Distributed Information Management through Coalition Shared Data

Barbara Essendorfer, Achim Kuwertz, Jennifer Sander
Fraunhofer IOSB,
Fraunhoferstr. 1,
76131 Karlsruhe
GERMANY

Barbara.Essendorfer@iosb.fraunhofer.de, Achim.Kuwertz@iosb.fraunhofer.de,
Jennifer.Sander@iosb.fraunhofer.de

ABSTRACT

Information superiority is a key factor in maintaining nation's security. Sensors and information systems produce huge quantities of data and the challenge is to identify, access and use relevant information in time. Operational processes as defined within Joint ISR (Intelligence, Surveillance and Reconnaissance) and the Intelligence Cycle need to be supported by adequate solutions. The Coalition Shared Data (CSD) concept provides a solution by enabling more efficient information management processes.

Information products are here produced in a network of physically distributed sites by systems and services from different nations and vendors in an interoperable way through the usage of standardized coordinated services, interfaces and formats. Techniques of data and information fusion can be added at the system level, other information can be integrated through semantic world models. To ensure data integrity multilevel security measures need to be combined with the existing concept. Information quality management (IQM) on service and system level is needed to ensure interpretability and confidence and to enhance user acceptance.

The paper describes the CSD concept based on STANAG (NATO Standardization Agreement) 4559 Edition 4 and connects it to operational processes. It addresses multilevel security requirements and examines how IQM can add to information confidence in a distributed multinational cooperation.

1. INTRODUCTION

Globalization has created complex economic and sociological dependencies. The nature of conflicts has changed and nations are being confronted with a vast number of new threat scenarios. Information superiority is a question of being able to get the right information at the right time and subsequently draw the right conclusions. Technology allows us to disseminate information in near real-time and enables both aggressors and defenders to act remotely and network over time and space. Technologies in the areas of sensors and platforms as well as network technology and storage capacity have evolved to the level where mass data can also be easily shared and disseminated. To make use of these new capabilities, there is a need for systems and services that can interact with each other in a well-defined way. Efficient information management can be achieved if the participating actors can define common processes and create a common understanding of their overall goals.

In this paper, first the relevant NATO processes for Joint ISR (Intelligence, Surveillance and Reconnaissance) are introduced with a focus on the data and information flow throughout the processes, and high level requirements are identified. Chapter 2 introduces the Coalition Shared Data (CSD) concept as a mean to support those processes. Chapter 3 highlights the aspects of information quality management (IQM) in combination with CSD and chapter 4 summarizes and concludes the paper.

1.1 Joint Processes for Data and Information Management

In NATO operations intelligence is produced through the efficient management of (ISR) assets and actors available within coordinated processes. "*The Intelligence Cycle is the sequence of activities whereby information is obtained, assembled, converted into intelligence and made available for users.*" [1]. In Figure 1, the Intelligence Cycle (IntelCycle) is depicted with five phases. Those are *Planning & Direction*, *Collection*, *Processing*, *Analysis & Production* and *Dissemination*.

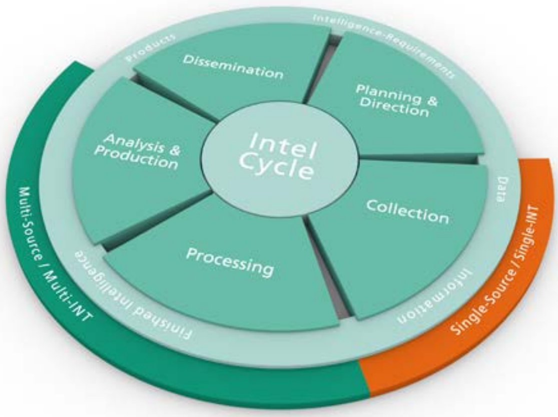

Figure 1: IntelCycle with 5 Phases and the Artefacts that are Relevant in those Phases

In the *Planning & Direction* phase, relevant questions are formulated, prioritized and planned as detailed in the IRM&CM (Intelligence Requirements Management and Collection Management) process [2]. The overarching information elements[1] here are *Information Requirements (IRs)* that are formulated, coordinated and prioritized. Within the *Collection* phase *Data* is collected (based on the *IRs*) and turned into (single-source) *Information*. As depicted in Figure 2, the *Collection* (and parts of the *Direction*) phase is supported by a second complete process that will be introduced later on. In [2], the *Processing* phase also includes the *Analysis & Production* phase. In Figure 1, this phase is separated into two phases (also done in [3]), as it can potentially include many steps and many procedures. In these phases (multi-source), *Finished Intelligence* is produced by fusing and analyzing information and connecting different information elements acquired earlier in the cycle. Through the *Dissemination* phase, the finished intelligence *Products* are shared with the relevant actors. Based on these results, existing *IRs* can be fulfilled, adapted or new ones can be created.

