pure data might be described by metadata or maybe even more sophisticated semantic models, the terms used, the connections between those terms and the formats differ and so do the ways to interface the data sources. Data sharing thus is a complex task and the question is how it can be achieved best.

For most domains standards to share data or even standardized processes have been developed. In some domains these standards are widely spread and used, in other domains standardization is still at the beginning. The question is how can we support cross domain data sharing better and how can the domains "learn" from one another?

In this paper we limit ourselves to interoperability within a limited set of domains. Although there are many different scenarios how it would be beneficial to link domains to each other or why it would be of interest to adapt standards we would like to focus on two scenarios and provide an insight how standards adaption could work in these scenarios.

2. INTEROPERABILITY

2.1 Definition

What is interoperability? The word "interoperability" is being used in several contexts and on different levels of abstraction. Commonality [3], interchangeability [3] and interoperation [4] are strongly related topics with certain similarities but with other focus or areas of application. All of those terms address specific aspects of entity-to-entity relationships that are necessary to make two or more entities work together in a well-defined way.

The Institute of Electrical and Electronics Engineers [5] defines interoperability as "The ability of two or more systems or components to exchange information and to use the information that has been exchanged" which is a broad and rather unspecific definition but already differentiates between the aspect of information exchange and the use of information.

E. Jones Wyatt [6] introduces the more differentiated description of a resource and adds a superior goal defining interoperability as "The ability of two or more systems or components to exchange resources in the form of data, information, materiel, and services, and to use the resources that have been exchanged to enable them to operate effectively together."

Based on these definitions in this paper interoperability refers to the ability of two or more entities to exchange and use resources following a well-defined and agreed process to achieve a common goal.

2.2 Interoperability levels

Derived from [6] and [7] four different levels of interoperability (see Figure 1) can be defined.

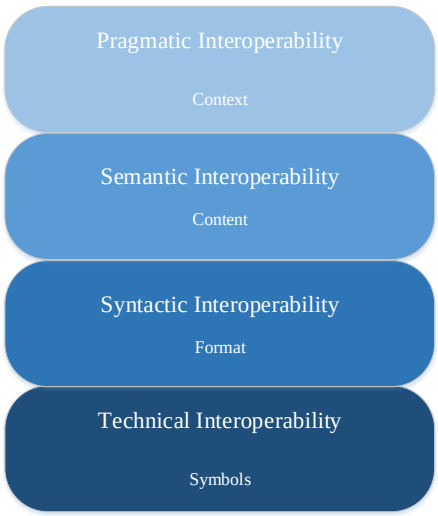

Figure 1. Interoperability Levels

Technical Interoperability describes the ability to operate two or more entities using physical interfaces or connections at hardware and software level or rather symbols as the lowest common denominator between those entities. Systems interoperating on this level are able to exchange data or rather use a common pool of symbols.

If these systems are also using common data formats or rather a common language we talk about *Syntactic Interoperability*. Syntactic Interoperability does not require the entities to understand the meaning of the exchanged data and assumes only syntactical correctness and not content accuracy.

Semantic Interoperability is achieved if the interconnected entities sharing data make use of agreed common concepts and are aware of the meaning of the exchanged data content. Syntactical correctness is a necessary, content accuracy and comprehension a sufficient criteria on this level. On this level pure data becomes *information*.

Pragmatic Interoperability deals not only with the exchange or understanding of data but with the usage of exchanged resources. The basis of correctly using shared data is an agreement on the process level following a common goal to be achieved. On this level, *understanding* what information means (knowledge) and being able to draw the right conclusions is a main aspect.

Table 1 shows exemplarily how the different levels of interoperability could be interpreted for three specific domains.

Table 1. Examples for Interoperability on Different Levels

Interoperability Level	**Example: Natural language**	**Example: Common data repository**	**Example: Military operations**
Technical Interoperability	Letter	Physical connection between the repositories	Physical connection between systems and units
Syntactic Interoperability	Spelling and grammar	Common data format for repository entries	Common language and data formats
Semantic Interoperability	Meaning of a sentence	Common terms, concepts and metadata model	Meaning of content and usage of common concepts
Pragmatic Interoperability	Understanding of a document's purpose	Common goals and processes for adding and making use of the repository content	Common goals, processes and doctrines

2.3 Data- and information sharing dimensions

In this paper the focus is on the technical side of standardization and not on the development of standard processes (operational). Still, technical standards only provide means to execute operational processes. Thus, developing technical standards always means that requirements need to exist (also see [7]).

