Trusted Data Sharing in Federated and Dynamic Mission Contexts: Improving Communication Flexibility with Emerging Data Control Architectures and Concepts

Simon Dalmolen, Maarten Kollenstart, Hans Moonen, and Harrie Bastiaansen

Operations in military missions may benefit considerably from improved dynamics in trusted sharing of information between partners, both military and civilian. Currently, new ICT concepts for dynamic and trusted data sharing are maturing in the civilian context. They are controlled and managed by advanced semantic concepts. The authors address how these developments may be applied in dynamic and federated military mission contexts.

Abstract

Operations in military missions may benefit considerably from improved dynamics in trusted sharing of information between partners, both military and civilian. Currently, new ICT concepts for dynamic and trusted data sharing are maturing in the civilian context. They are controlled and managed by advanced semantic concepts. This article addresses how these developments may be applied in dynamic and federated military mission contexts. Architecture, design, first demonstration results, and topics for future work are provided.

Introduction

In military missions, relevant information may be potentially available from an ever growing and diverse base of data sources, owned or controlled by various (military and civilian) mission partners. Therefore, being able to connect and exchange data in a dynamic and trustworthy manner between mission partners is of growing importance for effective and safe military operations [1].

However, a dichotomy exists. On one hand, digital collaboration, operational intelligence, and situational awareness in military missions may benefit from sharing this diverse set of data sources between partners. On the other hand, digital collaboration through data sharing with (possibly unexpected, deviant, and unknown) parties is strongly impeded in practice [1, 2] as:

- A federated data sharing environment overarching both military and civilian partners is lacking, in which the trustworthiness and security of the shared information can be guaranteed, and data sharing partners can be dynamically added or removed.
- This is hindered by potentially conflicting security policies between organizations.
- Findability and distribution of relevant information in larger partnerships are complex and labor-intensive, with a high risk of data overload in the case of inadequate data analysis and management support.

Consequently, information is not, or sub-optimally, shared. This leads to less effective decision making and mission support in the military context.

Hence, an advanced federated, dynamic, and trusted data sharing environment in military mission contexts is needed, with:

1. *Federated*, meaning that a group of disjoint partners pool their data resources, operations, and capabilities together to create an overarching data sharing environment while maintaining autonomy over the internal operations of their part of the infrastructure
2. *Dynamic*, meaning that interconnectivity between such disjoint data providing and consuming partners may change over time and does not have to be set up and configured beforehand
3. *Trusted*, meaning that adequate capabilities are provided by the environment to ensure data sovereignty and security on information flows

An infrastructure for federated, dynamic, and trusted data sharing based on broadly accepted and adopted standards may improve the exploitation of all potentially available information. It has both military and IT operations benefits in the tactical domain.

Military benefits are the provisioning of a highly versatile information sharing environment including:

1. Making the right information available to the user at the right time via a personal information profile, which helps to prevent information overload and supports users in optimizing their own information flow
2. A mission-adaptable information management toolset, in which new information sources/stakeholders can be simply onboarded, including a priori unknown partners that may already be using the standards in their (civilian) context and therefore need minimal integration and training effort [3]
3. Enabling users to share information securely in a simple way without following cumbersome declassification procedures, using a fine-grained mechanism based on metadata labels on content that help to indicate associated risk scores [4]

IT operations benefits are:

1. Improved ease of use for information managers through semantically coherent and assisted matching of information from different partners

Digital Object Identifier:
10.1109/MCOM.021.2100438

Simon Dalmolen, Maarten Kollenstart, and Harrie Bastiaansen is with TNO; Hans Moonen is with CGI.

0163-6804/21/$25.00 © 2021 IEEE

2. Built-in security through advanced and proven security gateway concepts being developed and standardized for the civilian environment, allowing for improved security, for example, through local processing of sensitive data within a confined security domain of the data provider/owner [5]
3. Standardization of content metadata in an automated manner to prevent users from having to use time-consuming training on information sharing tooling
4. Registration and logging of which data has been exchanged with whom, and which capability is currently mainly lacking due to stringent security policies [6]

It is the authors' view that much of the above can be provided by leading and maturing civil developments, in particular, new architectures, concepts, standards, and technology for federated, dynamic, and trusted data sharing for improved communications flexibility. The following sections detail how they can be adopted and adapted by the military. A recent deployment in a defense exercise, as a concept demonstrator, is used as an example with presentation of the results, findings, and conclusions.

