International Journal of Philology, 29(4), 2025
Journal homepage: https://philologicalscience.com.ua/en
Received 29.05.2025 Revised 13.10.2025 Accepted 27.11.2025 Published: 26.12.2025
ISSN 2706-9737 e-ISSN 2706-9745

UDC 811.111'373.46:004.056 DOI: 10.31548/philolog/4.2025.73

Conceptual and metaphorical models of contemporary English-language cybersecurity terminology

Vladyslav Zhovtiak*
Postgraduate Student
Yuriy Fedkovych Chernivtsi National University
58002, 2 Kotsiubynskoho Str., Chernivtsi, Ukraine
https://orcid.org/0009-0002-2043-7421

Abstract. The relevance of the study is conditioned by the rapid development of digital technologies and the need for linguistic understanding of how specialised terminology forms a professional picture of the world in the field of cybersecurity. The purpose of the study was to identify, systematise, and cognitively interpret conceptual metaphors in contemporary English-language cybersecurity terminology, and to determine their role in the processes of conceptualisation of digital threats and defence mechanisms. The research was based on the provisions of the theory of conceptual metaphor and was aimed at identifying mechanisms of linguistic conceptualisation of abstract processes related to information security, digital threat management, and the functioning of cyberspace. The material of this scientific research consisted of 4,000 English-language terms selected from the authoritative English-Ukrainian dictionary of terms on information technology and cybersecurity. The methodological basis was cognitive and metaphorical analysis, semantic classification, component and quantitative analysis, which helped to establish the hierarchy and performance of metaphorical models in the terminology under study. As a result of the analysis of cybersecurity terms, it was found that a significant part of them was formed based on conceptual metaphorisation. The most productive were ontological metaphors (436 units), in which cybersecurity was understood as a control, system, cipher, or data storage container. A significant group consists of natural metaphors that include models of fluids, plants, and animals, and medical metaphors related to the conceptualisation of computer viruses. Among the structural metaphors (416 units), the metaphor "cybersecurity is military operations" (attack, threat, combat, weapons) dominates, and the architectural model "cybersecurity is home" (access keys, locks, gateways). Orientation metaphors turned out to be small in number and perform mainly a navigation

Suggested Citation:
Zhovtiak, V. (2025). Conceptual and metaphorical models of contemporary English-language cybersecurity terminology. *International Journal of Philology*, 29(4), 73-87. doi: 10.31548/philolog/4.2025.73.

*Corresponding author

function, providing a hierarchy of concepts such as threat level, security level, attack vectors, and system boundaries. The practical significance of the study lies in the possibility of using its results in research on cognitive linguistics, terminology, discourse analysis, and in training courses and applied developments related to digital communication and information security

Keywords: cognitive linguistics; language conceptualisation; digital threats; term; figurative models

Introduction

In English-language terminology and professional cybersecurity discourse, conceptual metaphors play a key role in understanding abstract technical phenomena related to the protection of information, data, and digital systems. The relevance of the study is conditioned by the rapid development of digital technologies and the growing role of cybersecurity as a key factor in the functioning of contemporary society. Cyberspace is increasingly becoming an arena of conflicts, threats and risks, which requires not only technical, but also linguocognitive approaches to their understanding and representation. In this context, the language of cybersecurity performs not only a nominative, but also a conceptualising function, forming an idea of digital threats through the prism of everyday physical, social, and cultural experience of a person. The use of cognitive metaphors, which serve as the main mechanism for verbalising abstract and technically complex processes, becomes important. Despite the existence of separate studies of the conceptual metaphor in scientific and media discourse, metaphorical models of cybersecurity remain insufficiently systematised, and their role in shaping the professional picture of the world of specialists and non-specialists requires a thorough analysis. This necessitates a comprehensive linguocognitive study of metaphors in contemporary English-language cybersecurity discourse.

The tradition of metaphor research was formed primarily in cognitive linguistics, where metaphor was considered as a fundamental mechanism of conceptualisation and thinking. T. Dyrmo (2025) developed the ideas of an extended conceptual metaphor, suggesting a revision of the traditional hierarchy of levels of metaphorical organisation of meaning. The researcher introduced a multidimensional model of metaphorisation that combines semantic, cognitive, and semiotic parameters of analysis. Attention was paid to multimodal forms of metaphorical expression, which include the interaction of verbal, visual, and other semiotic resources in the process of constructing meaning. The researcher also introduced the concept of submetaphores as smaller cognitive structures that form more complex metaphorical systems in discourse. This approach allows describing the processes of the development of meaning as a multi-level dynamic system, where meaning is formed through the integration of various channels of perception and interpretation of information. Thus, O. Kramer (2025) considered the Extended Conceptual Metaphor Theory (CMT) in a new technological context, suggesting the use of cognitive and metaphorical principles as a basis for forming strategies for prompting large language models. The researcher proved that metaphorical structures can be used to improve the quality of text generation by artificial intelligence, since they reproduce the natural cognitive patterns of human thinking. The study analysed ways to integrate cognitive semantics with machine learning methods, in particular, through the use of metaphorical scenarios as templates for forming instructions for language models. The prospects of an interdisciplinary approach combining cognitive linguistics, computer

linguistics and artificial intelligence technologies were emphasised separately.

