High-Level Information Management in Joint ISR based on an Object-Oriented Approach

Achim Kuwertz, Jennifer Sander, Uwe Pfirrmann, Sergius Dyck
Fraunhofer Institute of Optronics, System Technologies and Image Exploitation IOSB
Karlsruhe, Germany

***Abstract*—We present research with regard to a world modeling component called Object-Oriented World Model (OOWM) in order to perform High-Level Information Management (HLIM) in Joint ISR (Intelligence, Surveillance, and Reconnaissance). The OOWM allows to structure a priori available domain knowledge as well as current information gathered, e.g., according to specific collection and exploitation tasks, in an object-oriented way, i.e., by storing all available information in a structure which explicitly represents state, properties and relations of the relevant objects in the environment. It serves as a central information hub for HLIM components like High-Level Data Fusion (HLDF) modules and, by the employment of a domain model, it allows establishing a common understanding of terms. The OOWM concept supplements the CSD (Coalition Shared Data) concept which is the agreed state-of-the-art approach for interoperable information sharing in Joint ISR. In this publication, a special focus is placed on using current information given in form of formal exploitation reports. Based on this, we also present a new concept called Object-Oriented Reporting (OOR) which corresponds to a version of formal reporting being even more suitable for and closely related to the OOWM approach than current formal exploitation reports already are.**

I. Introduction

In light of the increasing complexity and diversity of today's threats, reaching a considerable high level of Situation Awareness (SA) is a key aspect of assuring the security of society, of citizens and infrastructures as well as of crisis management. Budget restrictions combined with the fact that today's threats often transcend organizational and even national boundaries demand cross-organizational cooperation and even force nations to collaborate and share information in an appropriate manner with the aim of reaching and collectively maintaining an appropriate level of shared SA (under appropriate consideration for data protection and security issues) [1].

In the domain of Joint ISR, the CSD concept [2] and the connected standards are an important key for this. The CSD concept enables the sharing of various kinds of standardized ISR products in a coalition according to STANAG 4559 (STANAG: NATO STAndardization AGreement). Its practical application is based on a network of physically distributed CSD nodes. According to the CSD concept, information delivering systems like sensors or exploitation systems feed information products being considered as relevant for the coalition in a standardized format into the CSD network. This is done via a connected CSD node and the respective information products are then saved at this CSD node. Each CSD node shares information about its persisted information products using standardized meta-data entries of the products. By distributing these meta-data across all connected CSD nodes in the network using adequate synchronization protocols, a coalition-wide awareness of all information products being available in the CSD network is achieved. Combining this with the ability to retrieve the actual information products on demand enables ubiquitous access capabilities for all information products being available within the coalition with reduced network traffic. Originally, the CSD concept was focused on the sharing of large amounts of fixed, finished data such as exploitation reports, images and video clips. However, its scope has been extended over time and, today, there are also dedicated means available for sharing dynamic products being actively updated (like Collection and Exploitation Plans (CXP) and derived tasks) as well as for sharing streaming data (provided from sensors) being periodically updated (like video streams and Ground Moving Target Indicator (GMTI) data).

SA means the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future [3]. For reaching a considerable high level of SA, means for HLDF, which is defined as the study of objects and events of interest as well as their relationships within a dynamic environment [4], are essential. This coincides with fusion tasks on the levels one and two of the JDL (Joint Directors of Laboratories) data fusion model [5]. HLDF is often still based on human cognitive capabilities and there is a strong need to assist human operators by (semi-)automatic means, e.g., to avoid information overload, to complement human capabilities, and to compensate decreasing human attention in routine situations. Means of implementing such assistance functions include adequate structuring and preparation, in particular also visualization, of available information to facilitate selection, analysis and also correlation of relevant information for the human operator. They also include further assistance in the form of a software-technical realization of methods from the field of HLDF on the basis of suitable mathematical models.