Architecture

This chapter describes the architecture for the federated, dynamic, and trusted data sharing environment as described in the introduction. As such, the following sections subsequently describe the various The Open Group Architecture Framework (TOGAF) architecture perspectives [7]; that is, the business architecture, the information systems architecture, the technology architecture, and the solution architecture. The architectural concepts and solutions as elaborated build on current development thereof in the civilian sector.

Business Architecture

The business architecture describes the main strategic and organizational functions and needs. It encompasses two key capabilities for federated, dynamic, and trusted data sharing in mission contexts as described in the introduction: the "dynamic and trusted data sharing" capability and the "semantic management and control" capability.

The dynamic and trusted data sharing capability provides dynamic onboarding (flexibility for new partners to join) and trust (security and data control). For military operations, trust that the data is handled in a controlled, trusted, and secure way is a sine qua non condition for a military partner to be prepared to share (highly) sensitive data. This applies even more in dynamic mission contexts, in which new data sharing partners may be onboarded in near real time.

The semantic management and control capability provides findability and distribution of relevant information in larger mission partnerships, based on information profiling and information metadata and matching. By adding metadata, documents can be found more easily, and matched better with information requirements, and information profiles can be built that identify both the information availability (information production) and the information needs of users (information consumption). Once a user has received a suggested "match" from the system that information produced by another party is of interest to that user, the information may be proliferated depending on the classification level as indicated in the metadata, for example, freely shared with all users of the federated platform or also beyond the trusted data sharing infrastructure after explicit approval by a defense contact or information manager through additional classified channels.

The business architecture describes the main strategic and organizational functions and needs. It encompasses two key capabilities for federated, dynamic and trusted data sharing in mission contexts as described in the introduction: the "dynamic and trusted data sharing" capability and the 'semantic management and control' capability.

Information Systems Architecture

The information systems architecture (ISA) describes the structure and interactions of the ICT concepts and components to provide the key capabilities from the business architecture. They are elaborated in the following paragraphs.

Functional Services: The key capabilities in the business architecture are provided as functional services. They are derived from the federated mission context and include:

- *Metadata and Matching Service* for automatic extraction of metadata from a document uploaded by the end user, and comparison thereof with the information elements that are available in the database. It notifies end users that are subscribed to specific information elements of the availability of a new document.
- *Information Profiling Service* to allow a partner to define the type of information in which he/she is interested. In addition, it also contains the functionality for making an initial taxonomy and exposing the relevant information of the information profiles of end users.
- *Federated Info Release Service* taking care of advertising of available data in a controlled, trusted, and secure manner between mission partners. Data sovereignty is key and handled through a federated implementation, allowing the data providing partner to stay in control over the metadata on available data sources.
- *Manage Access Service* to exchange data over the data sharing infrastructure via classified channels according to the applicable terms of use (e.g., consisting of access and usage control policies) as defined by either the end user or the information manager.

Federation Structure and Organization Style: In a federated mission infrastructure, the mission partners have a high degree of autonomy in designing and deploying their own internal ICT landscape. Interface specifications are the essential design artefact of a federated architecture to manage and coordinate the information flows between federation partners.

The definition of these interfaces is closely related to the organizational style for the federation. Various organizational styles can be adopted in a federated architecture. The organizational style defines the rules according to which allocation of responsibilities, coordination. and supervision tasks and resources are allocated over the partners [8]. Various organizational styles for the federated architecture are depicted in Fig. 1 [8]:

- A *centralized federative style* in which all authority and power resides within one center (e.g. a top management unit or partner), providing a tight type of structure with centralized management and supervision.

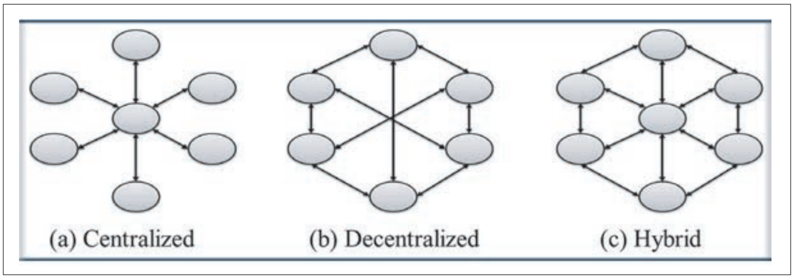

FIGURE 1. Organizational styles for a federated architecture [8].

