Http://online.unisc.br/seer/index.php/signo
ISSN on-line: 1982-2014
Doi: 10.17058/signo.v48i91.17937

Recebido em 06 de Dezembro de 2022 Aceito em 05 de Janeiro de 2023 Autor para contato: gustavo.silva@cefet-rj.br

Ataques cibernéticos: a metáfora de guerra em ciências da computação

Cyber attacks: The war metaphor in computer science

Gustavo Paiva Guedes e Silva

Lilian Ferrari

Centro Federal de Educação Tecnológica Celso Suckow da Fonseca – CEFET/RJ – Rio de Janeiro – Rio de Janeiro – Brasil

Resumo: Este trabalho investiga o papel da conceptualização metafórica no desenvolvimento da teorização científica na área de Ciências da Computação e, mais especificamente, na subárea de "Segurança Cibernética". Com base em dados retirados de artigos acadêmicos publicados em anais de conferências reconhecidas na área da Computação ou Engenharias, a análise evidencia que a metáfora conceptual COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA predomina na abordagem científica de interferências não autorizadas em sistemas computacionais. Em particular, os resultados indicam que termos relacionados à metáfora em questão ocorrem, de forma consistente, em todos os textos analisados, evidenciando o processo cognitivo de mesclagem conceptual (FAUCONNIER e TURNER, 2002), bem como o fenômeno discursivo de metaforicidade (CAMERON, 2003).

Palavras-chave: metáfora; segurança cibernética; mesclagem conceptual; metaforicidade

Abstract: This work investigates the role of metaphorical conceptualization in the development of scientific theorizing in Computer Science and, more specifically, in the field of "Cybersecurity". Based on data retrieved from academic articles published in annals of recognized events in the field of Computing or Engineering, the analysis shows that the conceptual metaphor ILLEGAL COMPUTER COMMUNICATION NETWORK IS WAR predominates in the approach to unauthorized interference in computer communication networks. It is also pointed out that different warlike terms occur, consistently, throughout all texts, reflecting the cognitive process of conceptual blending (FAUCONNIER and TURNER, 2002), as well as the discourse phenomena of metaphoricity (CAMERON, 2003).

Keywords: metaphor; cybersecurity; conceptual blending; metaphoricity.

1 Introdução

Desde o trabalho pioneiro de Lakoff e Johnson (1980), que lançou as bases para a Teoria da Metáfora Conceptual (TMC), o estudo da metáfora constitui tópico central em Linguística Cognitiva. Em alinhamento com a premissa fundadora da área de que fenômenos linguísticos refletem aspectos da cognição humana, a investigação da metáfora tem fornecido evidências de que associações conceptuais se estabelecem para além de usos individuais ou convenções linguísticas. Ao caracterizarem a metáfora como processo de pensamento, e não apenas como "figura de linguagem", Lakoff e Johnson (1980) atestam sua ocorrência frequente na linguagem cotidiana, abrangendo diferentes níveis de formalidade e contextos discursivos variados.

Há, entretanto, determinados tipos de discurso, como o científico, que costumam ser caracterizados como mais objetivos, neutros e isentos (GEERTZ, 1988; ZAMEL e SPACK, 1998). A questão que se coloca, portanto, é: qual o *status* da metáfora nesse tipo de discurso? Com o objetivo de lançar luz sobre essa questão, o presente artigo investiga a ocorrência de metáforas no discurso científico, elegendo como foco de investigação as Ciências da Computação e, mais especificamente, a área de "Segurança Cibernética" voltada para a "Comunicação Ilegal em Redes de Computadores".[1]

O artigo está organizado em quatro seções principais. A seção 2 apresenta os pressupostos teóricos da pesquisa, detalhando as premissas básicas da Teoria da Metáfora Conceptual. Na seção 3, os procedimentos metodológicos explicitam o recorte do objeto de estudo, a origem dos dados, os objetivos e hipóteses da pesquisa. A análise, na seção 4, evidencia que os artigos científicos selecionados utilizam, consistentemente, o domínio-fonte GUERRA para estruturar metaforicamente o domínio-alvo de COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES. Mais especificamente, as expressões metafóricas mais frequentes nos artigos analisados são identificadas, quantificadas e exemplificadas, além de serem associadas ao processo discursivo de metaforicidade. Por fim, são discutidos os principais achados, explicitando a organização do *frame* que estrutura a metáfora COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA, e destacando as expressões que evidenciam a mesclagem conceptual associada a esse processo metafórico.

O trabalho tem como uma de suas principais contribuições o fornecimento de evidências de que a metáfora conceptual permite estruturar o pensamento científico na área de Ciências da Computação que, principalmente por fazer parte das chamadas "ciências duras", costuma ser considerada objetiva e literal. Além disso, não apenas são identificadas diferentes expressões metafóricas nos dados, como também se descrevem as inter-relações entre essas expressões na organização textual, com base na noção discursiva de metaforicidade.

