Formal Reporting for Information Exploitation and Dissemination in Joint ISR

Jennifer Sander, Barbara Essendorfer, Sergius Dyck, and Uwe Pfirrmann

Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Fraunhoferstraße 1, 76131 Karlsruhe, Germany

ABSTRACT

In complex operational scenarios where multiple nations and forces cooperate, flexible System of Systems (SoS) architectures being customizable to specific operations are needed. Relevant operational processes as defined within Joint ISR (Intelligence, Surveillance and Reconnaissance) and the Intelligence Cycle need to be supported. To maximize efficiency and effectiveness of Joint ISR capabilities, each Joint ISR result needs to answer the corresponding information requirement accurately. Commanders must receive the relevant information in a condensed, well-prepared manner instead of being overflowed with large amounts of (raw) data. Ensuring a common understanding of each exchanged piece of information within the defence coalition is also of utmost importance. Architectures supporting these requirements need to make use of relevant standards and agreements for data/ information management. As reports may be provided by all Joint ISR capabilities, the topic of reporting is of high importance, here. Within the described context, our publication deals with formal reporting which can be defined as organizational process at which relevant information is provided as formal reports, i.e., as documents being structured according to pre-defined (agreed) rules. We present means for ensuring allied interoperability and further (semi-)automatic processability of the information being contained in formal reports by technical means and under consideration of the relevant doctrines and standards. We also address specific means needed to ensure the creation of formal reports of high quality. Finally, we discuss current issues and new requirements on formal reporting which have to be still addressed in the field of Joint ISR.

Keywords: Joint ISR, formal reporting, interoperability, defence coalitions, STANAGs, workflows, information processing

1. INTRODUCTION

Budget restrictions combined with the fact that, today, often not single nations but whole areas are subject to attacks demand cooperation between national organizations and even force nations to collaborate. Also in light of the increasing complexity and diversity of today's threats, commanders and other decision makers need increased situational awareness. Initiating the right reactions and deciding on the best course-of-action becomes more and more a question of working together with maximum efficiency and effectiveness at collecting, analyzing and sharing data/ information and at creating intelligence[*] from it. To this aim, flexible means to collaborate and to share capabilities as well as resulting data/ information are needed. This holds with regard to the same and between various command levels. More efficient data and information management can be achieved additionally if the participating actors have common processes and a common understanding of their overall goals.

In NATO operations, where different military forces cooperate within a coalition, data/ information and intelligence, respectively, are passed on through the Joint ISR (Intelligence, Surveillance and Reconnaissance)

Further author information: (Send correspondence to Jennifer Sander)
Jennifer Sander: E-mail: jennifer.sander@iosb.fraunhofer.de, Telephone: +49 721 6091-546
Barbara Essendorfer: E-mail: barbara.essendorfer@iosb.fraunhofer.de, Telephone: +49 721 6091-596
Sergius Dyck: E-mail: sergius.dyck@iosb.fraunhofer.de, Telephone: +49 721 6091-465
Uwe Pfirrmann: E-mail: uwe.pfirrmann@iosb.fraunhofer.de, Telephone: +49 721 6091-588

[*]In NATO, intelligence (INTEL) is defined as "product resulting from the directed collection and processing of information regarding the environment and the capabilities and intentions of actors, in order to identify threats and offer opportunities for exploitation by decision-makers."[1]

process and the Intelligence Cycle. In this context, our publication deals with formal reporting at which relevant findings are provided (digitally) as (textual) documents being structured according to pre-defined (agreed) rules. Formal reporting is essential to support an adequate data and and information management for Joint ISR.

In the next section, central aspects with regard to data and information management for Joint ISR are introduced. First, in Sec. 2.1, the relevant operational processes are sketched and central aspects regarding corresponding information needs are briefly described. In addition, in Sec. 2.2, the topic of interoperability which is a key aspect with regard to adequate data and information management in the considered context is addressed in more detail. In Sec. 3, formal reporting is introduced and considered in-depth with regard to different aspects. Subsequent to the introduction of central terms, it is discussed in Sec. 3.1 how formal reporting supports Joint ISR in terms of adequate data/ information management. In Sec. 3.2, selected standards and agreements being relevant for formal reporting are introduced exemplarily and the connections between them are outlined. Sec. 3.3 and Sec. 3.4 asses how formal reporting can be supported by adequate tools and workflows and introduce appropriate solutions being usable also in an operational context. While Sec. 3 mainly deals with the current state of formal reporting, Sec. 4 focuses rather on aspects to be considered with regard to a future-oriented concept for formal reporting. This is done by addressing current issues with regard to relevant standards and agreements in Sec. 4.1 and by summarizing additional new requirements for formal reporting which have to be still addressed in the field of Joint ISR in Sec. 4.2. Finally, in Sec. 5, a short conclusion is given.

