GIS Odyssey Journal

2026 • Volume 6 • Number 2

https://doi.org/10.57599/gisoj.2026.6.2.23

Jaroslaw Koszela[1], Arkadiusz Orzeł[2]

CYBERNER SEMANTIC METAMODEL AS AN INTERMEDIATE LAYER FOR GEOSPATIAL DATA TRANSFORMATION IN CYBERSECURITY SYSTEMS

Abstract: Modern cybersecurity systems process data from heterogeneous sources, a significant part of which carries geospatial information such as IP address geolocation, geographic coordinates, hostnames, data center identifiers, cloud regions and location data of users and assets. Because widely used schemas – the Elastic Common Schema (ECS), Structured Threat Information Expression (STIX) and the Open Cybersecurity Schema Framework (OCSF) – represent this information in different ways, transformations between them often lead to the loss of semantic context. The article presents a conceptual approach in which the CyberNER semantic metamodel acts as an intermediate layer supporting the transformation of geospatial data between heterogeneous cybersecurity schemas. CyberNER is not another target schema, but an M2-level metamodel based on entities, semantic roles, relationships, attributes and contexts, in which the geospatial layer is a specialization of the semantic core rather than an autonomous domain model. The proposed approach is illustrated with a proof-of-concept transformation example and is expected to increase the completeness and fidelity of the semantic transformation of geospatial data and to reduce information loss in relation to direct transformations based solely on field mapping. The study is conceptual and methodological in character; its main limitation is the lack of large-scale quantitative validation, which is indicated as the direction of further research.

Keywords: CyberNER, semantic metamodel, geospatial data, data transformation, cybersecurity, ECS, STIX, OCSF, cognitive SOC

Received: 4 May 2026; accepted: 29 June 2026; revised: 22 July 2026

[1]Military University of Technology, Cybernetics Faculty, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0001-9774-1873, email: jaroslaw.koszela@wat.edu.pl

[2] Military University of Technology, Cybernetics Faculty, Warsaw, Poland, ORCID ID: https://orcid.org/0000-0003-0684-1946, email: arkadiusz.orzel@wat.edu.pl

Introduction

Modern cybersecurity systems operate in conditions of increasing data heterogeneity. Security events originate simultaneously from operating systems, applications, network devices, security sensors, cloud platforms, threat intelligence sources, and other relevant infrastructure elements. Each of these sources uses its own way of describing events, its own naming conventions, and a different structure of information representation. As a result, two records describing semantically similar operational phenomenon may require completely different interpretations before they become useful from the point of view of security analysis.

Geospatial information is a particularly important category among this data. In the domain of cybersecurity, it is not limited to geographic coordinates. It also includes the geolocation of IP addresses, endpoint locations, data center identifiers, cloud providers' regions and availability zones, network segments, and other forms of logical and infrastructure location. This information plays a vital role in incident correlation, event attribution, anomaly detection, risk analysis, distributed infrastructure protection, and compliance with regulatory requirements for data location (Alarabi, 2025; Esri, 2014).

The problem is particularly evident in the context of widespread security data schemas, such as the Elastic Common Schema (ECS), Structured Threat Information Expression (STIX), and the Open Cybersecurity Schema Framework (OCSF), which represent geospatial information in a different way. These differences concern not only field names, but also the level of detail, the relationship model, the way locations are encoded, and the extent of the metadata retained. As a consequence, the transformation between schemas often leads to the loss of some semantic meaning, impoverishment of context, or the generation of a formally correct representation that requires completion analytically.

Dominant approaches solve this problem primarily by using parsing rules and direct mapping of data to specific target schemes. These solutions are effective in well-known and relatively stable environments, but their maintenance is becoming more and more expensive with the increase in the number of sources, formats and output models. Each new source or each change in the data structure requires the preparation of new data parsers or configurations. The burden of interpretation thus falls upon the technical implementation, and not on the side of the model describing the meaning of the data.

As a consequence, the transformation of geospatial data should not be considered only as a problem of technical field mapping. It requires the introduction of a semantic layer that allows the representation of the meaning of data regardless of the specific input and output scheme. Such a function can be performed by the CyberNER metamodel, understood as an intermediate layer that allows for recognition, unification, normalization and transformation of the meaning of data before it is mapped to the selected target model.