The IntelCycle is closely linked to the Joint ISR Process depicted in Figure 2. The Joint ISR Process starts with a *Validated Collection Requirement* (CR) [4], as depicted in Figure 2. This CR should be answered sufficiently and as timely as required. This means that the input from the IntelCycle is an information element that needs to be followed up during the upcoming process to make sure it is eventually fulfilled with a *Joint ISR (JISR) Result* and supports the creation of *Finished Intelligence*. The Joint ISR Process is quite complex covering multiple roles and loops in organizing the tasking of assets, the collection of sensor data, the (single-source) processing and exploitation of this data and information and finally the dissemination of the result to fulfil the IR the process started with. As this process can include different units, systems and tools, it is necessary to ensure that these information elements are interpretable independently of the individual units, systems and tools and that the information itself remains intact throughout the process.

[1] An information element here is an abstract construct for any (part of) information independent from its format or encoding.

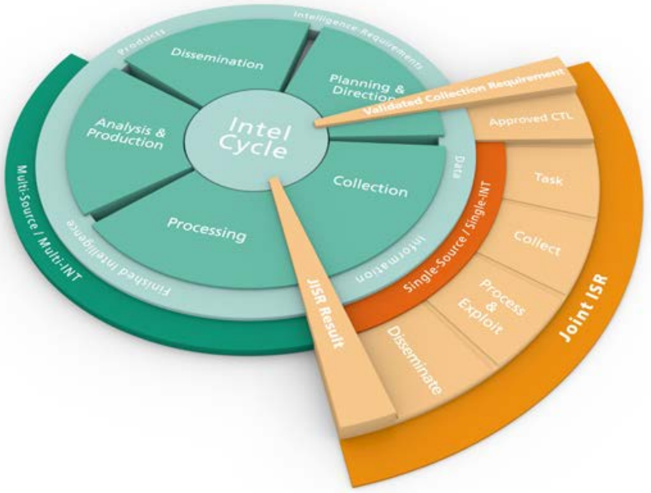

Figure 2: IntelCycle and Joint ISR Combined

1.2 Requirements for Data and Information Management

Creating intelligence following the phases of the IntelCycle and the Joint ISR Process described above points out a number of requirements relevant in terms of the management of information. During the different phases, multiple information elements are created with some of them only being relevant during a short timeframe or within one specific phase and others being relevant throughout the whole IntelCycle.

Some information elements are created during the Planning & Direction phase of the IntelCycle and are carried on until the Dissemination phase. An example for that is an Area of Interest (AOI) that is linked to an IR and disseminated to a sensor system within the Collection phase. The sensor system produces an image that covers that AOI. Subsequently, a (single-source) exploitation product during the Process & Exploit phase of the Joint ISR Process is created with the AOI linked to (or integrated in) it. The product (e.g., an annotated imagery or an exploitation report) is disseminated back into the IntelCycle as (part of) a JISR Result. To enable information processing and eventually fusion with other information elements, this AOI needs to be available even here. Throughout the life cycle of this AOI, different formats might be used, it might be transferred via different networks and security domains and through multiple systems.

This implies that it must be ensured that the information itself remains *intact* and *interpretable* throughout the whole life cycle. Information (exchange) must be *reliable* and *accurate.* In general, the whole process must be *coordinated* and *flexible* (responding to emerging events and to loss of own assets). To enable higher-level information management techniques, the data and information models as well as the data formats that are present throughout the life cycle need to be *interoperable. Security* rules (on multiple levels) as well as *time constraints* must be obeyed.

In the next chapter, a concept and its implementation is introduced that takes into account the above described processes and requirements.

2. COALITION SHARED DATA

The CSD concept was developed gradually within the multinational projects CAESAR (Coalition Aerial Surveillance and Reconnaissance), MAJIIC (Multi-source Aerospace-ground Joint ISR Interoperability Coalition) and MAJIIC 2 (Multi-Int All-source Joint ISR Interoperability Coalition) (see [5]). The approach here was for groups of experts with different background (operational, technical) and from different nations (and NATO) to analyze existing standards, add documentation where necessary and have the standard implemented by different institutions and companies. The result was then tested in interoperability exercises on a technical and procedural level using simulated and, in a final stage, live data. The exercises were accompanied by a test team that documented the lessons learned. These were subsequently analyzed by the expert groups and the whole process started again. The outcomes were adapted processes, specifications and information models. The supporting multinational project has now been concluded and the final results are being consolidated by the Custodian Support Team of STANAG 4559 and brought into Edition 4 of STANAG 4559.