2. ASPECTS OF DATA AND INFORMATION MANAGEMENT FOR JOINT ISR

2.1 Operational Environment

In NATO operations, intelligence is produced and made available through the management of capabilities (assets and actors) within the intelligence cycle.[1,2] The intelligence cycle constitutes a coordinated sequence of activities comprising different dedicated phases which can be divided in "Planning and Direction", "Collection", "Processing", "Analysis and Production", and "Dissemination". As illustrated in Fig. 1, the intelligence cycle is closely linked to the Joint ISR process[†].

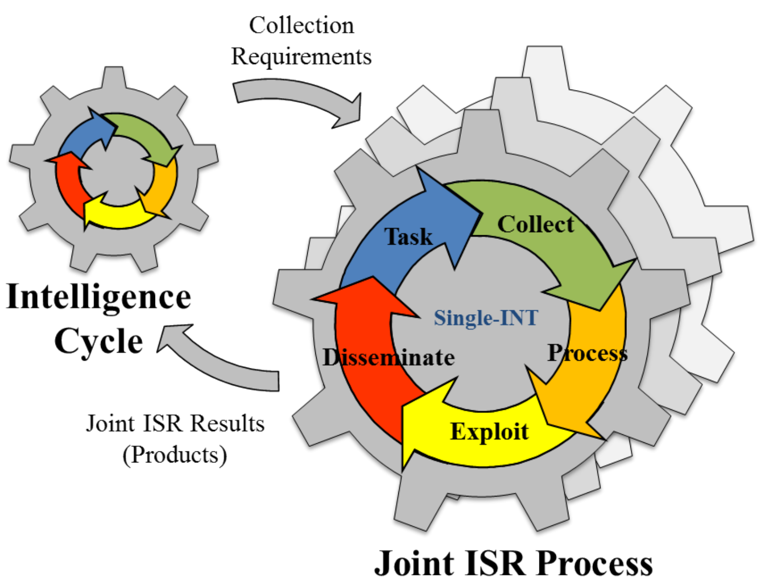

Figure 1. Illustration of the Joint ISR process and its connection to the intelligence cycle.

[†]As described for example in Ref. 3, the Joint ISR process can support both, current operational requirements as well as the production of (finished) intelligence within the intelligence cycle. In this publication, we focus on the second aspect.

Via the Joint ISR process, (single) information requirements, corresponding to relevant questions, shall be satisfied by Joint ISR capabilities in a synchronized and integrated manner.[3] More precisely, the Joint ISR process starts with a (validated) collection requirement which has to be answered adequately via Joint ISR results. The Joint ISR results are derived from single source/ single intelligence disciplines[‡] like Imagery Intelligence (IMINT), Open Source Intelligence (OSINT), Human Intelligence (HUMINT). They are created via the Joint ISR process on basis of five steps which are "Task", "Collect", "Process", "Exploit", and "Disseminate" (TCPED) and finally fed back in the intelligence cycle for the creation of (finished) intelligence via multi source/ multi intelligence fusion and analysis. In total, the Joint ISR process constitutes a complex framework comprising multiple roles and loops and involving different units, systems and tools. In Fig. 1, this complexity is illustrated graphically via the overlaying cogwheels on the right side.

During the different phases of the described operational processes, multiple data and information elements are created, processed, combined, and disseminated. To ensure that thereby "all cogwheels mesh optimally", the right data/ information has to be passed appropriately to the right addressee (actor or system) at the right time. This implies a number of requirements in terms of data and information management.[2] Of particular importance is to ensure that all data/ information elements are accurate, reliable, and interpretable independently of the individual involved units, systems, and tools on basis of a common understanding. To avoid information overflow and losing the sight of what is really important, relevant findings must be also provided in a condensed, demand-oriented manner to the systems and/ or actors requesting them. Interoperability and the provision of JISR results on basis of standard (agreed) formats are key aspects, here.

2.2 Interoperability

According to the definition given in Ref. 5 (which is derived from the definition given in Ref. 6), interoperability is understood as "the ability of systems, organizations or discrete parts of the same organization to provide metadata and information to and accept metadata and information from other systems, organizations or discrete parts of the same organization, and to use the metadata and information so exchanged to enable them to operate effectively together". Attaining interoperability requires the consideration of different aspects which are of both, technical and organizational nature.