The aim of the article is to present the concept of using CyberNER as an intermediate layer for the transformation of geospatial data in cybersecurity systems. It is assumed that the use of a semantic intermediate metamodel increases the completeness of

transformation, reduces information loss and makes the standardization process independent of a specific target scheme. At the same time, the geospatial problem is embedded in a broader Cognitive SOC architecture, in which data analysis does not end with the syntactic ordering of information, but also includes the interpretation of the meaning of events, their participants and the relationships between them.

Recent work on cybersecurity data standardization has focused primarily on target schemas used for data exchange and analytics. ECS provides a practical normalization layer for operational telemetry (Elastic, 2025), STIX offers an object-oriented representation of cyber threat intelligence (OASIS OPEN, 2025), whereas OCSF aims at a broader event-oriented interoperability model (OCSF, 2026). Although these standards significantly improve syntactic interoperability, they do not fully address the problem of semantic equivalence between heterogeneous representations of the same operational phenomenon, especially when geospatial attributes are distributed across different objects, contexts and levels of detail.

A complementary line of research concerns ontology-based integration and mediation models. Studies on semantic integration emphasize the role of conceptual layers that separate source representation from target representation, while cybersecurity ontologies such as UCO show the analytical value of explicit semantic relations in cyber data processing (Bakirtzis et al., 2022). However, existing approaches are usually oriented either toward formal knowledge representation or toward a specific exchange standard, and much less attention is given to an intermediate semantic model dedicated to practical transformation of security telemetry with geospatial context.

Against this background, the research gap addressed in this article concerns the lack of an intermediate semantic layer that would jointly preserve event context, provenance, uncertainty and geospatial meaning during schema transformation. The contribution of the paper is therefore twofold: first, it structures CyberNER as an M2-level semantic metamodel; second, it demonstrates how this metamodel can support geospatial transformation between heterogeneous cybersecurity schemas.

Background of the problem and research motivation. Modern SOC environments are evolving from static data processing models to more adaptive, contextual, and cognitive architectures (Fig. 1). In this approach, data analysis should not be limited to the technical matching of fields and saving the document in the target schema but should also include recognizing what phenomenon has been observed, what elements are involved in it, and what dependencies occur between them.

Standards such as ECS, STIX and OCSF have the function of organizing and normalizing security data. They define the way information is represented, but they do not fully solve the problem of semantic interpretation of input data. Therefore, it is possible that a document is saved according to the requirements of a specific schema but still does not create a coherent and globally interpretable representation of an event. Structural conformity is not the same as semantic conformity.

This phenomenon takes on particular significance in relation to geospatial data. The same location information can be expressed as an IP address, city name, country code, geographical coordinates, cloud service region identifier or data center name (Sohacheski

& Itzhak, 2017). From a technical point of view, these are different types of data and different schema fields. From an analytical point of view, however, they refer to a common dimension of location that requires uniform treatment and embedding in the context of a security event.