2.1 CSD Concept

The CSD concept is essentially based on having a network of physically distributed sites (network nodes) which are connected using the available network infrastructure (see Figure 3). Among the sites, each node shares information about its persisted content through CSD using (meta-)data entries. A global awareness of available data is achieved by distributing the (meta-)data across all instances of participating sites using appropriate synchronization/transfer protocols. Combining this awareness with the ability to retrieve product files and streams on demand ensures ubiquitous access capabilities for data stored on any of the sites in the entire network with reduced network traffic. The CSD concept started with the sharing of static, finished data such as reports, images and video clips. Over time the scope was extended to include the ability to share dynamic, mutable data – such as we can encounter in collaborative business processes where multiple parties modify a common piece of data – and constantly changing data such as video streams.

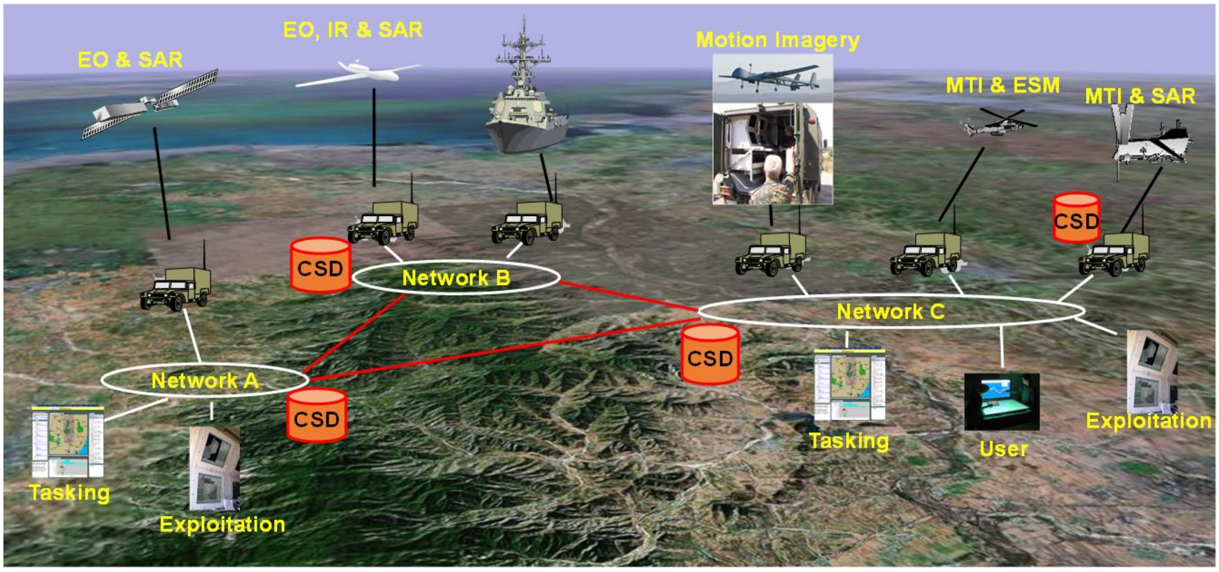

Figure 3: Information Dissemination in a CSD Network

2.2 STANAG 4559 Edition 4

The Custodian Support Team (CST) of STANAG 4559 picked up the relevant results of the MAJIIC 2 project and consolidated them into the standard STANAG 4559 Edition 4 [6]. With the new Edition of STANAG 4559, the three aspects regarding the nature of the data (sharing of static, stream and dynamic data) are now split into three specifications (AEDPs (Allied Engineering Documentation Publication)) and thus three technical approaches (pillows) addressing the individual requirements of each aspect. In the next chapters, those aspects are described in more detail.

2.2.1 AEDP-17: Dissemination of Finished Products via the CSD Server

AEDP-17 [7] was created for finished (static) products. Following the Joint ISR process, these products are usually created based on a specific task. In case of a sensor system these products can for example be imagery from ground, airborne or maritime platforms or video clips acquired in a specific AOI. An exploitation system will for example disseminate annotated imagery, documents or specific exploitation reports. The products can be linked to each other via associations and are annotated with metadata. The metadata model as well as the interfaces to store and retrieve products are specified within AEDP-17 as well as means to share data within a larger network among different system nodes. The metadata enables to catalogue (and query) products according to aspects like the geographic area or the time covered, the type of product (e.g., imagery, document, report), the source (e.g. sensor system) and publisher (e.g. exploitation system) as well as security aspects like the classification, the policy or other more type specific aspects like the type of image (e.g., infrared) or an information rating of a report.

