Improving Interoperability among Defence and National Security Ontologies: Analysis and Evaluation Tasks

Jonathon Dilworth[†,1] [0009−0009−0260−0492], Pedro Giesteira Cotovio[†,1,2] [0000−0001−6724−899X], David Herron[†,1] [0009−0008−2736−6789], Paul Cripps[3], Nigel Dewdney[4], Catia Pesquita[2] [0000−0002−1847−9393], and Ernesto Jiménez-Ruiz[⋆1] [0000−0002−9083−4599]

[1] City St George's, University of London, London, UK
ernesto.jimenez-ruiz@citystgeorges.ac.uk
[2] LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal
[3] Defence Science and Technology Laboratory, UK
[4] The Alan Turing Institute, UK

Abstract. The use of ontologies and knowledge graphs is becoming increasingly widespread in the *defence and national security* domain. Numerous ontologies have been developed through initiatives led by academia, industry, and government. Achieving interoperability across diverse *defence and national security* ontologies remains a major challenge due to the domain's breadth and specialisation. In this work, we analyse and document over 60 publicly available ontologies and introduce a new track for the Ontology Alignment Evaluation Initiative (OAEI). This track comprises eight matching tasks, consensus alignments and manually-curated (silver-standard) mappings. The consensus alignments are derived by aggregating the outputs of several state-of-the-art ontology alignment systems. The silver-standard is obtained from the manual validation of the consensus alignment together with a subset of the unique mappings (*i.e.*, mappings suggested by only one system).

Resource Type: Dataset and benchmark.
DISO Repository: https://github.com/city-artificial-intelligence/diso
OAEI Track: https://city-artificial-intelligence.github.io/diso-oaei/
Codes: https://github.com/city-artificial-intelligence/DISO-mappings
Permanent repository: https://doi.org/10.5281/zenodo.20059506
License: MIT License

Keywords: Ontology Matching · Ontology Alignment · Network of Ontologies · Defence & National Security · Evaluation · OAEI

1 Motivation

Defence and national security is one of the main UKRI[1] priorities, where AI techniques can play a crucial role in preventing and mitigating threats. Indeed, the work

[†] These authors contributed equally to this work.
[⋆] Corresponding author.
[1] UK Research and Innovation (UKRI) funding body.

presented in this paper is conducted within the scope of the GUARD project,[2] which focuses on *Ensuring Interoperable and Trustworthy Knowledge Graphs for Defence and National Security AI*. GUARD has been funded by The Turing Defence & Security Grand Challenge, a collaborative effort towards meeting the strategic requirements of UK Government agencies for *systematic sensemaking at scale and pace*.

The development of hybrid learning and reasoning systems in general, and Neurosymbolic (NeSy) AI systems [17] in particular, is gaining increasing attention to overcome the challenges of purely data-driven models (*e.g.*, LLMs - Large Language Models [44]) with respect to fairness, privacy, correctness, data and energy efficiency, identifiability, and eXplainability (XAI). In a domain like *defence and national security*, the design and development of robust, reliable and semantically sound AI models is paramount to support the notion of systematic sensemaking. Knowledge Graphs (KGs) [25] play a key role in orchestrating diverse and heterogeneous data sources, while providing a semantic and mathematical (*i.e.*, logic-based) representation of the domain. KGs are becoming essential components of NeSy systems [23] to *(i)* increase the coverage, validity and quality of the available data, *(ii)* impose constraints during the learning process, *(iii)* reason about what has been learned (*i.e.*, validity of the predictions), and, ultimately, *(iv)* enable well-informed decision-making.

One of the main challenges when working with KGs is the definition of an ontology to model the domain. The domain for a *defence and national security* application can be, however, quite broad as it may require the interplay of several subdomains to cover, among others, threats (*e.g.*, physical and cyber), relevant actors (*e.g.*, government, terrorist groups, intelligence services), operations (*e.g.*, military, emergency response), infrastructure (*e.g.*, airport, bases), policies (*e.g.*, defence strategy, international law), and geolocations.

There are several contributions from academia, industry, and government to create ontologies and knowledge graphs for security and defence. Prominent examples are the general-purpose models IES[3] and DoDAF.[4] IES (Information Exchange Standard) has been developed by the UK Government; while the DoDAF Formal Ontology has been implemented by the Department of War/Defense Chief Information Officer and serves as a NATO/multi-national model for defence. The IES models embrace semantic web technologies to represent general domain concepts such as locations, legal events, states, and measures. MITRE, funded by the National Security Agency, has also launched a family of cybersecurity ontologies to formalise offensive and defensive techniques [30].[5] The Department of Homeland Security has also designed a core Ontology for the maritime domain.[6] Efforts from academia include ontologies for military (*e.g.*, [11,60,35,41]), national security (*e.g.*, [8,42,7]), and cybersecurity (*e.g.*, [46,47,59,57]). There are also prominent examples of collaborations among government, academia and industry. For example, the Intelligence Community (IC) Ontology Working Group (DIOWG), from the US Department of Defense, is leading on the development and

[2] GUARD: `https://ernestojimenezruiz.github.io/projects/guard/`
[3] `https://github.com/IES-Org/ont-ies`
[4] `https://dodcio.defense.gov/Library/DoD-Architecture-Framework/`
[5] `https://d3fend.mitre.org/`
[6] `https://bit.ly/ontology-maritime-domain`

implementation of a National Security Ontology Foundry (NSOF), which will rely on the Basic Formal Ontology (BFO),[7] and the Common Core Ontology (CCO)[8] as their baseline standards.[9] BFO is an academia-driven upper-level ontology, widely adopted in life sciences ontologies (*e.g.*, OBO Foundry[10]), but with an increasing presence in government-related ontologies. NATO are also actively investigating the application of ontologies in the Command and Control space. As part of their work on the Data Centric Reference Architecture for the Alliance (DCRA),[11] they have outlined the need for a domain upper ontology for defence and security (CXCSRM) and ontology management services, with objectives closely aligned to those of the NSOF.

The interoperability among ontologies at the upper- and mid-level has been facilitated by efforts like IES, BFO and CCO. However, although IES and BFO are, in principle, compatible, a complete and formal alignment still needs to be established [4]. Furthermore, achieving interoperability across application ontologies may be particularly challenging in domains that require reconciling both the wide-ranging scope of concepts and the highly specialised representations in the subfields. *Defence and national security* is an example of such domains. An ontology foundry for *defence and national security*, as the one proposed by the DIOWG,[12] should ensure that its application ontologies achieve interoperability, comprehensive coverage, and high quality. Without these guarantees, the deployment of ontologies and KGs risks limiting their effectiveness in supporting downstream *defence and national security* tasks.

In this paper, we focus on the analysis of the interoperability among *defence and national security* ontologies. Our contributions are summarised as follows. *(i)* We have collected and documented 60+ public ontologies relevant to the *defence and national security* domain. *(ii)* We have analysed their intersection by performing ontology alignment over 1,653 ontology pairs. *(iii)* We have designed a new OAEI track including 8 matching tasks where we have compared the outcomes of several state-of-the-art alignment systems, created a consensus-based alignment, and manually verified a silver-standard reference alignment. The silver-standard has been generated by manually curating the consensus alignment and a subset of the unique system-generated mappings (*i.e.*, those suggested by only one system). The rest of the paper is organised as follows. Section 2 introduces the Defence, Intelligence and Security Ontologies (DISO) network, and the motivation for gathering and integrating these ontologies. The new DISO-OAEI evaluation track is described in Section 3, together with a comparison among the state-of-the-art systems. Section 4 summarises the created resources. Finally, future work directions and conclusions are given in Section 5.

[7] https://basic-formal-ontology.org/
[8] https://github.com/CommonCoreOntology/CommonCoreOntologies
[9] https://bit.ly/us-dod-ontology-news
[10] https://obofoundry.org/
[11] NATO. Data Centric Reference Architecture for the Alliance (2025): https://nhqc3s.hq.nato.int/apps/DCRA_Report/
[12] Recently rebranded as NSOWG (National Security Ontology Working Group).

Table 1: A view of the conceptual structure of the DISO collection of defence, intelligence and security ontologies. The clusters (or subdomains) of the DISO collection are listed together with the number of ontologies assigned to each.