I. Kryknitska (2024) proposed a modified algorithm for analysing conceptual metaphors aimed at improving the accuracy of identifying metaphorical units in the text. The proposed method was based on a combination of cognitive and semantic analysis with a procedural approach to processing speech material. The algorithm allowed automating some of the analytical procedures related to identifying source and target domains, and establishing hierarchical relationships between different levels of metaphorical generalisations. The researcher also noted the possibility of using the proposed algorithm to investigate complex discursive structures and analyse metaphorical networks in large text cases. M. Banevych (2025) investigated the functioning of conceptual metaphors in political discourse, focusing on their pragmatic and manipulative role in shaping public opinion. The researcher showed that political metaphors perform not only a nominative function, but also act as a tool for evaluating political events, constructing ideological positions and influencing the emotional perception of the audience. The researcher analysed strategies for metaphorical representation of political actors and events, demonstrating how metaphors can be used to strengthen argumentation, create emotional resonance, and form a cognitive framework for interpreting political information. H. Stroganova (2025) conducted a comprehensive analysis of the evolution of scientific views on the linguocognitive nature of metaphor, tracing the transition from classical structural models to contemporary cognitive and discursive and multimodal approaches. The paper emphasised that metaphor was considered not only as a stylistic tool, but also as a universal mechanism for conceptualising experience and categorising reality in human thinking. The researcher analysed in detail the relationship between cognitive processes, socio-cultural context and linguistic representation of meanings, emphasising the role of discursive practices in the development and transformation of metaphorical models. Attention was paid to integrating cognitive linguistics with semiotic and communicative approaches to metaphor analysis.

D. Gaskins (2024) applied a usage-based approach to the study of metaphorical structures in children's speech, combining cognitive linguistics with empirical methods for analysing speech corpus. The paper used the step-by-step Metaphor Identification Procedure (MIP) and its extended and improved version of the Metaphor Identification Procedure Vrije Universiteit (MIP-VU) to systematically identify metaphorical units and analyse their functioning in children's natural speech. The researcher demonstrated that the development of metaphorical models in children's speech was associated with the frequency of language constructions, contextual support for meanings, and the gradual development of abstract thinking. In addition, the study in question confirmed that metaphorisation plays an important role in a child's cognitive development, in particular, in the processes of categorising experience and forming semantic networks of meanings. The research has formed the theoretical and methodological framework of contemporary metaphor studies, focusing on CMT expansion, analysis automation, and interdisciplinary connections. The purpose of the study was to identify, systematise, and cognitively interpret conceptual metaphors in contemporary English-language cybersecurity terminology, and to determine their role in the processes of conceptualisation of digital threats and defence mechanisms. To achieve this objective, the following tasks were set: to summarise theoretical approaches to the study of conceptual metaphor within the framework of cognitive linguistics, followed by the identification of the main conceptual metaphorical models in the material under investigation; to classify metaphors by source domains (human, war, medicine, space,

container, etc.); to determine the quantitative ratio of the main metaphorical models.

Materials and Methods

The research material consisted of 4,000 terminological units of English-language cybersecurity terminology selected from the English-Ukrainian dictionary of information technology and cybersecurity terms (Hladun *et al*., 2018). The use of a dictionary source ensured the standardisation of the material, the representativeness of the terminological system, and the ability to analyse well-established lexical units of industry discourse. Additionally, scientific monographs, articles on cognitive linguistics, and terminological encyclopaedic sources were used for theoretical substantiation, which provided the development of a conceptual and methodological base for research (Gibbs, 1994; Selivanova, 2008; Steen *et al*., 2010). The methodological basis of the study was based on a combination of general scientific, cognitive and linguistic, and quantitative and statistical methods of analysis. The leading method was cognitive and metaphorical analysis, applied within the framework of the theory of conceptual metaphor (Lakoff & Johnson, 1980). Its use was conditioned by the need to identify mechanisms for conceptualising abstract cybersecurity phenomena through the prism of more specific human experience. The method helped to identify correspondences between the source sphere (man, war, disease, container, space, etc.) and the target sphere (cybersecurity as a conceptual domain), and to describe cognitive models of understanding cyberspace as part of socio-psychological and cultural experience.

To systematise the empirical material, the semantic field method was used, which was used to group terms according to common conceptual features. This method allowed establishing thematic and semantic links between metaphorical categories that represent various aspects of cybersecurity, in particular, threats, protection, information processes, and cyberspace. The semantic field method helped to further typologise metaphorical models and determine their system organisation within the terminological subsystem. Component analysis was used to clarify semantic transformations and analyse the internal structure of terms. This method determined the semantic components of the meaning of terms, in particular, to identify the actualisation of individual semes during metaphorical transfer (for example, the semes of defence, aggression, penetration, control, violation of integrity). The use of component analysis was important for establishing mechanisms of terminological metaphorisation and determining the cognitive characteristics of the field under study. An important role in the study was played by the quantitative method of analysis, which was used to determine the frequency of use of various types of metaphorical models. Quantitative analysis allowed providing an objective interpretation of the results by statistically comparing the performance of conceptual schemes and establishing dominant metaphorisation trends in the English-language cybersecurity discourse. Frequency counting was carried out by continuous sampling of terminological units, followed by their classification grouping. The theoretical basis of the study was the provisions of the theory of conceptual integration, which explained the process of forming complex abstract concepts through the combination of several cognitive spaces (Fauconnier & Turner, 2002). The use of this theory allowed interpreting complex metaphorical structures as the result of the interaction of several cognitive scenarios and explaining the mechanisms of development of metaphorical submodels.