A system that implements AEDP-17 is called a CSD Server. The interfaces to connect to the CSD Server are defined via CORBA or (optionally) via SOAP. To store and retrieve data, sensor, exploitation or IRM&CM systems implement those interfaces and act as a CSD client. CSD Servers in a CSD network communicate via CSD Server synchronization. Here, the servers exchange catalogue entries (i.e., metadata entries). On demand, CSD clients can then retrieve product data (files). The new version of the standard allows extending the metadata model beyond the given attributes to enable exchanging new data types or new attributes.

2.2.2 AEDP-18: Stream Dissemination via the CSD Streaming Server

In AEDP-18 [8], the exchange for data streams such as video streams, Link 16 and GMTI (ground moving target indicator) is described. The specification is implemented by systems called CSD Streaming Servers. Through defined interfaces, other systems (e.g., sensors) can interact with these CSD Streaming Servers and provide or retrieve data. CSD Streaming Servers can also synchronize their content (e.g. systems located in different nodes). Interfaces to provide live streams to users and to retrieve those are defined in AEDP-18 as well as a metadata model to describe the content of each stream. The metadata model is similar to the one provided in AEDP-17 (see chapter 2.2.1). The interfaces described in AEDP-17 are also reused, where possible. An (optional) bridge between the CSD Server and the CSD Streaming Server is also defined here. By implementing this, proxy products for data streams can be created in a CSD Server, enabling associations with other products or the linkage to AEDP-19 information elements (as described in chapter 2.2.3).

2.2.3 AEDP-19: Dissemination of Dynamic Products via the ISR Workflow Architecture

In AEDP-19 [9], the data exchange for products like tasks, requests, plans and AOIs according to the Joint ISR Process is described. AEDP-19 states: *“NATO Standard ISR Workflow Architecture provides standard interfaces for enabling Joint ISR processes and exchanging JISR workflow elements through suitable applications maintained by NATO and NATO Nations.”* (see [9], chapter 1.2). Through a service oriented architecture (SOA), services on different levels are defined that enable for example the exchange of tasks and requests from IRM&CM systems to sensor/exploitation systems and the management of the subsequent workflow (e.g., status review). In addition, workflows like requirements management between IRM&CM

systems of different units or the exchange of ORBATs (order of battle) can be handled through this. Products (results) that were stored within a CSD Server or a CSD Streaming Server are linked to tasks via product IDs. By these linkages information elements of different process phases can be connected. In an overall architecture, low level services from different nodes can exchange information via a specific replication interface. To enable business processes as described in [4], choreographies are defined that describe the workflow of information elements within AEDP-19 and beyond.

2.3 Integration of the CSD Concept into Operations

The CSD concept provides support for requirements mentioned under 1.2 that address issues of interoperability. It provides a solution for the Joint ISR Process and for interoperable intelligence production and dissemination through the usage of common formats, data models, interfaces, services and workflows. To integrate the CSD concept into an operational environment, additional aspects have to be taken into account that are not covered by the STANAG 4559 itself, as these are individual for the respective (national) networks, security requirements and use cases.

In an operational environment, multilevel security is very important and CSD systems thus need to be connected to additional systems and services. STANAG 4559 provides elements to enable this. Metadata attributes are available that define the classification, the policy and the releasability of information elements shared within a CSD network. Authorization and authentication systems are connected within a operational project defining the relevant security environment. To enable data exchange via different security domains, additional services are included for a seamless data transfer. An example for such a service can be the CSD-XDT (cross-domain transceiver) provided by Fraunhofer IOSB that enables CSD Server synchronization according to AEDP-17 and data replication as defined in AEDP-19 via an accredited security gateway. To enable integration of the service architecture of AEDP-19 with WS-Security services [10], security attributes were integrated in the respective service specifications.

In order to ensure information confidence in a distributed multinational cooperation, a concept for IQM is needed. The next chapter details such a concept (which has been worked out by the authors) and in particular describes means for ensuring information quality (IQ) throughout a CSD network as well as for implementing IQ management in practice.

3. INFORMATION QUALITY MANAGEMENT FOR A COALITION

In Joint ISR coalitions, the data and information shared via CSD Servers, CSD Streaming Servers and the ISR Workflow Architecture is essential for timely and adequate decision processes. Yet, as a physically distributed and networked enterprise, a Joint ISR coalition is also prone to local differences in operational processes or interpretation of ISR products (such as images, reports, video clips, etc.), which (though standardized) can result in different ways of how ISR products are created. Specifically, differences in product contents can occur – e.g., usage of fields, missing information, alternative content formatting, etc.

Such differences make it harder to achieve pragmatic interoperability in a Joint ISR coalition, i.e., the common understanding and interpretation (in terms of derived actions) of exchanged ISR data and information. To counter such effects, a pro-active management of IQ in coalitions is required. The management of IQ also constitutes a key aspects in the IntelCycle and the Joint ISR Process.