- A *decentralized federative style* without any central management unit or partner; that is, authority, management and decision power are shared among the distributed, organizational, subunits, and partners.
- A *hybrid federative style* combining the features of both the centralized and decentralized federative style. The centralized functionality may be limited (e.g., to a [minimum] required set of functions) to ensure the operations and continuity of the federation. The distributed organizational subunits and partners together share control of the central body, and each subunit enters the larger association voluntarily.

In tactical networks deployed in operational military missions, the available bandwidth is limited. Consequently, connectivity to partner infrastructures is limited or may even be unavailable at all. This also holds for the local civilian partners and for a partner performing centralized management and control tasks (e.g., mission headquarters). On the other hand, military personnel and vehicles have ever more sensing, processing, storage, and communication devices at their disposal. A federated adaptive infrastructure may overcome the issues with such disadvantaged tactical mission networks [9]. Distributed cloud orchestration technologies allow either the data and/or the applications to be moved, enabling information to be processed with the optimal available resources, considering the local and current availability of data storage, processing power, and network connectivity. This leads to the observation that reliance on (the availability of) a centralized federation control function should be minimized.

Hence, the decentralized federative organization style should (by default) be preferred over a centralized federative organization style in mission contexts. Nevertheless, a centralized role in the federative architecture may still be required in providing a minimal basic set of essential (management) functions.

Dynamic and Trusted Data Sharing: Onboarding: Initially, the dynamic and trusted data sharing infrastructure as described in this article may be implemented for a federative mission context with mission partners that are well known and with which agreements on data sharing can be made prior to the mission, being either military mission partners in a joint operation or friendly civilian partners (non-governmental operators, NGOs) known to be active in the geographic operations area. These a priori mission partners may be well known and have proven to be trustworthy. An adequate trusted data sharing infrastructure with such mission partners can be agreed upon and configured prior to executing the mission, as well as the type, format, and semantics of information and data to be shared. Therefore, its functionality is limited.

As the next step and in addition to the a priori mission partners, ad hoc data sharing in the tactical mission context may be needed with new partners, either military organizations (e.g., friendly forces active in the same geographical area) or civilian organizations (e.g., urban areas operating a city video surveillance infrastructure). With such ad hoc partners, the data sharing infrastructure, data formats, and semantics may not have been agreed upon and configured prior to executing the mission. Hence, (near)-real-time onboarding processes for potential new mission partners with mission-relevant data sources must be supported. The minimal set of functions that allows them to be added in the mission context include:

1. Trusted and secure connectivity based on reliable identities over a secure handshake protocol with the partner's security gateway
2. Exposing the data and service capabilities of the partner

Functions for information profiling and/or information metadata and matching may not be required.

Semantic Management and Control: Interoperability: Semantic management and control is a relatively novel topic in applied software architectures [10]. It encompasses the tools, concepts, and process for seamless integration in a heterogeneous cross-domain environment. The goal of semantics in the dynamic data sharing architecture is to provide interoperability in a flexible and responsive manner to enable and/or support controlled sharing of data. It addresses three key elements

- *Accessibility of data*: to enable controlled and secure access without the need to know how and where the data is stored and which type of hardware, operating system, and database are being used. The information can be accessed via a single access point even if the data is being stored in multiple databases. The objective is to provide easy and seamless connectivity.
- *Interpretation of data*: to facilitate the interpretation of information based on message standards. The objective is to increase semantic interoperability among organizations with heterogeneous information systems in order to facilitate the communication, understanding, and exchange of resources and information.
- *Organization of data*: An entity-centric approach is used to reduce the complexity of the available data into individual and smaller parts. The information about each entity is collected and stored. Therefore, using an ontology as the semantic model is essential.

Technology Architecture

The technology architecture describes the logical technology principles and functions to implement the ISA for the federated, dynamic, and trusted data sharing infrastructure in mission contexts. It is based on the following guiding principles:

- Universal Internet standards are used with which new parties can easily be onboarded.
- Each participant is connected to infrastructure by means of an access point, referred to as a "node." The nodes mutually provide the functional services in a federated and distributed manner. A "federation control" capability additionally provides a minimal set of centralized functions to support dynamic and trusted data sharing (e.g., on partner identities).
- The platform has a modular design based on the functional services as defined in the ISA. These are implemented in a decentralized federative style and exposed by the nodes by means of well-defined application programming interfaces (APIs). Each partner may provide its own internal implementation of these services.
- Documents (texts, images, etc.) are made accessible by uploading them to a node for processing and distribution by functional services with semantic management and control.
- Data and metadata flows are separated. Metadata about (the content of) documents is exchanged without sharing the document itself. Documents are always shared peer-to-peer between nodes.
- Classification of data can be supported in various options through classifying metadata.

