DOI: https://doi.org/10.46687/CBZV3576

ON CORPUS STUDIES OF MILITARY METAPHORICAL EXPRESSIONS IN THE ENGLISH CYBER SECURITY DISCOURSE

Stela Zhelezova

Abstract: *The current paper investigates the metaphorical model "Cyberspace is a battle" within the discourse of cybersecurity, with a particular focus on the prevalence and function of military metaphors across both professional and popular contexts. Building upon existing literature that underscores the importance of metaphor in comprehending intricate domains such as cybersecurity, the study posits that metaphors fulfill distinct pragmatic functions depending on the discourse type, especially in contrasting professional and popular scientific texts. Utilizing a corpus-based methodology, the research analyzes a range of texts from NATO documents alongside popular scientific literature to systematically identify and categorize military metaphors. The study compiles four specialized corpora, revealing that military metaphors significantly permeate cybersecurity language. Terms such as "cyber attack" and "cyberspace operation" are frequently employed to articulate strategic concepts, thereby highlighting the metaphor's role in shaping discourse within the field.*

Key words: *cybersecurity, military metaphors, corpus-based approach*

ЗА КОРПУСНИТЕ ИЗСЛЕДВАНИЯ НА ВОЕННИ МЕТАФОРИЧНИ ИЗРАЗИ В АНГЛИЙСКИЯ ДИСКУРС ЗА КИБЕРСИГУРНОСТ

Стела Железова

Анотация: *Статията изследва метафоричния модел „Киберпространството е битка" в дискурса на киберсигурността, като се обръща специално внимание на разпространението и функцията на военните метафори както в професионален, така и в популярен контекст. Въз основа на съществуващата литература, която подчертава значението на метафората за разбирането на сложни области като киберсигурността, изследването изказва предположението, че метафорите изпълняват различни прагматични функции в зависимост от типа дискурс, особено в контрастиращите професионални и популярни научни текстове. Използвайки корпусна методология, изследването анализира редица текстове от документи на НАТО заедно с научнопопулярна литература, за да идентифицира и категоризира систематично военните метафори. Изследването съставя четири специализирани корпуса, които разкриват, че военните метафори проникват значително в езика на киберсигурността. Термини като „кибератака" и „операция в киберпространството" често се използват за формулиране на стратегически понятия, като по този начин се подчертава ролята на метафората за формиране на дискурса в тази област.*

Ключови думи: *киберсигурност, военна метафора, корпусно изследване*

I. Introduction

In recent years, the study of metaphors has expanded significantly, with numerous works being published from various perspectives. The foundation for linguistic research in cybersecurity is based on the idea that thinking about cyber security "from a metaphorical perspective could lead to a deeper understanding of current approaches to cyber defense and perhaps to some creative new approaches". (Moore, Parrott & Karas 2008).

Investigating all aspects of metaphorical expressions in English cybersecurity discourse extends far beyond the scope of a single academic article.

Cybersecurity discourse involves various types of knowledge. They are presented through different metaphorical models from cybersecurity terminology. The conducted analysis of academic publications on metaphor use in cybersecurity discourse allows formulating the hypothesis that metaphors in professional discourse serve different pragmatic purposes compared to those in popular scientific discourse and mass media.

This work is only the first stage of research on the metaphorical model "Cyberspace is a battle" proposed by the author. From the author's view the term "cyberspace" is a metaphor based on its etymology.

It is not by chance that the work studies metaphors, which are military expressions. As George Lakoff and Mark Johnson (1980) noted in their seminal work *Metaphors We Live By*, our everyday thinking often operates in terms of warfare.

War metaphors are ubiquitous in discussions of everything from political campaigns to battles with cancer to wars against crime, drugs, poverty, and even salad. (Flusberg et al. 2018; Sun 2010).

In Russian academic discourse, there are numerous publications dedicated to the use of military metaphorical expressions in English-language political discourses.

Research indicates that military metaphors comprise up to 30% of metaphors in different groups (Fedotova 2018). In English-language popular scientific discourse, the metaphorical model of war has great potential for interpreting cyber threats and measures aimed at their prevention (Savchenko 2023).

