Data centric information provision: an outline

Reinout Pieneman, Mike Schenk, Bas Gerrits, Casper van den Broek (TNO)

Summary

Military organizations want to increase the effectiveness of their actions with 'intelligence'. There is a need for intelligence that enables the military user to take the right actions earlier and faster. To improve decision-making, the collection, processing, integration and use of real-time intelligence needs to be strengthened. Currently, this process is organized reactively, with the military user mostly looking for the information himself. The amount of information that is becoming available is constantly increasing. In the future, the search for information itself will be replaced by intelligence modules that push information in which the military user is automatically provided with tailor-made information, depending on the situation he is currently in. This raises the following question: how do you determine which information is relevant for which user? (Galliers, 2014)

Artificial Intelligence (AI) is a promising research field which generates the most benefit when data is freely available and can be combined across multiple domains. However, data is often collected for a specific purpose and only accessible to the limited set of applications that support that purpose. Therefore in order for AI to flourish, the first necessary step is to free up data from its application stovepipes.

We therefore propose that a data centric approach for the enabling infrastructure may provide a better and future-proof basis than a traditional application centric architecture, which has been a major focal point for IT-design and development over the last decades. The outline of this data centric approach is described in this concept paper, to ultimately enable proactive intelligence provision for the military user.

Issue

As the amount of structured and unstructured data continues to grow, the importance of providing military users with relevant information is becoming increasingly urgent. Because the number of and diversity of information sources continues to grow, we expect that;

1) The added value of user centric military infrastructure will increasingly move from collecting better data, to the smarter combination of existing data and unlocking the results towards the user at the right time. (Lupelli, 2017)
2) An automated consideration is required between the speed of disclosure and the integrity of the information in which the context of the user (identity, role, location, etc.) is taken into account. This is because in an operational environment where some information in the ‘fog of war’ will not always be a 100% certain and correct, yet life-and-death decisions depend on it. As not all source data will be error-free, conclusions based on this source data (even if it is correct) will not be flawless. (Matilla, 2017)

Concept outline

The design of this enabling infrastructure can therefore be based on the assumption that data is the really valuable asset. This approach will require a different way of implementing the enabling infrastructure through various emerging trends and technologies including data centric infrastructures, containerisation and (micro-)service development. (van der Geest, 2018)

The availability of a data centric military infrastructure

Over the last decades, the application centric architecture has been the major focal point of the IT industry, in which the applications were the primary structural element, supported by middleware solutions to enable interconnectivity. With the growing omni-presence of ICT, the number and intensity of interactivity between organizations and the resulting complexity of operations, it is becoming clearer that a data centric approach might provide a better way forward. This is driven by the observation that the data in the application is the really valuable asset, not the applications. Therefore, leading organizations are currently focusing on a data centric approach. In the military domain, developments as described in the Fraunhofer Shared Information Space pave the way to a similar data centric approach. (Angelsdorf, 2017)

The use of containerized deployment approach

Containerized service deployment technology allows processing functions, applications and services to be frequently and rapidly deployable, allowing computer code to be shipped and deployed nearly instantaneously when needed on a specific location and/or computing platform.

Applying a (micro-)service architecture approach

A microservice architecture enforces loosely coupled components in the design of a software application. It can be seen as counterpart of monolith applications, where you typically have a single, big code base. In a microservice architecture, each microservice implements a set of narrowly, related functions. The advantages of a microservice architecture are that individual services can (more) easily be extended, updated or replaced and that separate development teams can work on the microservices simultaneously. Moreover, testing and deploying the software becomes easier. (van der Geest, 2017)

Prototype design outline

The prototype that will be built on the basis of this concept is ultimately offered as a set of modular building blocks to an official who is in charge of the management of information reprocessing technologies. Each building block comprises different combinations of technologies. In the first instance, three logical building blocks can be thought of: collect, process and disclose. As the amount of operational applications and new technologies increase, multiple types of modular building blocks can be developed. Which combination of building blocks is used in which operational context depends on a large number of variables (e.g. network, bandwidth, threat level, quantity and diversity of information sources).