3.1 Exemplary Consequences of Lacking Information Quality

Not considering IQ in a coalition can lead to serious problems. Regarding for example the ISR products contained in a CSD Server, users in need of information can search for contained product based on metadata values such as location, time, type of product, etc. If, for example, a product is not situated (in its CSD metadata) at the correct location, the user will not be able to find this product and, thus, cannot consider its contained information when making decisions. Not containing the correct location can be caused by several issues, including: no location being given for the product, an incorrect location being given in the product, or an incorrect mapping of information from the product to its metadata.

Besides not being found by users due to wrong metadata values, it is also possible for a product not to be found because it is not known to the local CSD Server (in the coalition of networked CSD Servers) the user is connected to. In a Joint ISR coalition, ISR products are created by producers such as exploitation systems and inserted into the coalition network by publishing the products to the CSD Server local to the producer. During synchronization of CSD Servers, the metadata of locally inserted products is exchanged in between all the CSD Servers connected to the coalition network. For this metadata exchange, each CSD Server may perform validation checks regarding e.g. the completeness or syntactic compliance of each synchronized metadata element, and thus discard individual elements not complying with its validation checks. In this way (due to localized validation policies), it is possible that no synchronized view on the shared information can be achieved over the whole coalition network, due to single products being available only in certain parts of the network. This has the same effect on decision making as incorrect metadata: required information cannot be considered when needed for making decisions.

As a final example for the potential consequences of lacking IQ in a Joint ISR coalition, the regulatory compliance of distributing classified information can be mentioned. Here, also the consistency of product data with its CSD metadata is the main concern. If, for example, the values describing the classification, releasability or policy of an ISR product are not consistently transferred between product and (CSD) metadata, this information may get lost. If a CSD product is then passed on without its metadata (e.g., to other users in the same unit), no classification or releasability might be available.

3.2 A Joint ISR Coalition as a System-of-Systems in Information Quality Management

IQM should be seen a necessary pre-requisite when integrating the CSD concept into operations. A Joint ISR coalition is a complex enterprise, therefore, a structured approach to IQM is needed, which must be explicitly tailored to the specifics of the coalition.

In a Joint ISR coalition, different types of systems interact which each other. On the one hand, there are systems producing ISR and publishing their products to the CSD network, e.g., sensor systems produce sensor data, exploitation systems produce annotated imagery and exploitation reports, and IRM&CM systems produce information requirements and collections tasks, etc. On the other hand, there are systems consuming the products published to the CSD network, e.g., for creating intelligence or contributions to situation pictures. Often, systems can act as both, producers and consumers, e.g., a sensor data exploitation system which consumes imagery products and produces exploitation reports. In between producing and consuming systems, the network of CSD data storage systems exists (as mentioned in chapter 2.2).

The main use cases of the CSD network in a Joint ISR coalition are thus the retrieval of published ISR products, by users in need of respective information, including the use of the retrieved products (e.g., for being at least partly integrated into a situational picture), and the publishing of ISR products to the CSD network. IQM for a Joint ISR coalition, in consequence, has to support these use cases, i.e.,

- ideally, enable a user to find and retrieve valid, consistent and current ISR products according to his or her (informational) needs,
- or, more generally, enable a user to handle his or her required ISR products based on the assessed and known quality of these products,
- and support a user when producing and publishing valid and consistent products to the CSD network.

3.3 Coalition IQM

When considering IQM in a Joint ISR coalition, the CSD network can be abstracted to consist of three types of systems: tools for producing ISR products, (a network of) CSD storage systems, and CSD clients to ingest products into the CSD network. Measures for ensuring IQ of ISR products can now be employed at different locations of a Joint ISR coalition:

- within the tools creating ISR products,
- within clients publishing the created products to the CSD network,
- at the boundary of the CSD network (i.e., at the CSD storage system receiving the product to be published form a client)
- or within the CSD network (i.e., when products that have been published to one CSD storage system are being synchronized to other CSD storage system in the network).

3.3.1 Validation within the CSD Network

Ensuring the quality of produced/published products by validating these products at different locations in a coalition has different consequences – e.g., in terms of available actions to perform on products failing validation checks, in terms of quality guarantees that can be given for (parts of) a coalition network or in terms of emerging side-effects. When validating ISR products within the CSD network, three different types of validation strategies (differing in which part of the network they encompass) can be distinguished:

- (system-)local validation strategies,
- validation strategies concerning only parts of the coalition,
- and coalition-wide validation strategies.