2 Pressupostos teóricos

A Teoria da Metáfora Conceptual (LAKOFF; JOHNSON, 1980) tem como premissa básica a ideia de que nosso sistema conceptual ordinário, em termos do qual pensamos, falamos e agimos, é fundamentalmente de natureza metafórica. Trata-se de um processo que envolve, fundamentalmente, dois domínios cognitivos: o domínio-fonte, correlacionado com a experiência corporal e sensório-motora, e o domínio-alvo, mais abstrato. A metáfora conceptual resulta do estabelecimento de um mapeamento (mapping[2]) entre elementos do domínio-fonte e do domínio-alvo.

Um dos exemplos retomados por Lakoff e Johnson (1980) é a projeção metafórica COMUNICAÇÃO VERBAL É TRANSFERÊNCIA FÍSICA, inicialmente discutida por Reddy (1979) sob a denominação "Metáfora do Conduto". Reddy (1979) observou que nossa linguagem cotidiana sobre a

[1] Como ficará claro no decorrer do trabalho, a denominação oficial da área – "Segurança cibernética" - já reflete a conceptualização metafórica que norteia a investigação científica sobre o assunto.

[2] O termo inglês *mapping* tem sido traduzido em português como mapeamento, correspondência ou projeção (entre domínios).

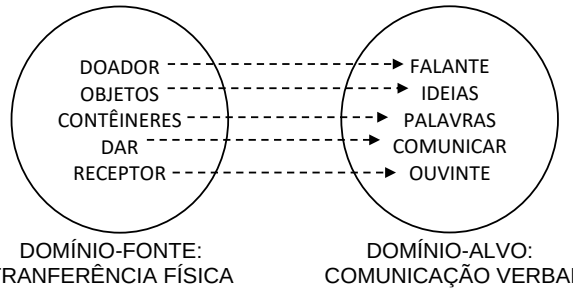
linguagem costuma se estruturar com base na ideia de transferência física de um objeto de um doador para um receptor.

A Metáfora do Conduto foi documentada, em inglês, com base em mais de cem tipos de expressões sobre a comunicação verbal, concebida como um processo no qual o falante coloca ideias (objetos) em palavras (contêineres) e as envia (por um conduto) para o ouvinte que retira as ideias/objetos das palavras/contêineres. Consideremos alguns exemplos originais, e suas traduções em português:

(1a) *I gave you that idea.*
(1b) Eu te dei aquela ideia.
(2a) It's difficult to put my ideas into words.
(2b) É difícil colocar minhas ideias em palavras.

Os exemplos (1a)-(2a) e (1b)-(2b) evidenciam a ocorrência da Metáfora do Conduto em duas línguas distintas - o inglês e o português, respectivamente. No diagrama a seguir, é possível perceber como a correlação entre conceitos do domínio-fonte de TRANSFERÊNCIA FÍSICA são mapeados para conceitos do domínio-alvo de COMUNICAÇÃO VERBAL:

Figura 1: Mapeamento metafórico COMUNICAÇÃO VERBAL É TRANSFERÊNCIA FÍSICA.



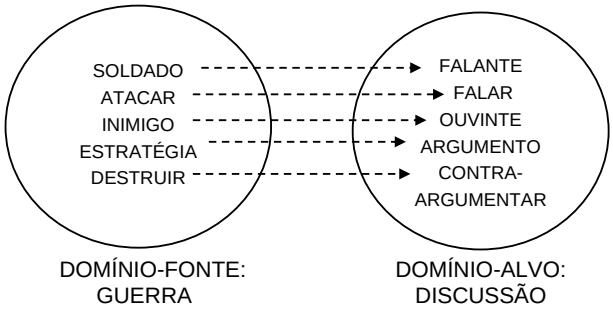
O mapeamento metafórico ilustrado na Figura 1 destaca a correspondência entre elementos do domínio-fonte de TRANSFERÊNCIA FÍSICA e elementos análogos no domínio-alvo de COMUNICAÇÃO VERBAL. Assim, "comunicar a respeito de uma ideia" é metaforicamente concebido como "dar a ideia para o interlocutor".

Outro exemplo emblemático discutido por Lakoff e Johnson (1980) é a projeção metafórica DISCUSSÃO É GUERRA. Vejamos alguns exemplos listados pelos autores e suas respectivas traduções em português:

(3a) *He attacked every weak point in my argument.*
(3b) Ele atacou cada ponto frágil do meu argumento.
(4a) *If you use that strategy, he'll wipe you out*.
(4b) Se você usar aquela estratégia, ele vai te destruir.

Os exemplos (3a)-(4a) e (3b)-(4b) refletem a compreensão, culturalmente motivada, de que discussões são concebidas como guerras. A projeção entre domínios pode ser assim representada:

Figura 2: Mapeamento metafórico DISCUSSÃO É GUERRA.



A Figura 2 destaca a correspondência entre elementos do domínio-fonte GUERRA e do domínio-alvo DISCUSSÃO.