Military metaphors are understood as expressions involving elements of military action characterized by opposition ("us" versus "them," i.e., enemy) and the use of weaponry (Savchenko 2023). A military metaphor is defined as a type of metaphor where the semantic structure explicitly or implicitly represents the concept of "war" (Fedotova 2018). According to Yutkina (Yutkina 2017) a military metaphor can be defined as a metaphor that focuses on a lexeme that denotes a military reality, while the context, the environment of that lexeme may be unrelated to the military theme. For the purposes of this study, the author uses Yutkina's definition of a military metaphor, as it is the most comprehensive.

The objective of this study is to examine the content of the metaphorical model "Cyberspace is a battle" within the professional discourse of cybersecurity and within NATO's normative documents related to this field. Additionally, the study proposes a corpus-based approach to facilitate the analysis of military metaphorical expressions in this context. The corpus research primarily focuses on texts from the popular domain and on NATO's normative and regulatory documents. The subject of the study is the semantic content of the proposed metaphorical model, while the object is the systematic investigation of this model within the specified contexts.

II. Discussions

At present, new works on the study of metaphorization processes based on different approaches are published. The corpus method, the study of linguistic phenomena on the basis of corpus data of a language, is considered to be the most promising. This method is represented by a large number of works covering various fields of research - lexicographic, semantic, grammatical and discursive (Ryukova 2023). The application of corpus methods in the analysis of metaphors and metaphorical

models is reflected in Ryukova's work (Ryukova 2023). Researchers use two ways of involving corpus data in metaphor research. First, the dominant metaphors in the discourse are discovered. Then, with the help of corpus tools, verify, confirm or refute various, sometimes contradictory, claims about the nature of metaphor (Ryukova, 2024). For comparison of the approach of the current study two examples of corpus research could be used.

A publication by Cariola (Cariola 2015) presents a research corpus "Cyber Security Corpus". It is a half million-word corpus that includes a total of 313 texts. Search terms used include "cyber security", "cybersecurity", "cyber risk", "cyber security risk", "cybersecurity risk", "cyber attack", "cybersecurity attack", "cyber security attack", "information assurance", etc. The results showed that the most common nouns (e.g. "security", "cyber") often formed part of compound nouns that express abbreviated information, such as "cyber security" and "cyber attack/s".

An example of corpus-based metaphor research is a Zeng and Ahrens' study (Zeng, Ahrens 2023) on military metaphors, which used a corpus of 159,519 words from public speeches by politicians in Hong Kong. This study employed Critical Metaphor Analysis (CMA).

Instead of relying on large pre-parsed corpora, a small, targeted corpus was created and employed in real-time within the algorithm developed for the research of Hilton, Namin and Jones. A custom-built web scraper was used to gather the input data for evaluation.

For this corpus study, two glossaries were compiled from publicly available online sources. The first glossary, comprises 116 terms, which contain the word "cyber", including terms recommended by the NATO Standardization Office (NSO) (NATO 2021). The second one consists of 224 of the most commonly used English terms in professional cybersecurity discourse. These terms were used as keywords to search metaphors in the source corpora.

Four specialized corpora have been compiled as source to study metaphors in professional and popular scientific discourse on cybersecurity. The size of these corpora is sufficient to yield reliable research results:

- "NATO documents" – a corpus with current NATO military cybersecurity normative and regulatory documents (up to 2023), consisting of 252,922 words;
- "Corpus 3" – a corpus of popular scientific books on cybersecurity, containing 349,838 words;
- "NATO1123" – a corpus with summaries of the annual reports (2011-2023) of the NATO Secretary General, containing 39,859 words;
- "Stallings1"- a corpus of professional scientific books by the famous network security author W. Stallings, consisting of 154,222 words;

In corpus linguistics, **corpus-based** and **corpus-driven** approaches represent two different methodologies for analyzing language using corpora **(Seizova-Nankova 2016).** Here the corpus-based model is preferred. It is based on deduction or "top-down" approach, and the corpus only serves as a database of examples (Dagnev 2018).

From the most widely used corpus research software, AntConc platform (https://antconc.en.lo4d.com/windows) was chosen for the corpus studies in this paper because of its convenience and ease of use (Bogoyavlenskaya 2022).