A common scheme[§] for capturing different forms of interoperability on basis of a rather coarse distinction is illustrated in Fig. 2. In this scheme, interoperability is divided into four levels: level 1 – data interoperability (also called technical interoperability), level 2 – syntactic interoperability, level 3 – semantic interoperability, level 4 – pragmatic interoperability. Data interoperability deals with the physical networking of systems and the protocol level and enables basic data exchange between participating systems. Syntactic interoperability addresses aspects with regard to the grammar and formal rules underlying the respective data definitions. In this sense, it deals with the structure of a corresponding data model. Semantic interoperability addresses the meaning and the use of the data. It enables a common understanding of the exchanged contents on basis of a common language, i.e., it enables different parties to understand exchanged contents in the same way and without ambiguities. Hence, on the level of semantic interoperability, data becomes information.[8] Pragmatic interoperability addresses a uniform assessment of information with respect to consequences and decisions on basis of agreed procedures, operations, strategies and doctrines as well as high level objectives. The nested depiction in Fig. 2 is used in order to emphasize that, in general, reaching a certain interoperability level requires also reaching the corresponding lower interoperability levels as prerequisite.

To ensure the necessary levels of interoperability within a networked environment, architectures being both, flexible and capable of supporting the relevant operational processes, are needed. Respective architectural approaches need to take relevant standards and agreements into account and have to bring them together consistently.[9] Of central relevance with regard to ISR interoperability in the military domain is the NATO ISR Interoperability Architecture (NIIA) which outlines a top-level architecture for NATO and national reconnaissance and surveillance assets. The current release of the NIIA's architecture description,[3] which has been updated in 2018, points out the key role of the paradigm of service orientation for future operations. The basic idea behind the NIIA is that a system produces output and translates it into a standardized format that any other system/

‡For more detailed information on military intelligence disciplines, the reader is referred for example to Ref. 4.

§Compare for example Ref. 5 and Ref. 7.

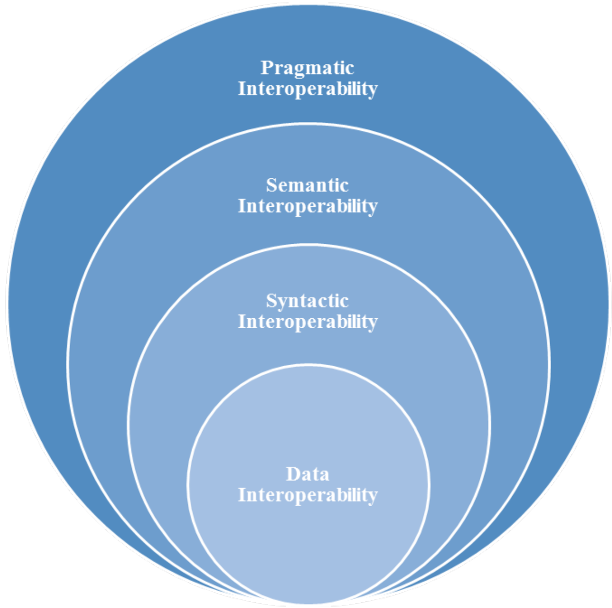

Figure 2. Interoperability levels.

service knowing that standard can ingest and process. An important aspect is that the NIIA considers not only the data and ISR products themselves but also metadata. Even more, it points out that appropriate metadata should accompany all ISR data and products to enable adequate data and information management in Joint ISR and addresses key aspects also with this regard.

The term metadata is literally defined as "data about data", which is a very broad definition. Metadata can capture both, synthactic and semantic information about data/ information elements. It is important to note that this has to be done in a structured manner and under consideration of semantics at least for aspects where the metadata have to be interpreted actually as (meta)information. To get a clearer conception, it is advisable to categorize metadata into different types with the categorization reflecting fundamental aspects regarding their intended functionality.[10–12] According to the architecture description of the NIIA, in Joint ISR, metadata should support/ enhance "Confidentiality and releasability marking", "Dissemination, Archival, Search and Retrieval (DSAR)", and "Processing, Exploitation, and Dissemination (PED), including geospatial refinement". In Joint ISR, multiple metadata standards exists across different ISR standards which are formulated as NATO STANAGs (NATO STANdardization AGreements). When using the metadata standards being contained in the different STANAGs in combination, such as foreseen by the NIIA, the topic of metadata harmonization which can be understood (according to Ref. 13) as "interoperability in the presence of multiple metadata standards" and which goes beyond the interoperability of metadata per se, becomes also relevant.

3. FORMAL REPORTING

3.1 What and Why

Coarsely spoken, a (military) report comprises an amount of findings, i.e., ISR information or intelligence being considered as relevant with regard to the (military) situation picture. Overall, formal reporting constitutes an organizational process at which these findings are captured (digitally) as structured reports which are passed to the respective requester.