DISO Cluster/Subcluster Name	Cluster Size	Subcluster Size
agentic	1	
ambient intelligence	1	
context awareness	3	
cyber-security	15	
digital twins	1	
information exchange	2	
information security	5	
mid-level	12	
risk management	1	
robotics	2	
situation awareness	4	
smart environments	8	
» smart buildings		4
» smart cities		2
» smart homes		2
upper-level	8	
totals	63	

2 Defence, Intelligence and Security Ontologies (DISO)

DISO (Defence, Intelligence and Security Ontologies)[13] is a collection of 60+ publicly available Web Ontology Language (OWL) [9] ontologies related to the *defence and national security* domain. The ontologies in DISO were identified and obtained during an ontology search exercise undertaken primarily during Nov/Dec of 2025, drawing on the academic literature (including surveys of cyber-security ontologies, *e.g.*, [36,52,53]), government and standards-body materials, and public ontology registries and repositories. An ontology was included in the collection if *(i)* it is publicly available, *(ii)* it is provided in (or has an available serialisation in) OWL, and *(iii)* it is relevant to the *defence and national security* domain, either directly (*i.e.*, developed by or for defence, intelligence and security organisations) or indirectly, through subdomains, such as 'situation awareness' or 'smart environments', that underpin *defence and national security* applications (as discussed below). Relevant ontologies distributed without a permissive (or confirmed) licence are not redistributed, but linked from their original locations. The provenance of each ontology (upstream source and licence) is recorded in the DISO repository, and future extensions of the collection are expected to follow the same criteria through a documented contribution protocol.

The DISO collection has been clustered into *defence and national security* categories (or subdomains). Table 1 shows the 11 clusters (or subdomains) of the DISO collection in alphabetic order along with the number of ontologies assigned to each

[13] `https://github.com/city-artificial-intelligence/diso/`

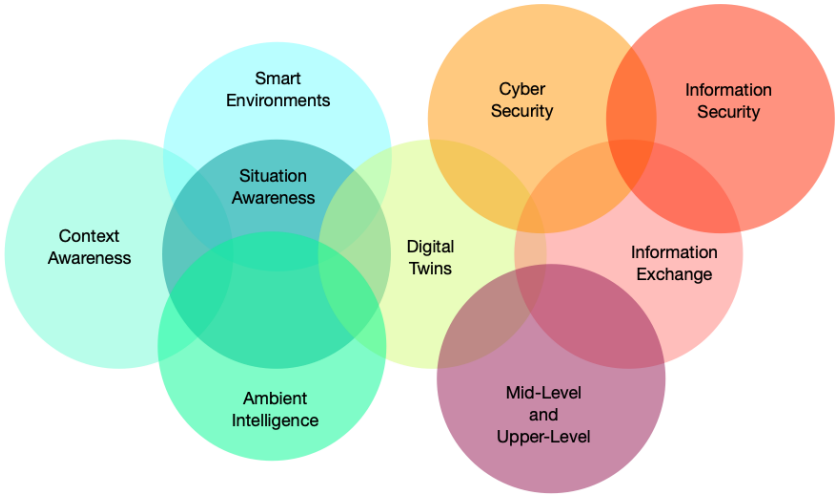

Fig. 1: A view of the conceptual overlaps that exist between some of the clusters (or subdomains) of the ontologies within the DISO (Defence, Intelligence and Security Ontology) collection.

cluster. Three factors make it difficult to provide precise counts of the number of ontologies in the DISO collection and within its component clusters. First, many of the ontologies obtained for DISO are physically represented as networks of multiple component ontology files. SOUPA [6], for example, an ontology for ubiquitous and pervasive computing whose development was partly funded by DARPA, and which is assigned to the DISO cluster 'situation awareness', is presented as a network of 18 component ontology files. For DISO ontology counting purposes, however, we count SOUPA as a single ontology. Hence, in this respect, the ontology counts reported in Table 1 significantly understate the number of physically distinct ontology files present within the DISO repository. Second, to make it easy for researchers to reuse such networked DISO ontologies, we have frequently merged such networks into single, all-inclusive ontology files. Third, some ontologies within DISO fit naturally into more than one DISO cluster. For example, the SOUPA ontology is regarded as being a member of both the 'situation awareness' cluster and the 'context awareness' cluster. Figure 1 illustrates the conceptual overlap that exists between the clusters (subdomains).

Regarding the FAIRness [18] of DISO , we have created metadata in RDF, extending the VoID and Dublin Core Terms vocabularies, to enhance the exploration of the DISO clusters and ontologies. The metadata includes links to the ontologies (remote and local versions), as well as their license. We have also added the repository to the LoD cloud.[14] to improve its findability. The DISO clusters and ontologies are also documented in our GitHub repository and summarised as follows:

Situation awareness. Situation awareness [12,39] has to do with perceiving and understanding the elements of a dynamic environment, and the relations between them, whilst

[14] `https://lod-cloud.net/dataset/DISO`

considering both space and time, and the prediction of the environment's future state(s). The generality of the notion of situation awareness is reflected in the number of other DISO clusters with which it has close conceptual associations.

Context awareness. 'Context awareness', for instance, has primarily to do with individuals and their immediate surroundings: their nearby environmental context. The common thread (and motivation) shared by the ontologies in this cluster is the idea of pervasive computing, where the objective is for mobile application services to be able to adapt their behaviour dynamically based on an application user's perceived current environmental context. Thus, the notion of context awareness can be regarded as a specialised form of situation awareness, where the situation of interest is the surroundings of a mobile, software application user.

Smart environments. It is similarly reasonable to regard smart environments (whether they be homes, or buildings, or cities) as being specialised forms of situations: built environment situations of various size and scale. The notion of 'smart' links to the notion of 'awareness' because the ontologies of the DISO 'smart environments' cluster generally presume some amount of sensor-based monitoring of the environment in question. For example, the DISO 'smart homes' ontology ThinkHome [51] has an emphasis on the monitoring and control of home energy use.

Ambient intelligence. Ambient intelligence [3] models devices that seamlessly interconnect and collaborate with each other as well as with human users. Like context awareness, ambient intelligence supports the idea of pervasive computing, but with more attention to supporting ideas like the Internet of Things (IoT). BOnSAI [55] is a smart building ontology for ambient intelligence, and is assigned to both the 'smart buildings' and 'ambient intelligence' DISO clusters.

Digital twins. Ontologies are well-suited to supporting the realisation of digital twins [38], and their use in connection with digital twins has been examined in a recent survey [31]. The notions of situation awareness, smart environments and ambient intelligence relate strongly to the notion of digital twins. Indeed, what DISO refers to as smart environments (smart homes, buildings and cities) are prime examples of the types of physical things that the UK's National Digital Twin Programme (NDTP)[15] envisages having digital twins. SAREF (a Smart Applications REFerence ontology)[16], created by the European Telecommunications Standards Institute (ETSI), is one of the main ontologies discussed in connection with creating digital twins for buildings in [38].

Information security. Information security has to do with protecting information in all its forms, whether physical or digital, tangible (*e.g.*, paperwork) or intangible (*e.g.*, knowledge), from things like unauthorised access or inappropriate use, modification, disclosure or corruption. DISO contains five ontologies covering this domain. One of these, MDISOnt [40], a multi-dimensional information security ontology, decomposes information security into several perspectives using dimensional views and modules.

Cyber-security. Cybersecurity is widely understood as a specialised form of information security that focuses on the digital domain and the protection of assets against digital threats. Three recent surveys of cyber-security ontologies [36,52,53] attest to the fact

[15] `https://ndtp.co.uk`
[16] `https://saref.etsi.org/`

that the cyber-security domain appears to appeal to ontologists. The DISO collection includes 15 such ontologies that are widely recognised in the literature. A prominent example is the MITRE Corporation D3FEND cyber-security ontology [30].

Information exchange. Ontologies in this cluster seek to standardise data representations so as to facilitate the exchange (and aggregation) of data across diverse domains, sectors, organisations and systems. The DISO collection contains two authoritative information exchange ontologies. One, IES (Information Exchange Standard)[17], is a standard for information exchange developed within the UK Government. DISO contains the IES version released in November 2025. The IES plays a critical role in enabling the UK's vision of a National Digital Twin (NDT). The other information exchange ontology in DISO is JC3IEDM, standardised by NATO and jointly developed under the Multilateral Interoperability Programme (MIP) for the exchange of consultation, command and control (C3) information.

