Towards Multi-Domain Multi-Tenant Situational Awareness Systems

Tobias Eggendorfer
TH Ingolstadt
Faculty of Computer Science
Ingolstadt, Germany
Email: tobias.eggendorfer@thi.de

Gerhard A. Schwarz
Bundeswehr
German Joint Support and Enabling Service Headquaters,
Bonn, Germany
Email: GerhardSchwarz@bundeswehr.org

***Abstract*—Situational awareness is vital and a life-saver in a multitude of environments - from disaster relief to military operations, from fire fighting to counter-terrorism. However, current systems are domain specific and do not provide for cross-domain interoperability. This is partly to scenario-specific semantics and partly due to privacy and confidentiality reasons. However, these single-domain single-tenant non-interoperable situational awareness systems hinder effective operations, they also prevent efficient and cost-effective evolution of these systems. In this paper we propose concepts for a shared situational awareness and report on a first prototype.**

***Keywords*-Security; Multi Domain; Interoperabitlity; Tactical Data Link; Military Information Systems; Situational Awareness; Information Dominance; Shared Information Space**

I. Introduction

Shared situational awareness, i.e., a multi-domain multi-tenant situational awareness, is relevant in multiple situations, be it in a humanitarian, police or military operation. While the respective measures and those operating in the field differ, all need a good overview of their own units, others involved, be it supporters, victims, criminals or supportive parties. However, they might also need additional information, such as weather data or information on the political or economical situation. Currently to generate situational awareness systems specific to a domain are used. While this seems legitimate at first, due to the rather small market for each domain, evolution of these systems is hindered, both from an information security perspective as well as from an usability, data-acquisition and data-management perspective.

A. Aim of this work

. This paper discusses how a more universal system for situational awareness could be designed, how it could provide additional information and support information interchange with other parties involved, while maintaining required confidentiality levels: Today's need for multi domain operations, which join political, economical, humanitarian, cyber-security and military efforts challenge all parties to share essential data, while they cannot disclose it completely with each others, e.g., patient data that cannot be forwarded to the military by the humanitarian or would need to be anonymized. The joint operations are similar to what the military defines as Political, Military, Economic, Social, Infrastructure, and Information (PMESII). PMESII describes the foundation and features of an enemy (or ally) state and can help determine the state's strengths and weaknesses, as well as help estimate the effects various actions will have on states across these areas [1].

B. Structure of this paper

The following paper is structured as follows: After this introduction (Section I) Section II provides relevant definitions and terminology used. The following Section III describes several use cases for situational awareness as well as data needed in these scenarios, how the differ, and how they are comparable. Section IV provides a short evaluation of the current state of research and technology. Based on this, Section V analyses how a future system should be designed. This is then taken one step further in Section VI, describing different potential solutions. Finally, Section VII provides a conclusion and our outlook on future work.

C. Our contribution

The Shared Information Space is a complete solution for information dominance compassing a technical as well as an organisational (information management) approach. We drive this existing and evaluated proof of concept in the military domain towards similar domains, e.g., security concerned organisations, by generalising the information management principle on top of a micro service based low code environment to suite multi domain operations. We aim to provide an universal toolbox consisting of various micro-serviced tools starting with data extraction, transformation, analytics, aggregation, manipulation, presentation and dissemination, which can be integrated and combined dynamically in the information flow driven by domain specific as well as interconnected semantics.

II. Terminology and definitions

This section provides an overview over the relevant terminology used in this paper,

A. Shared Situational Awareness

Situational Awareness was introduced by [2] as

> *an understanding of the activities of others, which provides a context for your own activity*

 ISBN: 978-1-68558-156-5

Especially in military operations, uncertainity of the general situation is known as ”fog of war” [3] and the increase of dimensions in space, time, quantity and dimensions multiplies by numbers. Therefore Shared Situational Awareness is widely considered to be the cornerstone for success in political, economical, military, environmental or scientific business, especially if the actors are forming an non-homogeneous working group. The more the collaboration is characterised by distributed activities, e.g., in terms of location, time or behaviours (different nationalities, communities, professions etc) the importance of Shared Situational Awareness among all participants and resources rises. Shared Situational Awareness emphasises the distributed and networked operating environment where resources and data are virtually accessible, while hosted at the point of origin and provided only on demand. Shared Situational Awareness imposes the need for supportive information systems, which handle netted information from distributed sources and supports collaboration across the various domains. In security and / or privacy sensitive organisations, like the military, police or health care, science and even economics, information sharing has to be controlled, at least (partially) limited to each authorised community.

