MASTERARBEIT / MASTER'S THESIS

Titel der Masterarbeit / Title of the Master's Thesis

„Konzeptuelle Metaphern in der IT-Sprache am Beispiel von Cybersicherheitsfachsprache auf Deutsch, Englisch und Russisch"

verfasst von / submitted by

Alekseeva Kseniia

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Arts (MA)

Wien, 2023 / Vienna 2023

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	UA 070 360 331
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Masterstudium Translation Russisch Deutsch
Betreut von / Supervisor:	Ass.-Prof. Mag. Dr. Dagmar Gromann, BSc

Inhaltsverzeichnis

1. Einleitung 6
1.1 Forschungsfrage und Annahmen 7
1.2 Motivation und Zielsetzung 8
2. Grundlagen 10
2.1 Einführung in den Fachbereich Cybersicherheit 10
2.2 Fachsprache 13
2.3 Konzeptuelle Metapherntheorie 14
2.3.1 Die Entstehung der Metapherntheorie 14
2.3.2 Konzeptuelle Metaphern 15
2.3.3 Erfahrung als Basis für konzeptuelle Metaphern 17
2.3.4 Auswirkung der konzeptuellen Metapherntheorie auf die Forschung 18
2.3.5 Identifizierung von Metaphern 19
2.3.6 Herkunftsdomäne und Image Schemas 23
2.4 Kulturelle Spezifik von Metaphern 25
2.5 Konventionalisierte Metaphern 30
2.6 Kritik an der konzeptuellen Metapherntheorie 31
3. Aktueller Stand der Forschung 35
4. Methodik 39
4.1 Korpuserstellung 39
4.2 Metaphernidentifizierung 41
4.3 Methodische Herausforderungen für die Russische Sprache 44
4.4 Validierung der Ergebnisse 44
5. Forschungsergebnisse 46
5.1 Sprachübergreifende Analyse 46
5.2 Vergleich der metaphorischen Mappings 47
5.3 Sprachspezifische Detailanalyse für Metaphern-Gruppen 54
5.3.1 Deutsche Sprache 54
5.3.1.1 Kriegsmetaphern 54
5.3.1.2 Erkrankungsmetaphern 57
5.3.1.3 Innen/Außen-Metaphern 59
5.3.1.4 Jagdmetaphern 60
5.3.2 Englische Sprache 62
5.3.2.1 Kriegsmetaphern 62

5.3.2.2 Erkrankungsmetaphern 65
5.3.2.3 Innen/Außen-Metaphern 67
5.3.2.4 Jagdmetaphern 69
5.3.3 Russische Sprache 70
5.3.3.1 Kriegsmetaphern 70
5.3.3.2 Erkrankungsmetaphern 72
5.3.3.3 Innen/Außen-Metaphern 73
5.3.3.4 Jagdmetaphern 75
5.3.3.5 Angelnmetaphern 76
5.4 Construction Patterns 77
5.5 Ergebnisse der Umfrage 84
6. Diskussion 90
7. Schlussfolgerungen 95
8. Literaturverzeichnis 97
9. Abstract (Deutsch) 108
10. Abstract (Englisch) 109
11. Anhang 110
11.1. Fragebogen Deutsch 110
11.2. Fragebogen Englisch 113
11.3. Fragebogen Russisch 116

Abbildungsverzeichnis

Abbildung 1: Cyber-sicherheit (vgl. Pohlmann 2022: 2) 11
Abbildung 2: Cybersicherheitsbedrohungen (vgl. Prasad & Rohokale 2020: 2) 12
Abbildung 3: Metaphernvererbungsnetz (vgl. Dodge et al. 2015: 41) 22
Abbildung 4: Frame-To-Frame Beziehungen (vgl. Dodge et al. 2015: 45) 22
Abbildung 5: Vergleich von zwei konzeptuellen Metaphern mit derselben Zieldomäne und unterschiedlichen Herkunftsdomänen 28
Abbildung 6:Vergleich von zwei konzeptuellen Metaphern mit derselben Zieldomäne und einer unterschiedlichen Anzahl an Herkunftsdomänen 29
Abbildung 7: Vergleich von zwei konzeptuellen Metaphern mit derselben Herkunftsdomäne und einer unterschiedlichen Anzahl an Zieldomänen 29
Abbildung 8: Die Identifizierung von Construction Patterns im Text mit Hilfe von CoreNLP Tool (vgl. CoreNLP 2022) 42
Abbildung 9: Nicht-metaphorische Beziehungen zwischen Frames „cure“ und „cancer“ (vgl. Dodge et al. 2015: 42) 42
Abbildung 10: Metaphorische Beziehungen zwischen Frames „cure“ und „poverty“ (vgl. Dodge et al. 2015: 45) 43

Tabellenverzeichnis

Tabelle 1. Grammatikalische Muster für Metaphernbildung (vgl. Dodge et al. 2015: 43) 23
Tabelle 2. Anzahl der Metaphern pro Metaphern-Gruppe pro Sprache 47
Tabelle 3. Anzahl der analysierten Sätze im Verhältnis zu gefundenen Metaphern 47
Tabelle 4. Vergleich der metaphorischen Mappings für Kriegsmetaphern 48
Tabelle 5. Vergleich der metaphorischen Mappings für Erkrankungsmetaphern 50
Tabelle 6. Vergleich der metaphorischen Mappings für Innen/Außen-Metaphern 51
Tabelle 7. Vergleich der metaphorischen Mappings für Jagdmetaphern 53
Tabelle 8. Vergleich der metaphorischen Mappings für Angelnmetaphern 54
Tabelle 9. Metaphern in der deutschen Sprache. Gruppe der Kriegsmetaphern 55
Tabelle 10. Metaphern in der deutschen Sprache. Gruppe der Erkrankungsmetaphern 58
Tabelle 11. Metaphern in der deutschen Sprache. Gruppe der Innen/Außen-Metaphern 60
Tabelle 12. Metaphern in der deutschen Sprache. Gruppe der Jagdmetaphern 61
Tabelle 13. Metaphern in der englischen Sprache. Gruppe der Kriegsmetaphern 63
Tabelle 14. Metaphern in der englischen Sprache. Gruppe der Erkrankungsmetaphern 65
Tabelle 15. Metaphern in der englischen Sprache. Gruppe der Innen/Außen-Metaphern 68
Tabelle 16. Metaphern in der englischen Sprache. Gruppe der Jagdmetaphern 70
Tabelle 17. Metaphern in der englischen Sprache. Gruppe der Kriegsmetaphern 71
Tabelle 18. Metaphern in der englischen Sprache. Gruppe der Erkrankungsmetaphern 72
Tabelle 19. Metaphern in der englischen Sprache. Gruppe der Innen/Außen-Metaphern 74
Tabelle 20. Metaphern in der englischen Sprache. Gruppe der Jagdmetaphern 75
Tabelle 21. Metaphern in der englischen Sprache. Gruppe der Angelnmetaphern 77
Tabelle 22. Construction Patterns für Metaphernbildung 83
Tabelle 23. Statistische Daten der Umfrage 89

1. Einleitung

Im Zeitalter der Digitalisierung, in der alle persönlichen Daten im Netz für immer abgespeichert werden, tritt das Problem der Cybersicherheit in den Vordergrund. Durch digitalen Fortschritt gelingt es Hacker*innen mehr Cyberangriffe durchzuführen. E-Mails, die Anwender*innen auffordern, dringend die Passwörter zu ändern, weil sie kompromittiert wurden, oder noch schlimmer, Infizierung von einem PC mit einem Virus, sind keine Einzelfälle. Mit diesen Beispielen lässt sich zeigen, wie der Cybersicherheit in letzter Zeit immer mehr Aufmerksamkeit geschenkt wird und aus diesem Grund wurde dieser Fachbereich für diese Untersuchung ausgewählt.

Auffällig für die Fachsprache der Cybersicherheit ist dabei, dass sie mit vielen fachlichen Ausdrücken wie „Trojaner", „Würmer", „Viren", „Datenlecks", „Sicherheitslücken", um nur einige zu nennen, einen reichen Boden für die Metaphernforschung darstellt. Diese Metaphorik wurde zum Gegenstand der vorliegenden Arbeit ausgewählt.

