European International Journal of Philological Sciences (ISSN: 2751-1715)

Received: 07 July 2026 | Accepted: 02 August 2026 | Published: 01 September 2026

RESEARCH ARTICLE

Metaphorical Frameworks in Contemporary English Cybersecurity Terminology

Dr. Kwesi Boateng
Department of Applied Philology, University of Ghana

VOLUME: Vol.06 Issue09 2026

PAGE: 01-07

Abstract

Contemporary cybersecurity terminology is characterized by a substantial use of metaphorical expressions through which technically complex, abstract, and often invisible processes are conceptualized in more accessible linguistic forms. Terms such as attack, defence, firewall, virus, phishing, trap, shield, and vulnerability demonstrate how cybersecurity discourse draws upon established conceptual domains, particularly warfare, biological processes, physical protection, and human interaction. This study examines the conceptual and metaphorical frameworks underlying contemporary English cybersecurity terminology and proposes an analytical model for interpreting the relationships between source domains, target concepts, and terminological functions. The research employs a qualitative conceptual analysis based exclusively on the theoretical and methodological perspectives represented in the selected literature. Conceptual Metaphor Theory, conceptual blending, extended approaches to metaphor, and systematic metaphor identification provide the principal theoretical foundation. The analysis indicates that cybersecurity metaphors are not merely stylistic devices but functional mechanisms of specialized conceptualization: they organize professional knowledge, structure threat perception, facilitate communication, and influence how digital risks are interpreted. The study further demonstrates that metaphorical cybersecurity terminology combines conventionalized conceptual mappings with context-dependent extensions, creating a dynamic terminological system. The proposed framework distinguishes between source-domain structure, conceptual mapping, terminological realization, and communicative function. The findings contribute to the linguo-cognitive study of specialized English terminology and provide a basis for more systematic analysis of metaphorical processes in cybersecurity discourse.

KEYWORDS

Cybersecurity terminology, conceptual metaphor, metaphorical models, English terminology, cognitive linguistics, conceptual domains, cybersecurity discourse, terminological analysis, conceptual blending.

1. INTRODUCTION

Cybersecurity represents a highly specialized field whose terminology must describe processes that are frequently intangible, technologically complex, and difficult to observe directly. Digital attacks, unauthorized access, malware propagation, data breaches, network vulnerabilities, and defensive mechanisms occur within computational environments, yet their linguistic representation frequently relies on concepts originating in physical, biological, military, and everyday human experience. The resulting terminology therefore constitutes an important area for examining how

language transforms specialized knowledge into cognitively accessible structures.

The central problem addressed in this study is the systematic role of metaphor in the formation and interpretation of contemporary English cybersecurity terminology. A metaphorical term does more than provide an alternative label for a technical phenomenon. It may activate a structured conceptual domain through which users understand the phenomenon itself. Lakoff and Johnson's foundational account establishes metaphor as a mechanism through which abstract conceptualization is structured by more concrete domains (Lakoff & Johnson, 1980). Gibbs (1994) similarly emphasizes the cognitive significance of figurative thought and its relationship to understanding. These perspectives provide a productive basis for examining cybersecurity terminology as a cognitively organized system rather than as an isolated collection of technical labels.

The relevance of such analysis has increased as cybersecurity has become integrated into institutional, commercial, governmental, and everyday communication. A term such as cyberattack, for example, immediately activates elements of confrontation, opposition, intentional action, and defence. Similarly, firewall evokes a physical barrier designed to contain or prevent destructive processes. Such expressions compress complex technical information into recognizable conceptual structures.

Previous metaphor research demonstrates that metaphorical interpretation can be investigated systematically rather than intuitively. Steen et al. (2010) provide a methodological foundation for linguistic metaphor identification, while Kryknitska (2024) emphasizes the importance of modifying analytical procedures to accommodate the complexity of conceptual metaphor. More recent scholarship also recognizes that metaphorical meaning may operate across different levels and modalities rather than through a single static mapping (Dyrmo, 2025).