When working on the technical side, differentiation needs to be performed for a variety of aspects. On the one hand, the information to be shared can be serialized in certain formats. On the other hand, the serialized information needs to be transmitted via a (set of) technical interface(s) between the communication partners. As such an interaction can be located within a business process; the syntactical and semantical consistency needs to be ensured throughout the individual interaction points. These technical mechanisms are then usually complemented by more human oriented mechanisms conveyed as business rules and procedures the operators using the systems have to follow (also known as Standard Operating Procedures – SOPs).

As each of these (technical and non-technical) mechanisms spans an interoperability dimension via the interoperability levels described in Chapter 2.2, a hyper dimensional interoperability cube is formed. In this hypercube the appropriate "overall interoperability" needs to be identified and worked out to solve the problem at hand.

As an example, consider the business case of sharing intelligence reports. In order to share, we need to take multiple aspects into consideration: the intelligence reports needs to be serialized, we need to establish the interface for interaction

and we need an interaction sequence between the participants. For each of these aspects, we have the interoperability levels described in Chapter 2.2.

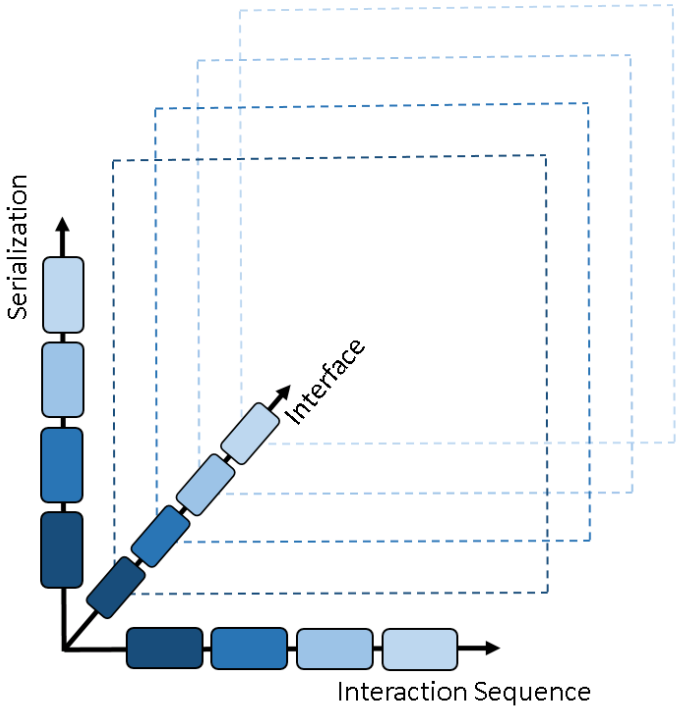

Figure 2. Depiction of a three dimensional interoperability space spanned by the aspects "serialization", "interface" and "interaction sequence".

For serialization, the lowest level requires an agreement on the symbols, which could mean agreement on the tokens employed in the intelligence report (e.g., UTF-8 character set in XML file). The next level could then describe the syntax of the serialization (e.g., the XML schema for human intelligence reports). On the semantics level, we would find semantic definitions of the serialization (e.g., an ALPS or OWL definition of the XML elements). The Pragmatic Interoperability level would associate the human intelligence reports with certain socio-economical values (i.e. the context) – for example the description of vehicle movement might be associated with little impact when observed in an area having low probability of warfare activities, whereas the same incident can imply danger to the lives of soldiers deployed in a mission.

Similar associations of the levels can be drawn for the other aspects. The interface interoperability might employ elements like SOAP messages, WS-Transfer, a "writeData" method and the concept of "sharing intelligence reports between bases".

From these three aspects in our example we can span a three dimensional interoperability space. Two communities that are used to share their intelligence reports in the same format and in the same interaction sequence would result in high serialization interoperability and high interaction sequence interoperability. If they are used to do so using different interfaces (transportation media) such as "email" vs. "FTP file sharing", their interoperability of the interface aspect would be rather low.