Figure 2 depicts the high-level technology architecture with the main functions, which are elaborated in the solution architecture in the following section.

Solution Architecture

The solution architecture realizes the technology architecture as described in the previous section. It implements the connectivity to the data sharing infrastructure by means of the nodes. The nodes realize and expose the services in the ISA as a set of loosely coupled components by means of well-defined APIs. Figure 3 depicts the federation of nodes and their solution components. In the federated approach, each mission partner may have its own specific internal implementation to implement the nodes and its services as defined in the ISA. As such, the solution architecture as elaborated in this paragraph should be interpreted as a reference solution architecture.

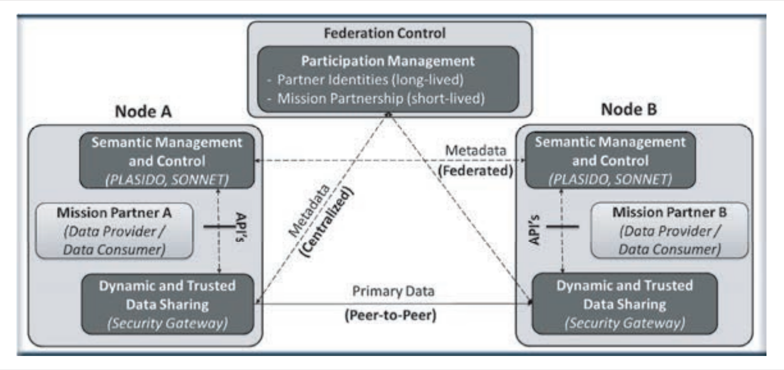
Federation Control
Participation Management
- Partner Identities (long-lived)
- Mission Partnership (short-lived)
Node A
Node B
Semantic Management and Control (PLASIDO, SONNET)
Mission Partner A (Data Provider / Data Consumer)
API's
Dynamic and Trusted Data Sharing (Security Gateway)
Metadata (Federated)
Metadata (Centralized)
Semantic Management and Control (PLASIDO, SONNET)
Mission Partner B (Data Provider / Data Consumer)
API's
Dynamic and Trusted Data Sharing (Security Gateway)
Primary Data
(Peer-to-Peer)

FIGURE 2. High-level technology architecture with the main functions.

The figure shows the main components of the solution reference architecture:

1. The capability for dynamic and trusted data sharing functions, as implemented by means of international data spaces (IDS) [11, 12] solution components
2. The capability for semantic management and control, as implemented by means of the PLASIDO and SONNET [13] solution components

These are further described in the following paragraphs.

Dynamic and Trusted Data Sharing: IDS: IDS facilitates the secure and standardized exchange and easy linkage of data in a trusted ecosystem. IDS supports the secure and controlled sharing of data (i.e. "data sovereignty") based on peer-to-peer data sharing. It is enabled by means of security gateways, referred to as IDS-connectors. Trust in the IDS is ensured by the use of certification of participants and components. The IDS reference architecture model [11] supports data sovereignty in the ecosystem through a mechanism for the description and enforcement of both access and usage policies. These policies can be negotiated between participants.

The IDS connector as depicted in the figure is an edge security gateway that can share data