Metaphern sind ein traditioneller Untersuchungsgegenstand für Literaturwissenschaft und Rhetorik und zwar als ein komplexes rhetorisches Stilmittel. Es ist schwierig, Literatur und Poesie ohne Metaphern sowie ohne andere figurative Sprachformen wie Satire, Ironie, Hyperbel, Idiome zu verfassen. Solche Stilmittel in der Literatur und Poesie dienen dazu, Gedanken der Autor*innen einprägsamer zu formulieren, bestimmte Gefühle in Leser*innen zu wecken und die Lektüre spannend zu machen.

Obwohl für die meisten Menschen Metaphern ein rhetorisches Stilmittel sind, das traditionell der Poesie und Rhetorik vorbehalten ist, unterscheiden sich konzeptuelle Metaphern deutlich davon und sind ein Untersuchungsgegenstand für kognitive Linguistik und Übersetzungswissenschaft. Lakoff und Johnson (1980) sind mit der Idee hervorgetreten, dass Metaphern mehr als ein rein sprachliches Phänomen sind, sondern dem Konzeptsystem, wie wir denken und handeln, zugrunde liegen. Seitdem diese Theorie von Lakoff und Johnson (1980) vorgestellt wurde, findet sie großen Zuspruch und wurde laut Google Scholar mehr als 70,000 mal zitiert. Csatár (2020) merkt sogar an, dass „die konzeptuelle Theorie von Lakoff und Johnson der meist verbreitete und ein auch über den engeren Forschungsbereich der Linguistik hinaus wohlbekannter Ansatz der zeitgenössischen Metaphernforschung ist" (Csatár, 2020: 423).

Die konzeptuellen Metaphern basieren auf unserer Erfahrung. Wir bekommen Zugang zu den Konzepten, die abstrakt oder nicht klar umrissen sind (Zeit, Emotionen, Ideen) über andere eindeutigere Konzepte wie Raumorientierungen, Objekte usw. Dadurch können wir mit Hilfe von Metaphern einen Erfahrungsbereich auf der Basis von einem anderen Erfahrungsbereich verstehen (vgl. Lakoff & Johnson 1980).

Eine der Thesen von Lakoff und Johnson war, dass die verschiedenen Kulturen verschiedene konzeptuelle Metaphern haben. Diese Tatsache ist darauf zurückzuführen, dass jede Kultur in einer gegebenen physischen Umwelt existiert. Die kulturspezifische Konzeption von physischer Realität hat Auswirkungen auf die über die Kultur geschaffene soziale Realität. Andererseits finden sich dank der Verwestlichung von Kulturen Übereinstimmungen in den metaphorischen Konzepten (vgl. Lakoff & Johnson 1980). Trim (2007) recherchierte, ob Netzwerkmuster für das Produzieren von Metaphern in verschiedenen Sprachen und Kulturen ähnlich sein können und stellte fest, dass

> In the case of European languages, they undoubtedly produce similar metaphoric mapping processes. Since all human bodies have certain physiological characteristics and conceptualization processes in common, such as the perception of gravity and spatial orientation in general, it may be assumed that the types of images produced by these processes may very well have universal trends across a large number of different cultures. (Trim 2007: 48)

Eine vergleichende Analyse konzeptueller Metaphern, die in einem bestimmten Fachbereich vorkommen, zwischen verschiedenen Sprachen, stellt einen potenziellen Untersuchungsgegenstand dar. Die Fachsprache der IT und der Cybersicherheit bietet viele Möglichkeiten im Bereich der Metaphernforschung als ein in der Literatur noch nicht ausdrücklich behandelter Fachdiskurs.

Die konzeptuellen Metaphern, die in der vorliegenden Arbeit untersucht werden, gehören zu den „konventionalisierten Metaphern“, d.h. sie strukturieren das gängige Konzeptsystem und werden in der Alltagssprache nicht als Metaphern wahrgenommen (vgl. Lakoff & Johnson 2021).

1.1 Forschungsfrage und Annahmen

Die vorliegende Arbeit befasst sich hauptsächlich mit der Frage, in welchen Metaphern sich in der Fachsprache welche menschliche Konzeptsysteme widerspiegeln. Da eine allumfassende Studie aller sprachlichen Wissensbereichen den Rahmen dieser Masterarbeit sprengen würde, liegt der Schwerpunkt der Untersuchung bei einem eng eingegrenzten Diskursbereich, nämlich Cybersicherheit. Aus den dargestellten Voraussetzungen lassen sich folgende zentrale Forschungsfragen für die vorliegende Arbeit ableiten:

1. Wie relevant sind die konzeptuellen Metaphern für die Cybersicherheitsfachsprache?
2. Welche konzeptuellen Metaphern werden im Bereich der Cybersicherheit in den Sprachen Englisch, Deutsch und Russisch verwendet?
3. Wie unterscheiden sich die Metaphern in den Sprachen?

In der Untersuchung wird von den folgenden Annahmen ausgegangen:

1. Konzeptuelle Metaphern sind in der Fachsprache präsent und prägen sie.

2. Konzeptsysteme weisen mehr Ähnlichkeiten zwischen verwandten Sprachen, wie Deutsch und Englisch auf, als zwischen Sprachen aus unterschiedlichen Sprachfamilien, wie Deutsch und Russisch.
3. Die Herkunftsdomänen, die der Mehrheit von Cybersicherheit-Metaphern zu Grunde liegen, sind Krieg („Hackerattacke“) und Medizin („Viren“, „infizieren“).

1.2 Motivation und Zielsetzung

Die Forschung in der kognitiven Linguistik beschäftigt sich aktiv mit der Frage, wie Kognition neue Möglichkeiten zur Aufdeckung von regelmäßigen Mustern der Metaphernbildung eröffnet (vgl. Trim 2007: 27). Wenn Menschen an ein Konzept wie etwa „Argumentieren“ in Kategorien von „Krieg“ denken, werden zusammenhängende Metaphern produziert, wie z.B. beim Argumentieren können Parteien „gewinnen“ oder „verlieren“; die Person, mit der argumentiert wird, ist ein „Gegner“, die Streitenden können eine „Attacke reiten“, „mit Argumenten schießen“ usw. (vgl. Lakoff & Johnson 1980). In der Forschungsliteratur wurde demonstriert, dass sich die kognitive Metapherntheorie nicht nur auf die Alltagssprache, sondern auch auf die Fachsprache anwenden lässt (vgl. Drewer 2003). Es bleibt noch zu erforschen, ob Konzeptsysteme auf allen Sprachebenen eine universelle Natur haben und dieselben Wege verfolgen, wie Trim (2007) vermutet, oder es von Sprache zu Sprache spürbare Unterschiede gibt. Erwähnenswert ist, dass die meisten Forschungsarbeiten im Bereich konzeptueller Metaphern nur einer oder maximal zwei Sprachen gewidmet sind (vgl. Drewer 2003, Wang et al. 2013) mit nur wenigen Ausnahmen (vgl. Sharifian et al. 2008), während die vorliegende Arbeit drei Sprachen abdeckt: Englisch, Deutsch und Russisch.

Die Sprachauswahl ist auf die universelle Verbreitung von Englischen als Lingua Franca und auf eine Statistik von Land-Sprache-Aufteilung von Softwareentwickler*innen zurückzuführen. Laut einer Studie steht im Vergleich zu anderen Ländern Europas die deutsch-sprachige IT-Community Deutschlands und Österreichs mit ungefähr 1 Mio. Softwareentwickler*innen auf Platz eins. Die russisch-sprachige IT-Community mit Entwickler*innen aus Russland und der Ukraine mit mehr als 500.000 IT-Experten*innen befindet sich auf Platz zwei (vgl. Daxx 2021). Angesichts der starken Vertretung von englisch-, deutsch- und russischsprachigen Informatiker*innen wird die Relevanz einer solchen Untersuchung ersichtlich.

Das Ziel dieser Masterarbeit ist es, die konzeptuellen Metaphern in der IT-Sprache am Beispiel von Cybersicherheit zu finden und zu analysieren, und zwar wie weit die Konzeptsysteme mit Deutsch verwandten und nicht-verwandten Sprachen Ähnlichkeiten und Unterschiede aufweisen, und konzeptuelle Metaphern aufzudecken, die über Kulturen hinweg konsistent sind. Die Recherche für jede Sprache wird in jeweils einsprachigen Paralleltexten durchgeführt; als theoretische

Grundlage dient die kognitive Metapherntheorie, auf deren Basis die Fachsprache der Cybersicherheit in Bezug auf ihre Metaphern kontrastiv analysiert wird.