Querying and subscription of information products according to the CSD concept is based on the CSD meta-data which are product-oriented in the sense that they in essence describe the information products per se, not the real-world objects about which information is contained in these products. This goes along with the fact that, in (Joint) ISR, the collection of data and information, respectively, usually takes place according to a specific task and that the information products being intended for the deposit of the collected data and information, respectively, are also of a task-related nature. For example, an exploitation report serves as a kind of envelope for data, meta-data and result information with regard to the respective collection and exploitation task. When storing the information products, e.g. in a CSD server according to STANAG 4559, it is (according to this principle) also intended to link them with the respective task and basis data. Hence, formats of information products and associations between them support a task-related information management very well. However, solely on the basis of these means, a collateral use of collected information, i.e., a use going beyond the use with regard to concrete tasks, as it will be necessary for using the full potential of HLDF, is possible only in a very limited way (e.g., on basis of certain meta-data describing parts of the object-related content of an information product). In essence, the underlying structures have not been designed to this aim.

To close this gap, a semantic world model like the OOWM can be used as an additional information management component. The OOWM allows to structure a priori available domain knowledge as well as current information gathered, e.g., according to specific collection and exploitation tasks, in an object-oriented way, i.e., by storing all available information in a structure which explicitly represents state, properties and relations of the relevant objects in the environment. By this, it serves as a central information hub for HLIM components like HLDF modules and, by the employment of a domain model, it allows establishing a common comprehension of terms. As the research on the OOWM is conducted under explicit consideration of the research done with regard to the CSD concept, both concepts integrate in a seamless manner.

In this publication, a special focus is placed on using current information in form of formal exploitation reports as input for the OOWM. When supporting a human operator at decision making in the military domain, relevant and high-value information is mostly contained in specific ISR products like the exploitation reports created by highly specialized military personal. Nowadays, such reports can be posted to shared data storages like a CSD server by their originators, and relevant reports can in turn be retrieved by the intelligence staff of a commander when needed. Based on this, we also present a new concept called Object-Oriented Reporting (OOR) which corresponds to a version of formal reporting being even more suitable for and closely related to the OOWM approach than current formal exploitation reports already are.

The rest of this publication is structured as follows: in the next section, world modeling on basis of the OOWM is introduced. Sec. III addresses relevant aspects of formal reporting in the military domain. Also, our approach to extract information contained in specific formal exploitation reports in an object-oriented manner for semantically interoperable integration into the OOWM is described. Sec. IV illustrates how the OOWM can be employed in practice for HLIM in terms of intelligence gathering and decision support. This is done on the basis of use cases being detailed to concrete application examples in Joint ISR. In Sec. V, the idea of OOR is described. Sec. VI is a short summary.

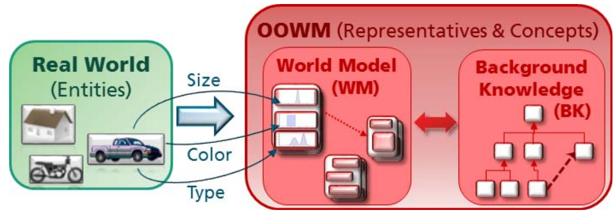

Fig. 1. In the OOWM, real-world entities correspond to representatives in the WM, based on a priori defined classes in BK. Representatives are modeled as objects defined by their attributes and can possess relations to other objects.

II. Object-Oriented World Model (OOWM)

World modeling or environment modeling is the task of creating and maintaining a system internal representation (i.e., a model) of the surroundings of a system and the entities occurring in this environment. A realization of such a world modeling component is given by the OOWM (see e.g. [6], [7]) which is designed as a system for modeling a spatio-temporal section of the real world in an object-oriented manner, i.e., based on the contained objects (or entities).