It is a common procedure in corpus linguistics for computer text processing to create a frequency list and to compare with reference corpora. Identification within

corpora could be done by isolating concordances - the list of uses of a given word in a corpus. This allows the researcher to see all occurrences of the word in the corpus, arranged around the search word.

Some scientific publications indicate that the most frequently used nouns in popular cyber security discourse are "ambush", "attack" (with the highest frequency), "battle", "campaign", "espionage", "intervention", etc. (Savchenko 2023). Therefore, the first experiments with the program were conducted using these keywords.

The first experiments were conducted to determine the highest frequency of the metaphorical expressions in the first 500 positions in the four corpora. In "NATO documents" corpus, the most frequent term is "cyberspace operations" with 766 hits, the second – "in cyberspace" (457 hits,) and the third – "of cyberspace" (411 hits). In "Corpus 3" the most frequent lexeme is "attack", followed by "cybersecurity". In "NATO 1123" corpus: first is "cyber defence" (151 hits), then "smart defence" (47 hits) and "cyber threats" (26 hits). In "Stallings1" corpus: "public key" (424 hits), "the client" (174 hits), "private key" (133 hits), "network security" (98 hits), and "intrusion detection" (71 hits).

As our study shows, the most frequent nominative metaphor in Corpus3 is the lexeme "attack" in various collocations (1286 hits), used as the most general term for denotation. The lexeme "attack" is part of the phrase "cyberspace attack" - an act or action initiated in or through cyberspace to cause harmful effects (NATO 2021).

Key expression (Words)	***Popular NATO1123 (39872)***	***Prof Books1 (583891)***	***Prof Stallings (154222)***	***NATO documents (212415)***
attack vector	-	9	-	1
bastion host	-	-	14	-
brute force attack	-	24	4	-
demilitarized zone	-	-	1	-
kill chain	-	11	-	-
logic bomb	-	-	11	-
reverse shell	-	2	-	-
sandbox	-	8	2	-
threat	38	111	43	492
agent	1	88	66	7
attack	13	1286	193	506
boundary	-	23	41	7
collision	-	4	17	1
impact	10	102	8	128
red team	-	2	-	4
total: 15 (100 %)	*4*	*12*	*11*	*7*
hits:	***27 %***	***80%***	***73%***	***47%***

Table 1. Frequency of Key Professional Cybersecurity Terms

In order to determine the correlation of the metaphorical expressions in the developed corpora with the military metaphors defined by other researchers, research was conducted with keywords - nouns only - defined by Savchenko (2023). The result allows the formulation of three semantic fields (frames) in the metaphorical model

"Cyberspace is a battle": "Military actions and events", "Participants in military actions", and "Weapons".

Table 2. shows the percentages of the results for each frame relative to the total number of nominations of the metaphorical terms. The closest in frequency percentage to the results of Savchenko (2023) are the results from the NATO1123 Corpus.

Frame	NATO 1123	NATO documents	Corpus 3	Stallings 1
Military Actions and Military Events	67%	62%	67%	65%
Participants in Military Operations	24%	23%	18%	26%
Weapons	9%	15%	15%	8%

Table 2. Percentage distribution of military-related frames across four different corpora

Using expertly selected key military metaphors from the compiled glossary on professional cybersecurity discourse, experiments were conducted with the software to determine the percentage ratio. The results are presented in the Table 3.

Key expression (Words)	***Popular NATO1123 (39872)***	***Prof Books1 (583891)***	***Prof Stallings (154222)***	***NATO documents (212415)***
cyber command	-	6	-	46
cyber arsenal	-	-	-	-
cyber attack	3	16	-	1
cyber espionage	-	6	-	1
cybersecurity	-	982	-	343
cyber incident	2	-	-	12
cyberspace	44	155	-	3236
cyberspace operation	-	-	-	19
total: 8 (100 %)	*3*	*5*	*0*	*7*
hits:	***38 %***	***63 %***	***0 %***	***88 %***

Table 3. Frequency of key cybersecurity terms including the word 'cyber' across four different corpora.