A (textual) formal report is a document being structured according to pre-defined rules, which assign a specific structure and form to it. This means that formal reports constitute data/ information with a pre-defined data model. In contrast to that, reports being represented by the use of e-mails, office documents (e.g., Word documents, Power-Point presentations) or PDF files do not constitute such kinds of structured data/

information. Technically, formal reports are often represented as XML (eXtensible Markup Language) documents being structured according to a certain XML scheme which has been agreed beforehand.[7,14]

Formal reporting is essential for the fulfillment of central requirements with regard to data and information management in Joint ISR. Being based on a pre-defined data model, it supports interoperability on the syntactic level substantially. In addition, it provides a sound basis for semantic interoperability, i.e., the establishment of a common understanding of the findings being contained in the reports. This holds with regard to both, comprehension of the findings by human readers as well as further automated processing. In particular, as formal reports can be processed automatically by workstations, formal reporting supports a continuous automatic processing chain – without the need for swivel chair interfaces. Semantic interoperability can be further supported by the incorporation of a semantic information model specifying concepts relevant to the considered scenarios and the respective findings which may be comprised in the formal reports.[14]

The specific structure of formal reports supports the accurate and complete acquisition of the findings being contained in the reports and enables targeted access to the report contents. Together with a common semantics, relevant information can easily and correctly be located and extracted for further purposes.[15]

At formal reporting, metadata can get incorporated into the formal reports themselves which is very favorable with regard to data and information management, especially also with regard to accompanying data/ information quality management[¶]. Incorporating the metadata into the formal reports themselves can avoid inconsistencies between the reports and the metadata. In addition, it is ensured that relevant information being encoded in the metadata (e.g., security markings like classification, policy, releasability) won't get lost when the reports are used (e.g., when they are downloaded from a repository). The specific structure of formal reports also offers significant possibilities for (semi-)automatic quality assessment and quality control, respectively, on basis of formal test procedures and test cases, which are automatically processable and/ or have to be performed by a human following a given test instruction[‖].

It should be noted that the metadata set of formal reports should contain all metadata which are required for their handling within the Joint ISR process. For example, as formal reports may be disseminated via a CSD (Coalition Shared Data) server according to STANAG 4559[16]/ AEDP-17 (Allied Engineering Documentation Publication 17),[17] they should contain at least the mandatory CSD metadata in a consistent manner. Additional appropriate report specific metadata can get included to enable searching, filtering, and sorting the reports according to certain (additional) criteria – which may be essential to provide the findings being contained in the reports sufficiently timely and completely.

At least from a technical point of view, it is rather unproblematic to fill structured parts of formal reports automatically. This can be done for example by mapping values of metadata being also contained in the metadata sets of exploited products (e.g., images according to STANAG 4545) to respective metadata fields of the formal reports. Another example was to automatically insert pre-configured values (e.g., exercise name) in certain fields of formal reports.

3.2 Selected Standards and Agreements

In this section, selected standards and agreements being relevant for formal reporting are introduced exemplarily and the connections between them are outlined. It should be noted that the standards and agreements introduced in the following are not the only ones and that they are also related to diverse other standards and agreements.

STANAG 3377 - Air Reconnaissance Intelligence Report Forms.[18] The purpose of STANAG 3377 is the standardization of reports in sensor-based air reconnaissance. It describes a set of report formats that contain evaluation results of data determined during reconnaissance missions with image-based sensors, whereby the missions are requested by authorized agencies and the results of these missions are sent back to the tasking agency in form of these operational exploitation reports.

[¶] For further details on the topic of data/ information quality management in Joint ISR, the reader is referred to Ref. 2.

[‖] As part of the research activities of Fraunhofer IOSB with regard to formal reporting, a prototypical tool providing respective functionalities has been worked out. The tool has been tested successfully in interoperability exercises, in the sense that it supported quality improvement of formal reports, actually.

The spectrum of STANAG 3377 comprises a total of six reporting formats, starting with time-critical information, which must still be submitted during the flight of the sensor platform, via detailed interpretation formats to special formats for the evaluation of radar images. In particular, STANAG 3377 specifies the format of the results of the interpretation. However, it only describes a structured text, but does not specify a formal report definition in the sense of an exact syntactic structure, such as can be specified by an abstract language. Some of the report formats refer to STANAG 3596, which defines the structure and partly also the value set of the results.

STANAG 3596 - Air Reconnaissance Requesting and Target Reporting Guide.[19] STANAG 3596 serves as a reference for requesting, planning and reporting of intelligence in the field of air reconnaissance.[3] It holds a total of 19 target categories, which are described in a tree-like structure by a uniform set of characteristics or Essential Elements of Information (EEI). Along with these target categories, STANAG 3596 specifies a terminology with which the purpose of a report in the areas new targets, change detection, planning, and damage assessment can be declared, and the EEIs to be reported can be determined by the tasking agency. By the definition of terms and characteristics for objects relevant for reconnaissance, STANAG 3596 is referenced by several other STANAGs and agreements, in order to structure their evaluation results and to establish specific sets of allowed values. Examples are STANAG 3377, report specifications according to MAJIIC 2 Baseline Bravo.1, and APP-11. It is likely that the content of STANAG 3596 will be merged with the content of STANAG 3920[20] in order to reduce the number of reporting relevant standards and agreements and thereby simplify reporting regulations and processes.[3]