In a *(system-)local validation strategy*, each single CSD storage system validates received products (via synchronization) according to its own set of validation rules. As a consequence, only validated products will be contained in this system, yet, no quality guarantees for the whole CSD network can be given. As an emerging side-effect, a local validation strategy can lead to a product-related partitioning of the CSD network, meaning that certain (considered as invalid according to the rule set of the validation system) products are not being synchronized over the network – and thus not available for certain users (compare the possible consequences as detailed in chapter 3.1).

In a *validation strategy concerning only parts of the coalition*, a single set of validation rules is employed by a subset of the storage systems in a CSD network. Each of these systems (and only these) thus validate in a unified manner. Such a subset can emerge for example from a national validation policy in a coalition, when one sub-segment of the coalition network solely consists of systems owned by this nation. In addition, such a subset can emerge when a larger part of the storage systems is provided by the same vendor, making these systems effectively copies with factory-set identical validation policies. In such a validation strategy, the CSD storage systems in the considered subset will contain only products validated according to the rules common to the subset. For this subset, thus, guarantees regarding the IQ of contained ISR products can be given. On the downside, no quality guarantees concerning the whole coalition can be given. Furthermore, in analogy to local validation strategies, validating only in parts of a coalition can lead to a partitioned CSD network where products being considered as invalid cannot cross over from one part to another. The side-effects at the boundary of the subset, introduced by this validation strategy, on the behavior of the whole CSD network, thus have to be carefully considered and analyzed when the strategy is employed.

Finally, in a ("global") *coalition-wide validation strategy*, a single set of validation rules is used for validation checks in all the storage systems contained in the CSD network of the coalition. Such a set of validation rules thus has to be agreed upon by all the stakeholders and nations participation in the coalition –

or being required by a respective standard (e.g., a STANAG or AEDP). Using a coalition-wide validation strategy, quality guarantees can be given for all the ISR products in the CSD network, and since all the contained storage systems are required to validate in the same fashion, no unintended side-effects of this validation behavior are to be expected. This is, however, on the pre-requisite that all validating systems (potentially owned and manufactured by different nations and stakeholders) implement the given validation rules in a consistent and compatible manner. The risk of implementation inconsistencies for validation rules in a coalition can be mitigated by using validation service with a centralized implementation of validation rules, e.g., integrated into the JISR workflow service stack.

3.3.2 Validation at the boundary of the CSD Network

Besides validation strategies within the CSD network, another import (design) aspect of product validation in a Joint ISR coalition is at which systems (at the boundary of the CSD network) validation checks are to be implemented: at CSD storage systems, further upstream in the product creation process at CSD clients or even at the beginning of the process in respective creation tools. These systems are depicted in Figure 4. Depending on the system performing product validation, different options for how to handle invalid products exist.

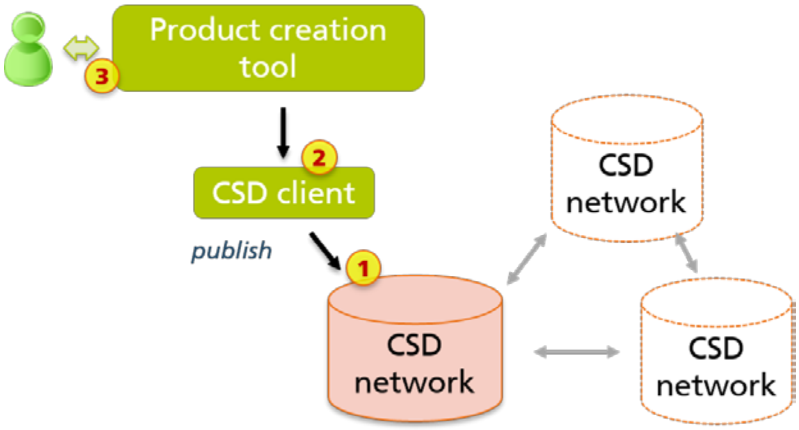

Figure 4: Locations for Validation at the Boundary of a CSD Network

The easiest way of handling invalid products is given in product creation tools, whereas in CSD clients and in CSD storage systems, this gets more and more complicated. If products are validated as early as during their creation, options such as (semi-)automated corrective measures and suggestions for improvement to the users creating the products are viable. In turn, since it can be expected that a user performs corrections to invalid products, a validation check in a product creation tool may prohibit a user from publishing invalid products – thus ensuring that only valid products can be entered into the CSD network. If validation is first performed further downstream in a CSD client, the technical capability for editing the (invalid) details of the product might not be given anymore (e.g., this could only be possible in the creation tool). Thus, is becomes more complicated (or even impossible) to implement corrections to the invalid product, in general, in a CSD client. Because of this, prohibiting the publication of invalid products at CSD clients may (at least) cause delays in the dissemination of products. Depending on the scenario in which the CSD network is employed for disseminating ISR, this can have serious consequences on decision making. Thus, an approach alternative to prohibiting the publication of invalid products has to be considered.