O desenvolvimento da Teoria da Metáfora Conceptual, a partir desses *insights* iniciais, envolveu uma série de refinamentos teóricos. Casasanto (2013) chamou atenção para o fato de que o termo "metáfora conceptual" foi usado, muitas vezes, de forma ambígua, referindo-se a expressões linguísticas propriamente ditas, a representações mentais não linguísticas e, outras vezes ainda, a pareamentos de representações linguísticas e não linguísticas. Para delimitar os conceitos de forma a evitar ambiguidades, o autor propôs o uso dos termos "metáfora linguística", para indicar expressões

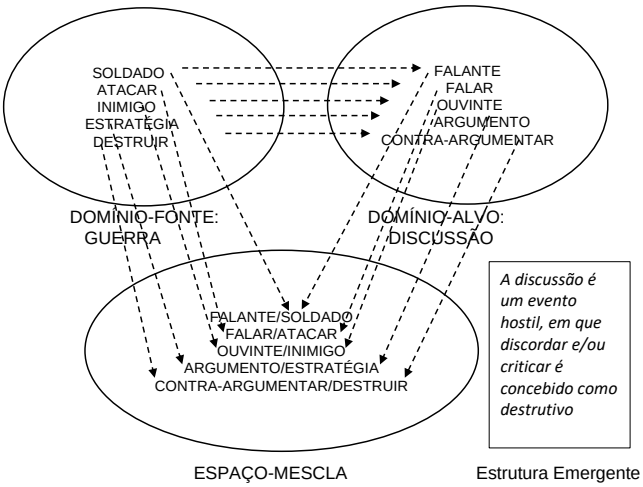
metafóricas na linguagem, e "metáfora mental", para referência ao mapeamento implícito entre domínio-fonte e domínio-alvo, subjacente às metáforas linguísticas. Em especial, as metáforas analógicas são metáforas mentais construídas através do mapeamento criativo e analógico entre os domínios fonte e alvo. No caso da Metáfora do Conduto, estabelece-se uma analogia entre as atividades de transferência física e a comunicação verbal. Da mesma forma, na Metáfora DISCUSSÃO É GUERRA, a analogia é estabelecida mentalmente, entre elementos dos domínios GUERRA e DISCUSSÃO, sem que haja necessariamente uma proximidade na experiência objetiva entre esses dois eventos.

Outro desenvolvimento teórico relevante com relação à conceptualização metafórica diz respeito à proposta, desenvolvida no âmbito da Teoria dos Espaços Mentais (FAUCONNIER, 1994, 1997) de que a construção criativa do significado envolve o processo de mesclagem conceptual (FAUCONNIER; TURNER, 2002). Os autores propõem que as metáforas ativam a integração conceptual dos domínios fonte e alvo em um espaço-mescla, no qual o significado novo é efetivamente criado.

Vale destacar que, sob essa perspectiva, os domínios fonte e alvo são concebidos como espaços mentais (*Input* 1 e *Input* 2), estruturados por *frames*, que constituem conjuntos de conhecimento inter-relacionados e culturalmente compartilhados, armazenados na memória de longo prazo (FILLMORE, 1982)[3]. Assim, o *frame* associado à GUERRA inclui, além das noções de *soldado, inimigo, atacar, estratégia e destruir*, que são relevantes para a construção do significado metafórico nas sentenças 3(a)-(b) e 4(a)-(b), outros elementos que podem ser ativados em outras sentenças. Por exemplo, a sentença *"O candidato foi bombardeado na entrevista*" faz referência à ação realizada com o material bélico "bomba", que também é parte do *frame* de GUERRA; no caso, a sentença destaca que o candidato foi duramente criticado pelos entrevistadores.

Retomando-se a metáfora DISCUSSÃO É GUERRA, a mesclagem pode ser assim representada:

Figura 3: MESCLAGEM CONCEPTUAL NA METÁFORA "DISCUSSÃO É GUERRA".



A representação da metáfora DISCUSSÃO É GUERRA em termos de mesclagem possibilita a explicitação do significado metafórico no Espaço-Mescla, onde ocorre, de fato, a fusão de elementos dos Inputs 1 e 2. O significado novo, oriundo da configuração dos elementos no espaço-mescla, é representado na Estrutura Emergente.

Por fim, vale notar que estudos recentes destacam a noção de *metaforicidade* (CAMERON, 2003; MÜLLER, 2008; MÜLLER; CIENKI, 2009), que leva em conta as relações entre metáfora e estrutura textual. Dentro dessa perspectiva, a metáfora mental é concebida como um fenômeno capaz de estruturar trechos extensos de discurso, não se limitando a uma associação estanque entre um processo cognitivo de projeção entre domínios e uma expressão linguística. Nesse sentido, adota-se uma visão processual em que a metáfora conceptual é tratada em termos de graus de ativação ao longo do texto. O processo discursivo reflete, portanto, o processo cognitivo subjacente.

[3] Adotamos, aqui, a proposta de Fauconnier (1997) de que *frames* e domínios (reconceptualizados como espaços mentais) são conceitos intimamente relacionados. Os *frames* são estruturas conceptuais armazenadas na memória de longo prazo que podem ser acessados para a estruturação de domínios locais – os espaços mentais -, à medida que o discurso se desenvolve.