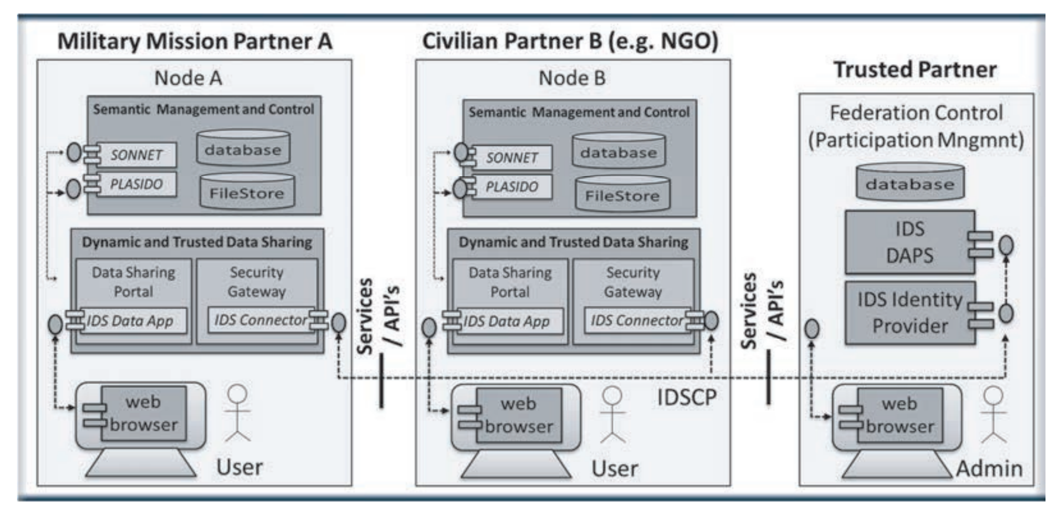

FIGURE 3. The technology architecture for the federation of nodes and their solution components.

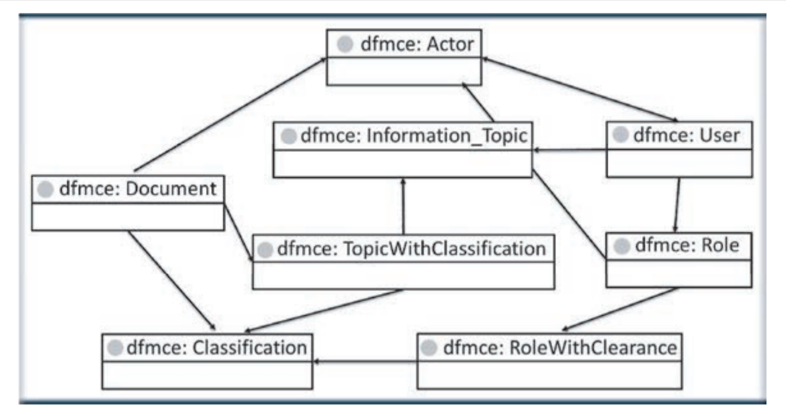

FIGURE 4. The ontology with main concepts and relations for the dynamic federated mission collaboration environment (dfmce).

across the nodes. The connector leverages container isolation to separate the data processing applications from the infrastructure capabilities. The heart of the connector is a core container that routes messages between data processing applications and other connectors. Identification and authentication of the nodes is handled by the core container in combination with the identity provisioning function as provided by federation control. It provides long-lived certificates for authentication and short-lived tokens (through a mechanism based on OpenID connect) containing attributes of the node and the party operating the node. This is handled by the dynamic attribute provisioning service (DAPS), which contains a trusted repository of these attributes.

The communication between the IDS-connectors in the nodes uses the IDS Communication Protocol (IDSCP), which is a WebSocket-based protocol. IDSCP allows remote attestation, a process for the verification of hardware and software integrity of the remote node, as well as meta-data exchange to be handled regardless of the content of the messages being exchanged [12].

The data sharing portal is an IDS data app that forms the bridge between the various components of the node and the IDS core container. The portal annotates outgoing messages with the IDS information model, indicating the metadata of messages that is used in the core container for routing the messages to the correct destination. All components in the node can only communicate with the portal. This allows the portal to handle all the logging for the node, ensuring a single point of truth that can be used for traceability purposes.

Semantic Management and Control: PLASIDO and SONNET: In the technology architecture, data access, authorization, and interoperability are managed by means of semantic technology. The basis is formed by an ontology, which is a formal description of knowledge as a set of concepts within a domain and the relationships that hold between them. It encapsulates the formal specification of components such as individuals (instances of objects), classes, attributes, and relations as well as restrictions, rules, and axioms.

An ontology can be seen as a semantic representation that computers can use as a data model. Ontologies are a real implementation of the definition of interoperability: connecting IT systems so that they can interoperate. These main concepts of the used ontology for the dynamic mission data sharing infrastructure are depicted in Fig. 4 and include Actor, User, Role, Information Topic, and Document.

As Fig. 3 depicts, the “semantic management and control” capability encompasses the PLASIDO and SONNET components.

The PLASIDO component maintains the current state of a node’s ontology. The main component is formed around a semantic triple-store. Its implementation has been extended with ontology base access control (OBAC) and allows read or write access for roles to information that adheres to specified patterns. OBAC policies are checked every time information is queried. This is especially useful when users from other nodes request information as specific patterns can be applied for users of different nodes.