The hierarchical approach to metaphor analysis developed by Z. Kövecses (2020) was also used, which predicted the distinction between general conceptual metaphors, specific submetaphores, and metaphorical consequences (entailments). The identification of

metaphorical terms was carried out using a step-by-step algorithm: development of the research corpus – selection of 4,000 terms from a specialised English-Ukrainian dictionary of information technology and cybersecurity; initial semantic analysis – establishing the literal and terminological meaning of the lexeme; identifying semantic discrepancies between the source domain and the target domain; determining the source domain and the target domain; classifying metaphors by types of conceptual models and calculating their frequency. The analysis of metaphorical models was based on the provisions of conceptual metaphor theory (Lakoff & Johnson, 1980), the principles of cognitive semantics (Selivanova, 2008), conceptual integration theory (Fauconnier & Turner, 2002), and a hierarchical approach to the organisation of metaphorical models (Kövecses, 2020). The identification of metaphorical units was carried out considering the procedural approach (MIP/MIPVU) (Gibbs, 1994; Steen *et al.*, 2010), which ensured the consistency and reproducibility of the results obtained.

Results and Discussion

As a result of the analysis of terminological material, a number of conceptual models of metaphorisation in the field of cybersecurity were identified. A significant group consists of ontological metaphors that represent the abstract concept of cybersecurity as an object, being, or substance. In particular, a common model is "cybersecurity is a person" (12 terminological units), implemented through the personification of systems that are attributed to physical or psychophysiological characteristics, in particular "vulnerability", "health" or "sustainability", for example: handshake, backbone, backbone network, biometric identification, blind copy recipient. In addition, ontological metaphors within the material being studied (Hladun *et al.*, 2018) perform not only a nominative, but also a cognitive and interpretive function, since they contribute to understanding complex technical processes through an appeal to everyday human experience. Personification of elements of cyberspace allows conceptualising security as a dynamic state that can change depending on the level of security of the system, the intensity of threats, or the effectiveness of defence mechanisms.

In the "cybersecurity is a person" model, the system appears as an entity capable of "interacting", "responding", or "being harmed", which reinforces the anthropocentric nature of cybersecurity discourse. Such a metaphorical projection also helps to simplify specialised terminology and facilitates its interpretation for both specialists and non-professional audiences. Within the same group, there is a metaphor "cybersecurity is medicine", where threats are understood as diseases or viruses, and protective measures – as treatment, immunity or prevention, for example: sanitising, vaccine, bacterium, virus. In the studied dictionary, 19 types of computer viruses were recorded, for example: boot virus, companion virus, file virus, macro virus, mutant virus, parasitic virus, resident virus, shattered virus, etc. The biological concept of a pathogenic microorganism is transferred to the field of information technology to describe programme code that can independently spread and damage the system. Due to this transfer, complex technical processes are explained through a well-known biological model of infection.

Metaphors are also ontological in nature, in which data appears as a physical substance or object. The "cybersecurity is food" (salt) and "cybersecurity is a container" models (16 units, for example: backing storage, external storage, internal storage, magnetic disk storage, main storage) represent information as something that can be "consumed", "accumulated", "stored" or "lost", and the systems themselves as a limited space with clear boundaries, penetration beyond which is a threat. An example is the term "honeypot", which comes from a household metaphor. In the literal sense, the

word refers to a vessel for storing honey that attracts animals or insects. In cybersecurity, this image is used to refer to a specially designed system or bait server designed to detect intruders. Metaphorical transference is based on a conceptual scheme in which the hacker is likened to a subject who succumbs to temptation.

A similar function is performed by the metaphor "cybersecurity is documentation", in which information processes are conceptualised through images of certificates, protocols, signatures and certificates. Thus, the following metaphorical submodels were identified: "cybersecurity is a protocol", within which 80 terminological units were recorded for various types of protocols, for example: address resolution protocol, authentication protocol, border gateway protocol, connectionless network protocol; "cybersecurity is a document", represented by 40 types of documents, for example, data protection document, guidance data protection document, hardware documents, etc.; "cybersecurity is a certificate" (17 units) – access control certificate, DevID Certificate, public key certificate, etc.; "cybersecurity is a signature" (13 units), for example: undoubted signature, virus signature, voice signature, etc. Thus, the metaphor "cybersecurity is documentation" reflects the desire for streamlining, formalisation, and normativity in the field of cyber defence, where security appears as a result of compliance with established rules and procedures. Conceptualisation of information processes through documentary images emphasises their legitimacy, reproducibility, and controllability. Within this metaphorical model, cybersecurity is understood as a set of formalised actions consolidated in texts, standards, and certification mechanisms that regulate access, authentication, and data exchange. The selected submodels demonstrate a high degree of structuring of the terminological field and confirm the dominance of regulatory logic, in which the security of the system depends on the correct "registration", "signing", and "confirmation" of information operations. This method of metaphorisation contributes to the cognitive simplification of complex technical processes and at the same time strengthens the idea of cybersecurity as a formally fixed and managed state. The metaphor "cybersecurity is a system" is also an ontological reification model, within which an abstract phenomenon is understood as an integral structured entity. It is represented by 32 elements, for example: system, subsystem, class (class AC/ADO/ADV/FDP/FIA, etc.), category (cloud service category, information struggle category, etc.), functional family, specification, model (comprehensive model, information leak channel functional model, model of threats to information), etc.