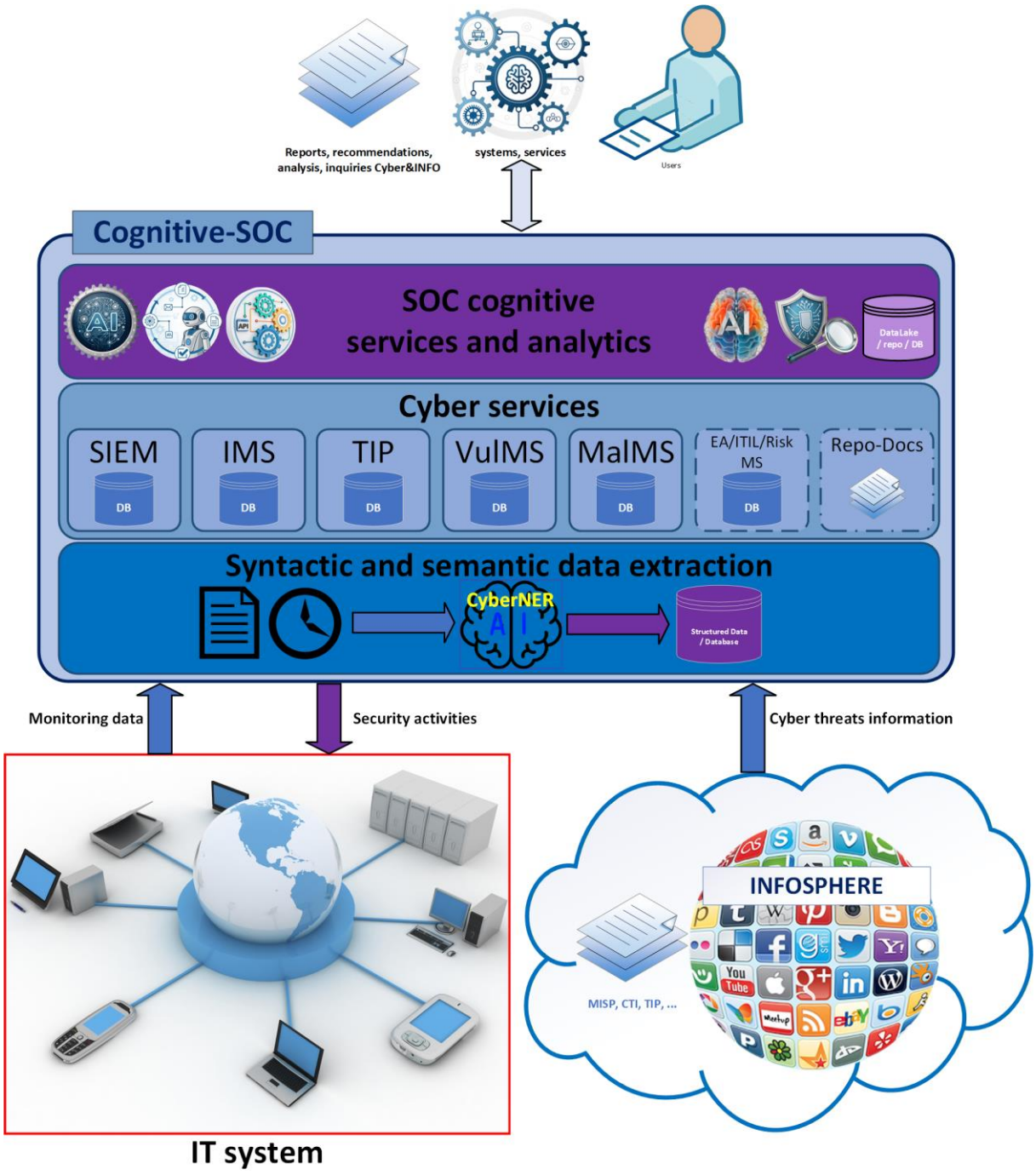

Fig. 1. Concept of Cognitive SOC
Source: own study

The introduction of an intermediate layer is therefore justified from both an integration and analytical perspective. This layer should not be another final schema, but a common interpretative plan for data coming from different sources and directed to

different target models. CyberNER responds to this need because it does not define the final form of the document, but the concepts used to describe the meaning of the data: entities, roles, relationships, attributes and contexts. Thanks to this, it becomes possible to semantically organize the data even before its technical transformation.

Material and methods

The study has a conceptual-methodological character supported by an illustrative transformation example. The research material consists of representative security data structures used in operational practice, in particular logs and records compatible with ECS, STIX and OCSF, as well as a demonstrative log line containing geospatial attributes. The method combines conceptual modeling, comparative schema analysis and stepwise semantic mapping through an intermediate representation defined by CyberNER.

From the methodological perspective, the proposed approach was developed in four stages: identification of semantically relevant elements in source schemas, definition of an abstract set of entities and relations at the M2 level, formulation of transformation rules from the intermediate representation to the target schema, and qualitative evaluation of the transformation result in terms of semantic completeness, traceability and preservation of geospatial context.

CyberNER as a semantic metamodel. CyberNER is designed as an intermediate layer that allows you to interpret the meaning of security events regardless of the data source and target schema. It creates a common semantic layer in which it becomes possible to map the meaning of data before it is written to a specific output model.

The basic assumption of CyberNER is to move away from treating a single log record as a complete unit of analysis. The model assumes that the significance of an observation is revealed only after taking into account a set of entities, their roles and relationships describing a specific fragment of operational reality. As a result, CyberNER does not model data as a flat set of fields, but as a semantic structure that allows for the description of an event, its participants, the subject of action, the infrastructural context and the time dimension.