Fig. 1 depicts an overview of the OOWM. The OOWM processes attribute information with regard to domain entity features like their size, position etc. and stores it within the World Model (WM), which constitutes the dynamic modeling component of the OOWM. Observed entities are associated to concept classes stored in the semantic domain model of the OOWM. This second OOWM component is denoted as Background Knowledge (BK) and contains the a priori domain knowledge generated for example by human domain experts and/ or on basis of a formal domain analysis. For representing all the information contained in the OOWM and for deriving further conclusions on it, a generic approach based on Bayesian information modeling and processing (see e.g. [8]) can be used. The representation of an observed domain entity in the WM is denoted as a representative R and stored as the set of observed entity attributes A_R. The information being available with regard to each attribute $a_R \in A_R$ is represented by a probability distribution $p(a_R|d_{R_a})$ describing the Degree of Belief (DoB) in the observed attribute value a_R in light of the given information d_{a_R} with regard to this attribute. Thereby, either discrete probability distributions or continuous Gaussian and Gaussian mixture distributions (over the set of possible attribute values) are employed to represent the information being available with regard to the attribute value in this manner. These types of distributions offer a reasonable trade-off between information representation and tractability of recursive computations during probabilistic information processing. The probability distributions form the basis of the probabilistic information processing employed in the OOWM, like linking new observations to representatives using data association methods, or updating stored observation values using Bayesian fusion methods. In addition, the background knowledge on domain objects of interest is represented as an a priori domain model, such as a domain ontology (e.g., modeled in OWL), in the BK. As the counter-piece to representatives in the WM, object-oriented class-like descriptions of relevant domain entities are contained in the BK, denoted as concept classes. A concept class C is represented in the same way as a representative R, i.e., characterized by a set of concept attributes and, in addition, a number of relations to other concepts. Concept attributes are again represented by discrete and continuous probability distributions $p(a_C|b_{a_C})$ corresponding to DoBs given the available background knowledge b_{a_C} with regard to the corresponding attribute $a_C \in C$. For connecting the two OOWM components, WM and BK, a probabilistic classification approach based on a so-called association probability has been derived in [6]. The association probability constitutes a discrete probability distribution $P(C|R)$ over all the concepts C, rating how well the observed attribute values of a certain representative R correspond to the concept attributes.

The OOWM has previously been employed as central information hub for HLIM components in different application domains, including autonomous service robotics [7], maritime situation assessment [9], and surveillance [10], [11]. While this publication focuses on exploitation reports as sources of current information being used by the OOWM, in these other publications also other kinds of input information, like video information, track data, and open source information have been considered. Reasoning performed by HLIM components using the OOWM is either performed on basis of the probabilistic (Bayesian) approach being inherently integrated in the OOWM or on basis of alternative approaches, e.g., logical approaches using tools for ontology reasoning in a description logic, also making use of probabilistic extensions to description logic. We also have used Markov logic networks so far to achieve probabilistic reasoning on top of a rule-based domain model. The results from reasoning and deriving further conclusions on the available information (e.g., by applying behavior analysis with regard to certain real-world objects) obtained by HLIM components is relayed back, if desired, to the OOWM, causing updates on respective attributes of concerned representatives (e.g., the threat level classification for observed objects). Furthermore, the current state of the observed domain as represented by the WM is suitable as input to a Common Operational Picture (COP) being displayed to human decision makers. Finally and considered more precisely in the following, the OOWM BK domain model is suitable as a semantic model for the interoperable extraction of information from formal exploitation reports.

III. Formal Exploitation Reports

In Joint ISR, formal reporting means the generation of exploitation reports according to a well-defined specification which assigns a specific structure and form to the reports. These reports enclose their content and the results of the exploitation in various levels of structuring. Fully-structured reports are completely specified by a restrictive set of rules determining the structure of the reports as well as the possible contents of their fields and the meaning of these fields. Semi-structured reports are divided into sections with determined meaning, but have free-text contents which are not subject to restrictions. Examples are reports structured according to rules which use semantically annotated outlines to separate different parts of the reports. Also, there exist reports being structured by prefacing the report sections with labels or special markings representing the meaning of these sections. The latter method includes the text-based report formats of STANAG 3377 which assign semantics to the text sections based on their position in the overall text or by specific labels. Taken alone, these textual descriptions are rather imprecise. The NATO projects MAJIIC (Multi-Sensor Aerospace-Ground Joint ISR Interoperability Coalition) and MAJIIC 2 (Multi-Intelligence All-Source Joint ISR Interoperability Coalition) filled this gap by the elaboration of XML schemas which detail the STANAG 3377 and STANAG 3596 report formats and also define further ones (e.g., for exploitation of motion imagery and GMTI data) on a sound technical base. One major advantage of using XML is the wide dissemination of the XML technology and the variety of supporting tools.