Mid-level and Upper-level. In addition to domain/application level ontologies, DISO also contains clusters for mid-level and upper-level ontologies as well. Upper-level ontologies seek to describe general concepts to embrace and orchestrate domain-level ontologies. Mid-level ontologies specialise upper-level ontologies for particular (vertical) domains, and thereby play a fundamental bridging role between (general) upper-level ontologies and (specialised) domain-level ontologies. The criticality of mid-level and upper-level ontologies for enabling integration of diverse, heterogeneous knowledge sources is evidenced by the next version of IES, which is being modularised with 'ies-top' and 'ies-core' to provide the common foundations for IES domain and sub-domain level ontologies.

2.1 Towards a network of DISO ontologies

Ontology alignment [13] is the process of finding correspondences or an *alignment* $\mathcal{M}$ among the entities (ontology classes, properties or instances) of two or more ontologies. A *mapping* involving two entities is typically represented as a 4-tuple $\langle e_1, e_2, r, c\rangle$ where e_1 and e_2 are entities of the ontologies $\mathcal{O}_1$ and $\mathcal{O}_2$, respectively, r is a semantic relation, typically one of $\{\sqsubseteq, \sqsupseteq, \equiv\}$, and c is a confidence value (usually a number between 0 and 1). An ontology *alignment system* is a program that, given as input two ontologies, generates an ontology alignment $\mathcal{M}^S$ between them.

We conducted a bulk ontology alignment exercise using the ontology alignment system LogMap [27,28] over the DISO ontologies, resulting in the (potential) generation of alignments for 1,653 ontology pairs. Table 2 compares the distributions of alignment sizes with respect to two different sets of DISO ontologies: *(i)* the full set of 1,653 DISO ontology pairs, and *(ii)* the subset of 105 DISO cyber-security ontology pairs derived from the 15 cyber-security ontologies. We observe that LogMap identifies an intersection between at least 647 ontology pairs (66 about cyber-security), indicating that the DISO ontology network has an important number of connections (*i.e.*, ontology mappings) across its ontologies as we advanced in Figure 1. The analysis of the bulk ontology alignment served as the basis to select a subset of ontology pairs for a

[17] `https://informationexchangestandard.org/`

Table 2: A comparison of the (partial) distributions of alignment size (measured in entity mapping counts) for two different sets of DISO ontology pairs, as generated by one ontology matching system.

	1653 DISO ontology pairs			105 DISO cyber-security ontology pairs		
Alignment Mapping Count	Ontology Pair Count	Ontology Pair Count Cumulative	Cumulative Pair Count As Proportion of Total Pairs	Ontology Pair Count	Ontology Pair Count Cumulative	Cumulative Pair Count As Proportion of Total Pairs
0	1006	1006	0.61	39	39	0.37
1	213	1219	0.74	17	56	0.53
2	107	1326	0.80	13	69	0.66
3	90	1416	0.86	11	80	0.76
4	48	1464	0.89	3	83	0.79
5	29	1493	0.90	3	86	0.82
6	31	1524	0.92	6	92	0.88
7	17	1541	0.93	2	94	0.90
8	14	1555	0.94	1	95	0.90
9	13	1568	0.95	0	95	0.90
$\geq$10	95	1653	1.0	10	105	1.0

new ontology alignment track, as described in the next section. Ultimately, the goal is to develop an integrated network of DISO ontologies that contributes to addressing the interoperability challenge in the *defence and national security* domain.

3 The DISO OAEI track

The Ontology Alignment Evaluation Initiative (OAEI) [49] is an annual campaign for the systematic evaluation of ontology alignment systems. The OAEI plays a key role in the benchmarking, comparison and reproducibility of ontology alignment systems. The OAEI includes different matching tasks involving small-sized (*e.g.*, conference [61]), medium-sized (*e.g.*, anatomy [10]), and large (*e.g.*, bio-ml [22]) ontologies.

Interoperability in the *defence and national security* domain has been recognised as a major challenge, and a community-driven initiative such as the OAEI can contribute to the integration of the DISO ontologies. At the same time, the *defence and national security* domain offers a promising real-world scenario and a set of non-trivial matching tasks for the campaign, as shown in this section. The bulk ontology analysis revealed an important potential intersection among the DISO ontologies. We analysed the ontology pairs sharing a larger amount of ontology mappings (as suggested by the LogMap system) and ranked them in terms of complexity of the alignment task; that is, ontology pairs where their entities have fewer identical labels were preferred. LogMap was selected to drive the task selection as it generates different types of outputs that enabled a fine-grained analysis. Additional information is provided in the GUARD project report (phase 1) [26]. Table 3 shows the top-8 candidate ontology pairs that emerged from

Table 3: The top-8 ontology pairs that emerged from the LogMap-driven analytic process. 'SA' refers to 'situation awareness'; 'CA' refers to 'context awareness'.

Task Subdomain	Source Ontology		Target Ontology		LogMap Alignment				
	Name	Cluster	Name	Cluster	All	Cls	Oprop	Dprop	Ind
cybersecurity	UCO	cybersecurity	STIX	cybersecurity	131	43	4	84	0
	STIX	cybersecurity	D3FEND	cybersecurity	37	31	0	6	0
SA	JC3IEDM	SA	mIO!	CA	219	12	0	0	207
	JC3IEDM	SA	Brick	smart buildings	49	6	0	0	43
	JC3IEDM	SA	Facility	cco-modules	44	44	0	0	0
smart envir	ThinkHome	smart homes	Brick	smart buildings	33	24	0	1	7
	Brick	smart buildings	SmartEnv	smart homes	32	25	0	0	7
	CityOWL	smart cities	Brick	smart buildings	24	16	1	0	7

the analytic process and form the basis for the new DISO-OAEI track. These ontology pairs cluster into three distinct subdomains: cybersecurity (2 pairs), situation awareness (3 pairs), and smart environments (3 pairs).

3.1 Ontology statistics and provenance

Table 4 shows the statistics of the ten selected ontologies for the DISO-OAEI matching tasks. For each ontology, we briefly describe its domain and provenance.

UCO: Unified Cyber Ontology UCO[18] is a domain-level ontology assigned to the DISO 'cyber-security' cluster. It focuses on concepts such as cyber investigations, network defence, threat intelligence, malware analysis, vulnerability research, and offensive operations. UCO is an open, community-developed ontology, partly funded by the Linux Foundation, with the ambition to support the cybersecurity domain in its entirety.

STIX: Structured Threat Information eXpression. STIX [5] is a domain-level ontology assigned to the DISO 'cyber-security' cluster. Initially developed by MITRE Corporation, STIX was designed as a language and serialisation format for exchanging cyber threat intelligence. The official STIX specification is managed by the OASIS Cyber Threat Intelligence (CTI) Technical Committee.[19]

D3FEND. D3FEND [30] is a domain-level ontology assigned to the DISO 'cyber-security' cluster. MITRE Corporation, its developer, refers to it as a knowledge graph of cybersecurity countermeasures, and as a framework for cybersecurity operations and strategic decision-making. Development of D3FEND was funded by the National Security Agency (NSA), the U.S. Cyber Warfare Directorate, and the U.S. Office of the Under Secretary of Defense for Research and Engineering.

JC3IEDM: Joint Consultation, Command and Control Information Exchange Data Model. JC3IEDM [43], standardised under NATO as STANAG 5525, is a domain-level ontology assigned to the DISO clusters 'information exchange' and 'situation awareness' [58]. The aim of the JC3IEDM is to support the exchange of consultation, command and control (C3) information, where heterogeneous command and control in-

[18] https://unifiedcyberontology.org/

[19] https://oasis-open.github.io/cti-documentation/

Table 4: Quantitative descriptions of the 10 ontologies appearing in the DISO-OAEI matching tasks. The metrics are as reported by the Protégé (`https://protege.stanford.edu/`).