Within the framework of the metaphorical model "cybersecurity is a system", the emphasis is shifted to the internal organisation, hierarchy and interdependence of the components of the security space. Cybersecurity appears as an ordered set of elements, each of which performs a specific function and is in a relationship of subordination or coordination with other components. This conceptualisation allows understanding the security of information resources not as a static state, but as a result of the coordinated interaction of subsystems, classes, and models that form a single functional whole. In general, the metaphor "cybersecurity is a system" reflects the scientific and technical way of understanding security processes and correlates with the desire for standardisation and a systematic approach in contemporary English – language terminology. A separate subgroup consists of metaphors of natural origin ("cybersecurity is nature"), where threats appear as animals, plants or liquids and are structured, respectively, by a number of sub – metaphors: "cybersecurity is a plant" (5 units), for example: sprout, tree, B-tree, search tree, tree structure; "cybersecurity is an animal", which includes the following 3 terminological units: Trojan horse, Trojan worm, bug; "cybersecurity is a liquid", represented by 29 units like data-flow, digital

flow, flow of documentary information, information flow, packet flow, information leak, etc.

Thus, metaphors of natural origin appeal to the basic schemes of human experience of interaction with the environment and serve as an effective means of conceptualising complex and dynamic processes in cyberspace. In the "cybersecurity is nature" model, security phenomena and threats are understood as those that can arise, spread, accumulate or get out of control, similar to natural processes. In particular, plant metaphors emphasise the hierarchy and branching of information structures, zoomorphic images emphasise the hidden, invasive or parasitic nature of malicious software, while fluid metaphors reflect the continuity of data movement and the potential uncontrollability of their distribution. This type of metaphorisation contributes to the development of the idea of cyber threats as dynamic and changing phenomena that require constant monitoring and timely intervention, and simultaneously enhances the emotional and evaluative component of cybersecurity discourse.

The ontological metaphor also includes "cybersecurity is a cipher" (59 units), in which abstract information security processes are objectified through material coding elements, for example: code element, code set, cryptic code, cipher, Aiken/Baudot/Gray/Manchester/Hamming, Huffman/Markovian code, cipher stability, cipher suite, decipherement, decode, etc. The metaphor "cybersecurity is a cipher" represents one of the most technically labelled types of ontological reification, in which security appears as a set of formalised codes and operations with them. Through this metaphorical projection, information security processes are conceptualised as those that can be created, hacked, enhanced, or optimised, just like material objects. Simultaneously, the cipher metaphor actualises the "available/unavailable" opposition, which is key to understanding information control in the digital environment. The conceptual metaphor "cybersecurity is control" also belongs to the ontological type, since the abstract sphere of cybersecurity is understood as an object of control that can be regulated, strengthened or lost. It is represented by 105 elements, for example: access check, check authenticity with artificial information redundancy, connection admission control, flow control. Based on this ontological projection, cyberspace is understood as a controlled object with certain points of intervention and monitoring, which contributes to the development of an idea of cybersecurity as a controlled and predictable process. Terminology units that implement this metaphor reflect various aspects of managing information flows, access, and authenticity, and emphasise the engineering and procedural nature of contemporary cyber defence.

Quantitative analysis has shown that these ontological models do not function in isolation, but form an interconnected conceptual network. The most productive models are "cybersecurity is control", "cybersecurity is a cipher" and "cybersecurity is a document", which together form the core of the term system. Their high frequency indicates that the professional picture of the world of cybersecurity specialists is based on the idea of the digital space as a managed system in which information is subject to formalised regulation, verification, and protection. Thus, these models can be considered as conceptual dominants that organise a significant part of specialised vocabulary and form a hierarchical structure of submetaphores. Structural metaphors play a leading role in the studied cybersecurity terminology, since they set the logic for interpreting the entire industry. The most dominant and extensive model is "cybersecurity is a military action", within which the following submethaphores are recorded: "cybersecurity is an attack" (49 units): active attack, attack to network of exchange of information, brute force attack, etc.; "cybersecurity is a fight" (3 elements): hash clash, collision; "cybersecurity is a fight" (13 terms): computer crime struggle, information

struggle, etc.; "cybersecurity is protection", which includes 9 units, for example: copy protection, data protection, password protection, redundancy protection, administrative security, communications security, compusec – computer security, COMSEC – communications security, cryptographic security; "cybersecurity is war", which contains 10 elements, for example: cryptography war, psychological warfare, radio [electronic] warfare, signs of preparation for armed struggle in psychological warfare field; "cybersecurity is a strategy" (4 units): information strategy, security strategy, etc.; "cybersecurity is a weapon" (9 terms): counteraction information weapons, information – algorithmic weapon; "cybersecurity is the enemy" (10 units): adversary, enemy, opponent; "cybersecurity is a threat", which is implemented by 20 elements, for example: covert threat, potential threat to security of information in local computer network, threat of dysfunction.