3. DATA SHARING IN DIFFERENT DOMAINS – APPROACHES AND STANDARDS

3.1 Benefits of domain specific data sharing

In conflicts and military operations within NATO, UN or EU the collaboration of different nations is necessary as one nation neither has the forces nor the assets to achieve sufficient situation awareness on its own [8].

An example for this is that one nation provides a surveillance asset like a drone with a video sensor as well as the sufficient data link to transport data to the proprietary ground station. The data supplied here should be processed by another nation analyzing the data according to a given task. In a scenario like this processes have to be in place to enable the data flow from one national system to another along with data formats and the interfaces to be able to share the data adequately. Additionally, it is necessary to share the understanding where, when and by what physical asset (along with details on the video sensor) the video was acquired to be able to adequately exploit the data and compare it with data from other sources. Along with the pure data formats also metadata has to be defined and agreed upon. Analysis often involves textual description of objects and events observed and thus a common language and commonly agreed terms are important.

Collaboration within the NATO Response Force (NRF) or collaboration within military partnerships like the Partnership for Peace (PfP) would not be working without the ability to share data and information on the multiple interoperability levels [8] and without common goals defined in doctrines as [9].

In the Civil Security Domain different organizations like public safety first responders have to collaborate in case of events of security violation (see [10]). To control critical infrastructure like airports, harbors or railways, systems acquire all types of data. The sensor types and platforms are heterogeneous and cover different aspects like physical access control (people entering a site), network access control (preventing cyber-attacks) or chemical sensors that react upon a change in a standard setting.

If an incident happens, data has to be passed to the local surveillance unit as well as to other first responders to provide adequate and fast reaction. Besides the technical ability to communicate (for example within talk groups on a predefined channel), SOPs have to be established to ensure a quick and adequate response [10]. Still, data protection guidelines (e.g., [11]) and laws still have to be obeyed and thus data sharing methods must support those aspects adequately.

In the Biodiversity Domain institutions and organizations like the Natural History Museums have collections on specific species. To be able to link aspects from one collection to another, for example to understand how a population of a specific cat influences the population of a specific endangered bird in an area of interest, it makes sense to connect these data collections and gain a wider understanding. Among data sharing concepts and architectures it here is of specific interest to have a common way of sharing the attributes that describe those species as well as commonly agreed qualitative and quantitative measures. The concepts that structure those attributes have to be understood to be able to map the different collections to each other. This points to the development of common formats as well as a common metadata set or even a common syntax and semantic [12].

3.2 Domain specific interoperability standards

To achieve interoperability for the domains listed under Chapter 3.1 standards have been developed. To provide an impression how this is solved in different domains or on different aspects in the following section some standards are described.

In the Military Domain STANAGs are used to enable data sharing. Exemplary a few that support the above described scenario are listed.

- STANAG 4545 (“NATO Secondary Imagery Format”) [13] is being used to persist still imagery data. The files containing the imagery data can additionally also contain annotations (using geometric shapes and text as overlays to the image) and texts. The pure images are complemented with a commonly agreed set of metadata elements.
- STANAG 4609 (“NATO DIGITAL MOTION IMAGERY STANDARD”) [14] is being used to persist motion imagery data. The video streams are complemented by data streams containing additional information (keys and their semantics are defined in additional specifications). Depending on the dictionary key being used, information such as sensor platform location and orientation can be provided to the consumers.
- STANAG 4559 (“NATO STANDARD ISR LIBRARY INTERFACE (NSILI)”) [15] is a catalogue service that enables consumers to share and retrieve ISR products. This is done by cataloguing every ISR product using a defined metadata model and searching the stored metadata based on relevant criteria. Using the found metadata, the consumer can then retrieve the ISR product as a complete file or request a transformation (e.g., a certain section of a large image) of it. Among the supported ISR products are STANAG 4545 image files, STANAG 4609 video clips and a variety of report formats.

To enable higher level interoperability commonly agreed SOPs and doctrines [9] do exist.

The standards of the Open Geospatial Consortium (OGC) are used in many domains that involve the usage of geospatial data. Among the standards used here are:

- Catalogue Service [16]: publish and search collections of descriptive information (metadata) for data, services, and related information objects. Can be complemented with Cat: ebRIM App Profile: Earth Observation products [17].
- Land and Infrastructure [18]: model of land and civil engineering infrastructure, such as roads and facilities.
- Web Map Service [19], Web Map Tile Service [20]: allows access to geo registered imagery in an iterative way by requesting those sections of the image that are to be consumed, using different zoom levels.