Metric	UCO	STIX	D3FEND	JC3IEDM	mIO!	Brick	Facility	ThinkHome	SmartEnv	CityOWL
Axioms	11,552	3,903	32,832	26,622	7,727	117,811	7,083	8,122	4,146	7,387
Class count	429	88	3,495	2,922	624	2,305	859	1,109	161	516
Object property count	192	68	205	619	364	131	146	406	242	522
Data property count	581	386	42	313	310	80	12	303	50	162
Individual count	507	4	2,340	4,088	520	8,556	81	54	17	17
Annotation property count	43	6	35	2	24	165	40	22	44	42
Class axioms										
SubClassOf	444	1270	5,391	2,567	627	2,494	925	2,344	401	1,250
EquivalentClasses	0	0	0	272	36	105	25	282	6	2
DisjointClasses	8	18	8	0	62	15	23	123	21	36
Object property axioms										
SubObjectPropertyOf	11	0	250	0	92	19	84	61	164	48
EquivalentObjectProperties	0	0	0	0	0	4	0	0	13	13
InverseObjectProperties	9	0	41	116	70	9	63	48	80	7
ObjectPropertyDomain	10	89	2	503	344	0	127	350	177	517
ObjectPropertyRange	181	71	4	503	337	2	128	340	173	511
Data property axioms										
SubDataPropertyOf	40	1	42	0	92	6	0	12	13	9
EquivalentDataProperties	0	0	0	0	0	0	0	0	0	0
DataPropertyDomain	4	448	2	313	304	2	8	82	48	162
DataPropertyRange	579	385	17	313	284	2	8	277	43	159
Individual axioms										
ClassAssertion	558	0	1,194	4,088	904	18,882	83	53	29	25

formation systems (C2IS) are sharing military situational awareness data. This model has been further developed under the Multilateral Interoperability Programme (MIP) to deliver the MIP Information Model.[20]

mIO!: A Context Ontology for Mobile Environments. mIO! [50] is a domain-level ontology assigned to DISO cluster 'context awareness'. It is a context ontology network whose aim is to model context-related knowledge that allows mobile applications to adapt their behaviour based on user context. mIO! was developed by the Ontology Engineering Group at University of Madrid.[21]

Brick: A Uniform Metadata Schema for Buildings. Brick[22] is a domain-level ontology assigned to DISO cluster 'smart buildings' ('smart environments'). It is an open-source project whose aim is to standardise descriptions of physical, logical and virtual aspects of buildings, and the relationships between them. The Brick consortium comprises commercial and academic members.

Facility. Facility is a CCO (Common Core Ontology)[23] mid-level ontology assigned to DISO cluster 'cco-modules', within cluster 'mid-level'. This mid-level ontology was designed to represent facilities (such as buildings, campuses, etc.) that serve some specific purpose and which are common in multiple domains.

[20] The MIP Information Model (2025): `https://www.mimworld.org/`
[21] `https://oeg.fi.upm.es/index.php/en/ontologies/index.html`
[22] `https://brickschema.org/`
[23] `https://www.commoncoreontologies.org`

ThinkHome: Smart Home Ontology for Human Activity Recognition. ThinkHome [51] is a domain-level ontology assigned to DISO cluster 'smart homes' ('smart environments'). It is an ontology intended to support smart systems, especially those with a focus on home control, and particularly on energy efficiency. It consists of five component ontologies that address individual aspects of the target application domain: actors, buildings, energy resources, processes and weather. ThinkHome was developed at Technical University Vienna.[24]

SmartEnv: Smart Home Environments. SmartEnv [1,34] is a domain-level ontology assigned to DISO cluster 'smart homes' ('smart environments'). SmartEnv, initially referred to as 'E-care@home' in the literature [2], is a network of 8 component ontologies modelling various aspects of smart homes: temporal, spatial, objects, events, agents, observations, etc. Its notion of 'smart' refers to environments (such as homes) that are monitored by sensors of various kinds.

CityOWL. CityOWL is a domain-level ontology assigned to DISO cluster 'smart cities' ('smart environments'). It is an OWL rendering of a standard schema defined by the Open Geospatial Consortium called CityGML[25]. The standard defines a conceptual model for representing virtual 3D models (aka digital twins) of cities. The CityOWL ontology obtained for DISO was acquired from a URL associated with the Computer Science Laboratory for Image and Information Systems at the University of Lyon.[26]

3.2 Alignment evaluation

We executed several state-of-the-art systems on the DISO-OAEI matching tasks with two main objectives: *(i)* to assess the complexity of the tasks, and *(ii)* to generate silver-standard alignments for the track. We selected the following systems: AML [15], BertMap [21] (with variations using different BERT-based pre-trained models), BertMapLt, LogMap [27], LogMapLt, LogMapLLM [37], Matcha [16], ALOD2Vec [48], ATMatcher [24], Fine-TOM [33] and KGMatcher [14]. Table 5 presents the mappings computed by the ontology alignment systems in each of the DISO-OAEI tasks. Note that LogMapLLM, ALOD2Vec, ATMatcher, Fine-TOM, and KGMatcher were not able to produce mappings on all matching tasks. It can also be observed that the systems generated highly disparate sets of mappings in the DISO-OAEI tasks. For example, in the *JC3IEDM-mIO!* task, LogMap produces 234 mappings while AML generates 34.

Consensus alignments. We have computed consensus alignments of vote 2 and 3 (*i.e.*, mappings suggested by at least two or three systems, respectively). Note that, when there are several systems of the same family (*i.e.*, systems participating with several variants), their (voted) mappings are only counted once in order to reduce bias. Table 5 shows the number of consensus mappings voted by 2, 3 and all systems (Con-2, Con-3 and Con-all, respectively) and the number of system families contributing to the consensus (#SF). For example, in the *JC3IEDM-mIO!* task, 77 mappings were suggested by at least 2 system families, while only 11 mappings were recommended by all 8 families.

[24] `https://www.auto.tuwien.ac.at/index.php/projectsites/155-thinkhome`

[25] `https://www.ogc.org/standards/citygml/`

[26] `https://liris.cnrs.fr/`

Table 5: Number of system and consensus mappings for the selected matching tasks. #SF: number of system families contributing to the consensus. Con-x: consensus mappings with 'x' votes. Con-all: consensus mapping supported by all system families.

Matching task	System mappings						Consensus mappings			
	AML	BertMap	BertMapLt	LogMap	LogMapLt	Matcha	#SF	Con-2	Con-3	Con-all
UCO-STIX	43	21	21	131	177	692	4	171	39	21
STIX-D3FEND	27	17	18	37	28	102	6	45	32	17
JC3IEDM-mIO!	34	22	26	234	37	167	8	77	46	11
JC3IEDM-Brick	45	23	23	57	105	776	4	108	27	22
JC3IEDM-Facility	43	28	29	44	37	43	8	71	41	2
ThinkHome-Brick	112	13	17	55	141	312	4	95	58	16
Brick-SmartEnv	32	12	22	39	52	322	4	48	28	22
CityOWL-Brick	38	15	22	27	58	402	4	64	28	23

Table 6: Manual validation of unique and consensus mappings. For each system family, we provide the number of unique mappings and the ratio of correct ones in brackets. For Matcha, the ratio represents an approximation given the large number of generated mappings. *Others* aggregates ALOD2VEc, ATMatcher, Fine-TOM and KGMatcher.

Matching Task	Unique system mappings by family					Consensus-2 mappings		Silver
	AML	BertMap	LogMap	Matcha	Others	# Total	% Correct	# Total
UCO-STIX	1 (0%)	1 (0%)	43 (84%)	516 (10%)	0 (0%)	171	91%	194
STIX-D3FEND	2 (0%)	0 (0%)	10 (20%)	63 (10%)	0 (0%)	45	76%	39
JC3IEDM-mIO!	3 (0%)	0 (0%)	199 (97%)	113 (7%)	65 (9%)	77	87%	274
JC3IEDM-Brick	3 (0%)	2 (50%)	38 (5%)	662 (2%)	0 (0%)	108	67%	75
JC3IEDM-Facility	6 (0%)	3 (33%)	5 (60%)	0 (0%)	34 (0%)	44	94%	44
ThinkHome-Brick	45 (13%)	0 (0%)	80 (47%)	299 (6%)	0 (0%)	95	92%	134
Brick-SmartEnv	3 (0%)	0 (0%)	36 (31%)	274 (10%)	0 (0%)	48	77%	53
CityOWL-Brick	6 (0%)	0 (0%)	21 (57%)	339 (5%)	0 (0%)	64	83%	68

Manual assessment. Consensus alignment can serve as a reference for the agreement across systems; they are, however, not complete and may also include errors, as it only requires two systems to agree on an incorrect mapping [20]. Hence, we have performed a manual revision of the Con-2 consensus mappings and the mappings uniquely generated by a system or system family. Unique mappings may include potentially valid correspondences that were not identified by any other system family. Table 6 presents the results of the manual validation. Consensus mappings are typically precise, with 94% of the mappings in *JC3IEDM-Facility* classified as correct. Con-2 was less accurate for the *JC3IEDM-Brick* task. The quality of unique mappings varied across systems and tasks. For example, 80% and 13% of the unique mappings identified by LogMap and AML in *ThinkHome-Brick*, respectively, were annotated as correct. The manual revision led to the creation of a silver-standard for the DISO-OAEI tracks by merging the correct unique mappings and the correct Con-2 mappings. The manual validation was performed primarily by the authors. However, a broader validation involving multiple domain experts, together with an inter-annotator agreement analysis, is planned in the context of the OAEI 2026 campaign. The quality of the silver reference will also improve as more systems contribute mappings, and it will be updated with results from the OAEI participants.