MAJIIC 2 Baseline Bravo.1. In the multination projects MAJIIC[**] and MAJIIC 2[††] several report formats have been specified in a formal way using XML schema definitions. Among them are report formats that have been described in various STANAGs simply as structured text (e.g., the RECCEXREP according to STANAG 3377) as well as report formats that have been completely generated newly for specific purposes and sensors. Since an unambiguous interpretation and a high degree of interoperability and automatic processing are essential in the field of sensor-based reconnaissance, a report should be subject to strict regulations concerning structure and wording. MAJIIC 2 meets this challenge by specifying formal reports (as they are defined in Sec. 3.1) which is done via well-defined XML schemes. By definition, all report formats specified in this way by MAJIIC 2 include the metadata which are necessary to be conform to STANAG 4559/ AEDP-17, and thus to be able to insert a report into a CSD server[‡‡]. It needs to be borne in mind that the MAJIIC 2 XML schemes are not covered by any of the current reporting standards.

STANAG 7149 - APP-11 NATO Message Catalogue.[21] APP-11 (Allied Procedural Publication 11) specifies a catalog of Message Text Formats (MTFs) for the exchange of character-oriented messages.[7] The format of these messages is based on the standard ADatP-3 (Allied Data Publication 3), which defines the structure and rules for their structure.[7] In the first few years, the MTFs were defined by a structured, but textual description, since 2008 (APP-11(C), Baseline 13.1), their specification is based on XML schemes. The XML schemes are included along with the MTFs in the APP-11 Message Catalogue. Since this baseline, messages can not only be represented in their original format as tightly packed, structured text, e.g., when the transmission capacity is limited by a small bandwidth, but in form of XML documents. The current version of APP-11 contains over 400 message text formats. It is intended by the NSO (NATO Standardization Office) to migrate message formats from other Allied Publications to APP-11.[3]

3.3 Tool Support

There is a significant number of standards, agreements and directives being directly and indirectly applicable to reporting. Amongst other things, they describe which fields a formal report must contain, which of them are

[**] Multi-sensor Aerospace-ground Joint ISR Interoperability Coalition.

[††] Multi-intelligence All source Joint ISR Interoperability Coalition.

[‡‡] Inserting a report of a certain type in a CSD server according to STANAG 4559/ AEDP-17 further requires that the corresponding report type is available in the CSD data model. If this it not the case, this can basically be implemented by its additional inclusion in the standard or by a (e.g., national or operation specific) CSD data model extension as foreseen newly in STANAG 4559 (Edition 4). The report types whose technical formats have been specified by MAJIIC 2 via XML schemes as described are available in the CSD data model.

mandatory/ optional, which values are allowed for certain fields and how report contents have to be structured according to specific formats. Also, there may be further operational requirements that have to be respected by the reporter (e.g., being contained in SOPs (Standard Operating Procedures)).

Tool support of the reporter is essential in order to support compliance with these numerous regulations and specifications and to support him in producing correct and high-quality reports in the shortest possible time. Even if the focus of such tools may be on supporting the reporter, such a tool also has advantages for the requestor of the respective findings. Amongst other things, it can help that the requestor receives the findings in a unified form and in a shorter time. At least to a certain extent, such a tool can also perform quality control of the report contents and metadata, e.g., by validating entries into certain fields against an underlying scheme. In this sense and furthermore, such a tool can contribute to information quality management and support compliance with existing standards and agreements. Another example for a respective functionality was marking mandatory fields and enforcing that they get filled by the reporter.

In addition, by such a tool, the reporter can be supported with regard to usability aspects. For example, when he enters information, the tool may propose him the valid values (and only these values) for particular report fields, such that he can select the appropriate value comfortably. Incorrect entries (e.g., when a entered value is outside the range of values being allowed for the respective field) may be identified automatically by the tool such that the user can be notified to correct it. Also, the reporter can be supported in having certain information elements filled automatically. For example, mission data being specified in the corresponding task can get transferred automatically into the report without the reporter being required to do this manually and certain report fields can get filled automatically with pre-configured (e.g., mission specific) values. Another example was that such a tool could provide the opportunity to create and to use templates for fast report preparation. Finally, such a tool can support the dissemination of reports by interfacing with corresponding dissemination systems. A concrete example is that it could support the ingest into a CSD server according to STANAG 4559/ AEDP-17.