The results of the experiments conducted with the four specialized corpora support the hypothesis that professional military metaphors in cybersecurity appear with the highest frequency in corpora based on professional scientific texts. Only 38% of these terms in the table are used in the official statements of the NATO Secretary General, and 88% in the Alliance's normative and regulatory documents. 63% of the terms are used in the corpus composed of scientific publications in the field of cyber security. These data are in line with the conclusion of Isaeva (Isaeva 2013), that special knowledge is represented in different functional types of discourse by different metaphors.

As our research shows, the most frequent nominative metaphor in the NATO documents corpus are 766 colocations of the term "cyberspace operation" (19 hits in Table 3). The definition of "cyberspace operation" according to NATO is "actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and/or to create effects to achieve military objectives" (NATO 2021).

Research conducted with the compiled corpora revealed new metaphorical expressions, including "malicious cyber", "army cybersecurity", "offensive cyberspace", "cyberspace exploitation", and "smart defence".

III. Conclusions

Military metaphorical expressions are actively employed in English-language popular and science cybersecurity discourse. The metaphorical model of "battle" holds significant potential for interpreting cyber threats and the measures aimed at preventing them.

A novelty of the paper is the found images representing the metaphorical model "Cyberspace is a battle" in the English-speaking NATO discourse using corpus-based analysis. In the analyzed corpora, the model is represented by three semantic fields (frames). Pragmatically, the use of military metaphors in the popular scientific discourse of NATO public documents is related to the need to prove the seriousness of cyber threats and to motivate the target audience to comply with cybersecurity rules.

In professional cybersecurity discourse, military metaphors such as "cyber warfare", "cyber defense", and "cyber attack" are used with a focus on strategic thinking, technical accuracy, and informed decision-making, and are a starting point for professionals' search for approaches and tools to address them. The study of the frequency of these terms in the 4 corpora used and the prospective studies will be devoted to identifying three aspects - cognitive, semantic and pragmatic - of the use of military metaphorical expressions in the professional and popular discourse of NATO.

Future research will involve the continued collection of representative English-language material on metaphors in popular science texts related to cybersecurity. This will facilitate the identification of common metaphorical models and enable comparative analyses. The results from the analyzed corpora will be compared with those from a British reference corpus. Both the cognitive and pragmatic dimensions of military metaphors in professional and popular discourse will be explored. The research will seek to confirm the hypothesis that while metaphors in popular discourse highlight the importance of cybersecurity for society, those in professional and academic discourse serve as a foundation for developing tools and solutions to address specific cybersecurity challenges.

REFERENCES

Bogoyavlenskaya 2022: Bogoyavlenskaya, Y. Application of AntConc to study syntagmatic co-occurrence (based on adjectival collocations with components 'coronavirus' and 'Covid-19' in French). PNRPU Linguistics and Pedagogy Bulletin, (No. 1), 30-39 <https://doi.org/10.15593/2224-9389/2022.1.3 (status 23.10.2024)>.

Cariola 2015: Cariola, L. Introducing the Cyber Security Corpus (CySeC) – The use of semantic prosody in cyber security discourses [Conference presentation]. Social Networking in Cyberspace Conference (SNIC 2015), Wolverhampton, UK.

Dagnev, Saykova 2013: Dagnev, I., M. Saykova. Kriterii za sastavyane na korpus ot metaforichni termini pri sapostavitelno rzsledvane v balgarskata i angliyska anatomichna sistema. – V: Nauchnite trudove, tom LX „Hranitelna nauka, tekhnika i tekhnologii – 2013", 18-19 Oct. 2013, Plovdiv [Дагнев, И., М. Сайкова. Критерии за съставяне на корпус от метафорични термини при съпоставително изследване в

българската и английска анатомична система. – В: научни трудове, т. LX „Хранителна наука, техника и хехнологии – 2013“, 18-19 октомври 2013, Пловдив.

Fedotova 2018: Fedotova, N. Spetsifika upotrebleniya voennoy metaforay v sportivnom diskurse. // Filologicheskie nauki. Voprosay teorii i praktiki (vhodit v perecheny VAK). Tambov: Gramota. № 2. Ch. 2, 378-383 <http://dx.doi. org/10.30853/filnauki.2018-2-2.41 (status 12.11.2024)> [Федотова, Н. Специфика употребления военной метафоры в спортивном дискурсе. // Филологические науки. Вопросы теории и практики (входит в перечень ВАК). Тамбов: Грамота. № 2. Ч. 2, 378-383].