Grundsätzlich ist diese Arbeit für alle Personen gedacht, die Interesse an konzeptuellen Metaphern in Fachsprachen demonstrieren. Sie soll Interesse an der Frage wecken, inwieweit die kulturelle Distanz und die Unterschiede in konzeptuellen Systemen zusammenhängen. Vertreter*innen der Sprachwissenschaft, Übersetzungswissenschaft, Terminologielehre und kognitiven Linguistik können in den zu erwartenden Resultaten dieser Arbeit wertvolle Hinweise auf (nicht) kulturübergreifende Metaphern in der Fachsprache finden.

Im Kapitel 2.1 wird zunächst eine kurze thematische Einführung in das Thema Cybersicherheit vorgenommen. Im Kapitel 2.2 und 2.3 ist ein Überblick über Fachsprachen und die konzeptuelle Metapherntheorie von Lakoff und Johnson zu finden. Im Kapitel 2.4 wird auf die kulturellen Unterschiede in Bezug auf konzeptuelle Metaphern eingegangen. Im Kapitel 2.5 wird der Begriff „konventionalisierte Metapher" erläutert. Im Kapitel 2.6 wird die Kritik an der konzeptuellen Metapherntheorie diskutiert. Ebenso wird der aktuelle Stand der Forschung in einem separaten Kapitel thematisiert. Anschließend wird die geplante Methodik dieser Arbeit vorgestellt. Im Kapitel, das den Forschungsergebnissen gewidmet ist, werden die im Korpus identifizierten Metaphern nach Herkunftsdomänen gruppiert und zwischen den Sprachen verglichen. Eine Schlussdiskussion mit den Antworten auf die in der vorliegenden Masterarbeit diskutierten Forschungsfrage sowie einem Vergleich zu anderen Forschungsarbeiten und methodische Herausforderungen wird im vorletzten Kapitel vorgestellt. Ein Fazit dieser Arbeit einschließlich eines Ausblicks über mögliche weiterführende Forschungsfragen sind Gegenstand des letzten Kapitels.

2. Grundlagen

In diesem ersten Kapitel soll die notwendige theoretische Grundlage für die im darauffolgenden Kapitel vorgestellte empirische Untersuchung geschaffen werden. Zuerst werden Hintergrundinformationen zum Thema Cybersicherheit und Hackerattacken präsentiert, um den Einstieg in das Thema zu erleichtern. Weiter wird das Phänomen der Fachsprachen erläutert. Der dieser Arbeit zu Grunde liegenden konzeptuellen Metapherntheorie von Lakoff und Johnson (1980) wird ein separates Unterkapitel gewidmet. Auf die kulturelle Spezifik und mögliche Beziehungen zwischen Herkunftsdomänen und Zieldomänen in der Bildung von konzeptuellen Metaphern soll eingegangen werden, auf deren Basis sich Parallelen zwischen Sprachen ziehen lassen. Ebenfalls wird der Unterschied zwischen „konventionalisierten" und „neuen" Metaphern erläutert. Zudem wird der Frage nachgegangen, wie sich konzeptuelle Metaphern identifizieren lassen. Anschließend wird es einen Überblick über die Kritik an den methodologischen Schwachstellen der konzeptuellen Metapherntheorie und eine wissenschaftliche Auseinandersetzung mit der Gegenargumentation geben.

2.1 Einführung in den Fachbereich Cybersicherheit

Informations- und Kommunikationstechnologien (IKT) sind zu einem unabdingbaren Teil fast aller gesellschaftlichen Lebensbereiche geworden. Der Trend der Digitalisierung kann in Branchen wie Finanzwesen, Logistik, Versicherung, Industrie, Verkehr, Handel, Staatsinfrastruktur, soziale Medien und mehreren anderen Sektoren der Wirtschaft beobachtet werden. Für das normale Funktionieren sind entsprechende Organisationen auf Informations- und Kommunikationstechnologien bei der Verwaltung von Datenbeständen angewiesen. Im Laufe der Zeit wurden einzelne Server, Computer- und Informationssysteme und Mobilgeräte massiv vernetzt (vgl. Weber 2020: 11).

Diese Vernetzung ist eine Stärke und eine Schwachstelle zugleich. Obwohl die neusten Technologien die Kommunikation und Interaktion zwischen Menschen, Organisationen, Staaten und Kontinenten erleichtern, bleiben die vernetzten und komplexen Informationssysteme anfällig für Hackerattacken von außen. Laut Einschätzung von Cybersicherheit-Forscher*innen (Weber 2020, Branch 2021, Holt et al. 2020) steigt das jährlich durch Cyberattacken verursachte Ausmaß des finanziellen Schadens kontinuierlich und erreicht Maßstäbe der Haushalte ganzer Staaten. Niemand ist vor Cyberattacken sicher: von einzelnen Individuen, bis hin zu großen und kleinen Unternehmen, Behörden und ganzen Regierungen. Als Folge der Attacken wird die Infrastruktur beschädigt, ohne

die die moderne Gesellschaft nicht funktionieren kann, merkt Weber (2020: 10-11) an. Ein ähnliches Bild ergibt sich aus den Berichten von amerikanischen Forscher*innen, wie etwa Branch (2020). Laut Branch (2020) hat das Internet selbst für mächtige Staaten grundlegend neue Sicherheitslücken geschaffen, darunter Wirtschaftsspionage, Datenschutzverletzungen, Eindringen in Regierungsnetze, Bedrohungen der physischen Infrastruktur und Beeinflussung von Online-Wahlen. In den meisten Fällen steht das finanzielle Interesse dahinter, aber nicht selten sind die Attacken Akte kreativer Selbstentfaltung oder politisch und ideologisch motiviert (vgl. Holt et al. 2020).

Als Grundlage der vorliegenden Masterarbeit kann folgende Definition von Cybersicherheit herangezogen werden:

> Cybersecurity is a science, designed to protect your computer and everything associated with it – the physical environment, the workstations and printers, cabling, disks, memory sticks, and other storage media. But most importantly, cybersecurity is designed to protect all forms of memory, that is, the information stored in your system […] to protect against outside intruders, but also both malicious and benign insiders. (Patterson et al. 2019: 3)

Schematisch kann Cyber-Sicherheit (auch Internet-Sicherheit genannt) als ein Netz von zwischen miteinander verbundenen IT-Infrastrukturen von Unternehmen, Institutionen, Behörden und privaten Nutzer*innen und Datenverkehr zwischen ihnen und Servern, dargestellt werden (siehe Abb. 1):

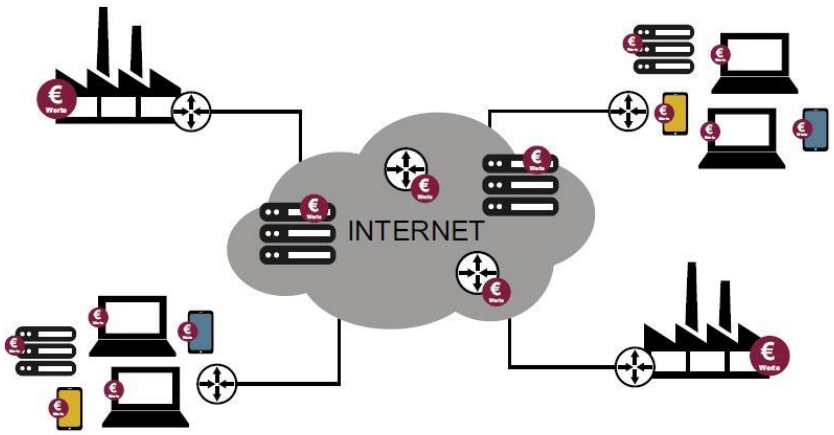

Abbildung 1: Cybersicherheit (vgl. Pohlmann 2022: 2)

Pohlmann (2022) gibt eine detaillierte Liste von Aufgaben, die in den Verantwortungsbereich von IT-Sicherheit fallen:

> IT-Sicherheit befasst sich daher mit IT-Sicherheitsmaßnahmen, die Informationen auf IT-Systemen sowie IT-Systemen selbst vor dem Verlust der Vertraulichkeit, Authentifikation, Authentizität, Integrität,

Verbindlichkeit, Verfügbarkeit und Anonymisierung/Pseudonymisierung schützen. IT-Sicherheit beinhaltet auch die Aspekte der Softwaresicherheit und Zuverlässigkeit von IT-Systemen (vgl. Pohlmann 2022: 3).