B. Shared Information Space

A part from the concept of the Shared information Space condensed

> *as a universal collaboration space where all actors share their data, information, knowledge, concepts and its respective awareness towards a common goa*l

[4], the implementation of a Shared Information Space involves all technical aspects of an information system as well as the organisational and social implications on all collaborators in terms of information management and mind set. On top of the knowledge-base the shared information can be collaboratively processed and used in parallel by all actors for sense-making and common conclusions. The Shared Information Space consists of the following elements:

- A knowledge-base of connected and relevant information of all actors as netted information conserving context and semantic,
- actual data and information, which is dynamically updated, improved and documenting the rationality, for shared awareness,
- individual selection (reuse) and representation of content,
- collaboration amongst all users or groups forming appropriate information flows,
- ad-hoc adaption of tools for data analytics and manipulation using Low-Code approaches and
- support for different domains and use-cases via semantics.

III. Use cases and scenarios

This section gives an overview of different scenarios and their requirements on situational awareness systems.

A. Military operations

In a military operation, tracking of the own forces as well as those of allies, but also those of the adversary has always been a top priority. To do so, several technologies were used, back in the old ages, riders were sent. More modern techniques include Tactical Data Link (TDL) or Internet Protocol, providing units with an opportunity to both receive and transmit information as well as provide command and control facilities [5] [6]. This information is then presented in a human readable and rapidly comprehensible format. It provides the basics of situational awareness.

However, in a more complex scenario, additional information is required to operate in the field, such as information on weather conditions for more remote units or wind conditions for airborne operations. The information requirements are not limited to the originator and direct users as shown in the example above. Information gathered by one systems will be shared and reused by many actors across the field and even further in the broader context of a multi-domain operations.

Due to the strategic and tactical relevance of situational awareness - and partly also due to the funding possibilities, the military has a long history of optimising and researching means to provide their forces with situational awareness. Early work on distributed and networked knowledge-bases for information sharing investigated meta data registry and repository using the ebXML standard [7] for organising models and data. Consequently the approach was not limited to models or metadata, but also included content and its handling. The last generation of research modernised the early conceptional approach in terms of architecture (micro-services), data management (e.g. graph databases), semantically data organisation and introduced an additional organisational and social dimension (distributed information management cycle) to the prototype implementation based on Structr [8] in order to complete the Shared Information Space solution.

B. Humanitarian operations

Other scenarios require the same level of attendance, however, they hardly have the means for research. An example are humanitarian missions, such as providing relief after an earth quake or flooding, or supporting civilians in need during a military operation or adverse governmental situation.

In all these contexts, besides knowing where supportive units are deployed and people in need of help are located, further information is needed, such as the risk of new incidents, such as aftershocks or cholera outbreaks. In the context of support operations political and economical background information is of high relevance in order to provide support as needed and as appropriate and in a manner accepted by the political leaders. Weather could prevent access to some scenes.

C. Police operations

In police operations like a pursuit of a fugitive criminal or special units trying to extract hostages, besides tracking own forces and the offenders, it is important to map buildings including their known or identified ground layout, import

 ISBN: 978-1-68558-156-5

information about hostages and the offenders and identify potential movement areas, depending, e.g., on traffic and road conditions.

In a police context, forensic evidence is also relevant and might need its own situational awareness, i.e., a virtual "Lieutenant Columbo" identifying a speeding camera photo taken a mile away from the scene as relevant, as well as providing all evidence collected on scene. Although the authors assume it to be feasible to also provide this kind of information in their suggested system's concept, at this stage it is considered to be worth further discussion while the suggested situational awareness concept is being implemented.