Flusberg, Matlock, Thibodeau 2018: Flusberg, S. J., T. Matlock, P. H. Thibodeau. War metaphors in public discourse. Metaphor and Symbol, 33 (1), 1-22. <https:// doi.org/10.1080/10926488.2018.1407992 (status 12.11.2024)>.

Hilton, Siami Namin, Jones 2022: Hilton, K., A. Siami Namin, K. S. Jones. Metaphor identification in cybersecurity texts: a lightweight linguistic approach. // SN Appl. Sci. 4, 60 <https://doi.org/10.1007/s42452-022-04939-8 (status 12.11.2024)>.

Isaeva 2013: Isaeva, E. Models of metaphor in computer security discourse (doctoral dissertation) (in Russian) <http://vak.ed.gov.ru (status 12.11.2024)>.

Lakoff, Johnson 1980: Lakoff, G., M. Johnson. Metaphors we live by. 1st ed. Chicago: University of Chicago Press.

Moore, Parrott, Karas 2008: Moore, J., L. Parrott, T. Karas. Metaphors for cyber security. Sandia National Laboratories <https://core.ac.uk/download/ pdf/71317606.pdf (status 02.11.2024)>.

NATO 2021: NATO Preferred 2021, Record 40601 NATO glossaries: AAP-06 <https://nso.nato.int/natoterm/content/nato/pages/home.html?lg=en (status 05.11.2024)>.

Ryukova 2023: Ryukova, A. Corpus studies of metaphor (on the example of metaphorization of nominations of natural phenomena)<https://orcid.org/0009-0005-7278-8276 (status 15.10.2024)>.

Ryukova 2024: Ryukova, A. R. Korpusno-oriyentirovannyye issledovaniya yazyka: kratkiy obzor dostizheniy i trudnostey. // *Russian Linguistic Bulletin, (1)* (49) <https: //cyberleninka.ru/article/n/korpusno-orientirovannye-issledovaniya-yazyka-kratkiy-obzor-dostizheniy-i-trudnostey (status 15.10.2024)> [Рюкова, А. Р. Корпусно-ориентированные исследования языка: краткий обзор достижений и трудностей. // *Russian Linguistic Bulletin, (1)* (49)].

Savchenko 2023: Savchenko A. A. Militarnaya metafora v angloyazychnom nauchno-populyarnom diskurse po kiberbezopasnosti: semanticheskiy, kognitivnyy, pragmaticheskiy aspekty. // Filologicheskiye nauki. Voprosy teorii i praktiki. Tom 16. Vypusk 9, 3028-3034 <https://doi.org/10.30853/phil20230473 (status 15.10.2024)> [Савченко А. А. Милитарная метафора в англоязычном научно-популярном дискурсе по кибербезопасности: семантический, когнитивный, прагматический аспекты. // Филологические науки. Вопросы теории и практики. Том 16. Выпуск 9, 3028-3034].

Seizova-Nankova 2016: Seizova-Nankova, T. Lexicogrammar of V_hand(s) collocations. A corpus-driven analysis. Shumen: Konstantin Preslavsky University Press.

Sun 2010: Sun, L. A cognitive study of war metaphors in five main areas of everyday English: Politics, business, sport, disease, and love [doctoral dissertation] <https://www.diva-portal.org/smash/get/diva2:397473/FULLTEXT01.pdf (status 02.11.2024)>.

Yutkina 2017: Yutkina, S. V. Funktsii voyennoy metafory v angloyazychnykh gazetakh. // Nauka bez granits, № 4 (9), 130-135. <https://cyberleninka. ru/article/n/funktsii-voennoy-metafory-v-angloyazychnyh-gazetah/viewer (status 02.11.2024)> [Юткина, С. В. Функции военной метафоры в англоязычных газетах. // Наука без границ, № 4 (9), 130-135].

Zeng, Ahrens 2023: Zeng, W. H., K. Ahrens. Corpus-Based Metaphorical Framing Analysis: WAR Metaphors in Hong Kong Public Discourse. Metaphor and Symbol, 38(3), 254–274 <https://doi.org/10.1080/10926488.2022.2158088 (status 02.11.2024)>.