Against this background, the present study aims to identify major metaphorical frameworks relevant to contemporary English cybersecurity terminology, explain their conceptual organization, and assess their functional significance. Particular attention is given to the interaction between conventionalized metaphorical terms and broader conceptual models. The study also considers how metaphor contributes to terminological accessibility, threat conceptualization, and professional communication.

2. LITERATURE REVIEW

The theoretical foundation of the study begins with Conceptual Metaphor Theory. Lakoff and Johnson (1980) conceptualize metaphor as a systematic relationship between conceptual domains rather than merely a linguistic ornament. This approach is particularly applicable to cybersecurity because many technical concepts are represented through mappings from familiar experiential domains. A cybersecurity attack, for instance, can be understood through a WARFARE source domain, whereas a virus activates a BIOLOGICAL source domain.

Gibbs (1994) extends the cognitive perspective by treating figurative language as closely connected with conceptualization and interpretation. His approach supports the assumption that metaphorical terminology can influence how specialized information is mentally processed. In cybersecurity discourse, the cognitive value of metaphor is therefore associated not simply with lexical novelty but with the activation of structured knowledge.

Kövecses (2020) develops an extended perspective on conceptual metaphor, allowing greater attention to contextual and communicative factors. This is significant for cybersecurity terminology because a single metaphorical source domain may generate different expressions depending on technological context. The metaphor of warfare, for example, may structure terminology relating to attacks, defence, targets, and countermeasures, but the precise interpretation of each term depends on the cybersecurity context.

Fauconnier and Turner (2002) provide a complementary theoretical perspective through conceptual blending. Rather than viewing meaning exclusively as a direct mapping between two domains, blending theory makes it possible to explain how elements from multiple conceptual spaces can combine to produce emergent meaning. Cybersecurity terminology frequently demonstrates this complexity because technical phenomena may simultaneously be conceptualized through physical, military, biological, and social frames.

Research specifically addressing metaphor identification provides an important methodological dimension. Steen et al. (2010) develop MIPVU as a systematic approach to linguistic metaphor identification. Its relevance to cybersecurity terminology lies in the possibility of distinguishing metaphorically motivated expressions from expressions whose metaphorical origins have become conventionalized. Gaskins,

Falcone, and Rundblad (2024), using a usage-based approach, further demonstrate that metaphor identification can be connected to actual patterns of language use rather than exclusively theoretical categorization.

Recent studies demonstrate the continuing development of metaphor analysis. Banevych (2025) examines conceptual metaphor realization in political discourse, illustrating how metaphors can structure specialized communicative environments. Pasternak (2024) specifically addresses military metaphor as conceptual metaphor, providing a useful comparative foundation for understanding cybersecurity's extensive reliance on conflict-related conceptualization. Khmelnytskyi (2024) examines the conceptualization of emotion through a container metaphor, demonstrating how abstract phenomena can be structured through physical spatial relations.

Abu Rumman et al. (2023) demonstrate the value of corpus-assisted cognitive analysis in examining metaphorical structures. Their work is particularly relevant to the present study because it illustrates how metaphor can be investigated through the interaction of linguistic evidence and cognitive interpretation. This methodological orientation supports the analysis of cybersecurity terminology as a patterned system rather than as a collection of individually interpreted expressions (Abu Rumman et al., 2023).

The literature also indicates that metaphorical terminology is not restricted to general discourse. Sapozhnyk and Surodeikina (2025) examine metaphorization in specialized legal terminology, showing that metaphorical processes can contribute to the development of professional vocabulary. Selivanova (2008) provides a broader terminological framework for understanding linguistic categories and specialized vocabulary, while Hladun et al. (2018) directly document English cybersecurity and information-technology terminology.

A further contemporary dimension is introduced by Kramer (2025), who examines Conceptual Metaphor Theory as a prompting paradigm for large language models. This development is relevant because automated systems increasingly interact with specialized cybersecurity language. If metaphorical structures organize cybersecurity terminology, computational systems must be capable of recognizing both literal terminology and the conceptual structures underlying metaphorical expressions.