A proposta de Ferrari e Felippe (2021) sobre metáforas no discurso acadêmico ilustra esse processo. As autoras analisaram artigos científicos nas áreas de ECONOMIA e BIOLOGIA, demonstrando que as metáforas analógicas ECONOMIA É SER VIVO e BIOLOGIA REPRODUTIVA É ATIVIDADE ECONÔMICA, respectivamente, estruturam os artigos analisados, ocorrendo com diferentes graus de ativação. Sendo assim, ao longo do texto de ECONOMIA, ocorreram instanciações da metáfora mais esquemática ECONOMIA É SER VIVO (exemplo 5), mas também instanciações mais específicas dessa metáfora como, por exemplo, MERCADO DE CAPITAIS É SER VIVO (exemplo 6):

(5) Este artigo é uma resenha sobre políticas publicas e *crescimento econômico* [...], (ECONOMIA É SER VIVO)
(6) Vale lembrar que, num país com *mercado de capitais em estágio embrionário* [...], (MERCADO DE CAPITAIS É SER VIVO)

Do mesmo modo, ao longo do artigo de BIOLOGIA, além da metáfora esquemática BIOLOGIA REPRODUTIVA É ATIVIDADE ECONÔMICA (exemplo 7), ocorreram também instanciações mais específicas, como, por exemplo, AGENTES DE POLINIZAÇÃO SÃO CONSUMIDORES (exemplo 8):

(7) Foram realizados 100 horas de observações durante o período de janeiro de 2005 [...] visando identificar os visitantes florais e os *consumidores primários de frutos.* (BIOLOGIA REPRODUTIVA É ATIVIDADE ECONÔMICA)
(8) Nas 100 horas de observação apenas em três momentos foram visualizados esses *consumidores*. (AGENTES DE POLINIZAÇÃO SÃO CONSUMIDORES)

A contribuição de Ferrari e Felippe (2021) lança luz sobre o fato de que o pensamento científico, tradicionalmente tratado como literal e objetivo, também se estrutura metaforicamente. Confirmando o que foi apontado por estudos anteriores em Linguística Cognitiva (LAKOFF e NUÑEZ, 2000), as autoras demonstram que, embora várias metáforas mentais ocorram em artigos científicos das áreas de Economia e Biologia, uma determinada projeção metafórica tende a ser predominante em cada área, ocorrendo com diferentes graus de ativação em função do processo de metaforicidade. Na esteira dessas propostas, o presente trabalho enfoca a produção acadêmica na área de "Segurança Cibernética", com base nos critérios metodológicos descritos a seguir.

3 Metodologia

Para investigar a estrutura conceptual envolvida na abordagem científica na área de "Segurança Cibernética", a pesquisa tem por objetivo identificar a conceptualização metafórica do campo. Os dados foram retirados de cinco artigos científicos, a saber:

Artigo 1- A segurança e as ameaças cibernéticas (DA SILVA; MORESI, 2013)

Artigo 2 -Um Sistema Autoadaptável para Predição de Ataques DDoS Fundado na Teoria da Metaestabilidade (PELLOSO et al., 2018)

Artigo 3 - Utilização de Redes Neurais Nebulosas para criação de um Sistema Especialista em Invasões Cibernéticas (BATISTA et al., 2018)

Artigo 4 - Análise de ataques cibernéticos de *jamming* e *spoofing* em drones (PEY; NZE; ALBUQUERQUE, 2022)

Artigo 5 - Uso de Workflows Científicos para Apoiar a Elaboração de Técnicas de Predição de Invasão de Sistemas (ALVES et al., 2014)

Os artigos foram selecionados no Google Scholar utilizando os termos: “segurança cibernética” e “ataque cibernético” e, entre aspas. Em seguida, foram selecionados cinco artigos em português, publicados em conferências reconhecidas na área da Computação ou Engenharias, dado que ambas as áreas estudam os fenômenos de ataques ilegais em redes de computadores.

Tomando por base os dados coletados, o objetivo principal do trabalho é verificar a ocorrência de conceptualização metafórica na estruturação dos artigos científicos selecionados. Em particular, o objetivo é verificar se há uma metáfora mental específica que se expresse por meio de diferentes metáforas linguísticas nos textos analisados, caracterizando o fenômeno de metaforicidade.

Com base nesses objetivos, as seguintes hipóteses foram estabelecidas: (i) os artigos científicos investigados refletem a ocorrência de conceptualização metafórica na área de “Segurança Cibernética”; (II) os artigos científicos investigados exibem metaforicidade, estruturando-se em torno de uma mesma metáfora mental, ativada em diferentes trechos do discurso.

Para investigar as hipóteses propostas, procedeu-se, inicialmente, a uma análise qualitativa, em que a ocorrência de conceptualização metafórica para referência à segurança cibernética foi identificada e classificada. Em seguida, foram selecionadas e quantificadas as expressões linguísticas mais frequentemente utilizadas para a expressão da metáfora mental que estrutura a conceptualização da área de Segurança Cibernética.