D. Further scenarios

There are a lot more use-cases that might be relevant, such as a fire brigade operating in a building with a need to track those inside wearing a breathing apparatus or larger incidents for ambulance services, such as accidents involving busses or shootings, requiring a more complex management. Also complex and long-lasting combined rescue and relief operations, such as the flooding of the river Ahr in Germany in 2021, where most streets where not usable, some areas completely unreachable from the ground [9], and new access roads had to be established and cartographed, i.e., provided for shared situational awareness.

These and more use-cases demonstrate the need for shared situational awareness.

E. Conclusion on scenarios

All scenarios demonstrate that information from several sources needs to analysed, aggregated and augmented to provide appropriate situational awareness, going beyond current systems and what they provide. They highlight the following four high level requirements for

- common understanding of the different sources on the semantic level (starting from data up to conceptional level [10])
- flexible inclusion of newly identified information sources and services as well as processing capabilities
- dynamic update and renewal of changing data including the ability to investigate on the timeline (rewind for historic and "fast forward" for predictive review). This is consequently extended to other types of data like locations, quantities and qualities etc.
- ad-hoc response to changing actor demands, whether it deals with data or information bases, focuses on application as well as human user interfacing, levelling or rearranging information flows and dissemination of computing results and "command relevant information".

Such well defined, but general requirements are suitable for various services or communities in the area of security concerned organisations like cyber crime investigations, economical or financial control, environmental sustainability, fake information discovery and many more, even temporarily formed communities handling seriously their responsibility for intellectual property rights, prevention of data abuse and information security as well as privacy. Basically, all organisations and communities in the broader field of PMESII can be interconnected following the "multi domain operation" doctrine.

IV. State of research and technology

Whereas in the civilian area Industry 4.0 has the effect of a current innovation impulse, and Internet of Things (IoT) shows a facet of Weiser's vision of "ubiquitous computing" [11], this development is known in the military area as Network Enabled Operations (NEO) [12] [13] [14]. Ubiquitous computing emphasises that the path to success is not only in the field of technology or applications, but in the integration of the user with his or her knowledge, his or her potential for sense-making and his or her creativity that is needed to gain the essential superiority.

The Shared Information Space defines an information network, which dynamically connects humans and technology through information (Human – Information - Technology). In its semantic order, this information hub realises the idea of Shared Information Space. Using the new information management cycle, users organise their command and control information and collaboration in a self-synchronising manner pursuing a common goal (command intent) to achieve agility and a lead. Tried and tested procedures including modern technology stacks (Web-Oriented Architecture, microservices, etc.) [15] [16] are not replaced, but enclosed by the information networks and newly connected in a flexible way.

Derived from the sense-making requirement in network enabled operations a generic information model has been defined as depicted in Figure 1. The model allows handling of netted information including its context, its relations to other information as well as flexible characterisation by semantic techniques. According to the micro-service approach, functionality for retrieval, transformation, analysing, processing, presentation, dissemination of information can be dynamically adopted [17]. The information flow is adapted by a graphical user interface providing flexible response to changing user needs. Especially the semantic characterisation of various information elements fosters interoperability and the reuse of elements and functionality in other domains [18] [19]. Semantic search and also access control [20] is realised as combined effort.

Even that the stated requirements from above are widely adopted, there is room for improvement in terms of further increased dynamics [21] using low-coding techniques.

V. Requirements of a future system

To support all these scenarios a shared situational awareness system must be both agnostic to the scenario in how it handles data and understand the scenario in order to support the specific operation. While this sounds contra-dictionary it might not be: If data is kept in a unified format, only the presentation needs to be adapted to a specific use case. This adaption must be done in such a way that any user would be able to create or modify scenarios.