The primary advantage of formal reporting is that it establishes a sound basis for semantic interoperability, i.e., a common understanding of the content of reports. This is especially important in Joint ISR, since misunderstanding exploitation information may e.g. lead to start military activities in an unintended geographic area, it may even lead to friendly fire or firing at civilians, scenarios which must not happen under any circumstances. Further automatic processing of exploitation results is enabled by the capability of random access to the sections of a structured report. Together with a common semantic, relevant information can easily and correctly be located in a report and extracted for further purposes. Another major advantage of formal reporting is the potential to record meta-data about the content of the report in the report itself. These meta-data facilitate, improve or even enable capabilities to search, filter and sort reports. Beyond that, structured and semi-structured reports avoid, or at least reduce, the overhead of Natural Language Processing (NLP) [12] being necessary to analyze free-text. Such free-text must be transformed into a formal representation for using it with regard to an automatic processing of information. Usually, this transformation is accompanied with uncertainty.

In order to extract information from (semi-)structured MAJIIC (2) XML exploitation reports as they are foreseen to be provided by a CSD server, we developed a prototypical software component called Information Extractor (IE). This information extraction component relies on a domain model for specifying concepts relevant to a considered scenario, including the names used to denote these concepts as well as their relevant features. We use an ontology as domain model for the IE. By this, a tight coupling between the OOWM and preceding information extraction is possible, since the OOWM BK can be used as domain model. This approach has the advantage of not requiring further syntactic or semantic alignments of the information provided by the IE when used as input for the OOWM (since the domain models are the same). The IE locates entities described by the classes of the domain model within a given exploitation report. If such an entity has been identified, the IE extracts values for the attributes of the entity defined by the domain model, as well as defined relations. As result of the information extraction, object descriptions according to the domain model are returned for all the entities that have been identified in the structured parts of the (semi-)structured exploitation reports. We created an (unpublished) domain ontology on basis of a formal domain analysis done under consideration of STANAG 3277, STANAG 3377, and STANAG 3596 as well as certain operational extensions and accompanying documents like AAP-6 (NATO Glossary of Terms and Definitions). The resulting domain ontology primarily models the target categories of STANAG 3596 together with their properties as possible objects. In addition, further objects which can be described via the MAJIIC (2) XML report formats (e.g., vehicles, weapon activities) are also modeled.

IV. USE CASES

In this section, two use cases are presented illustrating how we propose to employ HLIM for intelligence gathering and decision support on the basis of the OOWM. The first use case considers monitoring of mission-relevant Critical Infrastructures (CIs). Here, for a better insight, the underlying principles and assumptions are discussed in a generic manner before this use case is detailed with regard to a concrete application example, the protection of road networks. The second use case addresses monitoring of activities of enemy forces, concretely, the detection of redeployment of troops.

A. Monitoring mission-relevant critical infrastructures

CIs in general (e.g., power stations, waterworks) as well as mission-relevant CIs (e.g., patrol roads, bridges, military camps) are particular targets of interest for disruption or manipulation. A manual monitoring of all such elements in a mission area is often not possible due to operational restrictions, e.g., the lack of personnel. Here, HLIM on basis of the OOWM assists operators by integrating and fusing current information extracted e.g. from exploitation reports with background knowledge and additional information being already contained in the WM component of the OOWM and by generating alerts in case of events with a high DoB of being critical. For this, the following information contained in the OOWM (as part of both, BK and WM), is used:

- background knowledge on the CIs in the mission-relevant Area of Interest (AoI) like their location and function, established access restrictions to them, their mission-criticality (e.g., necessary for supply or troop movement),
- information about regular activities in the CI's vicinity (e.g., usual traffic on roads or bridges, daily postal services, day-to-day activities at installations) as well as information about scheduled (irregular) own activities (e.g., transport activities, road works, repair works),
- information about the status of own forces (e.g., locations of own vehicles in ongoing operations),
- knowledge and rules, respectively, about suspicious behavior patterns with respect to classes of CIs (e.g., persons or vehicles staying for a unusually long time in the vicinity of a CI may indicate a possible threat),
- current information, e.g. from exploitation reports.