Given the quantitative indicators and diversity of submethaphores, it can be assumed that the military model serves as a leading conceptual macromodel, within which a significant part of metaphorical projections in cybersecurity terminology is organised. It forms the basic cognitive framework for understanding digital threats, where cyberspace is interpreted as a field of confrontation between subjects, tools, and strategies. The frequency of such source areas as attack, enemy, threat and defence correlates with the nature of contemporary digital risks and reflects the professional paradigm of cybersecurity, in which the activities of specialists are thought of as a system of permanent defence, monitoring and counteraction. Structural metaphors also include "cybersecurity is a home" and "cybersecurity is a transport" (platform, pilotless vehicle, terminal, traffic). In the first case, digital systems are understood as architectural structures with entrances, exits, and hidden passageways, while in the second case, data transmission is interpreted as traffic on transport routes. Thus, the metaphor "cybersecurity is a home" is implemented through submodels: "cybersecurity is a lock" (16 units): data interlock, deadlock, software lock; "cybersecurity is a door/gate" (12 elements): trapdoor, gateway, etc.; "cybersecurity is a key" (62 units): access control key, compromised key, database key, long-term key; "cybersecurity is a wall" (2 terms): firewall, brandmauer. An illustrative example of metaphorical transfer within this model is the term "firewall". In the original sphere, the word refers to a physical fire barrier designed to contain the spread of fire between parts of the building. In the field of cybersecurity, this material construct serves as a source for conceptualising a software or hardware mechanism that blocks unwanted network traffic. Thus, the complex technical process of data filtering is understood through the image of a material barrier, which enhances the visibility and clarity of the term in professional discourse.

The metaphor "cybersecurity is home" allows conceptualising information security through images of architectural elements, emphasising the structure and hierarchy of the security system. Each component of the "house" performs a specific function: walls block unwanted access, locks, and keys regulate control over resources, doors, and gates coordinate interaction between subsystems. Through this structural metaphorisation, terminological units reflect order, control, and security, which provides a cognitive picture of cybersecurity as a reliably organised, managed, and predictable space. In general, this type of metaphor helps to understand data protection processes not only at the technical level, but also at the level of intuitive perception, enabling an easy interpretation of complex security mechanisms through familiar architectural images. Less productive are the metaphors "cybersecurity is work" (4 elements, for example: sniffer, spy, scout, recruitment) and "cybersecurity is mathematics" (24 terms: Euler phi function Bell-LaPadula model, radix, matrix, variable, zero, algorithm, gamma,

graph), which, however, emphasise the rational, manageable and formalised nature of information security processes. Mathematic metaphors in cybersecurity reflect the desire for rational organisation, formalisation, and accuracy of information security processes. The metaphor "cybersecurity is mathematics" allows understanding cyber defence through algorithmic and structured operations, where data and processes obey logical rules and formal laws. In particular, Bell-Lapadula access models provide mathematical formulation of privacy policies in information systems. Algorithmic concepts such as the Leonhard Euler function or Richard Hamming codes are used to build error-resistant encryption systems and verify data integrity. Graph structures and matrices reflect the relationships between objects, data streams, and transmission channels, which allows for formalised risk assessment and threat modelling. In this case, metaphorisation is based on transferring the properties of mathematical accuracy, formalisation, and algorithmicity to the field of information security. Such conceptual modelling allows interpreting cybersecurity as a system of computational processes where risks, vulnerabilities, and security mechanisms can be formally described and predicted. As a result, mathematical concepts perform not only a terminological, but also a cognitive and organisational function, structuring knowledge about the security of digital systems.

Socially oriented structural metaphors are represented by the models "money" (3 units – cybermoney, e-money, electronic money), "economy" (15 terms, for example: economic management/rivalry/efficiency, resources/distribution/registration/infrastructure/strategy, databank, stakeholder, transaction), and "powers" (6 elements, for example: authentication, credentials, administrative domain, expert), and "cybersecurity is law", which traces further internal differentiation. This model is structured into the following submethaphores: "cybersecurity is a right" (12 elements): copyright law, digital law, (military) legislation, jurisprudence, evidence, verdict; "cybersecurity is a crime" (16 units, for example: false, falsification, computer crime, criminal, infringer, violator, etc.). The sub-metaphors "law" and "crime" reflect opposition to legitimate and disruptive behaviour in a digital environment where policies, norms, and sanctions form the framework for action, and cybercrimes are presented as specific violations of these rules. They conceptualise cybersecurity through norms, responsibilities, data values, and access distribution, reflecting the managerial and institutional nature of modern cyberspace.

Peripheral, but cognitively significant are the metaphors "film" (scenario, screening) and "art" (information portrait). Despite the relatively small number of such units, their presence indicates the expansion of the conceptual space of cybersecurity beyond purely technical models. The use of cultural sources, such as art or cinema, reflects the desire to interpret complex information processes through scenario or image structures. This demonstrates a tendency to integrate technical, social, and cultural experience into the development of contemporary cybersecurity terminology. Orientation metaphors based on spatial axes and scales complement the overall picture. The "cybersecurity is movement" models (3 elements, for example: routing – routing, running, move), "direction" (3 terms, for example: backward channel, backward recovery) and "space" (32 units, for example: cyberspace, OSI environment, closed-security environment) form an idea of the dynamics, trajectories, and operating environment of digital systems. The above examples show that the "cybersecurity is movement" model focuses on data movement, packet transmission, and task execution in time and space, emphasising the activity and processability of information flows. The "direction" metaphor reflects the orientation in the logic of data flows and the ability to return the system to its previous state, which forms an idea of controlled correction and

recovery. The "space" model reveals the functioning environment of digital systems, their interdependence and security levels, which allows imagining cyberspace as a structured but dynamic environment where the movement and position of objects are of key importance.