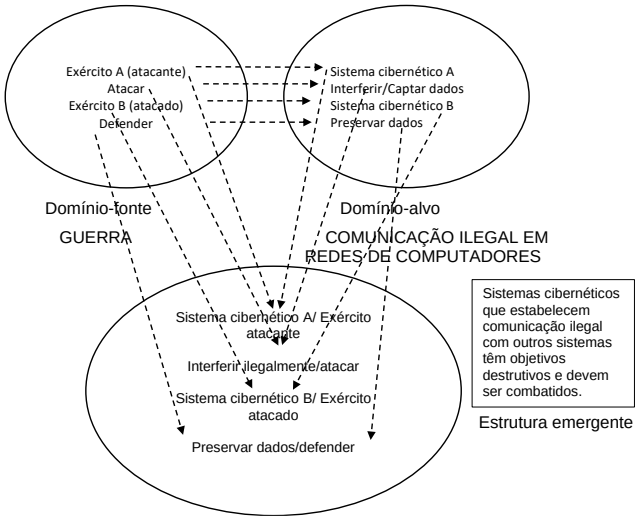
Na seção de análise, são apresentados exemplos selecionados, aleatoriamente, do total de ocorrências de cada expressão identificada. Nos casos em que um mesmo grupo abriga termos relacionados (ex. “ataque” e “atacante”), ou termos que diferem em função da presença ou ausência de modificador (ex. “ameaça” e “ameaça cibernética”), foram apresentados exemplos de ambos os usos.

4 Análise

A Tecnologia da Informação e Comunicações é essencial na sociedade contemporânea, envolvendo o acesso à Internet e à interconectividade entre sistemas de informação. A conceptualização desses fenômenos tem sido feita com base em metáforas mentais, tais como INTERNET É ESPAÇO (ex. *espaço cibernético*) e, ainda, INTERNET É ECOSSISTEMA (ex. *ecossistema cibernético, fluxo corrente de rede*, etc.).

Embora expressões metafóricas associadas a essas metáforas mentais sejam geralmente utilizadas para referência à Tecnologia da Informação, de um modo geral, no que diz respeito à área de “Segurança Cibernética”, que é foco do presente trabalho, a análise identificou a ocorrência da metáfora mental COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA[4]. A mesclagem conceptual associada a essa metáfora pode ser assim esquematizada:

Figura 4: Projeção metafórica COMUNICAÇÃO ILEGAL EM REDE DE COMPUTADORES É GUERRA.



[4] Vale destacar que as metáforas mentais INTERNET É ESPAÇO, INTERNET É ECOSSISTEMA e COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA são compatíveis. O que ocorre é que as duas primeiras se relacionam à conceptualização da internet, de um modo geral, enquanto a última é usada, mais especificamente, para a conceptualização da comunicação ilegal em redes de computadores, que é o foco da subárea de “Segurança cibernética”.

O mapeamento metafórico representado na Figura 4 apresenta os elementos básicos do domínio da GUERRA que estruturam o domínio-alvo COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES. Para que a projeção ocorra é preciso que haja, pelo menos, dois exércitos e uma relação bélica de ataque e defesa entre eles.

A análise permitiu a identificação de 9 termos/expressões metafóricas que ocorreram sistematicamente na maioria dos artigos para referência à comunicação ilegal em redes de computadores. A Tabela 1, a seguir, lista essas expressões, apresentando a frequência de cada uma delas em cada artigo e o total geral de ocorrências:

Tabela 1: Distribuição de expressões relacionadas à guerra.

EXPRESSÕES RELACIONADAS À GUERRA	Art. 1	Art. 2	Art. 3	Art. 4	Art. 5	Total de ocorrências
1. Ataque(s)/atacante(s) (cibernético(s))	29	129	35	25	43	261
2. Segurança (cibernética)	23	-	16	13	6	58
3. Invasão (cibernética)	6	1	17	3	11	38
4. Ameaça(s) (cibernética(s))	23	1	2	3	1	30
5. Alerta	-	16	1	-	1	18
6. Estratégia(s)/estratégicos(as)	6	2	4	1	4	17
7. Vulnerabilidade	6	3	2	4	1	16
8. Alvo	2	2	1	3	-	8
9. Proteção	1	-	3	2	2	8
Total	96	154	83	54	69	456

Como a Tabela 1 indica, os termos *ataque* e *atacante*, muitas vezes acompanhados do adjetivo *cibernético,* são os mais frequentes, correspondendo a 261 casos, distribuídos por todos os artigos. Consideremos os seguintes exemplos:

(9) Antes de qualquer resposta às questões formuladas, mesmo se a vítima de um *ataque cibernético* não planeja lançar um *ataque cibernético* em resposta, é importante caracterizá-lo como recebido para efeitos de aplicação da lei. (Artigo 1)
(10) A fim de sobrecarregar os servidores ou enlaces da rede, *os atacantes* empregam técnicas cada vez mais sofisticadas. (Artigo 2)

O termo *segurança,* também com a possibilidade de modificação adjetival – *cibernética* -, ocupa o segundo lugar geral em termos de frequência, correspondendo a 58 casos, distribuídos por quatro artigos. Vejamos:

(11) À medida que a utilização de *drones* provê maiores facilidades para o dia a dia das pessoas, os problemas de *segurança cibernética* são gradualmente expostos. (Artigo 4)