In the following, we assume that assets in form of sensors and corresponding carriers perform (wide area) surveillance of the mission-relevant AoI. The collected data are exploited by human experts, generating exploitation reports. Depending on the concrete nature of the collected data, the following MAJIIC (2) XML report formats are foreseen: MTIEXREP (Moving Target Indication Exploitation Report) in case of GMTI data, MIEXREP (Motion Imagery Exploitation Report) in case of motion imagery data, RECCEXREP (Reconnaissance Exploitation Report) in case of still imagery data. The exploitation reports as well as relevant collected data are disseminated by ingesting them into the CSD network via a connected CSD node (thereby, they are associated together and with the respective surveillance task). On the basis of a subscription, the OOWM system is notified about new exploitation reports being available in the CSD network (via a connected CSD node). The OOWM downloads these new information products and starts to process them. By this processing, performed by the IE, the relevant information from these reports is extracted in an object-based matter and provided to the OOWM. Thereby, the IE can be configured with regard to the question of which kinds of objects defined in the underlying domain ontology are of relevance, such that only this information is extracted and provided to the OOWM. Here, this is information about observed vehicles and/ or persons, being described by attributes like their locations (also over time), colors, dimensions. The OOWM integrates and fuses the received object-oriented information with other existing information and domain background knowledge (as described in the first list above). As a result, the new information is contained in the WM component of the OOWM.

The integration of new information triggers a reasoning process at HLIM components acting on top of the OOWM, which detects and evaluates activities in the vicinity of the CIs, here. Thereby, activities are evaluated according to their DoB of being unusual. If, with a DoB exceeding a pre-defined threshold, an unusual activity has been detected, a human operator is alerted. Based on the information contained in the OOWM and, if necessary, additionally based on the respective information contained in the CSD network (here: tasks, exploitation reports, and sensor data), the operator decides on further actions such as tasking the acquisition and exploitation of additional sensor data, or, if enough information is given, the preparation of counter measures (in the case that he rates the detected event as actually being critical).

A concrete application example for the use case described so far could deal with the monitoring of theater patrol routes in the following manner. A vehicle drives along a road which is often used by patrols and stops there for a certain amount of time on the roadside before it continues its ride. The road is part of the mission-relevant AoI which is observed by a

GMTI sensor platform in the scope of a surveillance task. The sensor data is exploited and an MTIEXREP is created. After dissemination via the CSD network as described above, the relevant information about the vehicle is extracted from the MTIEXREP by the IE and integrated into the OOWM. In the OOWM, the route of the vehicle (known by the track information contained in the MTIEXREP) is correlated with background knowledge indicating the road being used as a regular patrol route, marking it as a mission-relevant CI. Since in regular cases, vehicles usually pass the road without stopping anywhere (known due to the existence of a suspicious behavior pattern used by the HLIM components) the behavior of the vehicle is considered to be unusual with a high DoB. Thus, an alert is created and forwarded to a human operator. Using only the current information about the unusual track which is derived from the GMTI data, it is not possible to derive details about the nature of the probably unusual activity (i.e., the cause of the stop, like vehicle repair vs. an IED (Improvised Explosive Device) placement) or to classify the observed vehicle (e.g., its type). Due to this, the human operator searches and retrieves electro-optical images of the road from a former mission using a connected CSD node. At the same time, he acquires further information by requesting an imagery-based reconnaissance task of the road together with a change detection RECCEXREP. Based on this additional exploitation report, the type of the vehicle is determined to be a truck and manipulations on the roadside are identified. Together with the assessed unusual behavior of the vehicle, the manipulations indicate the likely placement of IEDs. By integrating the relevant information contained in the RECCEXREP into the OOWM, the HLIM components confirm this by concluding a high DoB for the IED placement.

B. *Monitoring activities of enemy forces*

This use case is detailed with regard to the detection of troop redeployment within the mission-relevant AoI. For the sake of brevity, the given description has to focus on the most relevant aspects, here. As in Sec. IV-A, it is assumed that assets in form of sensors and corresponding carriers perform (wide area) surveillance of the mission-relevant AoI, that corresponding exploitation reports in form of RECCEXREPs, MTIEXREPs, and MIEXREPs, respectively, are created, and that dissemination of the relevant information via the CSD network takes place in the previously described manner. On the basis of a subscription, the OOWM gets continuously notified when new exploitation reports become available in the CSD network. Each time this is the case, the OOWM downloads them and the IE extracts information about locations (also over time) and the types of vehicles being present in the AoI. Over a certain time period (e.g., one week), HLIM modules infer from reasoning on this information an increasing DoB that opposing armored wheeled vehicles from different regions are relocated to a new common location within the AoI (in essence, on the basis of the number of such vehicles arriving and staying at the new common location). When the DoB for this troop redeployment event exceeds a pre-defined threshold, human operators are alerted to decide on further actions (e.g., requesting further detailed reconnaissance tasks of the target area, redeployment of own forces).