As the standards are per se focused on the use case of sharing geospatial information they must be seen in connection with other standards that cover other aspects of a domain's use cases (e.g., within the Civil Security Domain). What can be of interest here is that they open up the opportunity to connect domains on the geospatial level without interfering on other levels. To further use the data provided by those standards, however, a mapping to existing domain specific standards still is necessary.

The OASIS (Organization for the Advancement of Structured Information Standards) Society should also be named here as they provide standards for security and emergency management among other areas. Some standards can be used domain independently (e.g., WS-Transfer for data dissemination) but OASIS has a clear focus on the ability to combine those aspects with security features as provided by WS-Trust or WS-Security. Other standards focus on security specifically, among them the Biometric Identity Assurance Services (BIAS), the Common Alerting Protocol, and the SAML standard that is a XML-based framework for creating and exchanging security information between online partners [21]. Similar to the OGC standards, these standards can be used in different domains and cover specific aspects.

In the Biodiversity Domain many institutions and organizations have built up their own libraries of species, collections of specimen and observation databases. To organize their private repositories they began to categorize and catalog their repository items. Proprietary identifiers and formats evolved over time (e.g., [12]). As the desire arose to share and exchange knowledge and experiences between the different players the need for standards and common formats became clear. Different projects and initiatives dealt with this new challenge to open the different collections to a wider audience. In the following some important standards and initiatives are listed and briefly summarized.

- Darwin Core [22] (DwC; an extension of Dublin Core for the Biodiversity Domain) and the Access to Biological Collection Data (ABCD) schema [23] have been developed to serve as a standard for describing Biodiversity-related entities. While Darwin Core uses a flat structure, ABCD allows the creation of complex types. To make them compatible with each other, mappings between elements of both standards exist.
- The Global Biodiversity Information Facility (GBIF) initiative provides a free and open access to Biodiversity data. It operates by the use of common standards and through a network of nodes provided by co-operating partners. It provides a single point of access and uses the ABCD schema.
- The Biological Collection Access Service (BioCASe) [24] is a transnational network of biodiversity repositories which links together specimen data with information from huge observation databases. BioCASe is a GBIF Participant Node and uses the ABCD schema.
- The German Federation for Biological Data (GFBio) [25] is a national data infrastructure in Germany enabling organizations, institutes, museums and universities to share data for biological and environmental research. It deals with the management and standardization of biological research data during the entire data life cycle (from data acquisition over data publication to data archiving). The GFBio network uses and supports different standard like DwC and ABCD.

4. CROSS DOMAIN DATA SHARING AND STANDARDS ADAPTION

In the previous chapter we elaborated why it makes sense to domain specifically share data and provided examples on existing standards. In the following chapter we will focus on the aspects of cross domain data sharing and the adaption of standards to enable data sharing across domains or to reuse existing standards and standard solutions.

4.1 Benefits of cross domain data sharing

A good example for data sharing across domains is a combined civil and military security setting in civil-military co-operation (CIMIC). As already stated in [7] connecting the Military and the Civil Security Domain is of interest in security operations. This covers all kinds of operations that focus on the continuation, stabilization or recovery of public security. Threats can be natural or man-made disasters (or a combination of both), (terrorist) attacks on network, transportation, public areas and borders, as well as uncontrolled border crossing, smuggling and trafficking. Depending on the type of threat this can be on a national, union or international level. Operations like these can get quite complex and thus the number of organizations involved in these types of operations can be quite high. Those organizations often have own assets to operate and specific sensors and sources to contribute to situation awareness. In an environment where different military forces cooperate within a coalition, intelligence and reconnaissance data is passed on through Joint ISR (Intelligence, Surveillance and Reconnaissance) and the Intelligence Process Cycle. In civil security operations forces such as border protection units, the police, firefighters, ambulances and government organizations collaborate with each other. Depending on the type of threat, these collaborations might be well planned or ad hoc. In CIMIC, for example when restoring public security after a military conflict, the above mentioned forces have to collaborate and very different processes as well as technology (levels) have to be aligned. In most security operations time plays an important role. Information has to be passed on quickly to enable decision makers to enforce the right reaction. Not all information can be openly passed on to achieve knowledge superiority and subsequently react correctly – some information is sensitive and must be protected.