This approach is particularly valuable in heterogeneous environments, where different sources describe similar phenomena using different fields, conventions, and structures. CyberNER shifts the burden of interpretation from the level of parsers and technical rules to the level of the conceptual model. This allows the same event to be recognized as semantically equivalent, even though it will be described differently in different sources.

Semantic context as the basic unit of analysis. In CyberNER, the basic unit of analysis is not a single log record, but a semantic context, understood as an ordered set of entities, their roles and relationships, which together describe a single event or a fragment of a broader security scenario. Such an approach is a significant departure from classic approaches based solely on the structure of the log.

The importance of this assumption becomes especially evident in a situation where a single log does not contain complete information about the nature of the observed

activity. An example HTTP entry containing the source address, destination address, request method, resource and response code can be saved as a set of independent fields in a classic system. In CyberNER, the same observation is interpreted as a minimal semantic context in which it is possible to identify the actor responsible for the operation, the source-target relationship for network communication, the type of action, the object of the operation and its result. Therefore, the model answers not only the question of what fields occurred in the log, but above all the question of who performed a particular action, against which resource and with what effect.

The importance of context increases even more in the analysis of events distributed over time. A single log can only indicate a login attempt, a process starts, or access to a resource. Only a combination of such observations allows you to recognize an operational scenario, for example, gaining access, executing a privileged command, and reading a sensitive file. For this reason, CyberNER treats context as a proper unit of analysis, not just a supporting structure grouping source fields.

Formal definition of the model. In a formal approach, CyberNER can be treated as a metamodel consisting of an ordered set of entities, roles, relationships, contexts and attributes. Assuming such an assumption, the model can be written in the form of:

$$CyberNER = (E, R, T, C, A) \tag{1}$$

where:
E - a set of entities,
R - a set of semantic roles,
T - a set of relationship types,
C - a set of contexts,
A - A set of attributes assigned to entities and relationships.

In this view, entities represent the basic elements of an event description, roles define the function of entities within a given context, relationships describe the relationships between entities, and attributes store their detailed properties, such as identifiers, timestamps, addresses, parameter values, and operation results. Such formalization allows you to separate the level of meaning from the level of a specific technical representation.

A single semantic context can be described as a graph:

$$c = (V_c, E_c) \tag{2}$$

where:
$V_c \subseteq E$is a set of entities occurring in a given context,
$E_c \subseteq T$means a set of relationships between these entities.

A graph representation allows you to formally describe both the structure of an event and the relationships between its elements. In practice, this means the ability to model dependencies such as connection initiation, access to a resource or communication

between hosts. Thanks to this, CyberNER is not just a catalog of entity classes, but a model that allows for relational mapping of security events.

CyberNER as an M2-level metamodel. CyberNER is positioned at the M2 level, i.e. at the level of a metamodel that describes the concepts used for semantic interpretation of data, rather than its direct technical representation. This means that the model does not operate at the level of individual log records or at the level of specific fields present in schemas such as ECS, STIX, OCSF or CIM, but defines more general categories of description, including entities, roles, relationships, attributes and contexts.

Adopting this level of abstraction allows you to separate the semantic layer from the implementation layer. As a result, the same event can be recognized as semantically equivalent, even if it is written in different systems using different field names, different document structures, or different data modeling conventions. CyberNER therefore does not act as another target format, but is a common conceptual layer, mediating between the input data and the final schemas.

In this approach, source observations can be treated as the M0 level, data schemas used by specific tools as the M1 level, and CyberNER as the M2 level, whose task is to ensure semantic consistency between them. Such a model organization makes it possible to analyze and compare events not on the basis of their structural similarity, but on the basis of their importance. From the perspective of the Cognitive SOC architecture, this is important because it allows you to build an environment in which data can be interpreted uniformly regardless of its source, format and target processing system.

Main entities of the CyberNER model. The CyberNER model is based on a set of basic semantic classes that form its core layer and remain independent of a specific data source or target schema. These classes include actor, host, network, process, object, event and time. Their task is to capture the most important elements that make up the description of a security event, without referring to the implementation names of fields characteristic of specific standards.

The actor class describes the entity involved in the execution of an action, which can be a user, account, system, or other entity that initiates an activity. The host class refers to the environment in which the event occurs, including both physical devices and virtual resources such as virtual machines, cloud instances, and containers. The network class is used to represent the communication aspect of an event, including addresses, ports, protocols, transmission direction, and other characteristics that describe the flow of data between systems.