Obviously, despite the automatic reasoning mechanisms of HLIM components described so far, also the possibility to use the information contained in the OOWM as input to visual situation displays like a COP is of high operational value. Observing the possible troop redeployment over time as well as analyzing the final situation (at the time of the alert) and its history, using such a visual representation strongly supports the operator at making well-founded decisions. Due to this, also HLIM components based on techniques for visual analytics, which can be interactively applied, are part of our research.

V. Object-Oriented Reporting (OOR)

OOR is a concept aimed at shaping a version of formal reporting suitable for and closely related to OOWM. The current concept of formal reporting, as explicated previously, is not designed to convey information in a way where objects act as the first-class citizens of formal reports.

In STANAG 3596, the main element of a formal report is a target category (TC). The notion of TCs subsumes ISR-relevant entities of different types, ranging from installations (airfields, ports, camps, power production, water control etc.) over structures (bridges, tunnels etc.) and terrains to activities (movements, shipping, weapons etc.). Each TC is described by a set of attributes (concerning its status) and subordinated elements. These elements describe equipment, defenses or facilities observed for the reported TC instance. To some degree, this structure suits an object-oriented representation of reported information. But there are certain drawbacks. First, from an ontological point of view, TCs do not necessarily represent adequate object types for OOWM concept classes. Some TCs, for example, can be mapped to more than one object type (e.g., the bridges and tunnels TC). In addition, the concepts described by TCs can vary significantly in their ontological level of abstraction, and thus, in the information reported by the TC. Second, in subordinated elements, information about buildings, vehicles, persons etc. can be reported. This information also concerns observed real-world objects. From an object-oriented point of view, these objects exist independently of the observed TC instance. Thus, they should be reported at the same structural level as the TC (using relations between the objects and the TC to indicate their connections). Similar drawbacks wrt. to OOWM can also be found in the MAJIIC (2) XML reporting formats. Current formal reporting was not designed to be an ontologically sound, object-oriented knowledge model, but to lay down ground rules for task-based, machine-processable reporting. The major drawback of current formal reporting thus is the ontological bias of how reported information is structured. This structure is not object-based in the sense that

- information contained in one report often concerns more than one real-world entity,
- contained information often describes different objects at varying levels of detail,

- not always an explicit, ontologically suitable categorization of objects is given.

Another difficulty is that, even in formal reports, there may still be parts containing unstructured text (e.g., the subordinated elements of TCs). This makes extracting information (attributes, relations) about observed real-world object a tedious tasks requiring the use of NLP techniques for OOWM.

An object-oriented version of formal reporting has to address these issues. The approach taken in OOR is to formalize and transform the reported information as early as possible into an object-oriented structure: at the source of the information, the human user, when a report is created. The goal of OOR is to generate information formally structured according to the principles of OOWM, which easily integrates into the OOWM. The generation of this information is designed to be a background process, with as minimal implications as possible for the user creating the report. In formal reporting, specialized tools are used for report creation. OOR is intended as an assistance function for such a tool: when a user enters the information to be contained in a formal report, a representation of this information, structured according to the requirements of OOWM, is created in parallel. The parts of the entered information which could not be (fully) processed automatically will be presented to the user for feedback and corrections, as will be the final results of transforming the entered information. These results are represented as a kind of semantic network: objects with their respective attributes and relations between these objects. The types of the reported objects, attributes and relations have to correspond to the concept classes of the OOWM BK. The respective graph structures are then directly provided to the OOWM. Using such formal structures, OOR also allows making more of the reported information available to OOWM on a semantic level.

For realizing OOR, a new interactive approach to information formalization is proposed, described in the following. First, in a formal report structured according to STANAG 3596, the locations where objects are reported have to be identified. Instead of entering objects as text, in OOR, the user now will be prompted to select the desired object type from a list of allowed types when creating a new object (e.g., an observed TC instance). The list contains a subset of the object types given in the OOWM BK, specifically tailored to the element to be reported (e.g., TCs vs. subelements). This allows the identification and categorization of reported objects on the fly. Based on the selected object type, the user will be presented with mandatory and optional attributes for this type, as defined in the respective concept classes in BK. Values provided by the user (for object types and attributes) will automatically be encoded into the formal report as well as into the semantic network output. In the same manner, the objects contained in the subelements of a TC will be reported. In the semantic network, these objects will be represented as fully fledged objects, with relations (such as *is_located_in*, *is_part_of*, or *defends*) marking the relationship of the represented object to the reported TC instance.