Generalisation of the results obtained allows presenting metaphorical models of cybersecurity as a hierarchically organised and clustered system. At the upper level, there are three main types of metaphors – ontological, structural, and orientation, which form the macro level of conceptualisation. Within each type, thematic clusters are distinguished that are united by common source areas (war, medicine, architecture, nature, control, etc.). At a lower level, these clusters are implemented through submetaphores that specify certain aspects of cybersecurity (attack, protection, key, virus, data flow, etc.). Interaction between clusters has a network character: individual models (in particular, "cybersecurity is control, war, system") serve as nodes that integrate various conceptual projections and ensure the integrity of the term system. From a cognitive standpoint, the identified metaphorical models serve as conceptual schemas that structure knowledge about cybersecurity by transferring experience from specific areas to an abstract digital domain. In particular, the military model forms a conflict interpretation of cyberspace as a confrontation environment, where the key categories are threat, enemy, and defence. The control model provides insight into the manageability and manageability of information processes, while the container and space model organises an understanding of boundaries, access, and penetration. Together, these models implement basic cognitive conceptualisation mechanisms – objectification, structuring, and spatial organisation of knowledge, which allows interpreting cybersecurity as a systematic, dynamic, and controlled process.

The analysis shows that the conceptualisation of cybersecurity in English terminology is based on several basic cognitive mechanisms. Anthropomorphisation presents digital systems as objects with human properties, and reification (objectification) presents abstract processes as material objects under control. The conflict scheme structures cyberspace as an environment for countering threats and protection, spatial understanding reflects the boundaries, direction, and movement of information flows, and processalisation treats cybersecurity as a dynamic process of interaction and control. Together, these mechanisms form a cognitive model that provides interpretation of complex cyberspace phenomena through accessible human experience. The results obtained are consistent with the main provisions of the theory of conceptual metaphor. A significant contribution to its development was made by Z. Kövecses (2020), who proposed the concept of extended CMT. The researcher noted that metaphorical models are formed under the influence of physical experience, cultural models, social communication scenarios, and individual cognitive factors. He also emphasised the variability and contextual conditionality of metaphorical projections between domains of knowledge. This approach is consistent with the results of the current research, since the identified metaphorical models in the cybersecurity term system reflect not only universal cognitive mechanisms, but also the specifics of professional discourse and ways to conceptualise the digital environment.

Research has demonstrated the effectiveness of metaphorical models in various types of discourse. Corpus study by R. Abu Rumman *et al*. (2023) showed that metaphors play an important role in the translation and subtitles of audiovisual texts, where they can be stored or transformed depending on cultural and communicative conditions. The researchers proved that metaphorical structures are an important means of conveying conceptual content in cross-language communication. The results of the study support this conclusion, as they

confirm the universality of cognitive mechanisms of metaphorisation, which are manifested both in media discourse and in specialised terminology. Similar results were obtained by R. Khmelnytskyi (2024), who analysed the ontological metaphor "emotion is a substance in a container" in artistic discourse based on the material of the novel by F. Herbert "Dune" and its Ukrainian translation. The researcher has shown that such a metaphorical model provides effective verbalisation of complex emotional states through the image of spatial constraints and content. The researcher noted that ontological metaphors contribute to the conceptualisation of abstract psychological phenomena. This conclusion was confirmed by the results of the conducted study, which also demonstrated that ontological metaphors play an important role in structuring complex and abstract concepts in cybersecurity terminology.

Researchers paid special attention to the role of structural metaphors in the development of social and discursive narratives. T. Pasternak (2024) investigated the functioning of the military metaphor in media discourse and demonstrated its ability to conceptualise social processes through a model of struggle, confrontation, and strategy. The researcher stressed that such metaphors can influence the interpretation of socio-political events and the development of ideological frameworks. These results are largely consistent with the results the current research, because in the field of cybersecurity, metaphors of conflict, defence, and attack are also widely used to describe the interaction between subjects of the digital space. Metaphorisation of specialised terminology can also be traced in other areas of knowledge. The study by I. Sapozhnyk & T. Surodeikina (2025) analysed the metaphorical mechanisms of the development of English-language terms in the fields of art and commercial law. The researchers proved that metaphor is one of the key cognitive tools for expanding and systematising terminological systems. They also emphasised the role of interdisciplinary conceptual projects in shaping new meanings. The data obtained indicate in favour of this opinion, since the results of the current research confirmed that metaphorical modelling is an effective mechanism for conceptualising complex technical phenomena in the cybersecurity term system.