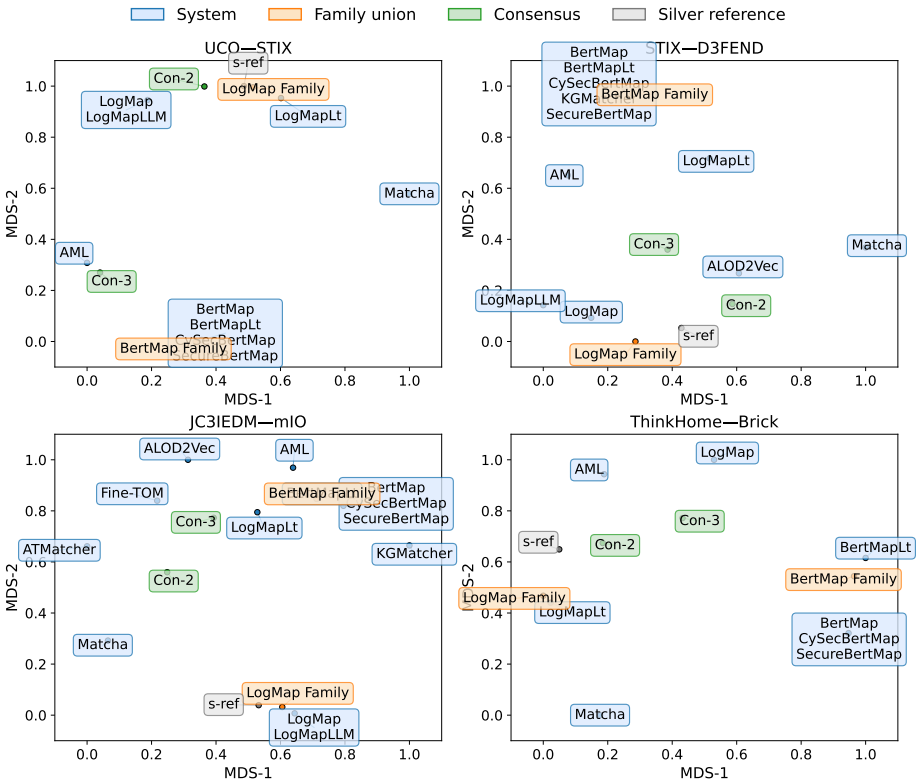

Fig. 2: Visual representation of the Jaccard distances among mapping sets.

Mapping comparison. Table 5 and the consensus mapping extraction have revealed a significant disparity among the evaluated systems, which is further illustrated in Figure 2. This confirms that the selected matching task involves the discovery of non-trivial mappings. The figure presents two-dimensional scatterplots of the Jaccard distances between the compared mapping sets. Proximity to the consensus mapping set is not necessarily an indicator of better quality; rather, it reflects a higher agreement with the consensus. For example, in *JC3IEDM-mIO!*, LogMapLt is close to the Con-3 consensus but far from *s-ref* (the manually-curated silver-standard reference). System families are also visualised, representing the aggregation of all mappings produced by the corresponding system variants. We emphasise that the silver-standard is derived from the outputs of the participating systems, its recall is inherently bounded by what these systems can collectively discover, and it will favour systems that resemble those used in its construction. Thus, it should be regarded as a partial reference rather than a complete gold standard. For the same reason, we prefer not to report the actual precision and recall values of the participating systems with respect to the silver standard, but rather the proximity among the relevant mapping sets, as shown in Figure 2.

Table 7: Unsatisfiable classes led by system, consensus and silver-standard mappings, computed over the whole merged ontology with the OWL 2 El reasoner ELK [32], marked by $\geq$ (lower-bound), or a complete OWL 2 DL reasoner (JFact [56], otherwise HermiT [19]). *incons.* denotes a merged TBox detected as inconsistent by ELK.

Matching task	System mappings						Aggregated mappings	
	AML	BertMap	BertMapLt	LogMap	LogMapLt	Matcha	Con-2	Silver
UCO-STIX	122 (24%)	110 (21%)	110 (21%)	134 (26%)	131 (25%)	127 (24%)	122 (24%)	133 (25%)
STIX-D3FEND	2448 (68%)	2441 (68%)	2444 (68%)	2516 (70%)	2516 (70%)	2509 (70%)	2509 (70%)	2506 (70%)
JC3IEDM-mIO!	0	0	0	0	0	0	0	0
JC3IEDM-Brick	0	0	0	0	0	0	0	0
JC3IEDM-Facility	0	0	0	0	0	0	0	0
ThinkHome-Brick	1123 (33%)	0	$\geq$49 (1.4%)	0	1375 (40%)	$\geq$652 (19%)	907 (27%)	874 (26%)
Brick-SmartEnv	$\geq$12	0	$\geq$11	0	$\geq$844 (34%)	incons.	$\geq$844 (34%)	$\geq$842 (34%)
CityOWL-Brick	26 (0.9%)	0	20 (0.7%)	0	20 (0.7%)	279 (9.9%)	30 (1.1%)	21 (0.7%)

Ontology compatibility. Reasoning with the input ontologies and the mappings may lead to logical errors (*e.g.*, unsatisfiabilities). An alignment $\mathcal{M}$ is incoherent if $\mathcal{O}_1 \cup \mathcal{O}_2 \cup \mathcal{M} \models A \sqsubset \bot$ (for any class A). Table 7 shows the logical errors led by system-computed mappings and the generated consensus and silver-standard alignments. It is worth noting that even systems implementing (approximate) reasoning techniques like AML and LogMap [54] lead to a large number of unsatisfiabilities (*e.g.*, *UCO-STIX* and *STIX-D3FEND*). This highlights a modelling disagreement among the DISO-OAEI ontologies, bringing an interesting challenge to the OAEI from the logical and reasoning point of view. The silver-standard alignment, which involved manual curation, also leads to unsatisfiable classes, emphasising the need for reasoning techniques within the ontology alignment pipeline. For the DISO-OAEI 2026 track, the silver standard has been treated to fix logical errors and annotate incoherent mappings.

4 The DISO ecosystem

Resources are made available through a small ecosystem of three repositories, as depicted in Figure 3. In particular, the collection of *defence and national security* ontologies is curated in the *diso* repository[27] and mirrored to Zenodo[28] upon every major release. Since some of the ontologies are packaged as networked component ontologies, we ship both a canonical distribution and a compact distribution. The compact distribution merges networked ontologies into a single file for the convenience of downstream consumers. For instance, the compact distribution is consumed by our alignment extraction pipeline *diso-mappings*[29], which is the second repository in our ecosystem. It allows contributors to easily download the compact distribution, register new matching systems, and iteratively improve the reference alignment. *diso-mappings* is a Python pipeline that consumes the DISO compact distribution and produces pairwise alignments between selected ontology pairs. It uses a configurable set of ontology matching

[27] https://github.com/city-artificial-intelligence/diso
[28] https://doi.org/10.5281/zenodo.20059506
[29] https://github.com/city-artificial-intelligence/diso-mappings

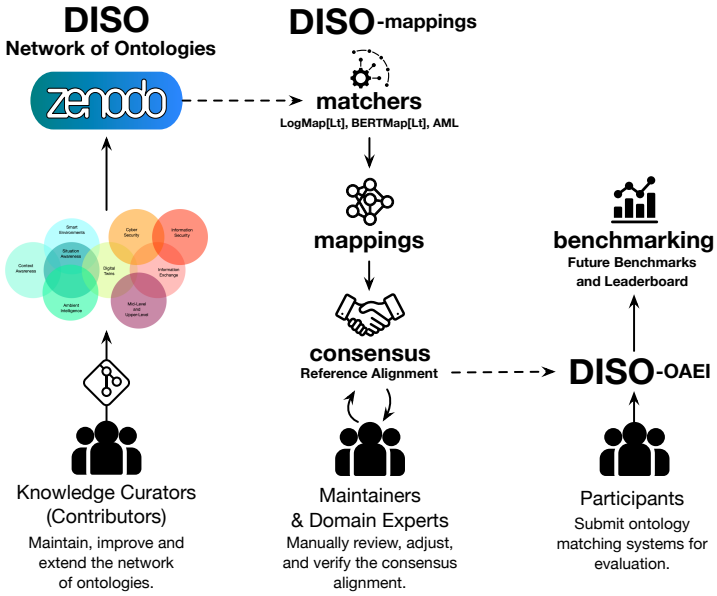

Fig. 3: The DISO ecosystem. The *diso* ontology collection aims to be extended through a collective effort by contributors and released through Zenodo. The diso-mapping pipeline runs a configurable, extendable set of matchers and aggregates their outputs into a family-based consensus alignment. The alignment is reviewed by maintainers and domain experts, and serves as a partial silver-standard reference alignment, forming the foundation for the *diso-oaei* track, where OAEI systems will be benchmarked.