For addressing the problem of unstructured information in formal reports, the tool support in OOR will consist of a background processing and parsing of entered text. In the military domain, often a specialized language with reduced vocabulary is used for reporting. OOR will exploit this fact to build a process for formal reporting in which, again, report contents and object-oriented information are created in parallel. For this purpose, the language and vocabulary to be used in reports has to be formalized to some degree. Based on such a specialized language in combination with a taxonomy of object types, their relevant attributes and possible relations, the idea in OOR is to use a simplified text processing for understanding and structuring the user inputs into an object-oriented semantic network. The network will be calculated on the fly while text is entered, such that immediate user feedback is possible. This user feedback includes adding non-inferred objects, changing the inferred type for objects, correcting the values of attributes, and adding or removing attributes or relations to objects.

VI. Conclusion

In this contribution, means for high-level information management (HLIM) in Joint ISR have been presented, based on an object-oriented approach which, in essence, comprises the concepts of an object-oriented world model, serving as a central information hub for HLIM components, and of object-oriented formal reporting, aiming at formalizing and transforming formally reported information as early as possible into an object-oriented structure.

References

[1] B. Essendorfer, C. Kerth, and C. Zaschke, “Adaptation of interoperability standards for cross domain usage,” in *Proc. SPIE 10207*. SPIE, 2017.

[2] C. Zaschke, B. Essendorfer, and C. Kerth, “Interoperability of heterogeneous distributed systems,” in *Proc. SPIE 9825*. SPIE, 2016.

[3] M. R. Endsley, “Toward a theory of situation awareness in dynamic systems,” *Human factors*, vol. 37, no. 1, pp. 32–64, 1995.

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

[5] M. E. Liggins, D. L. Hall, and J. Llinas, Eds., *Handbook of multisensor data fusion*. CRC Press, 2009.

[6] A. Kuwertz and J. Beyerer, “Extending adaptive world modeling by identifying and handling insufficient knowledge models,” *Journal of Applied Logic*, vol. 19, pp. 102–127, 2016.

[7] A. Belkin, A. Kuwertz, Y. Fischer, and J. Beyerer, “World Modeling for Autonomous Systems,” in *Innovative Information Systems Modelling Techniques*, C. Kalloniatis, Ed. InTech, 2012, pp. 137–158.

[8] J. Sander and J. Beyerer, “Bayesian Fusion: Modeling and Application,” in *Sensor Data Fusion: Trends, Solutions, Applications (SDF), 2013 Workshop on*. IEEE, 2013, pp. 1–6.

[9] Y. Fischer and A. Bauer, “Object-Oriented Sensor Data Fusion for Wide Maritime Surveillance,” in *Proc. of 2nd NURC International WaterSide Security Conference*. IEEE, 2010, pp. 1–6.

[10] T. Emter, I. Gheţa, and J. Beyerer, “Object Oriented Environment Model for Video Surveillance Systems,” in *Fraunhofer Symposium Future Security. 3rd Security Research Conference*, 2008, pp. 315–320.

[11] P. Bouvry, S. Chaumette, G. Danoy, G. Guerrini, G. Jurquet, A. Kuwertz, W. Müller, M. Rosalie, and J. Sander, “Using Heterogeneous Multilevel Swarms of UAVs and High-Level Data Fusion to Support Situation Management in Surveillance Scenarios,” in *2016 IEEE International Conference on Multisensor Fusion and Integration for Intelligent Systems (MFI)*. IEEE, 2016, pp. 424–429.

[12] F. Reinert, P. Waldschmitt, S. Leuchter, and R. Schönbein, “Informationsextraktion durch Verwendung Computerlinguistischer Verfahren in Texten mit Makrostruktur,” in *INFORMATIK 2007: Informatik trifft Logistik. Band 1. Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e.V. (GI)*, 2007.