4.2 Adaption of standards in absence of a data sharing scenario

Although there might be only a loose connection between two domains, it might make sense to adapt existing standards. An example can be given for the Military and the Biodiversity Domain. In both domains data ownership is an important aspect. Collections of artifacts in the Biodiversity Domain often belong to different research organizations and institutions. The reputation of those institutions is heavily linked to the data they collected and to the artifacts they store. The willingness to share the concrete objects is very limited. However the interest to know what exists in other institutions is very high and so is the will to share the knowledge that an artifact exists [26]. By connecting the different research results, repositories and observation databases higher level insights can be drawn leading to more research opportunities and both data providers can potentially benefit from this aspect.

High importance on data ownership also is a characteristic in the Military Domain. The concrete data might belong to one nation or to one specific mission and might also be highly sensitive, the need to share information is nevertheless there (see also the conflict “Need-to-know vs. Need-to-share”, e.g., [27]). Thus, there is an interest in having own databases that can be connected and information that can be shared across networks.

Within an organization / a nation those databases could provide more details and more objects than visible to the connected sites. Thus, an adaptable data model and role based access could be of interest for both domains.

4.3 Cross domain usage of applications and standards

As stated above, the adaption of standards for cross domain usage can make sense due to two main aspects:

- (1) The need of two separate domains to collaborate is very high and thus interfaces, data formats, common semantics and processes should be developed to enable information exchange if needed.
- (2) The use cases of the domains are similar and standard development in one domain is on a significantly higher level than in the other domain.

For both aspects, looking at interoperability through the hypercube described in Chapter 2.3 helps to identify what aspects might make sense to apply.

In case (1) the probability that domains need to be connected is high, the dimensions of interoperability need to be focused and a decision needs to be made to what level interoperability should be achieved. Besides identifying the technical aspects (data to be disseminated, interfaces and formats to be used, usage of common terms), the question is if SOPs for specific use cases should be developed. To achieve higher level interoperability it is then also of interest if these aspects should only be developed on a theoretical level (i.e. provide specifications and the relevant documentation for SOPs) or if those aspects should also be exercised to have evidence it works in case of an emergency. This exercise can involve the technical level (can systems interface and exchange data?) as well as the operational level (are the different organizations able to work together in an emergency scenario?).

In case (2) it should be observed if the problems identified in both domain are similar and if one domain has solutions and standards in place that the other domain could reuse.

Aspects that might be of interest are:

- Data ownership: there is an interest to share information about the existence of data or specific aspects of the data, but the source itself should not be shared (see also Chapter 4.2). Knowledge is the key in research as well as in security critical domains.
- Privacy policy: General Data Protection Regulations [11] come into place when personal data is shared. This is true for many domains where information is linked to a person, may it be in the civil security sector, medicine, the public sector or with insurances.
- Security Regulations: Combined with the above mentioned privacy policy for many domains security regulations do apply. Not all types of data should be accessed by all persons leading to the necessity of authentication and authorization when accessing data. In combination with this, data needs to be tagged to enable access depending on the role and on the rights to create, read, update or delete data. To identify security violations specific audit mechanisms might also be of interest.

For those aspects the under Chapter 3.2 mentioned standards might already have a solution or parts of the solution. Whereas OASIS standards [21] focus on aspects that come into place in security sensitive areas, the aspect of data ownership is already addressed in STANAG 4559 [15]. To be able to share data about a certain aspect but keep other aspects internal with a potential to share, the concept here foresees a common data model that can be extended. Those extensions then could be only used internally or within a specific group of users. In a domain where standards are already defined and especially the semantic and syntactic interoperability level has already been addressed by defining a (structured) vocabulary as in the Biodiversity Domain (e.g., [22], [23]) a combination of those standards is of interest and could help both communities of interest with enhancing the interoperability levels by learning from each other.

In the following an exemplary approach for a systematic adaption of an existing standard into another domain is described.