This line of reasoning also applies, even to its full extent, if product validation is performed at CSD storage systems (i.e., at the boundary of a CSD network). Here, it cannot be safely assumed that corrections to invalid products can be implemented (by users). Prohibiting the publication of an invalid product thus is equal to discarding the product (and all of its contained information). As an alternative option for handling invalid products, a marking of invalid products can be considered. Such quality markings then should consists of different information, including an overall quality rating for the product, a rationale for this rating (indicating e.g. why the product is considered as invalid or which parts are considered invalid) as well as quality ratings for each of the relevant parts of the product. The quality marking then has to be published to the CSD network as well and linked to the invalid (but, in this approach, yet published) ISR product. The approach of using quality markings thus does not enforce IQ in the sense that no invalid products can be contained in a CSD network (and therefore allows the dissemination of information in products with minor quality defects). Yet, it propagates and shifts the responsibility for handling (the information in) invalid products to the users searching for and retrieving ISR products (and the employed CSD clients) – thus enabling these users to handle ISR products according to their assessed IQ.

3.4 Implementing IQM in a Coalition

For implementing IQM in Joint ISR coalitions, different state-of-the-art approaches to IQM can be considered. The approach found to be most suitable for Joint ISR coalitions is known as total (data/information) quality management (TQM) [11], [12]. In TQM, quality management is regarded as an integrated, holistic approach considering the whole process of information production – and not just assuring the quality of completed information products. This also subsumes eliciting the quality requirements on products as desired by the consumers of those products as well as managing the measures implemented to ensures these requirements. In addition, TQM demands that IQ is considered as early as the development process of new information products, thus becoming an integral part of the product. Finally, and, in our case, one of the most important aspects, TQM advocates an incremental implementation of IQ in an enterprise. IQM is seen as a continuous and iterative process building up IQ step by step for different parts of the enterprise (e.g., in each step addressing the IQ of a different information product).

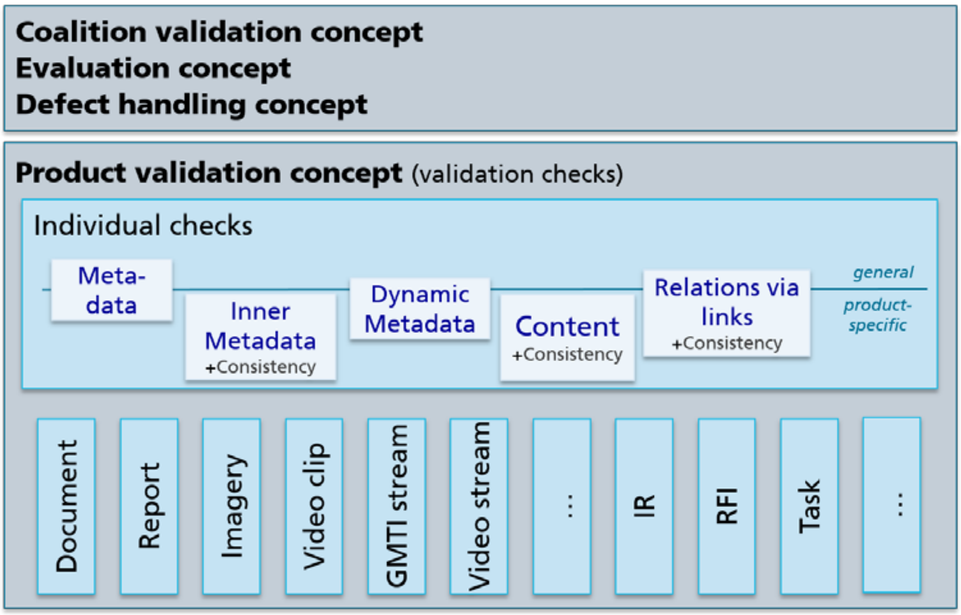

Figure 5: Implementation Map of IQM in a Joint ISR Coalition based on a TMQ Approach

Based on the principles of TQM, the implementation map for IQM in a coalition displayed in Figure 5 was elaborated. For implementing IQM in a coalition, general aspects (depicted in the upper box in the figure) as well as product-specific aspects (listed in the lower box in the figure) have to be considered. General aspects concern a concept for how to perform validation in a coalition (i.e., at what locations in the CSD network and at what systems - compare chapter 3.3), a concept for how to evaluate products in general (detailing what validation checks are to be performed, what the possible outcomes of these checks are, how to aggregate part results to an overall result, etc.) as well as a concept for handling defects (i.e., invalid products, also compare chapter 3.3).