systems (AML, LogMap, LogMapLt, BERTMap, and BERTMapLt by default; with an extendable Matcher base class that enables custom external matchers). The pipeline aggregates the per-system alignments into a consensus alignment via a family-based voting mechanism. This alignment is then manually verified, adapted and used as the basis for a partial silver-standard reference alignment. The computed alignments can easily be reproduced by following the steps within the repository's make workflow.

diso-oaei[30] is the home for the new DISO-OAEI track introduced in the OAEI 2026 edition. It contains the datasets, evaluation metrics, participation instructions, and will also host the OAEI benchmarking results.

5 Conclusions and sustainability of the resources

In this work, we have curated and described a collection of publicly available OWL ontologies covering the *defence and national security* domain, and proposed a new OAEI track for evaluating ontology matching systems on this collection. Our analysis identified eight candidate ontology pairs, spanning three distinct subdomains, supporting

[30] `https://github.com/city-artificial-intelligence/diso-oaei`

non-trivial ontology matching tasks across classes, properties, and instances. We released three resources in support of a rich and diverse track: *diso*, the curated ontology collection for defence, intelligence and national security; *diso-mappings*, a reproducible pipeline that aggregates the output of several state-of-the-art matchers into a consensus alignment via family-based voting; and *diso-oaei*, the home page for the new OAEI 2026 track. The consensus alignment was manually reviewed *(by the authors)*, leading to a silver-standard reference alignment.

This effort has been conducted as part of the GUARD project, funded by The Turing Defence & Security Grand Challenge. We are actively collaborating with experts from the UK Government intelligence community, the NDTP (National Digital Twin Programme), and the Dstl (Defence Science and Technology Laboratory), who will support the development and maintenance of the DISO ecosystem. The DISO ecosystems aim at serving both the broader research community and the UK's national needs on *defence and national security* with regard to the improvement of the interoperability of the relevant domain ontologies.

The *defence and national security* domain presents distinctive challenges for ontology matching: source ontologies span heterogeneous granularities (*e.g.*, upper-level, mid-level, temporal), numerous subdomains, and gold standard ground-truth coverage is limited. The OAEI community-driven evaluation will help to inform the future direction of research in this domain. The OAEI evaluation and the collaboration with domain experts will also support the extensions and improvement of the DISO ecosystem: ontologies, matching tasks, silver-standards, and, ultimately, the creation of an integrated network of DISO ontologies. For the OAEI 2026, we also plan to include automated benchmarking procedures, an active leaderboard, and a candidate mapping ranking task as in the bio-ml track [22] to attract the participation of machine learning systems.

DISO is not the first initiative to gather domain-specific ontologies. A prominent example is BioPortal [45], which has become the reference repository for biomedical ontologies. Similarly, the National Center for Ontological Research (NCOR) is developing a National Security Ontology Foundry,[31] with which we intend to explore potential collaborations. As DISO evolves, we will also explore adopting the OntoPortal technology to host and manage its ontologies [29].[32]

Acknowledgements. This research was supported by Turing Innovations Limited and The Alan Turing Institute's Defence and Security Programme via the project GUARD. It was also supported by FCT through the fellowship `https://doi.org/10.54499/2022.10557.BD` (Pedro Cotovio), the LASIGE Research Unit, ref. UID/00408/2025 and the CancerScan project, which received funding from the European Union's Horizon Europe Research and Innovation Action (EIC Pathfinder Open) under grant agreement No. 101186829. Views and opinions expressed are, however, those of the author(s) only and do not necessarily reflect those of The Alan Turing Institute, the European Union or the European Innovation Council and SMEs Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

[31] `https://ncor-network.org/`
[32] `https://ontoportal.org/`

Declaration of use of Generative AI. AI tools were used solely for grammar correction and minor language edits. They did not contribute to content creation, idea development, or substantive rewriting. The research design, experiments, analysis, and writing were carried out entirely by the authors.

References

1. Alirezaie, M., Hammar, K., Blomqvist, E.: SmartEnv as a network of ontology patterns. Semantic Web **9**(6), 903–918 (2018). https://doi.org/10.3233/SW-180303
2. Alirezaie, M., Renoux, J., Köckemann, U., Kristoffersson, A., Karlsson, L., Blomqvist, E., Tsiftes, N., Voigt, T., Loutfi, A.: An Ontology-based Context-aware System for Smart Homes: E-care@home. Sensors **17**(7) (2017). https://doi.org/10.3390/S17071586
3. Augusto, J.C., McCullagh, P.J.: Ambient Intelligence: Concepts and applications. Comput. Sci. Inf. Syst. **4**(1), 1–27 (2007). https://doi.org/10.2298/CSIS0701001A
4. Bailey, I., Beverley, J., Blackmore, H., Cola, A., Cripps, P., Colle, G.D., Donato, F., Hicks, A., Limbaugh, D., Milivinti, E., Partridge, C., Rafferty, R., Smith, B.: Comparing Information Exchange Standard and Basic Formal Ontology Design Patterns. In: Proceedings of the Joint Ontology Workshops (JOWO). CEUR Workshop Proceedings, CEUR-WS.org (2025), https://ceur-ws.org/Vol-4176/foust-6.pdf
5. Barnum, S.: Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX). Tech. rep., MITRE Corporation (2014), https://stixproject.github.io/getting-started/whitepaper/
6. Chen, H., Perich, F., Finin, T.W., Joshi, A.: SOUPA: Standard Ontology for Ubiquitous and Pervasive Applications. In: 1st Annual International Conference on Mobile and Ubiquitous Systems (MobiQuitous). pp. 258–267. IEEE Computer Society (2004). https://doi.org/10.1109/MOBIQ.2004.1331732
7. Chen, J., Lu, Y., Zhang, Y., Huang, F., Qin, J.: A management knowledge graph approach for critical infrastructure protection: Ontology design, information extraction and relation prediction. Int. J. Crit. Infrastructure Prot. **43**, 100634 (2023). https://doi.org/10.1016/J.IJCIP.2023.100634
8. Costa, D., Collins, M., Perl, S.J., Albrethsen, M., Silowash, G., Spooner, D.: An ontology for insider threat indicators: Development and application. In: Proceedings of the Ninth Conference on Semantic Technology for Intelligence, Defense, and Security. CEUR Workshop Proceedings, vol. 1304, pp. 48–53. CEUR-WS.org (2014), https://ceur-ws.org/Vol-1304/STIDS2014_T07_CostaEtAl.pdf
9. Cuenca Grau, B., Horrocks, I., Motik, B., Parsia, B., Patel-Schneider, P.F., Sattler, U.: OWL 2: The next step for OWL. J. Web Semant. **6**(4), 309–322 (2008), https://doi.org/10.1016/j.websem.2008.05.001
10. Dragisic, Z., Ivanova, V., Li, H., Lambrix, P.: Experiences from the anatomy track in the ontology alignment evaluation initiative. J. Biomed. Semant. **8**(1), 56:1–56:28 (2017), https://doi.org/10.1186/s13326-017-0166-5
11. Dragos, V.: Ontology modeling for intelligence: the ONTO-CIF model. In: Advances in Knowledge-Based and Intelligent Information and Engineering Systems - 16th Annual KES Conference. Frontiers in Artificial Intelligence and Applications, vol. 243, pp. 1543–1552. IOS Press (2012). https://doi.org/10.3233/978-1-61499-105-2-1543
12. Endsley, M.R.: Toward a Theory of Situation Awareness in Dynamic Systems. Human Factors **37**(1), 32–64 (1995). https://doi.org/10.1518/001872095779049543
13. Euzenat, J., Shvaiko, P.: Ontology Matching, Second Edition. Springer (2013)