In addition, SONNET is a text mining platform with which knowledge can be extracted from documents [13]. The platform contains natural language processing (NLP) algorithms that can generate a list of prioritized keywords/topics or a knowledge graph/ontology from a corpus of documents. SONNET is used as a standalone service that is called from the data sharing portal when new documents are added.

Status of Development

The architecture for federated, dynamic, and trusted data sharing in military mission contexts as described in this article has been developed and tested in close collaboration with a Light Infantry Brigade in The Netherlands. A proof of concept has been developed preparing for a large real-life testbed, integrated in a large military exercise of the brigade in April 2021. The basic components have been developed according to the architecture described in this article, together with technical use cases and supporting technologies. This has resulted in an initial version of the infrastructure for federated, dynamic, and trusted data sharing for military mission contexts. The implementation provides the required data sovereignty [14] over sensitive (meta)data based on the architecture and contains the functional services as previously described. The Metadata & Matching Service is based on the SONNET module, which is trained for a specific mission. The Federated Info Release Service is based on IDS, allowing new nodes to join the ecosystem by registering at the identity provider as depicted in Fig. 2. It will be extended with full stack integrity with both software and hardware verification via Trusted Platform Module (TPM) integration and with non-repudiation functionality. The Information Profiling Service is executed by PLASIDO as a configurable and loosely coupled module. The Manage Access Service provides functionality that has been hard to implement. In the initial version of the architecture, access control has been realized with the required identification and authentication functions. For the next versions, usage control is also considered through which data can only be used by the receiving node for specific purposes and contexts. This is hard to control and requires both procedural and technical capabilities.

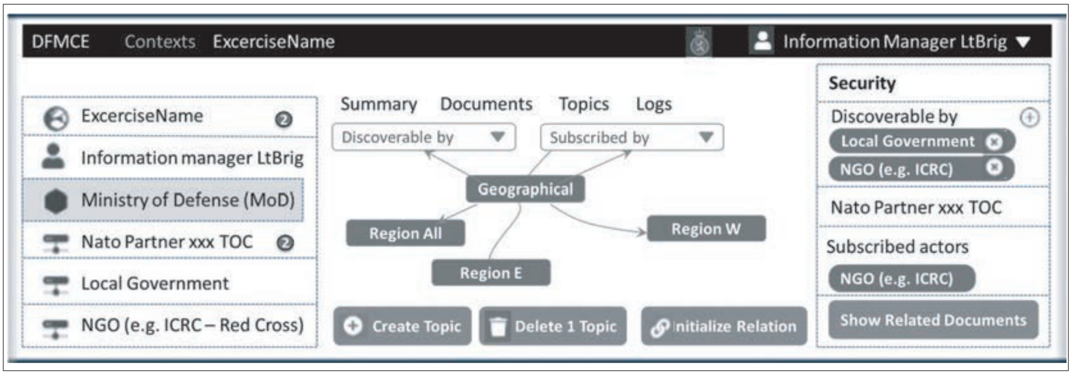

FIGURE 5. Screenshot of user interface of the Information Profiling Service.

A next version of the infrastructure is to be tested in another large military exercise in fall 2021 closely mirroring a tactical mission situation, and in collaboration with several NATO partners. This exercise will be more realistic, with more partners and bandwidth and connectivity challenges.

For interacting with the Data Sharing Portal, an initial user interface has been created with the primary aim of providing a concise representation that can easily be navigated through by users. A screenshot of one of the pages, for managing the Information Profiling Service, is shown in Fig. 5.

Assessment in a Military Excercise

In April 2021, the military exercise in The Netherlands took place. Document sharing scenarios with third (civilian) parties such as NGOs were tested and assessed. Test scenarios were prepared before. In the two-week exercise, the military personnel utilized the traditional data sharing processes in the first week. In the second week, they utilized the prototype system. The result is a series of observations and lessons learned, both technical as well as procedural.