The concept for validating individual products, depicted in the lower box of the figure, also consists of two parts. The individual checks depicted in the upper part can be performed for all or certain groups of CSD products. Checking the metadata of CSD products for completeness and validity can for example be performed for all the products stored in CSD Servers or CSD Streaming Servers. For products in CSD Streaming Servers (e.g., video streams or GMTI streams), also their dynamic metadata (i.e., metadata which is allowed and required to change over time, adapting to product content changing over time) can be checked for completeness and validity. For products being structured according to known standards, which also contain metadata (e.g., imagery or video products), this so-called inner metadata can also be validated. Here, also the consistency of inner metadata values with the values of the outer (CSD) metadata has to be checked. For products being related to other products (e.g., via associations in CSD Servers), also the metadata consistency can be checked, and, if appropriate for the type of product, also the consistency of their content. Finally, the contents of structured products (e.g., formal reports in a CSD Server) can be validated for consistency (inner, to metadata, etc.), completeness and validity of contained values.

4. CONCLUSION

In this paper, we introduced the CSD concept and the new Edition of STANAG 4559 based on process descriptions and requirements from NATO Intelligence and Joint ISR processes. Based on these processes, we identified the need for IQM in a coalition and proposed approaches how to implement IQM.

The processes defined under [2], [4] and related publications are complex and requirements for systems, services, interfaces, workflows, networks, IQ, etc. can be derived from it. In further research, (technical) requirements should be defined in more detail to be able to entirely map those to concepts existing and workflows implemented and subsequently adapt or complete those where necessary

For IQM in a coalition, the implementation map should be used to guide the step-by-step integration of IQ measures into the coalition. Here, first, the general aspects (coalition validation, defect handling in general, etc.) should be addressed, laying the foundation for the later realization of product-specific validation checks, which can then be added one at a time for each type of ISR product.

5. ACKNOWLEDGMENT

The CSD concept is part of the multination projects MAJIIC and MAJIIC 2, the STANAG 4559 CST is supported by multiple nations. The BMVg (Federal Ministry of Defence) has funded the work of Fraunhofer IOSBs work in both aspects. The authors acknowledge valuable help and contributions from all partners of the project and the CST.
The authors would like to thank their colleagues, who have contributed to the work presented in this paper, especially Christian Kerth and Philipp Klotz.

6. REFERENCES

[1] NATO Standardization Office, ALLIED ADMINISTRATIVE PUBLICATION (AAP)-06, NATO GLOSSARY OF TERMS AND DEFINITIONS, (2014)

[2] NATO Standardization Office, AJP 2.1 ALLIED JOINT DOCTRINE FOR INTELLIGENCE PROCEDURES, Edition B Version 1, (2016)

[3] Joint Chiefs of Staff, JOINT PUBLICATION 2-0, JOINT INTELLIGENCE, (2013), http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf (20. April 2018)

[4] NATO Standardization Office, AIntP-14 JOINT INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (JISR) PROCEDURES IN SUPPORT OF NATO OPERATIONS, Edition A Version 1, (2016)

[5] Essendorfer, B., Kerth, C., Zaschke, C., EVOLUTION OF THE COALITION SHARED DATA CONCEPT IN JOINT ISR. *IST/SET-126 Symposium on “Information Fusion (Hard and Soft) for Intelligence, Surveillance & Reconnaissance (ISR)".* (2015)

[6] NATO Standardization Office, STANAG 4559 EDITION 4, (2018)

[7] NATO Standardization Office, NATO STANDARD ISR LIBRARY INTERFACES AND SERVICES - AEDP-17 Edition A. (2018), http://nso.nato.int/nso/nsdd/apdetails.html?APNo=2272 (16. April 2018)

[8] NATO Standardization Office, NATO STANDARD ISR LIBRARY INTERFACES AND SERVICES - AEDP-18 Edition A. (2018), http://nso.nato.int/nso/nsdd/apdetails.html?APNo=2273 (16. April 2018)

[9] NATO Standardization Office, NATO STANDARD ISR LIBRARY INTERFACES AND SERVICES - AEDP-19 Edition A. (2018), http://nso.nato.int/nso/nsdd/apdetails.html?APNo=2274 (16. April 2018)

[10] OASIS, WEB SERVICES SECURITY (WSS) TC, (2006), https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss (24.April 2018)

[11] English, L. P., TOTAL INFORMATION QUALITY MANAGEMENT: A COMPLETE METHODOLOGY FOR IQ MANAGEMENT. *DM Review, vol. 9, no. 1-7. (2003)*

[12] Wang, R. Y., A PRODUCT PERSPECTIVE ON TOTAL DATA QUALITY MANAGEMENT. *Communications of the ACM, vol. 41, no. 2, pp. 59–65. (1998)*