 ISBN: 978-1-68558-156-5

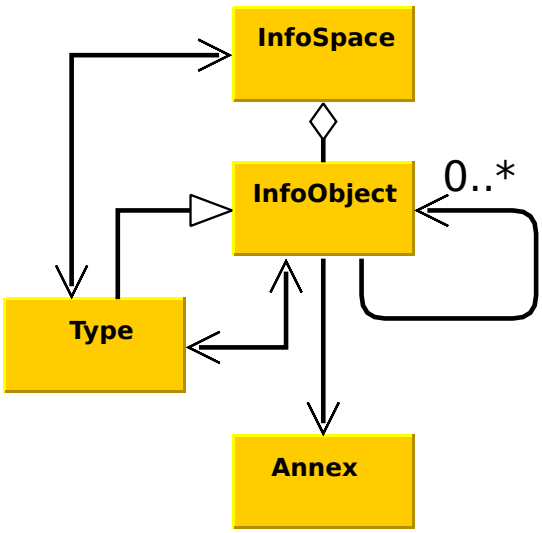

Figure 1. Semantically netted information forming a multi domain Shared Information Space

Obviously flexibility as to how and where data is acquired from is a must: Whether it is over a specific network such as TDL, a universal network such as the Internet, satellite data or photography, news, social media or any other Open Source Intelligence (OSINT) sources. In order to be able to adapt to new sources an open and easy to configure interface is required.

The data obtained needs to be presented to the user in a correlated manner, i.e., data from different sources should be provided in a unified way. Still a user should be able to dive into the sources and analyse their validity. Ideally the system would notify of contradictory information from different sources. It would also notify a user if new data for a monitored region becomes available.

In order to provide interoperability across domains, a data exchange mechanism maintaining security and confidentiality requirements is needed, e.g., in a humanitarian support operation in an armed conflict, the military should not receive health data of civilians to protect their privacy, while the humanitarian organisations should not receive detailed operational data from the military, however, should be warned if adversarial groups are active in their region.

VI. Concepts to implement a shared situational awareness system

For the several requirements of a shared situational awareness system, several potential implementation concepts exist. The following section provides an overview on these options.

A. Flexibility in scenario implementation

A major issue in the concept is to be able to provide the same technology to a multitude of use cases. Each of which has a different presentation. To do so, users must be able to adjust and modify their user experience accordingly.

1) Low-Code: In any operations the user has to focus on the goal and all tools and resources have to be already set up and available. The inclusion of resources may be adapted more easily. However, changes in the tool set are most likely a showstopper. Unless the circumstances changes fundamentally and a new or optimised tooling is required for gaining advantage and decision speed. In order to keep the user's experience as common as possible, it is proposed to benefit from low-coding techniques by

1) encapsulating all functionality in a well-known framework or ecosystem,
2) interacting with information including its presentation with standard elements,
3) adapting the elements and its connections modeling the requested information flow,
4) allowing high level adoption of elements and flows via a graphical interfacing,
5) integrating the user as much as possible in the change process,

in order to achieve dynamic and even ad-hoc customization of the Shared Information Space and its domain functionality. The chosen low-coding platform, which application service had been also the basis for the Shared Information Space, represents the functionality in the same graph models characterized by semantics. During the lifetime of the operation, this results in a complete domain specific knowledge base similar to model driven architecture techniques and can be used as a hot standby for quick response operations like in disaster relief, evacuation operations etc.

2) Alternatives: Besides Low-Code concepts there a several ideas on how to construct easily adaptable graphical front-ends, providing a no-code user experience, that is so simple that even children were able to successfully program robots [22].

Others suggest using Artificial Intelligence (AI), especially Large Language Models (LLM) to facilitate code generation [23] [24] or transformer based models to generate code from natural language specifications [25].

A new idea seems to combine the LLM concept with Low-Code [26] to further enhance the accuracy and speed of code generation.

All these concepts need to be evaluated and compared to the Low-Code idea for which a Proof of Concept (PoC) exists.

B. Flexibility in data correlation

New data should be automatically incorporated into the situation representation. However, data might be unstructured and correlation might not be immediately obvious. Therefore an implementation is more complex than simply moving data into a relational database.

1) Artificial Intelligence: Currently the most popular approach to solve this is requirement is probably AI, often implemented through Machine Learning (ML). In this concept the system learns from previous scenarios how to correlate data. These leanings are then applied to new scenarios. These could be used to re-enforce or update previous results, providing

 ISBN: 978-1-68558-156-5

dynamic updates. However, those concepts are criticised since an AI learns from an AI, which might result in a bad re-enforcement.