Mit der fortlaufenden Digitalisierung nehmen die Cybersicherheitsprobleme kontinuierlich zu. Die Situation wird dadurch erschwert, dass im Design der heutigen IT-Systeme, der Hard- und Software nicht ausreichend genug Cybersicherheitsschutz vorgesehen ist, sodass sie für böswillige Hacker anfällig sind. Die Cyberangreifer schrecken vor der immer steigenden Komplexität der IT-Infrastrukturen nicht zurück, wenden neue ausgefeiltere Methoden an und greifen neue lukrative Ziele an (vgl. Pohlmann 2022).

In Abb. 2 sind Cybersicherheitsbedrohungen dargestellt, die uns jeden Tag begleiten. Das sind Spyware, Viren, Malware, Phishing, Hackerattacken, Passwort-Diebstahl, Attacken auf Schwachstellen in Firewall. Zur Spyware gehören Programme, die Informationen auf Systemen oder Netzwerkverkehr ausspionieren. Ein Phishing-Angriff hat das Ziel die Nutzer*innen dazu zu bringen, freiwillig ihre persönlichen Daten oder Passwörter preiszugeben. Das kann schlicht eine E-Mail sein, die an die Opfer ausgeschickt wird und in der sie aufgefordert werden, auf schädliche Links zu klicken, oder eine gefälschte Webseite, die identisch mit einer Login-Webseite für eine Internet-Bank aussieht. Schwache Passwörter können erraten werden oder durch sogenannte Keylogger, die alle Eingaben auf der Tastatur registrieren, abgefangen werden (vgl. Prasad & Rohokale 2020).

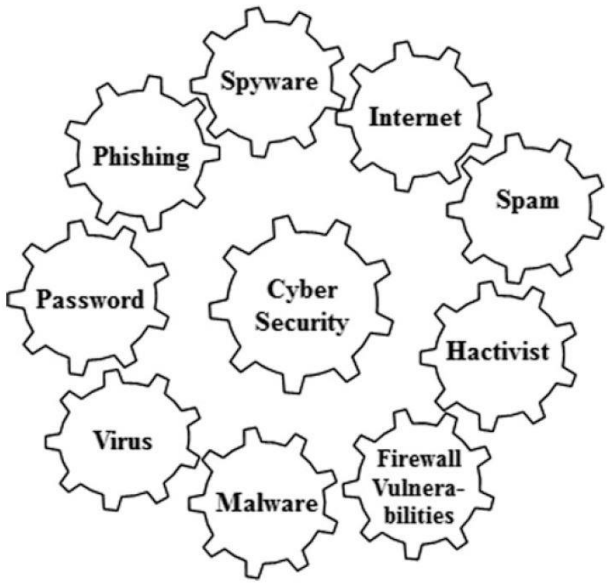

Abbildung 2: Cybersicherheitsbedrohungen (vgl. Prasad & Rohokale 2020: 2)

Die permanente Gefahr der Cyberattacken führt dazu, dass auf Cybersicherheit mehr und mehr Wert gelegt wird: „Je mehr Gesellschaften auf funktionierende IKT angewiesen sind, desto eher neigen sie dazu, (Cyber-)Sicherheit über alle anderen Werte zu stellen“ (vgl. Weber 2020: 12). Die Berichte zu

den Cybersicherheitsvorfällen enthalten Informationen, wie erfahrene Hacker Schwachstellen in Software ausnutzen, Malware verbreiten, Zugangsdaten zu persönlichen Accounts stehlen oder zu Endgeräten einen unbefugten Zugang bekommen (vgl. Pohlmann 2022). Als ein Thema, das aus oben genannten Gründen im öffentlichen und wissenschaftlichen Diskurs stark präsent ist, eignet es sich für eine korpusbasierte Studie in Anlehnung an die konzeptuelle Metapherntheorie, die in den nachfolgenden Kapiteln vorgestellt wird.

2.2 Fachsprache

In der vorliegenden Masterarbeit wird auf den Begriff Fachsprache näher eingegangen. Um ein vollständigeres Bild der theoretischen Grundlagen zum Thema Rahmen und Träger der Fachkommunikation zu erstellen, versuchte Stolze (2009) die Gesamtheit der zusammenhängenden Begriffe wie „Fach", „Fachleute", „Fachkommunikation" und „Fachsprache" zu definieren. Ein Fach ist „eine soziale Orientierungsgröße", die „eine fachliche Qualifikation voraussetzt" (vgl. Stolze 2009: 22). Die Handelnden im Fach, die Träger*innen des Fachwissens sind Fachleute, während die Fachkommunikation ein „Sprechen im und über das Fach" ist und sie mittels der Fachsprache durchgeführt wird (vgl. Stolze 2009: 23). Durch Fachkommunikation wird das Fachwissen laufend aktualisiert und ergänzt (ibid. 2009: 23). Hoffman (1984) gibt eine formalisierte Definition für Fachsprache:

> Fachsprache – das ist die Gesamtheit aller sprachlichen Mittel, die in einem fachlich begrenzbaren Kommunikationsbereich verwendet werden, um die Verständigung zwischen den in diesem Bereich tätigen Menschen zu gewährleisten (vgl. Hoffman 1984: 53).

Zu den sprachlichen Mitteln zählen Sprachelemente auf phonetischer, morphologischer, lexikalischer und syntaktischer Ebene, die in Form von Kommunikationsakten realisiert werden (ibid. 1984: 53).

Dass Fachsprache nur ein Überbegriff ist und eine Gliederung von Fachsprachen und Fachtextsorten notwendig ist, wurde von Roelcke (2014) behandelt. Er schlägt eine „horizontale" Typologie von Fachsprachen nach einzelnen Fächern und Wirtschaftssektoren vor, laut der die für diese Masterarbeit relevante Informatik-Fachsprache dem Zweig von technischen Fachsprachen und Fachsprachen angewandter Wissenschaften angehört (vgl. Roelcke 2014: 158). Im Rahmen einer „horizontalen" Typologie, die Fachsprache nach kommunikativen Ebenen unterteilt, können Fachspracheproduzent*innen nicht nur als Expert*innen und Lai*innen eingestuft werden, sondern die Rolle von Expert*innen wird präzisiert: das können Wissenschaftler*innen, Techniker*innen,

Leiter*innen der Produktion, Facharbeiter*innen, Vertreter*innen des Handels sein (vgl. Roelcke 2014: 162).

Die Anzahl der Fachsprachen wurde von Roche (1992) auf mehr als 300 eingeschätzt. Er postuliert, dass grundsätzlich für jeden Wissenschaftszweig eine eigene Fachsprache existiert, wie Fachsprache der Chemie, Physik, Medizin usw., dabei sind sie durch bestimmte Merkmale charakterisiert, wie Terminologie oder wie der Wortschatz gebildet wird (vgl. Roche 1992).

Ein Einblick in die fachspezifischen stilistischen Besonderheiten bei der Cybersicherheits-Fachsprache ist bei Quigley et al. (2015) zu finden. Laut ihrer Analyse sprechen die Cybersicherheitstexte ihre Leser*innen auf mehreren Ebenen emotional an, z.B. durch die Angst über die fehlende Fähigkeit der Menschen, Cyberbedrohungen zu kontrollieren und über das Potenzial der Technologien eine Katastrophe auszulösen. Die Cyber-Gefahr benimmt sich als eine unheimliche und motivierte Entität, die weltweit agiert und gleichgültig gegenüber menschlichem Leiden oder finanziellen Verlusten ist. Zu den meist verwendeten metaphorischen Bildern zählen die Idee vom Cyberspace als Kampffeld, auf dem die Informationstechnologie eine Waffe mit zerstörerischer Wirkung ist (vgl. Quigley et al. 2015). In einem Interview für Cooper (2021) stimmt ein Sicherheitsexperte zu, dass die Sprache in der Cybersicherheitsindustrie „aggressiv", „militaristisch" aber auch „männlich" ist, und weist darauf hin, dass die Industrie im Ganzen von Männern dominiert wird. Es kann um Leben und Tod gehen, wenn die kritische Infrastruktur angegriffen wird (vgl. Prasad & Rohokale 2020).

2.3 Konzeptuelle Metapherntheorie

In nachfolgenden Unterkapiteln wird der Begriff der konzeptuellen Metaphern vorgestellt. Es wird über die Entstehung, Entwicklung und einzelne Aspekte der Metapherntheorie berichtet. Diesen Fragen wird deswegen besondere Aufmerksamkeit gewidmet, weil die konzeptuelle Metapherntheorie im Wesentlichen den theoretischen Rahmen dieser Arbeit bildet und für das Verständnis von Forschungsergebnissen unentbehrlich ist.