The process class includes actions performed within the system, such as starting an application, executing a command, starting a script, or a child process. The object class represents the resource that is the subject of the operation, such as a file, service, URL, database, registry item, or other infrastructure object. The event class refers to the very fact that a specific activity occurs, while time introduces a time dimension, allowing you to determine when an event occurs and embed it in a wider sequence of observations.

A set of entities defined in this way includes the most important components needed to describe an event: the subject of the activity, the environment of its implementation, the communication channel, the object of influence, the course of the activity itself and its

location in time. Thanks to this, CyberNER allows you to build a representation that preserves both the technical and operational sense of the observed data. Since these entities are not tied to a single standard of representation, they can serve as a universal conceptual layer used when mapping to different target models.

Hierarchical interpretation and expandability of the model. An important feature of CyberNER is the ability to interpret events hierarchically. This means that an observation can initially be assigned to a general class and then refined to more and more specialized levels of description. This mechanism allows you to move from broad categories, such as system or network activity, to more specific classes, such as network events, authentication events, HTTP request, file access, or command execution.

This solution has significant practical value. It allows you to start the analysis even when the data is incomplete, ambiguous, or comes from a new source for which detailed interpretative rules have not yet been prepared. As additional context emerges, the system can move to more detailed levels of taxonomy, refining the interpretation without having to change the underlying model. This allows CyberNER to support both the recognition of known event classes and the embedding of new observations in the existing semantic structure.

From the perspective of the Cognitive SOC architecture, hierarchical interpretation allows you to compare events at different levels of abstraction, group similar observations, and adapt to new data sources without rebuilding the core of the model. The ability to maintain a stable semantic level while being interpretative extensible is one of the most important features of CyberNER.

Geospatial dimension of the CyberNER model. Against the background of the presented semantic core, geospatial data should be treated as a specialized interpretive dimension embedded in the main entities of CyberNER, and not as an independent domain model. This means that location does not function as a separate entity detached from a security event, but as a property or relationship related to an actor, host, network communication, object or infrastructure.

In practice, geospatial information can be assigned to different elements of context. For an actor entity, it can mean the location of a user, organization, or account. For an entity host, the physical location of a device, data center, or cloud region. For a network entity, the geolocation of IP addresses, ASN, operator affiliation, or network topology. For the object entity, the location of a resource, service, or piece of logical infrastructure. This ensures that geospatial data is modeled not as a collection of individual fields, but as an element of the semantic context of an event.

In order to organize this layer, three complementary classes of geospatial entities can be distinguished within CyberNER.

Physical location entities describe the location of objects in geographic space. They include geographic coordinates, administrative unit names, country codes, city names, zip codes, elevation, and location uncertainty level. In the CyberNER model, they can represent both precise positions and approximate locations, such as at the country or region level.

Logical location entities represent a location in non-physical spaces that are operationally important from a security perspective. These include cloud regions, availability zones, data centers, administrative domains, network segments, subnets, and VLANs. These entities are especially important in multicloud and distributed environments.

Network location entities describe the identifiers of resources in the network communication space, such as IPv4 and IPv6 addresses, host names, FQDNs, MAC addresses, ASNs, carriers, network service providers, and connection types. In practice, they are often the starting point for further data enrichment, for example by IP geolocation.

Such an approach maintains the consistency of the entire model. First, there is a general metamodel describing the meaning of security events, and then geospatial specialization is developed within it. From a methodological point of view, this solution is stronger than building a separate location model, because it shows that the geospatial component remains an integral part of the overall semantic representation.

Attributes of quality, provenance and uncertainty. An important feature of CyberNER is the storage of not only the semantic values themselves, but also information about their origin, quality and level of uncertainty. This is particularly important for geospatial data, as many of them are approximate, augmented, or derived from external sources of enrichment.

Each geospatial entity can be described by a set of meta-attributes that include, but are not limited to, the source schema, the source field path, the extraction or enrichment method, the confidence level, the location precision level, the processing timestamp, and the enrichment data source. This allows CyberNER to maintain full trace of the transformation.

This is especially important for the geolocation of IP addresses, data from cloud platforms, and context-based information. The model avoids imposing artificial precision where the source does not provide it but allows you to explicitly record whether the location has been determined at the level of country, city or exact coordinates. This approach increases the reliability of the representation and reduces the risk of erroneous analytical correlations.