Besides that, ML has its own issues: Famous examples include ML attempts to distinguish wolves from dogs, which seemed to have worked well on a training set, but later demonstrated to have chosen the wrong parameter: Canines in snow were always considered wolves [27] [28]. Training data therefore has a massive impact on the quality and usefulness of ML.

2) Graph-Databases: A PoC using a graph oriented database system (GraphDB) based on Labeled-Property Graph (LPG) and Graph Modelling Language (GML) [29] with the ability to trigger events to notify an overlaying application of relevant changes was considered a viable alternative to ML. In contrast to ML it has the advantage of being explainable and reproducible, which is still ongoing research for AI.

In a GraphDB data is stored in a graph, i.e., the data itself is a node, while the relation between to pieces of information is represented as the graph's edges. While providing data is simple, adding the relations is more complex. These relations however, determine how the data could be queried and selected for output in a scenario.

Hence providing a good rule-set (or even AI) to add relations on data is a challenge to be resolved.

C. Flexibilty in data acquisition

A less complex issue is to provide easy to configure and flexible interfaces to provide input data from. From a technology perspective, there are plenty of universal formats and description languages, like JSON or XML. All of these could easily be provided. From a usability experience, however, the issue is more complex: With the aim of empowering the end-user to add data sources as needed, easy to generate format specifications are needed.

Supporting user with domain specific knowledge rather than software developers to add and modify data sources could be achieved by either providing a graphical user interface (GUI) with the help of user experience (UX) design, by providing a low code alternative or even trying to support import of new data through AI generated interfaces.

D. Secure data exchange

Again more complex issues arise when information should be shared with other parties in that operation. A traditional approach is the "need to know" concept, where information is reduced to the absolute minimum required to solve a task. However, to do so, some operator needs to define who needs to know what. This seems hardly feasible in a dynamic and changing environment. If this cannot be boiled down to a rule-set, human interaction would be needed. But that interaction would slow down the process.

In data protection, aggregation, anonymization and pseudonymization are relevant concepts to prevent third parties to receive more data than they are entitled to.

1) Aggregation: By computing an average or generating a heat map over many data sets, they are aggregated, i.e., put together in a way they could not be recovered like it has been demonstrated with STRAVA, where [30] found a way to identify a single user despite only having aggregated data. This is useful in a data protection context, since aggregated data is often as helpful as the raw data for research, but does not affect individual rights.

Looking at the scenarios above a humanitarian relief operation in a military conflict does not need to know, which adversarial weapon systems are deployed in a certain region, however, a heat map indicating more intensive adversarial activities or – instead of providing the sheer amount of weapon systems – a level of "danger" in a region would be helpful to plan and organise relief operations without endangering civilians and own resources.

Aggregation again requires a level of understanding of the needs of the party the information is shared with. This is easier in a context where multiple entities of the same kind, e.g., two nations' armed forces, cooperate, but do not fully trust each other in providing all information. Since the sending party could easily anticipate the needs of the receiving one. In other contexts, either the sending party has its assumptions on the needs, or has to discuss requirements and needs with the other entities.

Once the aggregation concept has been decided upon, it needs to be implemented. Again, this implementation should be performed by the end user, depending on the operational context. To do so, the same options as mentioned above in Sections VI-A and VI-B2 apply.

2) Pseudonymization: While aggregation does not allow to identify a single data set, pseudonymization allows re-identification. To do so, in the simplest case, humans are assigned a number or a fake name (hence the Greek $\psi\epsilon\upsilon\delta\omega\nu\upsilon\mu o\sigma$). The same could be performed in some scenarios, the most obvious is again a humanitarian operation, where lists of names and addresses to provide support to are rewritten. This seems to be feasible for at least some scenarios.

3) Anonymization: While pseudonymization is a bi-jective function, anonymization is not: Anonymized data is impossible to attribute to a specific user, device or entity. Anonymization is a rather complex process with many options to end up with an incomplete anonymization, which could be reversed. This resulted in concepts, such as k-anonymity [31] [32] and differential privacy [33], which allow for a measurable level of anonymity in data.