In the context of the study of metaphorisation of anthropomorphic concepts, the study by N. Yesypenko *et al*. (2022), devoted to the analysis of the metaphorical representation of anthropomorphic images in British and American fairy tales, deserves attention. The researchers have shown that anthropomorphisation is an important cognitive mechanism that allows transfering human properties to abstract or inanimate objects. The researchers emphasised that such metaphors contribute to the development of understandable cognitive models for interpreting complex phenomena. Although their research has focused on artistic discourse, its findings are partially consistent with the present results, since cybersecurity terminology also shows a tendency to anthropomorphise processes and systems (for example, describing programme actions or attacks as agent behaviour). Also of relevance is the study by O. Tur *et al.* (2025), which analysed the discursive features of the use of generative artificial intelligence terminology in professional communication. The researchers found that the development of new terminology in the field of artificial intelligence is accompanied by active processes of semantic expansion, metaphorisation, and adaptation of general language vocabulary. They also noted that metaphorical models help specialists to interpret complex technological processes and make specialised knowledge more accessible in professional discourse. These results are consistent with the findings of the current study, as it confirms the important role of metaphorical mechanisms in the development of contemporary technological terminology.

In addition, the development of metaphor research is actively supported by current approaches in computational linguistics. In particular, D. Wang *et al*. (2025) proposed the CKEMI model, a conceptually oriented automatic metaphor detection system that combines machine learning techniques with conceptual knowledge. The researchers proved that the integration of semantic and cognitive models increases the accuracy of recognition of metaphorical constructions in large text cases. Although their research was mostly technical in nature, its results confirmed the importance of conceptual analysis of metaphors for the further development of automated speech processing systems. Thus, the results of the study are generally consistent with the conclusions of contemporary scientific papers that consider metaphor as an important cognitive mechanism for conceptualising knowledge. The revealed interaction of ontological, structural and orientation metaphors in the cybersecurity term system confirms that metaphorical modelling plays an important role in shaping the professional picture of the world and in understanding complex processes of cyberspace. In this context, the metaphor acts not only as a language tool, but also as a tool for the cognitive organisation of specialised knowledge.

Conclusions

The study showed that metaphorisation is one of the key mechanisms for the development of contemporary English-language cybersecurity terminology. The analysis of the corpus of terminological units helped to identify a system of conceptual metaphors represented by three main types: ontological, structural, and orientation, which provide cognitive understanding of complex processes of functioning of cyberspace and information protection. The most productive were ontological metaphors (436 units), within which cybersecurity phenomena are conceptualised through specific objects and systems. Such models contribute to the objectification of abstract information security processes and their systematisation in professional terminology. In this type, cybersecurity is conceptualised as a material object, control, system, container, living being, or substance that allows capturing its properties, states, and internal organisation. The models "cybersecurity is control", "cybersecurity is a document", and "cybersecurity is a cipher" serve as the basis for forming terms for designating structural elements, security mechanisms, and vulnerabilities.

An important role in the term system under study is played by structural metaphors (416 units) that reflect the understanding of cybersecurity through other areas of human experience. The most representative model is "cybersecurity is military action", which is implemented through tokens to indicate attacks, threats, combat, and means of protection. Along with it, there are other conceptual models, in particular "cybersecurity is home", "cybersecurity is mathematics" and "cybersecurity is law", which reflect ideas about the structure, organisation and regulation of information security processes. Orientation metaphors (30 units) are represented by fewer examples, but they perform an important function of spatial and hierarchical structuring of concepts related to the threat level, degree of security, attack directions, and system boundaries. Thus, the contemporary English-language terminology of cybersecurity appears as a multi-level metaphorical system in which different types of conceptual metaphors interact and provide a cognitive interpretation of the processes of information security and countering digital threats. Prospects for further research are seen in an in-depth analysis of cognitive mechanisms for the development of metaphorical models in the cybersecurity term system and the study of their functioning in contemporary professional discourse.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Abu Rumman, R., Haider, A., Yagi, S., & Al-Adwan, A. (2023). A corpus-assisted cognitive analysis of metaphors in the Arabic subtitling of English TV series. *Cogent Social Sciences*, 9(1), article number 2231622. doi: 10.1080/23311886.2023.2231622.

[2] Banevych, M. (2025). Conceptual metaphor realization in political discourse. *Studia Methodologica*, 59, 18-25. doi: 10.32782/2307-1222.2025-59-2.

[3] Dyrmo, T. (2025). Extending extended conceptual metaphor theory: Rethinking levels, modalities, and meaning-making. *Cognitive Semiotics*, 18(1), 23-51. doi: 10.1515/cogsem-2025-2001.

[4] Fauconnier, G., & Turner, M. (2002). *The way we think: Conceptual blending and the mind's hidden complexities*. New York: Basic Books.

[5] Gaskins, D., Falcone, M., & Rundblad, G. (2024) A usage-based approach to metaphor identification and analysis in child speech. *Language and Cognition*, 16(1), 32-56. doi: 10.1017/langcog.2023.17.

[6] Gibbs, R.W. (1994). *The poetics of mind: Figurative thought, language, and understanding*. Cambridge: Cambridge University Press.

[7] Hladun, A.Ya., Puchkov, O.O., Subach, I.Yu., & Khala, K.O. (2018). *English-Ukrainian dictionary of information technologies and cybersecurity terms*. Kyiv: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".

[8] Khmelnytskyi, R. (2024). Conceptual metaphor emotion is a substance in a container for verbalizing emotional concepts (based on Frank Herbert's Dune and its Ukrainian translation). *Black Sea Philological Studies*, 5, 143-151. doi: 10.32782/bsps-2024.5.21.