Data transformation process using CyberNER. Data transformation using CyberNER can be described as a multi-step process involving extraction, intermediate representation, enrichment and output transformation.

Extraction phase. The first step is to identify the semantic elements in the input. For structured sources, this process can rely on schematic adapters that recognize the meaning of fields based on known mappings. For semi-structured or unstructured data, semantic extraction mechanisms must be used.

Indirect representation phase. Once the data is extracted, it is mapped to CyberNER structures. At this stage, source values are no longer treated as technical fields and become instances of entities, relationships, and attributes embedded in a semantic context. For geospatial data, this includes assigning it to the appropriate physical, logical, and network location classes and binding it to an actor, host, communication, or object.

Enrichment phase. At the intermediate layer, it is possible to enrich data using external sources of knowledge. This includes, but is not limited to, geolocation of IP addresses, completion of ASNs, operators, network service providers, cloud regions, and compatibility between claimed and infused location. However, enrichment should not lead to the unconditional overwriting of source data, but to the parallel storage of origin and certainty information.

Initial transformation phase. The last stage consists in mapping the CyberNER representation to the selected target schema. At this level, it is possible to write data to fields specific to ECS, STIX or OCSF, as well as use metadata spaces or extensions for elements that do not have a direct equivalent in the target schema. This retains more of the meaning than in approaches based solely on direct field-to-field mapping.

The role of NER and LLM in the CyberNER architecture. It is important to distinguish between CyberNER as a metamodel and NER and LLM as semantics discovery mechanisms. CyberNER defines semantics, while NER and LLM models are responsible for recognizing it in inputs. The NER model supports the identification of entities and their underlying classes (Ech-Chammakhy et al., 2025; Zhang et al., 2026), while language models can be used to interpret new, ambiguous or previously non-existent data structures.

This distinction is of significant methodological importance. CyberNER is not a parser, but a conceptual layer. NER and LLM therefore do not replace the model but are tools for assigning inputs to its structures. The combination of a stable semantic model with adaptive extraction and interpretation mechanisms makes it possible to build an architecture in which the meaning of data is not encoded only in parsers and transformation rules. Semantics are separated from implementation, which makes it easier to develop the system, compare alternative interpretations, and integrate with multiple target schemes.

Results

The result of applying the proposed method is illustrated with a sample authentication log enriched with geospatial attributes and then transformed through CyberNER into an ECS-compatible JSON structure. The example is used to show that the intermediate semantic classification step preserves the meaning of the event more explicitly than a direct field-to-field transformation.

In the presented example, the source log (Table 1) is first interpreted at the CyberNER level before being transformed into the ECS-compatible structure used by Elasticsearch. Individual values from the log are assigned to CyberNER semantic classes and roles. The timestamp is classified as a *Time* entity with the role of *event_time*, the user identifier is classified as an *Actor* in the role of *initiator*, while the failed login operation is represented as an *Event* in the role of *observed_activity*. The source IP address is interpreted as a *NetworkLocation* entity, whereas the city, country and coordinates are represented as a *PhysicalLocation* entity describing the geospatial origin of the event.

Table 1. Sample log line with geo data

2026-04-30T12:21:10Z src_ip=83.24.10.15 user=akowalski action=login_result status=failed city=Warsaw country=Poland lat=52.2297 lon=21.0122

Source: own study

Table 2. Transforming the syntax and semantics of the example in Table 1 using the CyberNER to JSON format

```
{
 "@timestamp": "2026-04-30T12:21:10Z",
 "event": {
  "category": ["authentication"],
  "action": "login_result",
  "outcome": "failure"
 },
 "source": {
  "ip": "83.24.10.15",
  "geo": {
   "city_name": "Warsaw",
   "country_name": "Poland",
   "country_iso_code": "PL",
   "location": {
    "lat": 52.2297,
    "lon": 21.0122
   }
  }
 },
 "cyberner": {
  "semantic_class": "NetworkLocation",
  "semantic_role": "source_location",
                "context_id": "ctx-20260430-0001"
            }
}
```

Source: own study

CyberNER introduces an explicit semantic classification step between the raw log and the target ECS document. Therefore, the transformation is not limited to changing field names, but includes the recognition of entities, roles and relationships that define the meaning of the observed security event.