Military personnel utilizing the infrastructure were especially satisfied with the fact that the platform provided them a safe and secure environment that allowed them to share data intelligently with ad hoc partners and vice versa, based on keywords, topics, and subscriptions to the latter. The ease of bringing up new nodes was appreciated, highlighting the dynamic and federated aspects of the infrastructure. Also, the graphical user interface for the Information Profiling Service, as shown in Fig. 5, was well received. The separation between metadata flows and the peer-to-peer primary flow of actual documents turned out to be useful functionality as well. Allowing documents to remain at the local providing node until actually requested underlies the trusted aspect of the infrastructure. Moreover, the fact that all data transactions were logged in order to trace who had access to what (version of the) information at what point in time was indicated as being of major added value in the military context. Especially when faulty information was shared, this functionality was valuable. Several users asked for additional functionality to signal others that earlier received information is no longer valid.

Several other improvements to the functionality of the infrastructure are foreseen based on the outcomes of the military exercise. The most interesting feature is a more advanced version of the topic matching functionality that is able to match keywords extracted from documents to information topics and users based on the different information profiles of users. Nevertheless, several people pointed out the importance to not automate this entirely. They articulated the importance of having a human check before committing the topics, which leads to sharing of documents. NGOs asked specifically for functionality to ask questions about documents directly to the uploader. As language and jargon tend to differ, it is important to fully understand each other, especially in combat situations.

A next version of the infrastructure is to be tested in another large military exercise in fall 2021 closely mirroring a tactical mission situation, and in collaboration with several NATO partners. This exercise will be more realistic, with more partners and bandwidth and connectivity challenges.

Conclusions

The primary objective of this article has been to elaborate and assess the architecture for dynamic, federated, and trusted data sharing in military missions, yielding improved communications flexibility. It has described how emerging architecture concepts and standards stemming from the civilian environment can be used.

The expectation is that the deployment of the infrastructure will improve communications flexibility with military and civilian mission partners and improve the exploitation of available information in tactical mission contexts. For this, the Federated Info Release Service (sometimes also referred to as "data broker") is the key component. Through this service, the available data on nodes can be regularly updated and advertised by means of self-description. It ensures that partner nodes can always retrieve the latest information on all available nodes and data in the infrastructure. The ontology and the PLASIDO service make sure that new information sources can be (dynamically) added. Its ontology-based access control features make sure that partners in the mission are correctly authorized to access information elements.

The architecture uses IDS, which provides secure communication between connectors [11]. An important aspect is the remote attestation protocol of IDSCP, requiring the complete software and hardware stack to be certified in order to verify their correctness and trustworthiness.

The effectiveness of the architecture as described in this article strongly depends on performance in tactical mission networks with low bandwidth and unreliable connectivity. On this topic, several observations can be made. The architecture uses a peer-to-peer model, where all nodes communicate directly with each

Alignment of the proposed architecture with the NATO Federated Mission Networking (FMN) [15] architecture should be assessed (e.g., as part of the upcoming FMN Spirals). In addition, compliance with the NATO architecture approach and terminology should be assessed, such as the NATO Architecture Framework and C3 Taxonomy initiatives.

other, which improves performance efficiency. By leveraging reusable WebSocket connections between nodes, the performance impact of the peer-to-peer network is minimized. For very-low-bandwidth scenarios, additional tests should be conducted to verify the resilience to incomplete communication. This also hooks into the reliability, as resilience to failures of communication is of major importance in tactical networks.

Future Work

Future work items include continuing to better characterize the problem domain as well as exploring the options to include the proposed architecture within the international military developments. This includes architectural alignment and interoperability in NATO mission contexts, in which both military and civilian organizations will be involved. As such, alignment of the proposed architecture with the NATO Federated Mission Networking (FMN) [15] architecture should be assessed (e.g., as part of the upcoming FMN Spirals). In addition, compliance with the NATO architecture approach and terminology should be assessed, such as the NATO Architecture Framework and C3 Taxonomy initiatives.

Finally, the introduction of the proposed concepts and architecture will have implications on existing solutions. Explorations are required on topics such as the implications on IT operations management in mission contexts, application development, and deployment processes.

Acknowledgments

Special gratitude is given to Mr. Jack Verhoosel (TNO) for his valuable contributions to the development of the platform on semantic technology, including PLASIDO and SONNET. In addition, the work as presented in this article is being done as part of Dutch National Technology Project (NTP) “FEderated DIgital Collaboration Environment (FEDICE)” as supported by the Dutch Ministry of Defense. We would like to thank the Dutch MoD for providing us the opportunity to do this highly relevant and interesting research and the individual participating partners (as represented by this article’s authors) for providing valuable inputs within a stimulating and cooperative setting.