14. Fallatah, O., Zhang, Z., Hopfgartner, F.: Kgmatcher results for OAEI 2021. In: Shvaiko, P., Euzenat, J., Jiménez-Ruiz, E., Hassanzadeh, O., Trojahn, C. (eds.) Proceedings of the 16th International Workshop on Ontology Matching co-located with the 20th International Semantic Web Conference (ISWC 2021), Virtual conference, October 25, 2021. pp. 160–166. CEUR Workshop Proceedings, CEUR-WS.org (2021), https://ceur-ws.org/Vol-3063/oaei21_paper8.pdf
15. Faria, D., Santos, E., Balasubramani, B.S., Silva, M.C., Couto, F.M., Pesquita, C.: AgreementMakerLight. Semantic Web **16**(2), SW–233304 (2025)
16. Faria, D., Silva, M.C., Cotovio, P., Ferraz, L., Balbi, L., Pesquita, C.: Results for Matcha and Matcha-DL in OAEI 2023. In: Proceedings of the 18th International Workshop on Ontology Matching co-located with the 22nd International Semantic Web Conference (ISWC 2023), Athens, Greece, November 7, 2023. CEUR Workshop Proceedings, vol. 3591, pp. 164–169. CEUR-WS.org (2023), https://ceur-ws.org/Vol-3591/oaei23_paper6.pdf
17. d'Avila Garcez, A., Lamb, L.C.: Neurosymbolic AI: the 3rd wave. Artif. Intell. Rev. **56**(11), 12387–12406 (2023). https://doi.org/10.1007/S10462-023-10448-W
18. Garijo, D., Poveda-Villalón, M.: Best Practices for Implementing FAIR Vocabularies and Ontologies on the Web (2020), https://arxiv.org/pdf/2003.13084
19. Glimm, B., Horrocks, I., Motik, B., Stoilos, G., Wang, Z.: HermiT: An OWL 2 Reasoner. J. Autom. Reason. **53**(3), 245–269 (2014). https://doi.org/10.1007/S10817-014-9305-1
20. Harrow, I., Jiménez-Ruiz, E., Splendiani, A., Romacker, M., Woollard, P., Markel, S., Alam-Faruque, Y., Koch, M., Malone, J., Waaler, A.: Matching disease and phenotype ontologies in the ontology alignment evaluation initiative. J. Biomed. Semant. **8**(1), 55:1–55:13 (2017). https://doi.org/10.1186/S13326-017-0162-9
21. He, Y., Chen, J., Antonyrajah, D., Horrocks, I.: BERTMap: A BERT-Based Ontology Alignment System. In: Thirty-Sixth AAAI Conference on Artificial Intelligence. pp. 5684–5691. AAAI Press (2022), https://doi.org/10.1609/aaai.v36i5.20510
22. He, Y., Chen, J., Dong, H., Jiménez-Ruiz, E., Hadian, A., Horrocks, I.: Machine Learning-Friendly Biomedical Datasets for Equivalence and Subsumption Ontology Matching. In: 21st International Semantic Web Conference. Lecture Notes in Computer Science, vol. 13489, pp. 575–591. Springer (2022), https://doi.org/10.1007/978-3-031-19433-7_33
23. Herron, D., Jiménez-Ruiz, E., Weyde, T.: On the Potential of Logic and Reasoning in Neurosymbolic Systems using OWL-based Knowledge Graphs. Neurosymbolic Artificial Intelligence **1** (April 2025). https://doi.org/10.1177/29498732251320043
24. Hertling, S., Paulheim, H.: ATBox results for OAEI 2022. In: Shvaiko, P., Euzenat, J., Jiménez-Ruiz, E., Hassanzadeh, O., Trojahn, C. (eds.) Proceedings of the 17th International Workshop on Ontology Matching (OM). pp. 153–157. CEUR Workshop Proceedings, CEUR-WS.org (2022), https://ceur-ws.org/Vol-3324/oaei22_paper4.pdf
25. Hogan, A., Blomqvist, E., Cochez, M., d'Amato, C., de Melo, G., Gutierrez, C., Kirrane, S., Gayo, J.E.L., Navigli, R., Neumaier, S., Ngomo, A.N., Polleres, A., Rashid, S.M., Rula, A., Schmelzeisen, L., Sequeda, J.F., Staab, S., Zimmermann, A.: Knowledge graphs. ACM Comput. Surv. **54**(4), 71:1–71:37 (2022), https://doi.org/10.1145/3447772
26. Jiménez-Ruiz, E., Herron, D., Dilworth, J.: Phase 1 Report (GUARD / G2049a): Ensuring Interoperable and Trustworthy Knowledge Graphs for Defence and National Security AI (May 2026), https://openaccess.city.ac.uk/id/eprint/37459/
27. Jiménez-Ruiz, E., Cuenca Grau, B.: LogMap: Logic-Based and Scalable Ontology Matching. In: The Semantic Web - ISWC 2011 - 10th International Semantic Web Conference. Lecture

Notes in Computer Science, vol. 7031, pp. 273–288. Springer (2011), https://doi.org/10.1007/978-3-642-25073-6_18
28. Jiménez-Ruiz, E., Cuenca Grau, B., Zhou, Y., Horrocks, I.: Large-scale interactive ontology matching: Algorithms and implementation. In: ECAI - 20th European Conference on Artificial Intelligence. Frontiers in Artificial Intelligence and Applications, vol. 242, pp. 444–449. IOS Press (2012), https://doi.org/10.3233/978-1-61499-098-7-444
29. Jonquet, C., Graybeal, J.B., Bouazzouni, S., Dorf, M., Fiore, N., Kechagioglou, X., Redmond, T., Rosati, I., Skrenchuk, A., Vendetti, J., Musen, M.A.: Ontology repositories and semantic artefact catalogues with the ontoportal technology. In: 22nd International Semantic Web Conference (ISWC). Lecture Notes in Computer Science, vol. 14266, pp. 38–58. Springer (2023). https://doi.org/10.1007/978-3-031-47243-5_3
30. Kaloroumakis, P.E., Smith, M.J.: Toward a Knowledge Graph of Cybersecurity Countermeasures. Tech. rep., MITRE Corporation (2021), https://d3fend.mitre.org/resources/D3FEND.pdf
31. Karabulut, E., Pileggi, S.F., Groth, P., Degeler, V.: Ontologies in digital twins: A systematic literature review. Future Gener. Comput. Syst. **153**, 442–456 (2024). https://doi.org/10.1016/J.FUTURE.2023.12.013
32. Kazakov, Y., Krötzsch, M., Simancík, F.: The incredible ELK - from polynomial procedures to efficient reasoning with $\mathcal{EL}$ ontologies. J. Autom. Reason. **53**(1), 1–61 (2014). https://doi.org/10.1007/S10817-013-9296-3
33. Knorr, L., Portisch, J.: Fine-tom matcher results for OAEI 2021. In: Shvaiko, P., Euzenat, J., Jiménez-Ruiz, E., Hassanzadeh, O., Trojahn, C. (eds.) Proceedings of the 16th International Workshop on Ontology Matching co-located with the 20th International Semantic Web Conference (ISWC 2021), Virtual conference, October 25, 2021. pp. 144–151. CEUR Workshop Proceedings, CEUR-WS.org (2021), https://ceur-ws.org/Vol-3063/oaei21_paper6.pdf
34. Köckemann, U., Alirezaie, M., Renoux, J., Tsiftes, N., Ahmed, M.U., Morberg, D., Lindén, M., Loutfi, A.: Open-Source Data Collection and Data Sets for Activity Recognition in Smart Homes. Sensors **20**(3) (2020). https://doi.org/10.3390/S20030879
35. Leblanc, E., Nguyen, D., Balduccini, M., Regli, W., Kopena, J., Wambold, T.: Military ontologies for information dissemination at the tactical edge. In: Joint Ontology Workshops. CEUR (2015)
36. Lourenço, B., Adão, P., Ferreira, J.F., Marques, M.M., Vaz, C.: Structuring Security: A Survey of Cybersecurity Ontologies, Semantic Log Processing, and LLMs Application. CoRR **abs/2510.16610** (2025). https://doi.org/10.48550/ARXIV.2510.16610
37. Lushnei, S., Shumskyi, D., Shykula, S., Jiménez-Ruiz, E., d'Avila Garcez, A.: Large Language Models as Oracles for Ontology Alignment. In: 19th Conference of the European Chapter of the Association for Computational Linguistics (EACL 2026). Association for Computational Linguists (2026)
38. Maryasin, O.: Home Automation System Ontology for Digital Building Twin. In: 2019 XXI International Conference Complex Systems: Control and Modeling Problems (CSCMP). pp. 70–74 (2019). https://doi.org/10.1109/CSCMP45713.2019.8976546
39. Matthews, M., Shattuck, L., Grham, S., Weeks, J., Endsley, M., Strater, L.: Situation Awareness for Military Ground Forces: Current Issues and Perspectives. Human Factors **45**(4), 351–355 (2001), https://www.researchgate.net/publication/273594666_Situation_Awareness_for_Military_Ground_Forces_Current_Issues_and_Perspectives
40. Meriah, I., Rabai, L.B.A., Khédri, R.: Building a comprehensive and multi-dimensional information security ontology: elicitation process and OWL implementation. Knowl. Inf. Syst. **67**(1), 167–195 (2025). https://doi.org/10.1007/S10115-024-02308-Y