Despite these contributions, a specific research gap remains. Existing scholarship provides theories of metaphor, methodological approaches to identification, and studies of metaphor in various specialized domains, but comparatively less attention is devoted to integrating these perspectives into a unified framework for contemporary English cybersecurity terminology. The present study addresses this gap by developing a functional metaphorical framework that connects conceptual source domains, linguistic realization, cognitive interpretation, and cybersecurity-specific communicative functions.

3. METHODOLOGY

The study adopts a qualitative conceptual-analytical methodology. The methodological objective is not to measure the frequency of individual cybersecurity terms but to identify recurring conceptual structures through which cybersecurity phenomena are linguistically represented. The analysis integrates four analytical dimensions: source-domain identification, conceptual mapping, terminological realization, and communicative function.

The first dimension concerns the source domain. A source domain provides the experiential structure used to conceptualize a cybersecurity phenomenon. Four particularly significant domains can be distinguished for analytical purposes: WARFARE, BIOLOGY, PHYSICAL PROTECTION, and HUMAN/SOCIAL INTERACTION. These categories are analytically constructed from the conceptual principles established in the provided literature rather than treated as rigid taxonomies.

The second dimension concerns conceptual mapping. Mapping establishes which characteristics of a source domain are projected onto a cybersecurity target. In a WARFARE framework, for example, intentional confrontation, strategic planning, attack, defence, targets, and counteraction can be projected onto digital security events. The mapping does not imply that cyberspace literally constitutes a battlefield; rather, it provides a cognitive structure through which cybersecurity activity can be interpreted.

The third dimension is terminological realization. A conceptual mapping becomes linguistically observable through terms and expressions. Hladun et al. (2018) demonstrate the existence of a specialized lexical system encompassing information technologies and cybersecurity terms. Within such a system, metaphorical terminology can become sufficiently

conventionalized that users may no longer consciously recognize its metaphorical origin.

The fourth dimension is communicative function. Metaphorical terminology can simplify complex processes, organize expert knowledge, emphasize danger, establish relationships between events, and facilitate communication between specialists and non-specialists. The corpus-assisted perspective proposed by Abu Rumman et al. (2023) supports the methodological principle that metaphor should be examined in relation to linguistic context rather than through isolated lexical interpretation.

On this basis, the proposed analytical framework can be represented conceptually as:

Source Domain → Conceptual Mapping → Cybersecurity Target → Terminological Realization → Communicative Function

For example:

WARFARE → confrontation/attack/defence → cyber threat environment → attack, defence, target, countermeasure → threat interpretation and strategic communication.

A second example involves the biological domain:

BIOLOGY → infection/propagation/host → malicious software activity → virus, infection, propagation → explanation of malware behaviour.

A third example involves physical protection:

PHYSICAL BARRIER → containment/blocking → network security mechanism → firewall/shield/barrier → explanation of preventive security functions.

The framework also accommodates blended conceptualization. Fauconnier and Turner (2002) make it possible to understand cases in which multiple conceptual inputs contribute simultaneously to interpretation. A cybersecurity expression may therefore combine technological knowledge with military, biological, or physical schemas. This is particularly important where a technical process cannot be adequately explained through a single source domain.

The analysis further incorporates the distinction between conventional and contextually activated metaphors. Steen et al. (2010) provide a basis for systematic identification, while Dyrmo (2025) emphasizes the need to account for different levels, modalities, and meaning-making processes. Consequently, metaphorical analysis should not assume that every metaphor has identical cognitive salience for every user.

The methodological limitation is that a qualitative framework cannot by itself establish statistical frequency or population-wide interpretations. A larger corpus would be required to determine the productivity of particular metaphorical models, their distribution across cybersecurity subfields, and changes over time. Nevertheless, conceptual analysis is appropriate for establishing the structural relationships required for subsequent empirical investigation.