In each sub-step, multi-factor personalization (MFP) takes place; this means that each building block comprises a different combination of technologies to tailor the personalized information flow. Basically, MFP means that per collect, process and disclose step, a personal user profile is further enriched. This can be done on the basis of scrapers and classifiers, but also physical location, functional profile related to the role and task of someone (possibly already loaded by default) and (personally completed) expertise profile. Besides that you can use MFP to tighten your own profile based on multiple factors, you can also let the user determine the acceptable risk of sharing a piece of information under specific circumstances (eg different physical location, device, threat level increases)

At individual level, both a (default) functional and a personal profile are available. A set of individual profiles can serve as a basis for group profiles (eg at group, platoon or brigade level) and can be automatically loaded or actively managed by an individual or a specific official such as an information manager.

The prototype probably works best in a hybrid architecture: storing and processing locally as much as possible. Only the prioritized information is centrally stored and transmitted over the network. The prioritization takes place in each step collect, process and disclose, because you do not know at the start which information should be stored and / or sent locally or centrally. Locally collected metadata (and the subsequent ontologies) can be stored centrally and quickly with little bandwidth.

This approach provides a challenge for the application of AI algorithms, as these are currently designed to work on an infrastructure where data storage is centralized. However, only applying AI algorithms when local data is synchronized with the cloud, means essential time is lost. Therefore, we aim at creating distributed AI algorithms that can work on local data, upload the results to a centralized datastore and then do further processing centrally.

Prototype technical outline

The majority of the applications developed for use in a military environment use the application centric paradigm where the application is the one and only master of the data used and produced by the application. It is typically the application that takes care of storing this data in an application specific data store. The only access to this data is via the API's offered by the application.

The data centric paradigm puts the data central and an application is just an entity that performs an operation on some data and produces some new data. All data is stored in a generically accessible data store via a relatively small number of API's. No longer does an application requiring data from various sources, need to interface with a number of other applications, it simply interfaces to a single logical data store. (Bonomi, 2012)

This switch from an application centric to a data centric approach is illustrated in Figure 2-1. On the left side of the figure the Army, Navy and Airforce of a single or multiple nation have their own applications, each applications having its own data. On the right side of the figure there is a common data store (data cloud) from which all applications (the application cloud) from the Army, Navy and Airforce will receive and store their data.

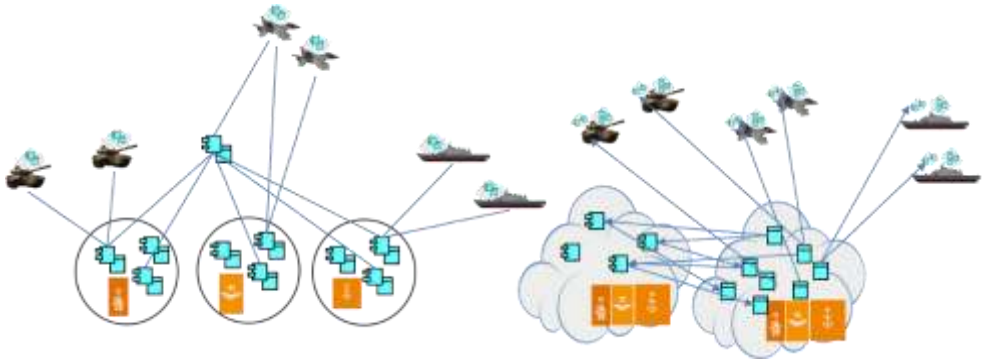

Figure 2-1: Comparison between an application centric (left) and data centric (right) approach.

Microservice Architecture

A microservice architecture enforces loosely coupled components in the design of a software application. It can be seen as counterpart of monolith applications, where you typically have a single, big code base. In a microservice architecture, each microservice implements a set of narrowly, related functions. (Du, 2018) Services communicate to each other using either synchronous protocols such as REpresentational State Transfer (REST) and Google Remote Procedure Call (gRPC) or asynchronous protocols such as Advanced Message Queueing Protocol (AMQP). (Godfrey, 2014)

Applicable over central (static) and decentral (tactical) mission domains

The (large-scale) acquisition and processing of data in the military context is not only restricted to central infrastructures (headquarter or compound), but can in an ever higher degree been done at the more 'decentralized' levels of the mission infrastructures. In military tactical (operational and decentralized) mission contexts, vehicles and military personnel have ever more IT and communication devices for acquiring, processing and communication of information. These improved sensing, mobile computing and on-board IT systems present great possibilities for the acquisition and processing of (big) data for AI and decision making. (Najafabadi, 2015)

Conclusion

In a complex NATO environment with largely distributed data sources, the data centric information provision concept is expected to yield major potential benefits for proactive release of information to military users. To operationalize this concept for the military user, data-centricity helps to improve the ease of development, simplicity and maintenance of the infrastructure leading to a high degree of reliability, performance, and capacity while taking account of the operational limitations and information needs of a military user. In combination with the loosely coupled, containerized microservices this concept of data centric information provision enables applications to be more easily made suitable for various military operational contexts.