2.3.1 Die Entstehung der Metapherntheorie

Der Entstehung der konzeptuellen Metapherntheorie ist eine lange Zeit vorausgegangen, in der Metaphern hauptsächlich als figurative Sprache in der Literatur und Poesie von Literaturkritiken analysiert wurden. Im Laufe dieser langen Zeitspanne wurde bei der Metaphernforschung das

Hauptaugenmerk fast ausschließlich auf die Schaffung und Interpretation von originellen Metaphern (vom Englischen „novel metaphors“) gelegt. Die originellen Metaphern sei ein Bereich gewesen, an dem sich die metaphorische Bedeutung und individuelle Kreativität habe entfalten können, so Gibbs (Gibbs 2018: 44).

Die Hypothese, dass die Metapher, die traditionell als ein spezielles Sprachmittel angesehen wurde, ebenso ein unabdingbarer Teil der gewöhnlichen Denkprozesse ist, wurde schon seit Jahrhunderten von einigen Rhetoriker*innen und Philosoph*innen aufgestellt. Dennoch wurde keine klare Theorie über die Verknüpfung von Metaphern mit den Denkprozessen formuliert. Erst in den 1980er Jahren begann die Verbreitung der konzeptuellen Metapherntheorie (vom Englischen „conceptual metaphor theory“ (CMT)) im Bereich der kognitiven Linguistik und die These „metaphor in thought“ hat große Aufmerksamkeit erhalten (vgl. Gibbs 2018: 3). Die Theorie wurde von Lakoff und Johnson (1980) vorgestellt und wurde in die meisten europäischen Sprachen übersetzt und in einigen dieser Sprachen sind mehrere Ausgaben erschienen, was als weiterer Beweis für den Erfolg des Werkes angesehen werden kann (vgl. Monti 2009: 207). Lakoff und Johnson (1980) postulierten als erste Personen, dass „systematic linguistic provided evidence to support the claim that there are metaphors in mind or ‚conceptual metaphors‘“ existiert (vgl. Gibbs 2018: 3).

2.3.2 Konzeptuelle Metaphern

Lakoff und Johnson sind davon ausgegangen, dass Metaphern kein rein sprachliches Phänomen sind, sondern, dass sich unsere menschliche Kognition auf Metaphern stützt. Das heißt, Metaphern als integraler Bestandteil der Alltagssprache spielen eine wesentliche Rolle darin, wie wir denken und handeln (vgl. Lakoff & Johnson 2021: 11)[1]. Dass „der größte Teil unseres alltäglich wirksamen Konzeptsystems im Kern metaphorisch angelegt ist“, haben die Forscher „aufgrund linguistischer Evidenz festgestellt“ (vgl. Lakoff & Johnson 2021: 12). Diese linguistische Evidenz verdient eine genauere Betrachtung.

Um zu demonstrieren, was ein metaphorisches Konzept ist und wie auf seiner Basis unsere Alltagshandlungen vordefiniert sind, werden mehrere Konzepte beschrieben, eines davon ist ARGUMENTIEREN IST KRIEG (seit Lakoff und Johnson den Begriff „Konzeptuelle Metaphern“ eingeführt haben, ist die gängige Konvention sie in Großbuchstaben, ohne Anführungszeichen zu schreiben). Diese konzeptuelle Metapher zeichnet sich einerseits durch viele Ausdrücke aus, in denen

[1] Es wird hier auf die neuste, 10. Auflage von Lakoffs & Johnsons Buch in der Deutschen Übersetzung verwiesen

das Argumentieren thematisiert wird, z.B. „Ihre Behauptungen sind unhaltbar“, „Er griff jeden Schwachpunkt in meiner Argumentation an“, „Seine Kritik traf ins Schwarze“, „Ich schmetterte sein Argument ab“, „Ich habe noch nie eine Auseinandersetzung mit ihm gewonnen“ usw. Andererseits zeichnet sich die Metapher durch Argumentationshandlungen aus, z.B. Menschen können beim Argumentieren gewinnen oder verlieren, haben Gegner, Positionen werden angegriffen und verteidigt usw. (vgl. Lakoff & Johnson 2021: 12). Basierend auf diesen offenbar bedeutungsmäßig zusammenhängenden lexikalischen Ausdrücken wird die Schlussfolgerung gezogen, dass „die konzeptuelle Metapher ARGUMENTIEREN IST KRIEG“ eine Metapher ist, „nach der wir in unserer Kultur leben; sie strukturiert die Handlungen, die wir beim Argumentieren ausführen“ (vgl. Lakoff & Johnson 2021: 12f). Wie sich eine konzeptuelle Metapher aus der Mehrzahl einzelner Metaphern ableiten lässt, zeigt die folgende Aussage:

> Was uns auf den ersten Blick wie zufällige, isolierte metaphorische Ausdrücke erscheint – z.B. *bestimmte Punkte abdecken, die Argumentation stützen, zum Kern vordringen, tiefer graben, eine Position angreifen und zerstören* –, ist alles andere als zufällig. Alle diese Ausdrücke sind Teile ganzer metaphorischer Systeme, die in ihrer Gesamtheit dem komplexen Ziel dienen, das Konzept einer Argumentation in all seinen Einzelaspekten zu beleuchten, wie wir uns diese vorstellen. (Lakoff & Johnson 2021: 124)

Lakoff und Johnson (2021) stellen weitere konzeptuelle Metaphern vor, wie ZEIT IST GELD („Sie vergeuden meine Zeit“, „Zeit sparen/investieren“ usw.), IDEEN SIND PFLANZEN („Ideen haben schließlich Früchte getragen“, „Diese Theorie ist ausgereift“, „fruchtbare Phantasie“, „diesen Gedanken ins Herz pflanzen“) oder LEBEN IST EINE REISE („am Scheideweg stehen“, „Lebenspfad“) (vgl. Lakoff 2021 & Johnson: 15, 57, 60). Insgesamt wurden mehrere Dutzende konzeptuelle Metaphern aufgelistet.

Lakoff und Johnson (2021) merken an: „Metaphorische Konzepte stellen Möglichkeiten dar, eine Erfahrung partiell in Begriffen einer anderen Erfahrung zu strukturieren“ (Lakoff 2021 & Johnson: 93). Ein Versuch, eine formalisierte Definition für den Begriff konzeptuelle Metaphern zu erarbeiten, wurde von Kövecses (2017) unternommen:

> The standard definition of conceptual metaphors is this: A conceptual metaphor is understanding one domain of experience (that is typically abstract) in terms of another (that is typically concrete) (Kövecses 2017: 15).

Lakoff und Johnson und später ihre Nachfolger*innen postulierten, dass systematische Beziehungen zwischen mehreren konventionalisierten Ausdrücken durch die zu Grunde liegenden konzeptuellen Metaphern bedingt sind (vgl. Lakoff & Johnson 2021, Charteris-Black 2004). Aus der Tatsache, dass

das menschliche Denken grundsätzlich metaphorisch ist, ergibt sich, dass das eine direkte Auswirkung auf unsere Überzeugungen und Handlungen hat (vgl. Gibbs 2018: 148).

Ein Grund, warum konzeptuelle Metaphern so verbreitet sind, ist, dass die Metaphern eine Möglichkeit bieten, einen komplexen Sachverhalt auf einen anderen Sachverhalt zu übertragen und dadurch verständlich zu machen. Solche, für uns wichtige Konzepte wie Emotionen, Ideen, Zeit usw. sind entweder zu abstrakt oder wir können nicht direkt über sie über unsere Sinnesorgane Erfahrungen machen, weswegen ein Zugang zu diesen Konzepten über andere greifbare Konzepte ermöglicht werden muss, wie etwa die Raumorientierungen – Oben/Unten oder die Objekte – Gefäß, Temperatur, Balance, usw. (vgl. Lakoff & Johnson 2021: 47, 135).

Gibbs (2018) teilte die Ansicht, dass Metaphern fundamentale Werkzeuge sind, die strukturieren, wie Leute in der Regel über abstrakte Ideen und Ereignisse denken und um zu unterstreichen, dass sie für eine lange Zeit geltend bleiben und verwendete den Terminus „enduring metaphorical schemes of thought“ (vgl. Gibbs 2018: 4). Wenn wir schwierige, komplexe, abstrakte und nicht klar umrissene Konzepte mit Hilfe vertrauter Begriffe zu verstehen versuchen, werden konzeptuelle Metaphern geboren (ibid. 2018: 4).