O termo *invasão* (e seus correlatos) é o terceiro mais frequente, correspondendo a 38 dos casos, distribuídos por todos os artigos. O termo faz referência à captação não-autorizada de dados, como ilustra o exemplo a seguir:

(12) Este trabalho propõe o uso de workflows científicos como uma forma de apoiar a elaboração de novas técnicas de predição de *invasão* de sistema, atuando na análise do fluxo de acessos e pacotes de dados, de forma a analisar e detectar comportamentos de tráfego suspeitos. (Artigo 5)

Nesse contexto, as anomalias da rede que possam preceder uma "invasão" são concebidas como "ameaças", e correspondem a 30 dados, distribuídos por todos os artigos. Consideremos os exemplos a seguir:

(13) O artigo sobre detecção de anomalias de rede com base em evolução de rede neural (...) descreve um sistema inteligente de aprendizagem de máquina, onde parte do sistema trabalha procurando *ameaças* conhecidas, e outra parte tenta detectar prováveis *ameaças* de acordo com atividades anormais que acontecem no sistema. (Artigo 3)

(14) Para o devido tratamento das *ameaças cibernéticas,* é necessário que a análise do problema seja baseada em uma visão mais abrangente (...)(Artigo 1)

Nos exemplos (13) e (14), o termo "ameaça" ocorre com diferentes modificações adjetivais: "ameaças conhecidas", "prováveis ameaças" e "ameaças cibernéticas".

O termo "alerta", por sua vez, corresponde a 18 casos, distribuídos por três artigos. Consideremos o seguinte exemplo:

(15) Caso um ataque DDoS[5] seja previsto, *um alerta* é emitido, sendo, neste trabalho, uma mensagem enviada para os sistemas de detecção ou mitigação, e/ou ao administrador da rede. (Artigo 2)

O exemplo (15) ilustra uma tendência comum nos dados que é a ocorrência dos termos *ataque* e *alerta* no mesmo contexto, evidenciando o processo de metaforicidade: uma vez que a metáfora COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA é ativada, expressões inter-relacionadas, associadas ao *frame* de GUERRA, também podem ocorrer ao longo do texto.

Os recursos computacionais que possibilitem lidar com programas capazes de captar dados de outro sistema são conceptualizados como "estratégias". O termo foi usado em todos os artigos, contabilizando 17 ocorrências. O exemplo (16) é uma delas:

[5] Um ataque distribuído de negação de serviço (do inglês, *distributed denial of service attack* - DDoS) é um tipo de ataque distribuído que ocorre a partir de muitos computadores. O objetivo é sobrecarregar os sites/serviços online com mais tráfego do que o servidor ou a rede podem comportar (GUPTA; DAHIYA, 2021).

(16) Nessa seção, é apresentada uma proposta de sistema de detecção de intrusão de tempo real cuja característica fundamental é a utilização de três workflows de apoio (...). A *estratégia* consiste em usar detectores avançados com o objetivo de monitorar a taxa de acerto do sistema. (Artigo 5)

Para referência aos casos em que o sistema não dispõe de "estratégias" para evitar a captação não-autorizada de dados, usa-se o termo *"vulnerabilidade"*. Foram identificadas 16 ocorrências, distribuídas por todos os artigos. O exemplo a seguir é um desses casos:

(17) Correios eletrônicos contextualmente relevantes são enviados para destinos específicos com documentos anexados que são encapsulados com código de exploração e *cavalo de Tróia*, visando tirar proveito de *vulnerabilidades* no software instalado no computador de destino. (Artigo 1)

Vale notar que o exemplo (17), além de fazer referência a "vulnerabilidades no software", usa a expressão "cavalo de Tróia", que remete à guerra entre gregos e troianos. Por analogia, a expressão faz referência a um programa que, embora pareça ter um conjunto de recursos úteis, é, na verdade, destrutivo.[6]

O termo "alvo", com 8 ocorrências distribuídas por quatro artigos, foi usado para referência a um computador ou sistema computacional (servidor) que sofre a interferência ilegal. Consideremos o exemplo a seguir:

(18) Nesse contexto, este trabalho advoga pela predição de ataques DDoS conhecidos (*known*) e desconhecidos (*unknown*). O objetivo é identificar esses tipos de ataques com antecedência à sobrecarga da rede ou do servidor *alvo* (...) (Artigo 2)

O exemplo (18) refere-se a servidores acessados ilegalmente como *alvo*, evidenciando a ativação da metáfora de guerra. Na verdade, a ocorrência da expressão "predição de ataques" no contexto imediatamente precedente deixa claro que a metaforicidade estrutura o texto como um todo.