A rather simple example of bad anonymization are to be found in data protection: Some web-site claim to log anomyized user data by only storing their IP adresses. This is not anonymization but pseudonymization, since it is reversible. Also removing the last octet of an IPv4 address might not anonymize the user, if more data, such as user-agent and language preferences sent by the browser are logged. The resulting combinations might be unique.

Proper anonymization therefore requires some analysis. Appropriate methods need to be investigated and implemented

for different scenarios in shared situational awareness.

4) Randomization: Rather than anonymizing data another option could be to modify it slightly, just so much that it is still usable. This might be feasible for, e.g., TDL-tracks, i.e., information on, e.g., aircrafts in operation. Moving them by a few hundred meters to another position in their 3D-world or changing their ground-speed should not have to much impact on a situation, however, it could obfuscate the actual precision of how data is acquired. There might be a context where this is a useful option.

5) Application to the scenarios: It is still to be analysed whether data in the scenarios described above could be modified using the concepts above and how users could apply those modifications in a reliable and secure manner without too much training required.

VII. Conclusion and outlook

In this paper we describe several concepts to implement a shared situational awareness system applicable to a multitude of domains, supporting several use-cases. To do so, we define the necessary requirements and propose to evaluate these concepts starting with a prototype based on Low-Code and a GraphDB. While the first results seem promising we still intend to evaluate other concepts.

As the next steps we intend to evaluate the other concepts as described in Section VI to store and correlate data and to provide it in an user-friendly shared situational awareness systems. As a general necessity for a multi domain Shared Information Space, we envision that security gateways have to become more dynamic as today by adopting modern REST and JSON interfaces.

More research is required into how to solve special data exchange requirements to maintain privacy and confidentiality of data while providing adequate levels of situational awareness to all participating parties in a scenario. Once appropriate concepts exist research needs to go into facilitating generation of code to adjust these measures to a specific use-case.

While we hope to have identified relevant concepts to provide a multi-tenant multi-domain shared situational awareness system, we appreciate further input from the community.

References

[1] PMESII, “PMESII wiki.” [Online]. Available: http://pmesii.dm2research.com

[2] P. Dourish and V. Bellotti, “Awareness and coordination in shared workspaces,” in *Conference on Computer Supported Cooperative Work*, 1992. [Online]. Available: https://api.semanticscholar.org/CorpusID:1359859

[3] C. von Clausewitz, *”Vom Kriege (Translated: About war)”*. Dümmlers Verlag, 1991.

[4] L. J. Bannon and K. Schmidt, “Cscw: Four characters in search of a context,” in *European Conference on Computer Supported Cooperative Work*, 1989. [Online]. Available: https://api.semanticscholar.org/CorpusID:2353141

[5] G. Teege, T. Eggendorfer, and V. Eiseler, *”Militärische Kommunikationstechnik (Translated: Military communication technology)”*, G. Teege, T. Eggendorfer, and V. Eiseler, Eds. ”Universität der Bundeswehr München”, 2009.

[6] ——, *”Mobile militärische Kommunikationsnetze (Translated: Mobile military communication networks)”*, G. Teege, T. Eggendorfer, and V. Eiseler, Eds. ”Universität der Bundeswehr München”, 2009.

[7] O. ebXML Core TC, “ebcore agreement update specification v1.0,” 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:211567713

[8] Structr, “Structr,” 2024. [Online]. Available: https://structr.com

[9] T. Guardian, “After the floods: Germany’s ahr valley then and now – in pictures.” [Online]. Available: https://www.theguardian.com/world/2022/jul/13/floods-then-and-now-photographs-germany-ahr-valley-flooding-disaster-july-2021

[10] A. Tolk and J. Muguira, “The levels of conceptual interoperability model,” 2003. [Online]. Available: https://api.semanticscholar.org/CorpusID:14286538

[11] M. Weiser, “The computer for the 21st century,” *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 3, no. 3, p. 3–11, jul 1999. [Online]. Available: https://doi.org/10.1145/329124.329126

[12] M. Dettman, “”net-centric implementation framework: Part 1: Overview, net-centric entreprise solutions for interoperability (nesi)”,” 2009.