Charteris-Black (2004) merkte an, dass bei der Analyse von konzeptuellen Metaphern auch der Kontext berücksichtigt werden soll, weil er den Schlüssel zum Verstehen der Absichten der/des Sprechenden enthält. Dies spielt eine besonders wichtige Rolle in bestimmten Kontexten, z.B. in politischen Reden, bei denen Metaphern vor allem eine überzeugende Funktion haben. Diesen Ansatz nannte er „pragmatic perspective on metaphor“ (vgl. Charteris-Black 2004:9f).

Zusammenfassend lässt sich sagen, dass Lakoff und Johnson die Existenz von konzeptuellen Metaphern in der Sprache durch systematische linguistische Argumentation umfassend belegt und an mehreren Beispielen demonstriert haben, wie die Metaphern eine entscheidende Rolle bei der Schaffung und dem Strukturieren von abstrakten Konzepten spielen (vgl. Gibbs 2018: 4). Wie später gezeigt werden soll, hat sich die Idee, dass die Metaphorik nicht nur für die literarische und poetische Sprache charakteristisch ist, sondern auch für die alltägliche Sprache, später zu der Idee entwickelt, dass konzeptuelle Metaphern auch in der fachsprachlichen Kommunikation zu finden sind (vgl. Elitze 2012: 63).

2.3.3 Erfahrung als Basis für konzeptuelle Metaphern

Eine große Aufmerksamkeit bei der konzeptuellen Theorie ist der Herkunft von konzeptuellen Metaphern gewidmet. Lakoff und Johnson (2021) stellten fest, dass sich die metaphorischen Konzepte aus unserer physischen und kulturellen Erfahrung entwickeln (vgl. Lakoff & Johnson 2021:23). Dazu zählen Erfahrungen, die durch unseren Körper gemacht werden (Wahrnehmung, Motorik, Emotionen), Interaktionen mit der physischen Umgebung (Bewegung, Orientierung, Manipulation von Objekten) aber auch Interaktionen mit anderen Menschen im Kulturkreis – auf der sozialen, politischen, wirtschaftlichen und religiösen Ebene (vgl. Lakoff & Johnson 2021: 137). So wurde aus der Erfahrung, dass eine niedergedrückte Körperhaltung eher für einen pessimistischen Gemütszustand charakteristisch ist, und jemand mit einem hoch erhobener Kopf Optimismus und Glück ausstrahlt, zwei konzeptuelle Metaphern GLÜCKLICH SEIN IST OBEN („hohe Stimmung“) und TRAURIG SEIN IST UNTEN („in eine Depression verfallen“) generiert (vgl. Lakoff & Johnson 2021: 23). Diese Beobachtung, dass konzeptuelle Metaphern durch physische Erfahrung mit der Umwelt motiviert sind und dass wir mit Hilfe von Metaphern einen Erfahrungsbereich von einem anderen nicht direkt damit verbundenen Erfahrungsbereich her verstehen können, haben Lakoff und Johnson folgendermaßen formuliert:

> Das Wesen der Metapher besteht darin, daß wir durch sie eine Sache oder einen Vorgang in Begriffen einer anderen Sache bzw. eines anderen Vorgangs verstehen und erfahren können. (Lakoff & Johnson 2021: 13)

2.3.4 Auswirkung der konzeptuellen Metapherntheorie auf die Forschung

Die konzeptuelle Metapherntheorie und die nachfolgenden empirischen Untersuchungen in diesem Bereich hatten eine Auswirkung in vielerlei Hinsicht auf die Geisteswissenschaften und kognitive Wissenschaften, so Gibbs (2018: 5).

Erstens hat die konzeptuelle Metapherntheorie die kognitive Linguistik in eine neue Richtung gelenkt, was linguistische Strukturen und menschliches Verhalten betrifft. Die kognitive Linguistik untersucht, wie die Kognition und die Sprache miteinander verbunden sind und dank der konzeptuellen Metapherntheorie konnte aufdeckt werden, wie abstrakte Konzepte und Symbole auf der Basis der Erfahrung strukturiert werden (vgl. Gibbs 2018: 5).

Zweitens schafft die konzeptuelle Metapherntheorie einen theoretischen Rahmen und gibt eine Orientierung für das Sammeln und Präsentieren empirischer Belege für weitere Studien, die sich

mit der universellen Verbreitung von metaphorischer Sprache und metaphorischem Denken in einer Vielzahl kultureller und sprachlicher Kontexte beschäftigen können (vgl. Gibbs 2018: 5).

Drittens hatte die neue Einsicht, dass das abstrakte Denken im Wesentlichen durch metaphorische „Mappings" (vom Englischen „metaphorical mappings") zwischen Herkunfts- und Zieldomänen motiviert ist, einen Einfluss auf die wissenschaftlichen Vorstellungen, in welcher Beziehung das Denken und die Sprache zueinander stehen. Die Tatsache, dass über abstrakte Wissensbereiche wie Politik, wissenschaftliches Argumentieren, Vorstellungen über sich selbst, Emotionen schon fixe konzeptuelle Metaphern existieren, führt dazu, dass über diese Themen im öffentlichen Diskurs auf eine bestimmte Weise gedacht und folglich diskutiert wird (vgl. Gibbs 2018: 5). Wie Lakoff und Johnson (2021) es formuliert haben: „Mit einer Metapher werden bestimmte Aspekte […] beleuchtet, andere Aspekte werden heruntergespielt und wieder andere verborgen" (vgl. Lakoff & Johnson 2021: 172)

Schließlich hat die Theorie einen besonderen Anklang in der Forschung über die „embodied cognition" gefunden, welche annimmt, dass Kognition und Sprache auf körperlichen, perzeptiven, sensomotorischen Erfahrungen beruhen (vgl. Weber, 2017: 58). Gibbs (2018) postuliert, dass sich wiederkehrende Mustern körperlicher Aktivität in metaphorischen Konzepten widerspiegeln, und diese körperlichen Handlungen als Quelle für das Verständnis vieler abstrakter Konzepte durch Menschen dienen. (vgl. Gibbs 2018: 5ff)

2.3.5 Identifizierung von Metaphern

Lakoff und Johnson (1980) verlassen sich beim Postulieren von konzeptuellen Metaphern auf ihre Erfahrung und Intuition verlassen, ohne explizit zu erklären, warum ausgerechnet diese metaphorischen Ausdrücke für die Analyse ausgewählt wurden und welche logischen Überlegungen hinter der Eruierung von konzeptuellen Metaphern stehen (vgl. Lakoff & Johnson 1980, Kövecses 2020: 86)

Seit 1980 haben sich Metaphernforscher*innen mit der Problematik aktiv auseinandergesetzt, wie von den einzelnen lexikalischen Metaphern (lexikalischen Darstellung von konzeptuellen Metaphern) z.B. „am Scheideweg stehen" die konzeptuelle Metapher DAS LEBEN IST EINE REISE abgeleitet werden kann (vgl. Gibbs 2018: 2). Als Erstes empfiehlt es sich die lexikalischen Metaphern zu sammeln. Kövecses (2020) widmet zwei Ansätzen besondere Aufmerksamkeit: dem lexikalischen und dem korpusbasierten. Bei dem lexikalischen Ansatz sind die Hauptrecherchequellen ein- und

zweisprachige Wörterbücher, Glossare, Wörterbücher für Kollokationen, Idiome und beliebige Sammlungen von Vokabeln und Wortschatz zum ausgewählten Thema. Als Nachteile dieser Herangehensweise nennt er, dass es keine Möglichkeit gibt, zu messen, wie oft eine Metapher vorkommt, um den Grad der Konventionalisierung zu definieren und als Vorteil, dass die Daten nicht vom individuellen Sprachgebrauch des*der individuellen Sprecher*in oder Autor*in abhängig sind. Dagegen eignet sich die korpusbasierte Untersuchung dafür, um die aktuelle Verbreitung von Metaphern im realen Diskurs zu verfolgen und quantitative Methoden für die Einschätzung der Häufigkeit einzelner Metaphern einzusetzen (vgl. Kövecses 2020: 87ff). Es soll angemerkt werden, dass außer der Analyse von konzeptuellen Metaphern auf der Textebene es andere Wege gibt, wie psycholinguistische, neurowissenschaftliche Experimente oder rechnergestützte Modellierung, die in der vorliegenden Arbeit nicht in Tiefe behandelt werden (vgl. Gibbs 2008, Desai 2021).