41. Morosoff, P., Rudnicki, R., Bryant, J., Farrell, R., Smith, B.: Joint Doctrine Ontology: A Benchmark for Military Information Systems Interoperability. In: 10th Conference on Semantic Technology for Intelligence, Defense, and Security. CEUR Workshop Proceedings, vol. 1523. CEUR-WS.org (2015), https://ceur-ws.org/Vol-1523/STIDS_2015_T01_Morosoff_etal.pdf
42. Mundie, D.A., Ruefle, R., Dorofee, A.J., Perl, S.J., McCloud, J., Collins, M.: An incident management ontology. In: Proceedings of the Ninth Conference on Semantic Technology for Intelligence, Defense, and Security. CEUR Workshop Proceedings, vol. 1304, pp. 62–71. CEUR-WS.org (2014), https://ceur-ws.org/Vol-1304/STIDS2014_T09_MundieEtAl.pdf
43. NATO/MIP: The Joint C3 Information Exchange Data Model Overview. Tech. rep., NATO/MIP (2007), https://brainsciencesjournal.org/2007.JC3IEDM.pdf
44. Naveed, H., Khan, A.U., Qiu, S., Saqib, M., Anwar, S., Usman, M., Akhtar, N., Barnes, N., Mian, A.: A comprehensive overview of large language models. ACM Trans. Intell. Syst. Technol. **16**(5) (Aug 2025). https://doi.org/10.1145/3744746
45. Noy, N.F., Shah, N.H., Whetzel, P.L., Dai, B., Dorf, M., Griffith, N., Jonquet, C., Rubin, D.L., Storey, M.D., Chute, C.G., Musen, M.A.: BioPortal: ontologies and integrated data resources at the click of a mouse. Nucleic Acids Res. **37**(Web-Server-Issue), 170–173 (2009), https://doi.org/10.1093/nar/gkp440
46. Obrst, L., Chase, P., Markeloff, R.: Developing an Ontology of the Cyber Security Domain. In: Proceedings of the Seventh International Conference on Semantic Technologies for Intelligence, Defense, and Security. CEUR Workshop Proceedings, vol. 966, pp. 49–56. CEUR-WS.org (2012), https://ceur-ws.org/Vol-966/STIDS2012_T06_ObrstEtAl_CyberOntology.pdf
47. Oltramari, A., Cranor, L.F., Walls, R.J., McDaniel, P.D.: Building an Ontology of Cyber Security. In: Proceedings of the Ninth Conference on Semantic Technology for Intelligence, Defense, and Security. CEUR Workshop Proceedings, vol. 1304, pp. 54–61. CEUR-WS.org (2014), https://ceur-ws.org/Vol-1304/STIDS2014_T08_OltramariEtAl.pdf
48. Portisch, J., Paulheim, H.: ALOD2Vec matcher results for OAEI 2021. In: Proceedings of the 16th International Workshop on Ontology Matching co-located with the 20th International Semantic Web Conference (ISWC). pp. 117–123. CEUR Workshop Proceedings, CEUR-WS.org (2021), https://ceur-ws.org/Vol-3063/oaei21_paper2.pdf
49. Pour, M.A.N., Blomqvist, E., Cotovio, P.G., Coulet, A., Ferraz, L., Hertling, S., Jain, S., Jiménez-Ruiz, E., Kraus, F., Lambrix, P., Li, H., Li, Y., Liu, X., Monnin, P., Paulheim, H., Pesquita, C., Sharma, A., Shvaiko, P., Silva, M.C., Sousa, G., Trojahn, C., Vatascinová, J., Yaman, B., Zamazal, O., Zhou, L.: Results of the Ontology Alignment Evaluation Initiative 2025. In: 20th International Workshop on Ontology Matching (OM). pp. 105–139 (2025)
50. Poveda-Villalón, M., Suárez-Figueroa, M.C., Garcia-Castro, R., Gómez-Pérez, A.: A Context Ontology for Mobile Environments. In: Proceedings of the Second Workshop on Context, Information and Ontologies, CIAO@EKAW. CEUR Workshop Proceedings, CEUR-WS.org (2010), https://ceur-ws.org/Vol-626/regular3.pdf
51. Reinisch, C., Kofler, M.J., Iglesias, F., Kastner, W.: ThinkHome Energy Efficiency in Future Smart Homes. EURASIP J. Embed. Syst. **2011** (2011). https://doi.org/10.1155/2011/104617
52. Rivadeneira, W., Gómez, O.S.: Cybersecurity Ontologies: A Systematic Literature Review. ReCIBE, Revista electrónica de Computación, Informática, Biomédica y Electrónica **9**, C1–C18 (2021). https://doi.org/10.32870/recibe.v9i2.181
53. Sikos, L.F.: Cybersecurity Knowledge Graphs. Knowl. Inf. Syst. **65**(9), 3511–3531 (2023). https://doi.org/10.1007/S10115-023-01860-3

54. Solimando, A., Jiménez-Ruiz, E., Guerrini, G.: Minimizing conservativity violations in ontology alignments: algorithms and evaluation. Knowl. Inf. Syst. **51**(3), 775–819 (2017). https://doi.org/10.1007/S10115-016-0983-3
55. Stavropoulos, T.G., Vrakas, D., Vlachava, D., Bassiliades, N.: BOnSAI: A Smart Building Ontology for Ambient Intelligence. In: 2nd International Conference on Web Intelligence, Mining and Semantics, WIMS. pp. 30:1–30:12. ACM (2012). https://doi.org/10.1145/2254129.2254166
56. Tsarkov, D., Horrocks, I.: Fact++ description logic reasoner: System description. In: Furbach, U., Shankar, N. (eds.) 3rd International Joint Conference on Automated Reasoning (IJCAR). Lecture Notes in Computer Science, vol. 4130, pp. 292–297. Springer (2006). https://doi.org/10.1007/11814771_26
57. Valero, J.M.J., Martínez, A.L., Sánchez, P.M.S., Navarro-Martínez, D., López, R.V., Lacal, J.I.R., Vivar, A.L., Monge, M.A.S., Pérez, M.G., Pérez, G.M.: Unlocking the potential of knowledge graphs: A cyber defense ontology for a knowledge representation and reasoning system. In: 19th International Conference on Availability, Reliability and Security (ARES). pp. 73:1–73:9. ACM (2024). https://doi.org/10.1145/3664476.3670916
58. Valiente, M.C., Machín, R., García-Barriocanal, E., Sicilia, M.Á.: An Ontology-Based Integrated Approach to Situation Awareness for High-Level Information Fusion in C4ISR. In: Advanced Information Systems Engineering Workshops. pp. 513–527. Springer (2011)
59. Wang, Z., Zhu, H., Liu, P., Sun, L.: Social engineering in cybersecurity: a domain ontology and knowledge graph application examples. Cybersecur. **4**(1), 31 (2021). https://doi.org/10.1186/S42400-021-00094-6
60. Yongqin, H., Xushan, C., Anlian, Y., Shuo, P.: Research on application of knowledge graph in war archive based on big data. In: Big Data and Security. pp. 234–247. Springer Nature (2023)
61. Zamazal, O., Svátek, V.: The ten-year ontofarm and its fertilization within the onto-sphere. J. Web Semant. **43**, 46–53 (2017). https://doi.org/10.1016/J.WEBSEM.2017.01.001