[9] Kövecses, Z. (2020). *Extended conceptual metaphor theory*. Cambridge: Cambridge University Press. doi: 10.1017/9781108859127.

[10] Kramer, O. (2025). Conceptual metaphor theory as a prompting paradigm for large language models. *ArXiv*. doi: 10.48550/arXiv.2502.01901.

[11] Kryknitska, I.O. (2024). Modification of the algorithm for conceptual metaphor analysis. *Transcarpathian Philological Studies*, 36, 89-93. doi: 10.32782/tps2663-4880/2024.36.14.

[12] Lakoff, G., & Johnson, M. (1980). *Metaphors we live by*. Chicago: University of Chicago Press.

[13] Pasternak, T. (2024). Military metaphor as a conceptual metaphor. *Research Bulletin. Series: Philological Sciences*, 210, 35-39. doi: 10.32782/2522-4077-2024-210-4.

[14] Sapozhnyk, I.V., & Surodeikina, T.V. (2025). Metaphorization of English terms in art and commercial law: Comparative aspect. *Transcarpathian Philological Studies*, 42(3), 299-303. doi: 10.32782/tps2663-4880/2025.42.3.47.

[15] Selivanova, O.S. (2008). *Modern linguistics: Terminological encyclopedia*. Poltava: Dovkillya-K.

[16] Steen, G.J., Dorst, A.G., Herrmann, J.B., Kaal, A.A., Krennmayr, T., & Pasma, T. (2010). *A method for linguistic metaphor identification: From MIP to MIPVU*. Amsterdam: John Benjamins Publishing Company. doi: 10.1075/celcr.14.

[17] Stroganova, H. (2025). Development of views on the linguo-cognitive nature of metaphor. *Studia Methodologica*, 59, 226-235. doi: 10.32782/2307-1222.2025-59-20.

[18] Tur, O., Shabunina, V., & Sarancha, V. (2025). Discursive features of the use of generative artificial intelligence terminology in professional communication: Analysis of trends and prospects. *Acta Academiae Beregsasiensis, Philologica*, 4(3), 140-157. doi: 10.58423/2786-6726/2025-3-140-157.

[19] Wang, D., Li, Y., Wang, S., Chen, X., Liao, J., Li, D., & Li, X. (2025). CKEMI: Concept knowledge enhanced metaphor identification framework. *Information Processing & Management*, 62(1), article number 103946. doi: 10.1016/j.ipm.2024.103946.

[20] Yesypenko, N., Pavlovych, T., Migorian, O., Bloshchynskyi, I., & Mysechko, O. (2022). Metaphorical representation of anthropomorphic concepts in British and American fairy tales. *Journal of Language and Linguistic Studies*, 18(1), 18-33.

Концептуально-метафоричні моделі сучасної англомовної термінології кібербезпеки

Владислав Жовтяк
Аспірант
Чернівецький національний університет імені Юрія Федьковича
58002, вул. Коцюбинського, 2, м. Чернівці, Україна
https://orcid.org/0009-0002-2043-7421

Анотація. Актуальність роботи зумовлена стрімким розвитком цифрових технологій і необхідністю лінгвістичного осмислення того, як спеціалізована термінологія формує професійну картину світу у сфері кібербезпеки. Метою дослідження було виявлення, систематизація та когнітивна інтерпретація концептуальних метафор у сучасній англомовній термінології кібербезпеки, а також визначення їхньої ролі у процесах концептуалізації цифрових загроз і захисних механізмів. Дослідження ґрунтується на положеннях теорії концептуальної метафори та спрямоване на виявлення механізмів мовної концептуалізації абстрактних процесів, пов'язаних із захистом інформації, управлінням цифровими загрозами та функціонуванням кіберпростору. Матеріалом даної наукової розвідки слугували 4 000 англомовних термінів, відібраних із авторитетного англо-українського словника термінів з інформаційних технологій та кібербезпеки. Методологічну основу становили когнітивно-метафоричний аналіз, семантична класифікація, компонентний і кількісний аналіз, що дозволило встановити ієрархію та продуктивність метафоричних моделей у досліджуваній термінології. У результаті аналізу термінів кібербезпеки встановлено, що їх значна частина сформована на основі концептуальної метафоризації. Найбільш продуктивними виявилися онтологічні метафори (436 одиниць), у межах яких кібербезпека осмислюється як контроль, система, шифр або контейнер зберігання даних. Значну групу становлять природні метафори, що включають моделі рідини, рослин і тварин, а також медичні метафори, пов'язані з концептуалізацією комп'ютерних вірусів. Серед структурних метафор (416 одиниць) домінує метафора «кібербезпека – це військові дії» (атака, загроза, боротьба, зброя), а також архітектурна модель «кібербезпека – це будинок» (ключі доступу, замки, шлюзи). Орієнтаційні метафори виявилися малочисельними і виконують переважно навігаційну функцію, забезпечуючи ієрархізацію понять ступіню загрози, рівня захищеності, векторів атак та меж системи. Практичне значення роботи полягає в можливості використання її результатів у дослідженнях когнітивної лінгвістики, термінознавства, дискурс-аналізу, а також у навчальних курсах і прикладних розробках, пов'язаних із цифровою комунікацією та інформаційною безпекою

Ключові слова: когнітивна лінгвістика; мовна концептуалізація; цифрові загрози; термін; образні моделі