Steen (1999) schlägt folgende 5 Schritte für die Metaphernidentifizierung vor:

1. Das Identifizieren des metaphorischen Fokuses (vom Englischen „metaphor focus identification“). Dieser Schritt beinhaltet das Identifizieren der lexikalischen Metapher im Text, eines Ausdruckes, der nicht rein wörtlich interpretiert werden kann, sondern übertragene Meinung enthält (vgl. Steen 1999: 4).
2. Das Identifizieren des metaphorischen Gedankens (vom Englischen „metaphorical idea identification“). Steen (1999) setzt die Methode der Propositionen ein. Vereinfacht kann diese Methode so gesehen werden, dass ein Ausdruck in mehrere Propositionen zerlegt wird. Eine Proposition ist eine minimale Sinneseinheit, die aus einem Prädikat und einem oder mehreren Argumenten besteht. Propositionen werden mit dem Buchstabe P und einer Nummer nummeriert und jede Proposition wird in Klammern gesetzt (vgl. Steen 1999: 62). Grammatikangaben werden nicht angegeben. Semino et al. (2004) führt das folgende Beispiel für den metaphorischen Ausdruck zum Thema Krebs an:

   „galloping away“

   P1 (GALLOP-AWAY CANCER) (vgl. Semino et al. 2004: 1282)
3. Das Identifizieren des nicht-wörtlichen Vergleichs („nonliteral comparison identification“). Der metaphorische Ausdruck wird in der Form eines nicht-wörtlichen Vergleichs umgeschrieben.

   (GALLOP-AWAY CANCER) → (∃ F) (∃y){SIM[F(CANCER), GALLOP-AWAY(y)]}

   (vgl. Semino et al. 2004: 1282). Ähnlich wie bei einer mathematischen Funktion ist gemeint, dass es eine Beziehung zwischen Funktion *F* und einer Entität *y* gibt, so dass eine Ähnlichkeit zwischen Aktivität F und y existiert (vgl. Steen 1999: 67).

4. Der vierte Schritt nennt sich das Identifizieren der nicht-wörtlichen Analogien („nonliteral analogy identification“). Die fehlenden Konzepte *F* und *y* werden ersetzt (vgl. Steen 1999: 68).

   (GALLOP-AWAY CANCER) → (∃ F) (∃y) {SIM[DEVELOP FAST (CANCER), GALLOP-AWAY(HORSE)]} (vgl. Semino et al. 2004: 1282).
5. Der letzte Schritt ist das Formulieren der konzeptuellen Metapher, oder laut Steen (1999) das Identifizieren des nicht-wörtlichen Mappings („nonliteral mapping identification“) (vgl. Steen 1999: 71).

   FAST DEVELOPMENT OF CANCER IS GALLOPING AWAY (vgl. Semino et al. 2004: 1282).

Basierend auf dem oben angeführten Fünf-Schritten-Modell ist es möglich, lexikalische Metaphern nach ihren Herkunftsdomänen zu gruppieren und konzeptuelle Metaphern zu eruieren. Für jede Metapher ist darüber hinaus eine kurze Beschreibung bzw. sachlicher Hintergrund notwendig. Besonders wenn es um fachliche Termini geht, kann auf einen inhaltlichen Exkurs nicht verzichtet werden.

Dodge et al. (2015) versuchte ein System zum automatischen Identifizieren, Kategorisieren und der Analyse von Metaphern in einem Korpus im Rahmen des Projekts MetaNet zu entwickeln und zu formalisieren. Das System besteht aus einem Repository von in früheren linguistischen Studien entdeckten konzeptuellen Metaphern, Frames, metaphorischen Ausdrücken und metaphorischen Beziehungen, aus einem Algorithmus zum automatisierten Extrahieren von Metaphern, der sich auf die im Repository gespeicherte Informationen bezieht, und aus computergestützten Instrumenten zur Bewertung, Analyse und Visualisierung der extrahierten Datensätze (vgl. Dodge et al. 2015: 41). Der Repository von Frames ist frei online zugänglich und stellt eine Sammlung von „conceptual gestalts: structured, schematic representations of different kinds of experiences, objects and events“ dar (vgl. MetaNet Frame Relation Type). So sind solche Frames aufgelistet wie z.B. „disease“, „family“, „game“, „poverty“ etc., die potenzielle Zieldomäne und Herkunftsdomäne für konzeptuelle Metaphern sind (z.B. GUNS ARE A DISEASE), insgesamt 576 Frames. Besonderes Augenmerk wird darauf gelegt, die hierarchischen Beziehungen zwischen Frames zu demonstrieren (DISEASE ist Unterbegriff von PHYSICAL AFFLICTION, der wiederum ein Unterbegriff von PHYSICALLY HARMFUL ist, siehe Abb. 3).

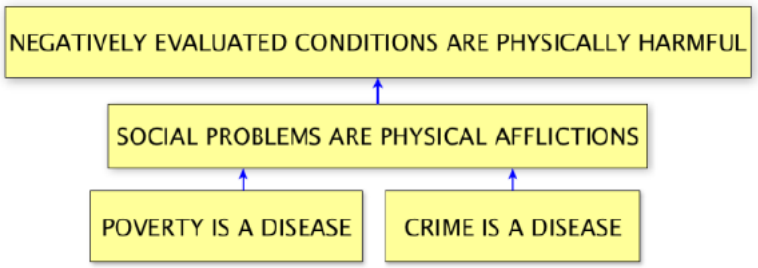

Abbildung 3: Metaphernvererbungsnetz (vgl. Dodge et al. 2015: 41)

Erk et al. definieren den Begriff „Frame“ als eine „abstrakte Situation“ (vgl. Erk et al. 2003: 537). Beispielsweise gehören zum Frame „Commercial transaction“ Buyer, Goods, Seller, Money, Purpose, Reason (vgl. Erk et al. 2003). Busse (2012) präzisiert, dass Frames konzeptuelle Wissenseinheiten sind, die es ermöglichen, die Bedeutungen sprachlicher Ausdrücke zu erfassen.

Frames enthalten Informationen, die sie kontextualisieren und die sie mit anderen Frames innerhalb eines größeren Netzwerks in Beziehung setzen. Zu diesen Frame-To-Frame Beziehungen zählen „makes use of“, „is a subcase of“, „is a subprocess of“, „incorporates a role“, „is related to“, „is in scalar opposition to“, „is in perspective on“, „is in casual relation with“ (vgl. MetaNet Frame Relation Type). Die metaphorischen Mappings, die auf der Basis von diesen Beziehungen entstehen, werden in Abb. 4 demonstriert.

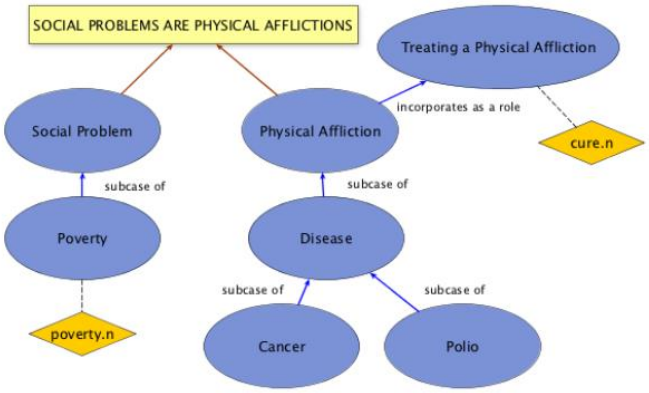

Abbildung 4: Frame-To-Frame Beziehungen (vgl. Dodge et al. 2015: 45)

Der Algorithmus für die Identifizierung von Metaphern beruht auf den früher identifizierten häufig auftretenden grammatikalischen Mustern für Metaphernbildung. In jeder grammatischen Konstruktion wird angegeben, welches Konstruktionselement der Herkunftsdomäne („source domain“, mit „S“ markiert) und welches der Zieldomäne („target domain“ mit „T“ markiert) entspricht. Die Liste ist in Tabelle 1 angeführt. Damit der Korpus in einer maschinenlesbaren Form

vorliegt, wird jeder Satz in ein sogenanntes RDF (Resource Description Framework) Format umgewandelt und jedes Wort wird mit Attributen versehen, die in der Web Ontology Language (OWL) definiert sind (z.B. Wortart, Position im Satz etc.). Die Texte werden nach Schlüsselwörtern mittels der Abfragesprache SPARQL untersucht (vgl. Dodge et al. 2015: 44). Wenn es Übereinstimmungen zwischen grammatikalischen Metaphernbildungsmustern und im Korpus gefundenen Ausdruck gibt und die identifizierten Frames schon als Herkunfts- und Zieldomäne für andere im Repository gespeicherten konzeptuelle Metaphern dienen, dann wird dieser Ausdruck positiv als potenzielle Metapher bewertet (vgl. Dodge et al. 2015: 45).