A concrete example for such a tool is i2exrep (interactive ISR exploitation report) by Fraunhofer IOSB, an interactive application for generating, editing and disseminating formal reports. Amongst others, the i2exrep provides the functionalities which have been described above. It has been developed by Fraunhofer IOSB in a company internal research project and, on the basis of subsequent research projects, it has been continuously improved and enhanced to meet operational requirements and to consider the change of the requirements situation of the armed forces. The i2exrep has been also used and tested in different external research projects like MAJIIC and MAJIIC 2. Also, the software has been delivered for operational use to the German Armed Forces and within the NATO context. Particularly developed with regard to the military reconnaissance and surveillance process, i2exrep is, in principle, also applicable in civil domains (e.g., to support emergency management, police, medical science). Worthwhile emphasizing is also that the tool actively supports the STANAG 3596 target categories (by allowing their presentation, navigating in them, and transferring respective information into certain report formats).

3.4 Support by the Use of Workflows

Guiding, controlling and supporting the process of creation, processing and validation of formal reports via the specification of a reporting workflow substantially contributes to the improvement of information quality. The term workflow comes from the field of organizational theory. In short, a workflow[22] is an orchestrated sequence of related activities in which the participating resources (usually specified as roles) are integrated into the processes by a systematic organization.

Ideally, a workflow is represented in a BPMN (Business Process Model and Notation) diagram. BPMN is a graphical specification language used to illustrate processes and workflows with multiple and different roles, activities, and artifacts in a vivid manner.

Fig. 3 shows a reporting workflow that has been worked out by Fraunhofer IOSB. In order to improve information quality, this workflow introduces, in addition to the reporter that creates, edits and processes reports, a superior control instance being responsible for verifying, accepting, rejecting and publishing reports. That means that, after the completion of the report, it is not published by the reporter himself, but first passed on to the control authority for review. This authority checks the report, and only if the result is positive, the report is published. Otherwise the report is sent back to the reporter for correction.

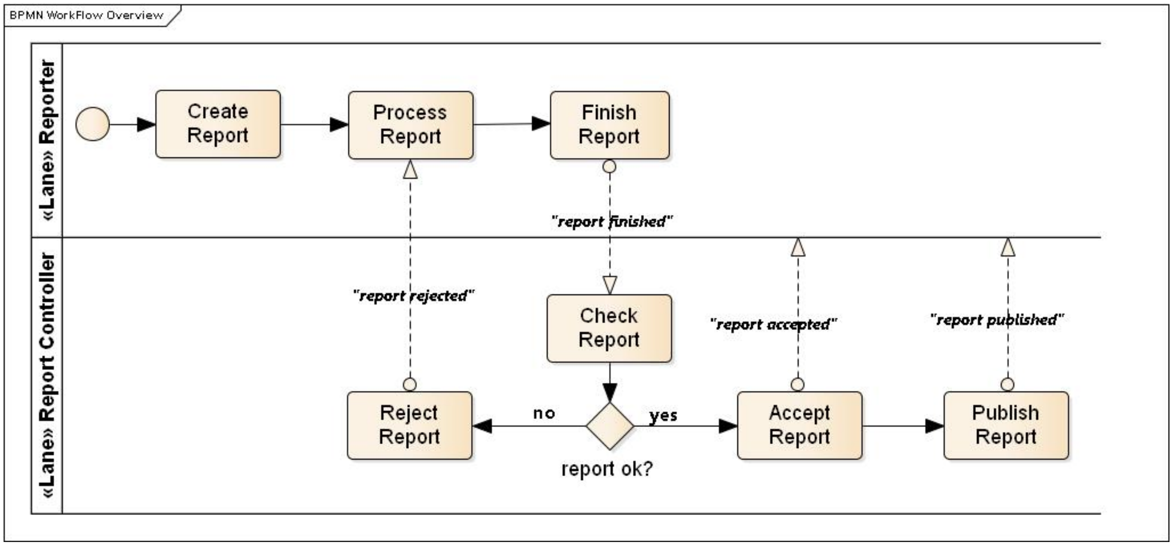

Figure 3. Reporting workflow as role-based user management with two participants (reporter and report controller).

The proposed workflow has been implemented prototypically as service and evaluated by several reporters during a technical interoperability exercise in the context of the MAJIIC 2 project. The assessments were consistently positive. By introducing a superior controlling authority, the workflow was rated as extremely useful in an operational sense. It improves the process of reporting in terms of simplification of work, timeliness and trust in the product created by the reporter.

4. CURRENT ISSUES

4.1 Standards and Agreements

Standards and agreements must be regularly adapted to changing operational parameters and requirements. In addition, they must be sufficiently precise and unambiguous. This is not always the case at the present for the standards and agreements being relevant for reporting.

These standards and agreements are in some cases outdated and not conform to current operational requirements, e.g., with regard to the nature of today's conflicts, to the possibilities modern technologies offer. Some STANAGs refer to other STANAGs that have already been canceled and/ or updated such that they are no longer consistent and/ or complete. Also, some report formats, e.g., RECCEXREP, are (under the same name) defined differently in different standards and agreements which can lead to confusion and interoperability issues at both, the technical and the process level. The current version of the NIIA's architecture description[3] illustrates some of these issues.