Por fim, o termo "proteção" também apresentou 8 ocorrências distribuídas por 4 artigos. Vejamos:

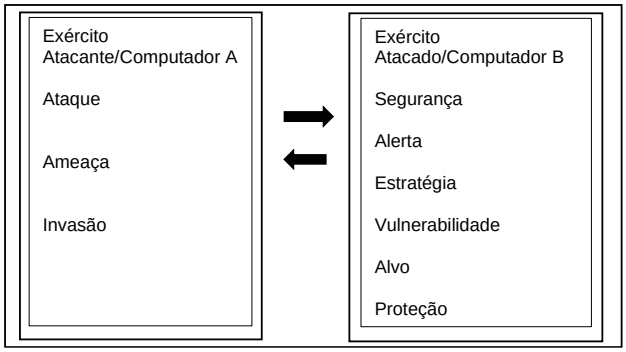
(19) Com o aumento do uso intensivo de dados e dos aplicativos em tempo real, a privacidade dos dados e os requisitos de segurança também devem ser reforçados a fim de proporcionar um confiável grau de *proteção* contra ataques de *jamming* e *spoofing*.

Mais uma vez, exemplo (19) evidencia uma tendência observada nos dados, que é a ocorrência do termo "proteção" associado às ideias de "segurança" e "ataque".

A análise apresentada nesta seção permite a compreensão de que conceitos inter-relacionados no *frame* de GUERRA são projetados para o domínio da COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES, e se refletem em expressões recorrentes na maioria dos artigos selecionados. Como se observa na Figura 5, os termos "ataque", "ameaça" e "invasão" referem-se a processos realizados pelo Computador A, de onde parte a comunicação ilegal em relação ao Computador B. Já os termos "segurança", "alerta", "estratégia", "vulnerabilidade", "alvo" e "proteção" dizem respeito ao Computador B, caracterizando problemas e modos de evitar os efeitos da comunicação ilegal.

Figura 5: *Frame* de GUERRA como estruturante da metáfora COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA.

[6] De acordo com a mitologia grega, o cavalo de Tróia foi um enorme cavalo de madeira, que se caracterizou como um falso presente, na medida em que seu interior abrigava inúmeros soldados gregos com a intenção de conquistar a cidade de Tróia.



Por fim, vale destacar que o termo "Segurança cibernética", utilizado oficialmente para nomear essa área de investigação, já ativa mesclagem conceptual. Tendo em vista que a noção de "segurança" é projetada do domínio-fonte da GUERRA e o elemento "cibernética" é projetado do domínio-alvo de COMUNICAÇÃO EM REDES DE COMPUTADORES, pode-se concluir que a expressão reflete a fusão desses dois domínios no espaço-mescla. Nesse novo domínio mesclado, é criada a construção de significado novo em que a comunicação ilegal em redes de computadores é, de fato, concebida como guerra.

Observação semelhante pode ser feita com relação aos termos "ataque cibernético", "ameaça cibernética" e "invasão cibernética", corroborando o caráter estruturante da metáfora de guerra (e da mesclagem conceptual que a representa) no desenvolvimento da investigação científica na área.

5 Considerações finais

Este trabalho enfocou a comunicação ilegal em redes de computadores, com o objetivo de investigar o papel da metáfora conceptual na estruturação do pensamento científico na área oficialmente denominada "Segurança Cibernética". Com base em artigos científicos que enfocam o tema, foi possível identificar que a metáfora COMUNICAÇÃO ILEGAL EM REDE DE COMPUTADORES É GUERRA como estruturante da investigação voltada para o desenvolvimento de conhecimentos que permitam solucionar os problemas advindos desse tipo de comunicação cibernética.

Os resultados indicaram que a mesclagem conceptual associada à metáfora identificada pôde ser evidenciada a partir de expressões associadas à guerra, que ocorreram, sistematicamente, na maioria dos artigos investigados. Em particular, os termos "ataque", "invasão" e "ameaça" relacionam-se ao computador de onde parte a interferência ilegal, enquanto os termos "segurança", "alerta", "estratégia", "vulnerabilidade", "alvo" e "proteção" costumam ser usados para referência ao computador que sofre esse tipo de interferência. É comum, ainda, o uso de alguns desses nomes modificados pelo adjetivo "cibernético(a)". Além da expressão "segurança cibernética", que dá nome à área, destacam-se, ainda, "ataque cibernético", "invasão cibernética" e "ameaça cibernética", que mesclam elementos dos domínios fonte e alvo.

Por fim, vale destacar que os termos aqui analisados não esgotam todas as ocorrências encontradas nos dados. Optamos, neste artigo, por enfocar as expressões metafóricas que ocorreram na maioria dos textos, com o objetivo de identificar os principais componentes do *frame* de guerra que estruturam a conceptualização da comunicação ilegal em redes de computadores, bem como os usos recorrentes desses termos no processo de metaforicidade. Entretanto, deve-se destacar que foram detectados uma série de outros termos relacionados à mesma metáfora, ainda que com frequência menos expressiva, como é o caso de "cavalo de Tróia" (cf. exemplo 15), que ocorreu em dois dos artigos analisados. A inclusão de termos desse tipo é um dos caminhos promissores de investigações futuras, na medida em que pode permitir o aprofundamento da análise e uma melhor compreensão dos fenômenos aqui descritos.