References

[1] D. Zheng and W. Carter, “Leveraging the Internet of Things for a More Efficient and Effective Military,” *Center for Strategic and International Studies (CSIS)*, Rowman & Littlefield, 2015. ISBN: 978-1-4422-5890-7.

[2] M. Tortonesi *et al.*, “Leveraging Internet of Things within the Military Network Environment — Challenges and Solutions,” *IEEE 3rd World Forum on Internet of Things 2016*, 216, pp. 111–16.

[3] M. Rudack, C. Palacios-Camarero, and H. Wietgrefe, “On the Creation of a Single Mission-Wide Information Domain in Military Operations: Application of the Information Clearing House and Release Gateway at NATO Exercise Trident Juncture 2015,” *ICMCIS 2016*, pp. 1–7. DOI: 10.1109/ICMCIS.2016.7496566.

[4] A. Domingo and H. Wietgrefe, “An Applied Model for Secure Information Release Between Federated Military and Non-Military Networks,” *IEEE MILCOM*, 2015, pp. 465–70. DOI: 10.1109/MILCOM.2015.7357486.

[5] L. Zhang *et al.*, “Modeling of Collaboration Archetypes in Digital Market Places,” *IEEE Access*, vol. 7, 2019, pp. 102,689–700. DOI: 10.1109/ACCESS.2019.2931762.

[6] B. Suzic and A. Reiter, “Towards Secure Collaboration in Federated Cloud Environments,” *11th Int’l. Conf. Availability, Reliability and Security 2016*, pp. 750–59. DOI: 10.1109/ARES.2016.46.

[7] The Open Group, “TOGAF 9.1”; https://pubs.opengroup.org/architecture/togaf91-doc/arch/, accessed Mar. 24, 2021.

[8] N. Lindström, B. Nyström, and J. Zdravkovic, “An Analysis of Enterprise Architecture for Federated Environments,” *The Practice of Enterprise Modeling*, Springer, 2017, pp. 156–70.

[9] H. Bastiaansen *et al.*, “Adaptive Information Processing and Distribution to Support Command and Control in Situations of Disadvantaged Battlefield Network Connectivity,” *2019 Int’l. Conf. Military Commun. and Info. Systems*, 2019, pp. 1–7. DOI: 10.1109/ICMCIS.2019.8842794.

[10] S. Dalmolen *et al.*, “Supply Chain Orchestration and Choreography: Programmable Logistics Using Semantics,” *2015 4th Int’l. Conf. Advanced Logistics and Transport*, 2015, pp. 76–81. DOI: 10.1109/ICAdLT.2015.7136596.

[11] B. Otto *et al.*, “International Data Spaces: Reference Architecture Model Version 3”; https://internationaldataspaces.org/use/reference-architecture/, accessed Mar. 12, 2021.

[12] DIN SPEC 27070, “Reference Architecture for a Security Gateway for Sharing Industry Data and Services”; https://www.beuth.de/en/technical-rule/din-spec-27070/319111044, accessed Mar. 22, 2021.

[13] M de Boer and J. Verhoosel, “Creating and Evaluating Data-Driven Ontologies,” *Int’l. J. Advances in Software*, vol. 12, nos. 3 and 4, 2019, pp 300–09.

[14] H. Bastiaansen *et al.*, “Infrastructural Sovereignty over Agreement and Transaction Data (“Metadata”) in an Open Network-Model for Multilateral Sharing of Sensitive Data,” *ICIS 2019*, Germany; https://aisel.aisnet.org/icis2019/economics_is/economics_is/23/, accessed Mar. 12, 2021.

[15] NATO, “Federated Mission Networking (FMN)”; https://www.act.nato.int/activities/fmn, accessed Mar. 16, 2021.

Biographies

Simon Dalmolen (simon.dalmolen@tno.nl) is a senior ICT architect and business consultant at TNO. He was lead architect for the dynamic and federated data sharing infrastructure as described in this article.

Maarten Kollenstart (maarten.kollenstart @tno.nl) is a scientist at TNO. His focus is on architecture and design of data sharing infrastructures as described in this article.

Hans Moonen (h.moonen@cgi.com) combines a job as expert smart logistics at CGI with a one day/week position at the University of Twente. His core expertise lies in chain integration, planning, and digital transformation in logistics.

Harrie Bastiaansen (harrie.bastiaansen@tno.nl) is a business consultant at TNO. His background is in telecommunications and large-scale ICT-architectures. He leads several defense and data sharing research projects.