At the beginning of all efforts the involved players have to get a common understanding about what needs to be done in the target domain. Therefore, a meeting between involved people of both domains (source and target domain) should be conducted to point out the general similarities and differences between the two domains and to work out the common goals to be achieved. It is encouraged to develop use cases as this helps to get a better understanding of the target domain and to work out representative examples as a basis for further considerations and migration steps.

In parallel, workshops with technical and domain experts are needed to cover both the technical and the content side. This is important to prevent technical incompatibilities (that are expensive to solve) as well as problems of comprehension which might lead to a technical sophisticated but not applicable solution. During the cooperative collaboration the technical experts should learn about the content-related requirements. The domain experts, for their part, should get a general understanding of the technical conditions and possible limitations that are of interest [28].

Developing prototypes, using test beds and setting up pilot projects and interoperability experiments [29] greatly contribute towards establishing and further enhancing a standard.

In order to achieve a high degree of overall interoperability, it is necessary to be aware of the interoperability aspects (serialization formats, business processes …) applicable for the specific task as defined in Chapter 2.3.

With the aspects identified, each can be analyzed for the already existing degree of interoperability using the existing solutions of the individual parties. Where the desired level is not yet reached by the participants, the next level(s) can be achieved choosing from a set of possible principles. A not necessarily complete list is comprised of:

1. Select one of the existing approaches that will be used by all participants,
2. Define a common approach that is to be used by all participants,
3. Define a container that enables a variety of approaches.

These principles differ by the amount of change the individual participants are required to perform and how the workload is distributed among them. Principle (1) has very little impact for the participant already providing the chosen principle

where the other participants are required to work towards the solution of others. In principle (2), all participants need to agree upon and adopt a common approach, implying there is work involved for everybody after the agreement is reached. It can also be seen to require more work than (3) for emitting as all participants need to adopt a new/different mechanism. For principle (3), participants can embed their existing mechanisms in a new carrier mechanism, thus reducing the amount of work compared to principle (2). Consumption is then however increased as a consumer does not have one way that needs to be dealt with, but rather any way that is being shared using the carrier mechanisms.

For the chosen principle, the technical/syntactical/semantical/pragmatic definitions can be derived per interoperability aspect. A representation model can be created for the syntax interoperability, thus creating platform specific models. An information model can be created for the semantic interoperability which raised the syntax definitions towards a platform independent model. A pragmatic model can be created to describe business concepts, moral standards or the other items necessary for task to achieve.

5. CHALLENGES AND FURTHER RESEARCH

"Interoperability often comes at a price. The costs may be difficult to define and estimate insofar as they consist of (…) expenditures to enhance interoperability as well as the economic and political costs incurred. The issue, of course, is what sorts of interoperability are worth what sort of costs:" [30]

The above described approach to reach interoperabilty by defining interoperability dimensions and examinating the diffent aspects to draw the right conclusions certainly comes at a price. Thus, it makes sense to decide first which interoperability level shall be reached. Depending on the focus there have been different approaches to help decision makers decide how to achieve the best possible interoperability level. Most of these methods have been focusing on pairs of systems. A methodology to measure interoperability of systems of systems (SOS) architectures has been introduced by [6].

After deciding on the right solution for a problem and the development of standards (pilot projects, exercises, interoperability experiments), the implementation of a standard (prototypes), abilities to test and certify (developing a testbed and instantiating a test/certification center) as well as the maintenance of standards (within a consortium or via a membership) have to follow. In a cost-benefit calculation these aspects need to be taken into account. From this point of view the approach to reuse standards seems to be a good idea as some of these follow up steps are likely already in place for existing standards. However, as stated under Chapter 4.3 depending on the perspective the cost calculation of stakeholders will differ as some will be able to reuse existing solutions while others might have to invest heavily.

The appropriate selection of the right decomposition is needed to end up with a workable solution that achieves interoperability. Techniques such as "divide and conquer", "service layering", "responsibility segregation" and best practices in software architecture can aid this process. However, it remains a human task usually requiring a tight interaction between domain experts and technical experts. Moderators can be of aid in these activities as the initial divergence in approaches and values on the pragmatic level can fuel heated discussions and argumental deadlocks among the participants.