Future research

Key for success is an advanced data exchange and service execution orchestration mechanism. One of those challenges is that the amount of data that can be acquired at a local/decentralized level can be much higher than the amount of data that can be processed at that level. Because connectivity over the disadvantaged tactical networks cannot be guaranteed, processing in a central infrastructure can also not be guaranteed. A more adaptive infrastructure may be required that allows either the data and/or the application to be moved, thereby allowing processing and information generation at the optimal location. This takes into account the local and current availability of data storage, processing power and connectivity between platforms. Therefore, new control strategies for matching data storage, processing and connectivity availability are needed, that orchestrate the distribution and execution of data and processing resources to generate information.

When designing a such a prototype mechanism, we expect a number of challenges to come forward.

- Service discovery; how does the infrastructure know where which services are available?
- Data synchronization and retrieval; how can the applications find the data when it can be stored in different locations, and how can one best ensure data availability under hardship conditions? Concepts like Data-centric networking may play an important role here.
- Coordination when distributing processing tasks to a number of processing units: how does one ensure that results from processing tasks are correctly combined? More specifically, how does this combination takes place when during data procession, some of the units fail to produce their results due to a failing connection?
- Governance; if a task is distributed to multiple processing units these units need to produce combinable results e.g. by running the same version of the service.
- Overhead; specifically when bandwidth is an issue, any overhead produced by synchronization and coordination should be as little as possible.
- Distributed AI algorithms; apply AI to omnipresent data, without the need to upload all local data to a central data store.

References

Angelstorf, F., Apelt, S., Bau, N., Jansen, N., & Käthner, S. (2017, May). Shared Information Space. In *Military Communications and Information Systems (ICMCIS), 2017 International Conference on* (pp. 1-7). IEEE.

Du, S. G., Lee, J. W., & Kim, K. (2018, January). Proposal of GRPC as a New Northbound API for Application Layer Communication Efficiency in SDN. In *Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication* (p. 68). ACM.

Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli , "Fog Computing and Its Role in the Internet of Things", in proceedings MCC'12 Helsinki, Aug 2012.

Galliers, R. D., & Leidner, D. E. (2014). *Strategic information management: challenges and strategies in managing information systems*. Routledge.

Godfrey, R., Ingham, D., & Schloming, R. (2014). Advanced Message Queuing Protocol (AMQP) WebSocket Binding (WSB) Version 1.0.

Van der Geest, J., van den Broek, C. C., Bastiaansen, H. H., & Schenk, M. M. (2018). Enabling a Big Data and AI Infrastructure with a Data Centric and Microservice Approach: Challenges and Developments. In *NATO STB IST-160 Specialists' Meeting*.

Lupelli, I., de Witt, S., Hollocombe, J., Muir, D., & Akers, R. (2017). Preemptive data distribution infrastructure for data centric analysis and modelling. *Fusion Engineering and Design*, *123*, 830-833.

Mattila, J., & Parkinson, S. (2017, September). Predicting the Architecture of Military ICT Infrastructure. In *ECISM 2017 11th European Conference on Information Systems Management* (p. 188). Academic Conferences and publishing limited.

Najafabadi, M. M., Villanustre, F., Khoshgoftaar, T. M., Seliya, N., Wald, R., & Muharemagic, E. (2015). Deep learning applications and challenges in big data analytics. *Journal of Big Data*, *2*(1), 1.

Pradhan, M., Tiderko, A., & Ota, D. (2017, May). Approach towards achieving an interoperable C4ISR infrastructure. In *Military Technologies (ICMT), 2017 International Conference on*(pp. 375-382). IEEE.

Wrona, K., de Castro, A., & Vasilache, B. (2016, December). Data-centric security in military applications of commercial IoT technology. In *Internet of Things (WF-IoT), 2016 IEEE 3rd World Forum on* (pp. 239-244). IEEE.