Com relação à área de "Segurança Cibernética" propriamente dita, a identificação da metáfora COMUNICAÇÃO ILEGAL EM REDES DE COMPUTADORES É GUERRA pode permitir que os cientistas que atuam na área reflitam sobre vantagens e desvantagens advindas desse tipo de

conceptualização. Embora a aplicação de conceitos associados ao domínio militar contribua para um *insight* global do fenômeno, destacando estratégias de ação e reação, a metáfora também pode ter aspectos limitantes quando se trata da compreensão da complexidade do fenômeno que, em última análise, é caracterizado pela incerteza e não linearidade.

Referências

ALVES, V. F.; SOUZA, C. G.; MACHADO, R.; OGASAWARA, E. BEZERRA, E. *Uso de Workflows Científicos para Apoiar a Elaboração de Técnicas de Predição de Invasão de Sistemas*. In XI Simpósio de Excelência em Gestão e Tecnologia, 2014.

BATISTA L. O.; DE SILVA G. A.; ARAÚJO, V. S; ARAÚJO, V. J.; REZENDE, T. S.; JUNIO, A.; GUIMARÃES, P. V*. Utilização de redes neurais nebulosas para criação de um sistema especialista em invasões cibernéticas*. In Anais do International Conference On Forensic Computer Science and Cyber Law (ICoFCS), 2018. DOI: DOI: http://doi.org/10.5769/C2018002.

CAMERON, L. *Metaphor and educational discourse*. London: Continuum, 2003.

CASASANTO, D. Development of metaphorical thinking: the role of language. In Mike Borkent, Barbara Dancygier, and Jennifer Hinnell (Eds.), *Language and the creative mind*. Stanford, CA: CSLI Publications, pp. 3–18, 2013.

DA SILVA, O. C. C.; MORESI, E. A. D. *A segurança e as ameaças cibernéticas*. In CISCI 2013 - Decima Segunda Conferencia Iberoamericana en Sistemas, Cibernetica e Informatica, Decimo Simposium Iberoamericano en Educacion, Cibernetica e Informatica, SIECI, 2013.

FAUCONNIER, G. *Mental spaces: aspects of meaning construction in natural language*. Cambridge: Cambridge University Press, 1994.

FAUCONNIER, G. *Mappings in thought and language*. Cambridge: Cambridge University Press, 1997.

FAUCONNIER, G.; TURNER, M. *The Way We Think*: Conceptual Blending and the Mind's Hidden Complexities*.* New York: Basic Books, 2002.

FERRARI, L.; FELIPPE, G. Metáforas no discurso acadêmico em Economia e Biologia: evidências sobre a natureza do domínio-fonte. *Revista Confluência*, vol. 60, pp. 173-197, 2021. DOI: http://doi.org/10.18364/rc.v1i60.409.

FILLMORE, C. Frame semantics. In The Linguistic Society of Korea (ed.), *Linguistics in the morning calm*. Seoul: Hanshin Publishing Co., pp. 111–137, 1982. DOI: http://doi.org/10.1515/9783110199901.373.

GEERTZ, C. *Works and lives:* The Anthropologist as Author**.** Stanford: Stanford University Press, 1988.

LAKOFF, G.; JOHNSON, M. *Metaphors we live by*. Chicago: Chicago University Press, 1980.

LAKOFF, G.; NUÑEZ, R. *Where mathematics comes from:* how t*he embodied mind brings mathematics into being*. New York: Basic Books, 2000.

GUPTA, B.B.; DAHIYA, A. *Distributed Denial of Service (DDoS) Attacks*: Classification, Attacks, Challenges, and Countermeasures (1ª ed.). CRC Press, 2021. DOI: http://doi.org/10.1201/9781003107354.

MÜLLER, C. What gestures reveal about the nature of metaphor. In: CIENKI, A.; _____. (Eds.), *Metaphor and Gesture*. Amsterdam: John Benjamins, pp. 219–245, 2008. DOI: http://doi.org/10.1075/gs.3.12mul.

MÜLLER, C.; CIENKI, A. Words, Gestures, and Beyond: Forms of Multimodal Metaphor in the Use of Spoken Language. In: FORCEVILLE, C.; URIOS-APARISI, E. (Eds.), *Multimodal metaphors.* Berlin, New York: Mouton de Gruyter, pp. 297-328, 2009. DOI: http://doi.org/10.1515/9783110215366.5.297.

PELLOSO, M.; VERGÜTZ, A.; SANTOS, A. Nogueira, M. *Um sistema autoadaptável para predição de ataques ddos fundado na teoria da metaestabilidade*. In Anais do XXXVI Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, pp. 726-739. SBC, 2018. DOI: http://doi.org/10.5753/sbrc.2018.2454.

PEY, J. N.; NZE, G. D.; ALBUQUERQUE. O. R. *Analysis of jamming and spoofing cyber-attacks on drones*. In 2022 17th Iberian Conference on Information Systems and Technologies – CISTI, 2022. DOI: http://doi.org/10.23919/CISTI54924.2022.9820201.

REDDY, M. The conduit metaphors. In A. Ortony (Ed.), *Metaphor and thought.* Cambridge: Cambridge University Press, 1979.

ZAMEL, V.; SPACK, R. *Negotiating academic literacies; teaching and learning across languages and cultures***.** New York: Rutledge, 1998.