4. RESULTS

The analysis indicates that contemporary English cybersecurity terminology can be interpreted through several interconnected metaphorical frameworks rather than through a single dominant model. The most structurally productive framework is the WARFARE model, in which cybersecurity is conceptualized through confrontation between opposing agents. Terms such as attack, defence, target, and countermeasure provide a coherent conceptual configuration. The significance of this model lies in its ability to organize multiple cybersecurity events within a recognizable strategic structure. Pasternak's (2024) treatment of military metaphor as conceptual metaphor provides a relevant theoretical parallel, while the cognitive approach of Abu Rumman et al. (2023) supports interpreting such patterns as systematic conceptual structures rather than isolated lexical choices.

A second major framework is the BIOLOGICAL model. Cybersecurity discourse frequently represents malicious software and digital compromise through concepts associated with organisms and disease. Expressions related to infection, propagation, and hostile biological agents provide an intuitive representation of how malicious code enters and spreads through digital environments. This model is particularly effective when the communicative objective is to explain process and transmission rather than intentional strategic conflict.

The third framework is the PHYSICAL PROTECTION model, which conceptualizes digital security through barriers, containers, shields, and controlled spaces. A firewall, for example, can be interpreted as a conceptual extension of a physical structure designed to prevent destructive forces from crossing a boundary. This framework makes otherwise abstract computational filtering processes more cognitively accessible.

A fourth framework can be described as the HUMAN/SOCIAL

INTERACTION model. Cybersecurity terminology also conceptualizes digital threats through deception, trust, intrusion, exploitation, and interpersonal interaction. Such expressions are particularly important in areas where human behaviour represents a central security factor. The metaphorical structure consequently shifts attention from purely technical mechanisms to relationships between agents.

The findings also demonstrate that these frameworks may overlap. A single cybersecurity event can simultaneously be understood as an attack, an intrusion, an infection, or a breach of a protected boundary. Such poly-conceptualization reflects the flexibility described in extended approaches to metaphor (Kövecses, 2020; Dyrmo, 2025). Rather than representing terminological inconsistency, the coexistence of models allows different aspects of the same phenomenon to be highlighted.

Another significant finding is the progressive conventionalization of metaphorical terminology. Once expressions become established technical terms, their metaphorical motivation may become less cognitively prominent. Nevertheless, their conceptual structure remains functionally significant because it continues to influence categorization and explanation. The systematic identification principles developed by Steen et al. (2010) are therefore important for distinguishing lexical conventionalization from complete loss of metaphorical motivation.

Finally, metaphorical cybersecurity terminology performs an important pedagogical and communicative function. It creates conceptual bridges between highly specialized computational processes and familiar experiential knowledge. This supports the broader conclusion that metaphorization is a productive mechanism of terminology formation rather than a peripheral linguistic phenomenon.

5. DISCUSSION

The findings suggest that metaphorical frameworks constitute an important cognitive infrastructure of contemporary English cybersecurity terminology. Their significance extends beyond lexical creativity because they determine which characteristics of a cybersecurity phenomenon become salient. A WARFARE model foregrounds agency, conflict, strategy, and defence; a BIOLOGICAL model foregrounds infection and propagation; a PHYSICAL PROTECTION model emphasizes boundaries and prevention; and a SOCIAL INTERACTION model emphasizes human relationships and behavioural manipulation.

This differentiation has theoretical implications for Conceptual Metaphor Theory. Lakoff and Johnson (1980) provide the fundamental premise that conceptual domains structure one another, while Kövecses (2020) demonstrates the importance of extending this perspective to contextualized conceptualization. Cybersecurity terminology supports this extended view because the same technical environment can generate multiple metaphorical interpretations depending on communicative purpose.

The findings also support the relevance of conceptual blending. Fauconnier and Turner (2002) allow metaphorical interpretation to be understood as an emergent process in which elements from different conceptual spaces can interact. This is especially valuable for cybersecurity because digital phenomena often combine properties that do not belong naturally to one experiential domain. A malicious program, for example, can be conceptualized simultaneously as an artificial agent, a biological contaminant, and an attacking force.

From a methodological perspective, the results indicate that cybersecurity metaphor analysis should combine systematic identification with cognitive interpretation. Steen et al. (2010) provide a foundation for linguistic identification, while Abu Rumman et al. (2023) demonstrate the value of corpus-assisted cognitive analysis. A future empirical cybersecurity study could therefore combine corpus frequency, contextual analysis, metaphor identification, and domain mapping. Such integration would reduce the risk of treating metaphor solely according to researcher intuition.