Meanwhile, diverse activities in respective NATO panels aim at solving the described issues. Relevant STANAGs are to be updated and consolidated. In the course of this revision, it should be also ensured that report formats are described unambiguously (and standardized) via precise technical definitions for example on the basis of XML schemes. An essential point is also that the total set of relevant standards and agreements should be consolidated in a manner such that it will be maintainable in the future. Where possible, updates of relevant standards and agreements should also address the fact that the current versions of them are often interoperable (only) at a syntactical level, neglecting semantic interoperability.

In order to support the flow of Joint ISR data/ information through the relevant operational processes (as they have been sketched in Sec. 2.1) adequately, it is also important to ensure that necessary dependencies between all Joint ISR relevant standards are maintained carefully and regularly. This means that, also with regard to this larger framework, potential inconsistencies, gaps, and ambiguities have to be addressed which may require coordination and possible also cooperation between the relevant stakeholders. A good example for a concrete issue to be seen in this context is the following one: the dissemination of Joint ISR products via a CSD server is based on STANAG 4559/ AEDP-17 and connected STANAGs, process descriptions and doctrines. The CSD data model includes report types that refer to the MAJIIC 2 XML schemes (as described in Sec. 3.2) which is an implicit link to them. The MAJIIC 2 XML schemes are not covered by any of the current reporting standards, however. Overall, important aspects that should be addressed also with regard to the described larger framework are of course interoperability issues between different STANAGs and especially also the topic of metadata harmonization (compare Sec. 2.2).

4.2 Additional Requirements

In this section, some additional requirements with regard to a substitutable future-oriented concept for formal reporting are sketched. The described aspects may be addressed in more detail in a subsequent publication.

Feedback obtained from operational users indicates that the current possibilities for preparing the contents of formal reports via demand-oriented and vivid depictions are insufficient such that, to this aim, new means are needed. In addition, it seems to be necessary to reduce the complexity of formal reporting (which is perceived to be high) for both, reporter and requester also with regard to other aspects. To this aim, in a first step, the usability of existing processes and tools should be evaluated in a structured manner.

Software tools supporting tasking, exploitation, and reporting should be interconnected as comprehensively as possible and under consideration of the relevant operational processes. Another aspect with this regard is that existing workflows, such as the concrete reporting workflow which has been described in Sec. 3.4, should be extended, e.g., to more comprehensive exploitation workflows.

A fundamental building block with regard to a substitutable future-oriented concept for formal reporting will be also the thoughtful integration of new technologies and research results. For example, as chat like functionalities are widely in use and, in a sense, predestinated for fast information exchange, using them for (formal) reporting may be promising. While the conceptualization and implementation of corresponding means may be realizable rather in the short to medium term, the realization of other promising possibilities may require some basic research work as pre-requisite. A concrete example for that was the incorporation of concepts and methods from the field of artificial intelligence for formal reporting, e.g., to increase its usability and flexibility.

5. CONCLUSION

Formal reporting, at which relevant findings are provided (digitally) as (textual) documents being structured according to pre-defined (agreed) rules, is essential to support an adequate data and information management for Joint ISR. In this publication, formal reporting has been considered with regard to different aspects, taking also into account the relevant operational processes and corresponding information needs. In the considered context, interoperability and the provision of JISR results on basis of standard (agreed) formats are key aspects.

With these considerations in mind, we introduced formal reporting and described how it can support Joint ISR in terms of adequate data and information management. We outlined and discussed several current standards and agreements being relevant for formal reporting and described how formal reporting can be supported by adequate tools and workflows – especially also with the aim of creating formal reports of high quality. Concrete approaches and solutions worked out by Fraunhofer IOSB in different research project have been presented.

Our publication points out that, currently, there exist different issues and new requirements on formal reporting which have to be still addressed. Various reporting relevant standards and agreements have to be updated and consolidated. In doing so, also their maintainability has to get improved (e.g., by reducing the number of different documents). In addition, it is also important to ensure that necessary dependencies between all Joint ISR relevant standards and agreements are maintained carefully and regularly which imposes additional requirements for the stakeholders being responsible for the respective standards and agreements.

Beyond that, a substitutable future-oriented concept for formal reporting needs to consider additionally also different technological and research aspects. This holds as new approaches and operational solutions are needed in order to comply adequately with additional/ new requirements. In support of this, in particular, promising technological and scientific developments should be examined to ascertain whether/ how they can be used for improving means and processes with regard to formal reporting.

ACKNOWLEDGMENTS

Parts of the work of the authors being presented in this publication has been funded by the BMVg (Federal Ministry of Defence). The authors are responsible for the content of this article.