Where participants do not want to diverge from their existing solutions, higher levels of interoperability might be achieved via a mediator. The mediator could interact with each participant on the existing lower interoperability levels, translating via the higher levels of interoperability. Further analysis of this and similar approaches could reveal additional technical approaches participants can choose from. Such an analysis then also needs to take the medium and long term implications into account as the mediator requires stakeholders for development and maintenance in addition to the development and maintenance efforts by each participant.

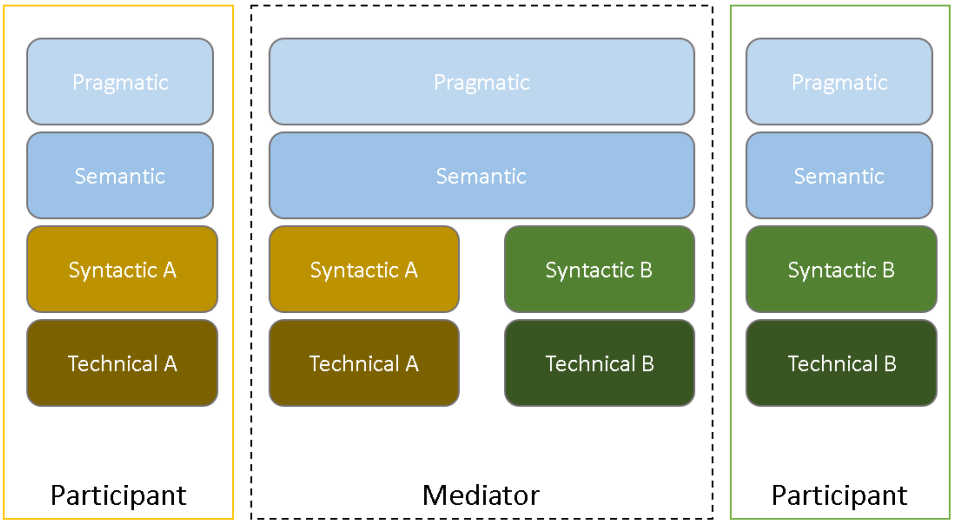

Figure 3. Depiction of participant interoperability using a mediator.

Looking into standardization across domains seems to be a promising approach to solve interoperability issues. To be able to support standard development adequately, the method of using the hypercube depicted under Chapter 2.3 needs to be elaborated in detail. To have a better understanding of the value of interoperability the methods for cost-benefit analysis must be further analyzed and a combination with the introduced methods then is of interest. What has to be taken into account are the psychological and sociological aspects of reaching a consensus in standards definition. Taking into account these aspects of interoperability and developing methods to objectify would probably help to reduce the cost of interoperability.

References

[1] NPIA, "Guidance on Multi-Agency- Interoperability," 2009, http://aace.org.uk/wp-content/uploads/2011/11/Guidance-on-MultiAgency-Interoperability-NPIA-2009.pdf (07 March 2017).

[2] Jiang, Y.; Aumann, H.; Wingyee-Lau, M. et al., "Climate change sensitivity evaluation from AIRS and IRIS measurements," Earth Observing Systems XVI, Vol. 8153(1), pp81531Z-81531Z-11, (2011).

[3] Moultona, C. L, Hepp J. J., and Harrell, J., "Commonality Based Interoperability," Proc. of SPIE Vol. 9831 (2016).

[4] Kubicek, H., Cimander, R., "Three dimensions of organizational interoperability", European Journal of ePractice, Nº 6 (January 2009).

[5] Institute of Electrical and Electronics Engineers, "IEEE standard computer dictionary: A compilation of IEEE standard computer glossaries," IEEE Std. 610, vol. 1991, p. 1 (1991).

[6] Jones Wyatt, E., "A reliability-based measurement of interoperability for conceptual-level systems of systems," Georgia Tech Theses and Dissertations, (2014).

[7] Zaschke, Ch., Essendorfer, B., Kerth, Ch., "Interoperability of heterogeneous distributed systems," Proc. of SPIE Vol. 9825 (2016).

[8] NATO Public Diplomacy Division, "Backgrounder. Interoperability for Joint Operations," Brussel, July 2006, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120116_interoperability-en.pdf (06 March 2017).

[9] NSA, "AJP-2 (A) ALLIED JOINT DOCTRINE FOR INTELLIGENCE; COUNTER-INTELLIGENCE AND SECURITY. Study Draft 1 – Version 1", (2012).