The practical implications are equally significant. For cybersecurity educators, metaphorical terminology can improve explanation of difficult technical concepts. For translators, awareness of source-domain structures can help preserve conceptual meaning across languages. For terminologists, metaphor analysis can assist in identifying relationships among apparently unrelated technical terms. The relevance of Hladun et al. (2018) is particularly clear in this context because specialized cybersecurity dictionaries provide an important lexical basis for examining such relationships.

However, metaphorical frameworks also have limitations. Metaphors simplify complex phenomena, and simplification can produce conceptual distortion. The WARFARE model may encourage an overly adversarial understanding of security, while the BIOLOGICAL model may emphasize propagation without adequately representing deliberate human agency. Similarly, physical-barrier metaphors may suggest that cybersecurity can be secured through static boundaries even

though contemporary digital environments are dynamic and interconnected.

The literature indicates that metaphorical interpretation is also context-sensitive. Gaskins et al. (2024) demonstrate the importance of usage-based analysis, while Dyrmo (2025) emphasizes the complexity of metaphorical meaning-making. Consequently, no metaphorical classification should be treated as universally fixed. Abu Rumman et al. (2023) further reinforce the importance of contextual and corpus-based examination when interpreting metaphorical structures.

A final limitation concerns technological change. Cybersecurity terminology evolves rapidly, meaning that new technologies may introduce new source domains or transform existing mappings. The framework proposed here should therefore be treated as an analytical model capable of expansion rather than as a closed taxonomy.

6. CONCLUSION

This study has examined contemporary English cybersecurity terminology as a cognitively structured system of metaphorical conceptualization. The analysis demonstrates that cybersecurity language relies on several major metaphorical frameworks, particularly WARFARE, BIOLOGY, PHYSICAL PROTECTION, and HUMAN/SOCIAL INTERACTION. These frameworks provide conceptual structures through which abstract digital processes become linguistically accessible and communicatively manageable.

The proposed framework—Source Domain → Conceptual Mapping → Cybersecurity Target → Terminological Realization → Communicative Function—integrates cognitive, linguistic, and functional dimensions of metaphorical terminology. It demonstrates that metaphorization contributes not only to naming but also to classification, explanation, professional communication, and threat perception.

The study further establishes that cybersecurity metaphors are dynamic rather than static. Conventionalized expressions may coexist with context-dependent metaphorical extensions, while multiple source domains can interact in the conceptualization of a single technical phenomenon. This finding supports extended and blending-based approaches to metaphor and highlights the importance of systematic identification methods.

The principal contribution of the research is therefore the conceptual integration of metaphor theory with cybersecurity terminology analysis. Future research should empirically test the proposed framework through large-scale English cybersecurity corpora, investigate metaphor frequency across cybersecurity subfields, compare metaphorical patterns across languages, and examine how emerging technologies reshape established conceptual mappings. Such work could strengthen the connection between cognitive linguistics, terminology studies, cybersecurity communication, and computational language analysis.

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.
2. Banevych, M. (2025). Conceptual metaphor realization in political discourse. Studia Methodologica, 59, 18-25.
3. Dyrmo, T. (2025). Extending extended conceptual metaphor theory: Rethinking levels, modalities, and meaning-making. Cognitive Semiotics, 18(1), 23-51.
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.
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.
9. Kövecses, Z. (2020). Extended conceptual metaphor theory. Cambridge: Cambridge University Press.
10. Kramer, O. (2025). Conceptual metaphor theory as a prompting paradigm for large language models. ArXiv.

11. Kryknitska, I.O. (2024). Modification of the algorithm for conceptual metaphor analysis. Transcarpathian Philological Studies, 36, 89-93.

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.

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.

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.

17. Stroganova, H. (2025). Development of views on the linguo-cognitive nature of metaphor. Studia Methodologica, 59, 226-235.