The authors would like to thank their colleagues, who have contributed to the work presented in this publication, especially Achim Kuwertz.

REFERENCES

[1] NATO Standardization Office (NSO), "ALLIED ADMINISTRATIVE PUBLICATION (AAP)-06, NATO GLOSSARY OF TERMS AND DEFINITIONS," (2018).

[2] Essendorfer, B., Kuwertz, A., and Sander, J., "Distributed Information Management through Coalition Shared Data," in [*NATO STO-MP-IST-160 Big Data and Artificial Intelligence for Military Decision Making*], (2018).

[3] NATO Standardization Office (NSO), "NATO INTELLIGENCE, SURVEILLANCE AND RECONNAISSANCE (ISR) INTEROPERABILITY ARCHITECTURE (NIIA) - VOLUME I: ARCHITECTURE DESCRIPTION, Edition B, Version 1," (2018).

[4] Das, S. K., [*High-Level Data Fusion*], Artech House (2008).

[5] Zaschke, C., Essendorfer, B., and Kerth, C., "Interoperability of heterogeneous distributed systems," in [*Proceedings of SPIE 9825*], (2016).

[6] Hura, M., McLeod, G. W., Larson, E. V., Schneider, J., Gonzales, D., Norton, D. M., Jacobs, J., O'Connell, K. M., Little, W., Mesic, R., and Jamison, L., [*Interoperability: A Continuing Challenge in Coalition Air Operations*], RAND (2000).

[7] Wunder, M. and Grosche, J., [*Verteilte Führungsinformationssysteme*], Springer (2009).

[8] Kubicek, H., Ralf, C., and Jochen, S. H., [*Organizational Interoperability in E-Government*], Springer (2011).

[9] Kuwertz, A., Sander, J., Schneider, G., and Essendorfer, B., "An Architectural Framework for ISR Analytics," in [*NATO Symposium on Architecture Assessment for NEC (SCI-254), Systems Concepts and Integration Panel, Tallinn, Estonia*], (2013).

[10] Riley, J., [*Understanding Metadata: What is Metadata, and What is it For? A Primer Publication of the National Information Standards Organization.*], National Information Standards Organization (NISO) (2017).

[11] Baca, M., [*Introduction to Metadata: Third Edition*], J. Paul Getty Trust (2016).

[12] Hlava, M., [*The Taxobook: Principles and Practices of Building Taxonomies, Part 2 of a 3-Part Series*], Synthesis Lectures on Information Concepts, Retrieval, and Services, Morgan & Claypool Publishers (2014).

[13] Nilsson, M., *From Interoperability to Harmonization in Metadata Standardization: Designing an Evolvable Framework for Metadata Harmonization*, PhD thesis, KTH, School of Computer Science and Communication (CSC), Media Technology and Graphic Arts, Media, Stockholm (2010).

[14] Kuwertz, A., Sander, J., Pfirrmann, U., and Dyck, S., "High-Level information management in Joint ISR based on an object-oriented approach," in [*2017 Sensor Data Fusion: Trends, Solutions, Applications (SDF)*], IEEE (2017).

[15] Kuwertz, A., Mühlenberg, D., Sander, J., and Müller, W., "Applying Knowledge-Based Reasoning for Information Fusion in Intelligence, Surveillance, and Reconnaissance," in [*Multisensor Fusion and Integration in the Wake of Big Data, Deep Learning and Cyber Physical System. MFI 2017. Lecture Notes in Electrical Engineering, vol. 501*], Lee, S. and Ko, H.and Oh, S., eds., Springer (2018).

[16] NATO Standardization Office (NSO), "STANAG 4559, Edition 4," (2018).

[17] NATO Standardization Office (NSO), "NATO STANDARD ISR LIBRARY INTERFACES AND SERVICES - AEDP-17, Edition A," (2018).

[18] NATO Standardization Agency (NSA), "STANAG 3596 - AIR RECONNAISSANCE REQUESTING AND TARGET REPORTING GUIDE, Edition 6," (2007).

[19] NATO Standardization Agency (NSA), "STANAG 3377 - AIR RECONNAISSANCE INTELLIGENCE REPORT FORMS, Edition 6," (2002).

[20] NATO Standardization Agency (NSA), "STANAG 3920 - HANDBOOK FOR AIR RECONNAISSANCE TASKING AND REPORTING - ATP-47(A), Edition 4," (2004).

[21] NATO Standardization Agency (NSA), "APP-11(C) - NATO MESSAGE CATALOGUE," (2009).

[22] Belhajjame, K., Vargas-Solar, G., and Collet, C., "A flexible workflow model for process-oriented applications," in [*Proceedings of the Second International Conference on Web Information Systems Engineering (WISE)*], IEEE (2001).