[13] G. F. G. DoD, “”weißbuch 2016: Zur sicherheitspolitik und zur zukunft der bundeswehr (translated: Whitebook 2016: Security policies and the future of the german federal armed forces”,” 2016.

[14] A. C. NATO, “Nato network enabled capability (nnec) data strategy,” 2006.

[15] M. Iorga, L. Feldman, R. Barton, M. J. Martin, N. S. Goren, and C. Mahmoudi”, “”fog computing conceptual model”,” 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:220041104

[16] P. M. Mell and T. Grance, “Sp 800-145. the nist definition of cloud computing,” Gaithersburg, MD, USA, Tech. Rep., 2011.

[17] R. Chandramouli”, “”implementation of devsecops for a microservices-based application with service mesh”,” 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:244253562

[18] G. Schwarz, *Vernetztes Informationsmanagement als Führungskultur im ”virtuellen IT-gestützten Informationsraum” (Shared Information Space) (Translated: Netcentric information management as leadership in a ”Shared Information Space” environment*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:250285420

[19] G. Schwarz and G. Teege, “”führen mit it (translated: Leading with it)”,” in *Wehrwissenschaftliche Forschung Jahresbericht 2020*, B. der Verteidigung, Ed., 2020.

[20] J. H. Saltzer and M. D. Schroeder, “The protection of information in computer systems,” *Proceedings of the IEEE*, vol. 63, pp. 1278–1308, 1975. [Online]. Available: https://api.semanticscholar.org/CorpusID:269166

[21] R. R. Leonhard, “Fighting by minutes: Time and the art of war,” 1994. [Online]. Available: https://api.semanticscholar.org/CorpusID:190927492

[22] T. Sapounidis, S. N. Demetriadis, and I. Stamelos, “Evaluating children performance with graphical and tangible robot programming tools,” *Personal and Ubiquitous Computing*, vol. 19, pp. 225–237, 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:18996142

[23] Y. Li and et al., “Competition-level code generation with alphacode,” *Science*, vol. 378, pp. 1092 – 1097, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:246527904

[24] E. Nijkamp and et al., “Codegen: An open large language model for code with multi-turn program synthesis,” in *International Conference on Learning Representations*, 2022. [Online]. Available: https://api.semanticscholar.org/CorpusID:252668917

[25] Z. Feng and et al., “Codebert: A pre-trained model for programming and natural languages,” *ArXiv*, vol. abs/2002.08155, 2020. [Online]. Available: https://api.semanticscholar.org/CorpusID:211171605

[26] Y. Cai and et al., “Low-code llm: Visual programming over llms,” *ArXiv*, vol. abs/2304.08103, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:258180418

[27] M. T. Ribeiro, S. Singh, and C. Guestrin, “”why should i trust you?”: Explaining the predictions of any classifier,” 2016. [Online]. Available: https://doi.org/10.48550/arXiv.1602.04938

[28] E. Yudkowsky, “”artificial intelligence as a positive and negative factor in global risk”,” in *”Global Catastrophic Risks”*. ”Oxford University Press”, 07 2008. [Online]. Available: https://doi.org/10.1093/oso/9780198570509.003.0021

[29] M. Roughan and S. J. Tuke, “Unravelling graph-exchange file formats,” *ArXiv*, vol. abs/1503.02781, 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:341087

[30] K. Childs, D. Nolting, and A. Das, “Heat marks the spot: De-anonymizing users’ geographical data on the strava heatmap,”

2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:259257088

[31] Z. Li and X. Ye, "Privacy protection on multiple sensitive attributes," in *Proceedings of the 9th International Conference on Information and Communications Security*, ser. ICICS'07. Berlin, Heidelberg: Springer-Verlag, 2007, p. 141–152.

[32] P. Samarati, "Protecting respondents identities in microdata release," *IEEE Transactions on Knowledge and Data Engineering*, vol. 13, no. 6, pp. 1010–1027, 2001.

[33] C. "Dwork, ""differential privacy"," in *"Automata, Languages and Programming"*, M. Bugliesi, B. Preneel, V. Sassone, and I. Wegener", Eds. "Berlin, Heidelberg": "Springer Berlin Heidelberg", "2006", pp. "1–12".