This intermediate classification makes it possible to preserve the meaning of the data before it is mapped to the target schema. In the output transformation phase, the CyberNER *NetworkLocation.ip* attribute is mapped to *source.ip*, while the associated *PhysicalLocation* attributes are mapped to *source.geo.city_name*, *source.geo.country_name*, *source.geo.country_iso_code* and *source.geo.location* (Table 2). The latter field is indexed in Elasticsearch as a *geo_point*, which enables direct visualization of the event in Kibana Maps (Fig. 2). At the same time, CyberNER metadata such as semantic class, role, context identifier, confidence and location precision are retained in the document, allowing the transformation process to remain traceable and semantically explainable.

The obtained representation shows that the same observation can be decomposed into a set of semantically meaningful components: event time, initiating actor, observed activity, source network location and associated physical location. As a consequence, the target ECS document does not merely store renamed fields but reflects an interpretation

that can be traced back to the intermediate semantic model. This strengthens the analytical value of the transformed record and facilitates later correlation, visualization and explanation of detection results.

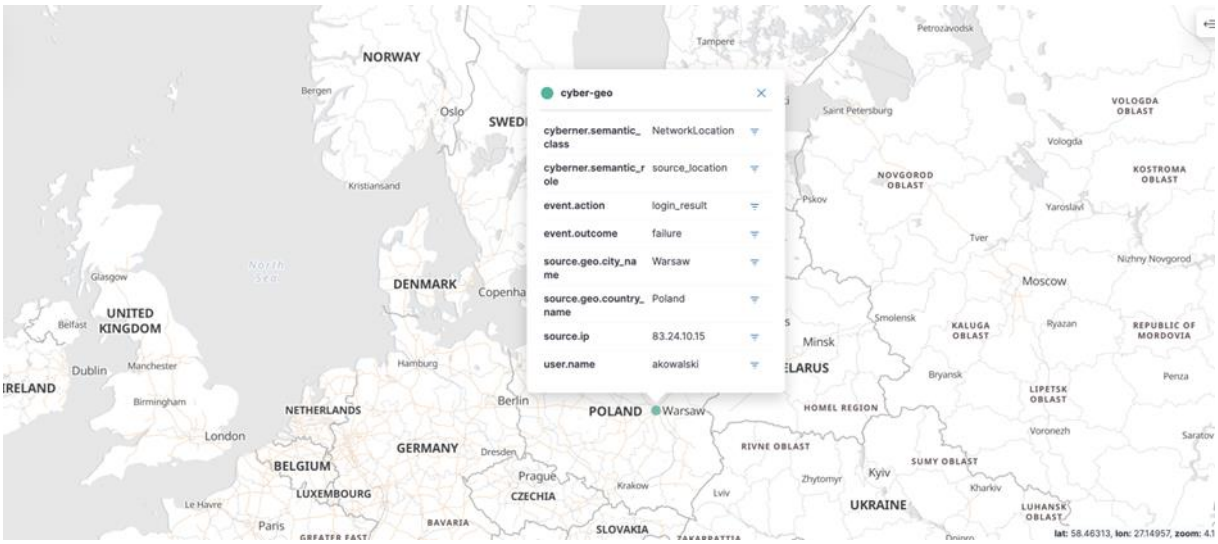

Fig. 2. Visualization of the event (Table 1, Table 2) in Kibana Maps tool
Source: own study

Discussion

The presented results should be interpreted as a proof-of-concept for the proposed modeling approach rather than as a full-scale quantitative benchmark. Their value lies in demonstrating that semantic mediation can be introduced before the target-schema stage and that geospatial meaning can be treated as part of a broader event context instead of a detached set of fields. This is particularly important in Cognitive SOC architectures, where downstream analytics depend on consistency of interpretation rather than on syntactic normalization alone.

From the geospatial perspective, the example demonstrates that CyberNER enables explicit preservation of the relationship between a network identifier and its physical location, while keeping open the possibility of recording confidence, precision level and provenance metadata. These properties are difficult to retain consistently in direct schema mapping workflows and therefore constitute a practical advantage of the proposed intermediate layer.