[10] Krauss, B.R., "Developing Interoperability. Standard Operating Procedures," COP, March 2012. http://www.search.org/files/pdf/IssueBrief_7_InteropSOPs.pdf (06 March 2017).

[11] European Parliament and Council, "EU Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and of the free movement of such data," 27 April 2016, http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (06 March 2017).

[12] Skevakis, G., Makris, K., Kalokyri, V. et al., "Metadata management, interoperability and Linked Data publishing support for Natural History Museums," Int J Digit Libr 14, 127 (2014).

[13] NSO, "NATO Secondary Imagery Format (NSIF) STANAG 4545 (Edition 2) Implementation Guide," May 2013. http://nso.nato.int/nso/zPublic/ap/aedp-4(2).pdf. (06 March 2017).

[14] NSO, "STANAG 4609 JAIS (EDITION 3) – NATO DIGITAL MOTION IMAGERY STANDARD," 13 October 2009. http://www.gwg.nga.mil/misb/docs/nato_docs/STANAG_4609_Ed3.pdf (06 March 2017).

[15] NSO, "STANAG 4559 JCGISR (EDITION 3) (AMENDMENT 2) – NATO STANDARD ISR LIBRARY INTERFACE (NSILI)," 3 August 2016. http://nso.nato.int/nso/zPublic/stanags/CURRENT/4559Eed03amdt2.pdf (06 March 2017).

[16] Open Geospatial Consortium Inc., "OGC® Catalogue Services 3.0 – General Model," 10 June 2016, http://www.opengeospatial.org/standards/cat (06 March 2017).

[17] Open Geospatial Consortium Inc., "OGC® Catalogue Services Standard 2.0 Extension Package for ebRIM Application Profile: Earth Observation Products," 10 February 2010, http://www.opengeospatial.org/standards/cat2eoext4ebrim (06 March 2017).

[18] Open Geospatial Consortium Inc., "OGC® Land and Infrastructure Conceptual Model Standard (LandInfra)," 20 December 2016, http://www.opengeospatial.org/standards/landinfra (06 March 2017).

[19] Open Geospatial Consortium Inc., "OpenGIS® Web Map Server Implementation Specification," 15 March

2006, http://www.opengeospatial.org/standards/wms (06 March 2017).

[20] Open Geospatial Consortium Inc., "OpenGIS® Web Map Tile Service Implementation Standard," 06 April 2010, http://www.opengeospatial.org/standards/wmts (06 March 2017).

[21] OASIS, "Standards," https://www.oasis-open.org/standards (10 March 2017).

[22] Biodiversity Information Standards, "Darwin Core," 05 June 2015, http://rs.tdwg.org/dwc/ (10 March 2017).

[23] Biodiversity Information Standards, "ABCD," 30 June 2007, http://www.tdwg.org/activities/abcd/ (10 March 2017).

[24] Döring, M., Güntsch, A., "Technical introduction to the BioCASE software modules," 19th annual meeting of the Taxonomic Databases Working Group (TDWG 2003) (2003).

[25] Diepenbroek, M., "Orientierung im Datenmeer – Infrastruktur für Umwelt- und Ökosystemdaten," Biospektrum, Springer, 5.15, 457 (2015).

[26] Scottish Wild Life Trust, "Policy – Biodiversity Data Access," 07 December 2005, https://scottishwildlifetrust.org.uk/wp-content/uploads/2016/09/002_057__policyonbiodiversitydataaccess_june2012_1371051510.pdf (10 March 2017).

[27] Best, R. A., "Intelligence Information: Need-to-Know vs. Need-to-Share," 06 June 2011, https://fas.org/sgp/crs/intel/R41848.pdf (26 February 2017).

[28] Essendorfer, B., Kerth, C., Zaschke, C., "Evolution of the Coalition Shared Data concept in Joint ISR," IST-SET-126 (2015).

[29] Bermúdez, L., "Interoperability and the value of standards," Revista Internacional de Estadística y Geografía, Vol. 3 Núm. 1 (2012).

[30] Hura, M., McLeod, G., Larson, E. et al., [Interoperability – A Continuing Challenge in Coalition Air Operations,] RAND, Santa Monica, CA, USA (2000).