At the same time, the approach has several limitations. First, the quality of the final representation depends on the quality of source data and enrichment services, especially for IP geolocation. Second, the article presents a methodological framework and an illustrative transformation path, but not yet a large-scale benchmark on heterogeneous datasets. Third, some schema-specific constraints may still require additional implementation rules at the output stage. These limitations define the main directions for future validation studies.

The structure of the article highlights CyberNER not only as a conceptual layer, but also as a research proposition that can be systematically analyzed within a scientific workflow comprising introduction, material and methods, results, discussion and conclusions. In this perspective, CyberNER provides a reusable semantic mechanism for geospatial data transformation in cybersecurity systems and offers a basis for future comparative experiments on transformation quality across heterogeneous schemas.

Conclusions

The presented concept shows that geospatial data in cybersecurity should be modeled not as a set of isolated attributes, but as part of a coherent semantic structure embedded in the context of an event, entity, and infrastructure. It is the context that determines its analytical value. The information that a given IP address is associated with a specific country has a different meaning than knowing that the same address belongs to a specific ASN, is located in a specific cloud region, and remains associated with an event involving a specific user or host.

The proposed approach strengthens the role of the intermediate layer in the processes of standardization and transformation of security data. CyberNER does not serve as a complete transformation method, but as a semantic representation mechanism that allows the separation of the level of meaning from the technical level of the mapping to the target schema. Such separation is important in multi-schema environments, where the final quality of the transformation depends not only on the correctness of the field mapping, but also on the ability to maintain the relationship, context and provenance of the data.

At the same time, it should be emphasized that the proposed model is conceptual and methodological in nature. Its full validation requires further experimental research conducted on heterogeneous data sets and a comparison of the quality of the intermediate representation with the results obtained in approaches based solely on direct schema mapping. The limitations of the model also result from the quality of the input data.

Funding

This work was financed/co-financed by Military University of Technology under research project UGB 531-000091-W500-22.

Declaration of Competing Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No public, restricted and proprietary data collected or analyzed.

Use of Generative AI and AI-Assisted Technologies

No generative AI or AI-assisted technologies were employed in the preparation of this manuscript.

References

Alarabi L. (2025). Spatial data: What is it and why is cybersecurity so vital to it? https://www.weforum.org/stories/2025/09/spatial-data-what-is-it-and-why-is-cybersecurity-so-vital-to-it/ [access: 30.04.2026].

Bakirtzis G., Sherburne T., Adams S., Horowitz B.M., Beling P.A., Fleming C.H. (2022). An ontological metamodel for cyber-physical system safety, security, and resilience coengineering. Software and Systems Modeling, vol. 21, pp. 113–137. https://link.springer.com/article/10.1007/s10270-021-00892-z [access: 30.04.2026].

Ech-Chammakhy Y., Motii A., Rabii A., Azrara O., Chbili J. (2025). CyberNER: A Harmonized STIX Corpus for Cybersecurity Named Entity Recognition. https://arxiv.org/pdf/2510.26499 [access: 30.04.2026].

Elastic (2025). Elastic Common Schema (ECS) reference. https://www.elastic.co/guide/en/ecs/current/index.html [access: 30.04.2026].

Esri (2014). The Geospatial Approach to Cybersecurity: Implementing a Platform to Secure Cyber Infrastructure and Operations. https://gis-and-cyber-security-esriaudefence.hub.arcgis.com/documents/ed70e99320b54c3c9e99364bec8cdf20/explore [access: 17.07.2026].

OASIS OPEN (2025). STIX Version 2.1 Errata 01 Version 2.1. https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html [access: 30.04.2026].

OCSF (2026). Open Cybersecurity Schema Framework v1.8.0. https://schema.ocsf.io/ [access: 30.04.2026].

Sohacheski D.B., Itzhak E. (2017). Geo-Cybernetics – Geographic Aspects, Mapping and Locations in Cyberspace. In: The 58th Conference of the Israeli Geographical Association. https://www.researchgate.net/publication/322056164_Geo-Cybernetics_--_Geographic_Aspects_Mapping_and_Locations_in_Cyberspace [access: 30.04.2026].

Zhang J., Shi F., Xu Ch., Li Y, Ge M. (2026). CyMapNER. CyMapNER: a named entity recognition model for cyberspace surveying and mapping domain. Cybersecurity, vol. 9, no. 146. https://link.springer.com/article/10.1186/s42400-026-00578-3 [access: 30.04.2026].