Constructional pattern	**Examples**
T-subj_S-verb	poverty infects
T-subj_S-verb-conj	poverty infects and maims
T-subj-conj_S-verb	homelessness and poverty infect
S-verb_T-dobj	escape poverty
S-verb_T-dobj-conj	escape despair and poverty
S-verb_Prep_T-noun	slide into poverty/pull up out of poverty
S-noun_of_T-noun	trap of poverty
T-noun_poss_S-noun	poverty's undertow
S-noun_prep_T-noun	path to poverty
T-noun_mod_S-noun	poverty trap
S-adj_mod_T-noun	burdensome poverty
T-noun_cop_S-noun-adj	poverty is a disease/poverty is burdensome

Tabelle 1. Grammatikalische Muster für Metaphernbildung (vgl. Dodge et al. 2015: 43)

2.3.6 Herkunftsdomäne und Image Schemas

Eine konzeptuelle Metapher kann man als eine Art Mapping von der Herkunftsdomäne auf die Zieldomäne verstehen. Im Fall von DIE LIEBE IST EINE REISE ist LIEBE die Herkunftsdomäne und REISE die Zieldomäne. Es werden nicht alle Aspekte einer Herkunftsdomäne 1:1 übertragen, als Folge werden bestimmte Aspekte der jeweiligen Zieldomäne hervorgehoben, andere aber verborgen (vgl. Gibbs 2018: 5). Beispielsweise gehört zum Konzept THEORIEN SIND GEBÄUDEN das Fundament („das theoretische Fundament der Theorie") aber nicht Fenster oder Treppenhäuser (vgl. Lakoff & Johnson 2021: 66).

Wie schon bereits erwähnt, sind Herkunftsdomänen in konzeptuellen Metaphern oft mit den körperlichen Handlungen und Erfahrungen der Menschen verbunden (vgl. Gibbs 2018:7). Die konzeptuelle Metapherntheorie postuliert, dass die Herkunftsdomäne für konzeptuelle Metaphern in einer Beziehung mit so genannten Image Schemas stehen und auf sich wiederholenden Instanzen der verkörperten Erfahrung (vom Englischen „embodied experience“) basieren. Johnson (1987) definiert „image schema“ als „recurring, dynamic pattern of our perceptual interactions and motor programs that gives coherence and structure to our experience” (vgl. Johnson 1987: xiv). Einige anschauliche Beispiele von Image Schemas, die oft an der metaphorischen Sprache und am Denken beteiligt sind, sind BALANCE, dessen Ursprung durch unsere Erfahrung mit Gleichgewicht und Ungleichgewicht und Gravitation bedingt ist (vgl. Gibbs 2018: 7) oder CONTAINMENT, das vermutlich dadurch entstanden ist, dass Menschen systematisch Erfahrung mit Einschließung und geschlossenen Räumen sammeln, Räume wie Zimmer betreten und verlassen können, in Transportfahrzeuge ein- und aussteigen usw., Objekte in Container platzieren und rausnehmen können (vgl. Johnson 1987: 21).

Die Bedeutung von Image Schemas für das Verstehen des Wesens von konzeptuellen Metaphern kann nicht überschätzt werden, denn der bildhaft-schematische Charakter metaphorischer Herkunftsdomäne stellt eine wesentliche Einschränkung dessen dar, was im konzeptionellen metaphorischen Denken gemappt wird (vgl. Gibbs 2018: 8). Gibbs (2018) postuliert, dass „the partial source-to-target domain mappings in conceptual metaphors generally preserve the image-schematic structure of the source domain” (vgl. Gibbs 2018: 9). Diese Projektionen aus der Herkunftsdomäne auf die Zieldomäne (vom Englischen “source-to-target domain correspondences” or “(mental) mappings”) werden in konkreten linguistischen Einzelmetaphern manifestiert (vgl. Gibbs 2018: 2). Die Übertragungen aus der Herkunfts- in die Zieldomäne für die konzeptuelle Metapher DAS LEBEN IST EINE REISE kann wie folgt abgebildet werden:

- Reiseführer → Ratgeber im Leben
- Reisende → Leute, die das Leben führen
- sich auf dem Weg bewegen → das Leben führen
- Zielort(e) → Lebensziele
- verschiedene Wege zum Ziel → verschiedene Mittel zur Erreichung des Lebensziels
- Strecke zurücklegen → Fortschritt im Leben
- Reiseabstände → Lebensabschnitte (vgl. Gibbs 2018: 2)

Aus den in diesem Kapitel präsentierten Begriffen „Herkunftsdomäne“, „Image Schema“ und „Mappings“ wird ersichtlich, dass dieses Wissensfeld gut terminologisch ausgearbeitet ist und in der englischsprachigen Forschungsliteratur eine terminologische Einheit herrscht, was in der deutsch-

sprachigen Literatur nicht immer der Fall ist. So ist das Paar „target domain“ manchmal als „Herkunftsdomäne“, „Ausgangsdomäne“, „Quelldomäne“ oder sogar „Bildspender“ übersetzt, „source domain“ als „Zieldomäne“ oder „Bildempfänger“. Das bereits erwähnte Image Schema hat auch mehrere Äquivalente, wie „Bildschema“, „Image Schema“. Für den Begriff „source-to-target domain mappings“ oder „cross-domain mappings” (vgl. Lakoff 1993) existieren ebenso mehrere Varianten „das Cross-Domain-Mapping”, „die Projektion zwischen Herkunftsdomäne und Zieldomäne“ usw. Obwohl es hinsichtlich dieser Inkonsistenz terminologische Verwirrungen gibt, lassen sich für eine*n Leser*in, der*die mit der englisch-sprachigen Forschungsliteratur im Original vertraut ist, für jeden deutschsprachigen Terminus einen entsprechenden englisch-sprachigen ursprünglichen terminologischen Ausdruck zuordnen. Für den Zweck der terminologischen Konsistenz werden in der vorliegenden Arbeit ausschließlich die Begriffe „Herkunftsdomäne“ und „Zieldomäne“ verwendet.

Aus den oben genannten Gründen wird in manchen Forschungsarbeiten beim Einführen von einem Begriff sein englischsprachiges Äquivalent in Klammern angegeben. Dieser Ansatz wurde in der vorliegenden Arbeit übernommen.

2.4 Kulturelle Spezifik von Metaphern

Der Thematik der kulturellen Spezifik in Bezug auf konzeptuelle Metaphern soll besondere Aufmerksamkeit gewidmet werden, da dieser Aspekt im Mittelpunkt der vorliegenden Masterarbeit steht, deren Ziel ist, die kulturellen Unterschiede und Varietäten in konzeptuellen Metaphern zu verfolgen.

Eine der Thesen von Lakoff und Johnson (2021) war, dass die verschiedenen Kulturen verschiedene Konzeptsysteme haben. Diese Tatsache ist darauf zurückzuführen, dass jede Kultur in einer gegebenen physischen Umwelt existiert und dass unsere Erfahrungen von Kultur zu Kultur verschieden sind. Andererseits finden sich dank der Verwestlichung von Kulturen und dank der Tatsache, dass einige Erfahrungsarten universalen Charakter haben, Übereinstimmungen in den metaphorischen Konzepten (vgl. Lakoff & Johnson 2021: 39).

Trim (2007) bestätigte, dass es eine Abhängigkeit zwischen der kulturellen Distanz und den existierenden konzeptuellen Metaphern gibt:

> It is likely that there is a relationship between cultural distance and the types of underlying conceptual metaphors. The greater the distance between cultures, the more likely there are differences in conceptual metaphors between two languages. (Trim 2007: 29)

Charteris-Black (2004) vertritt eine ähnliche Meinung, da er anmerkt, dass sich der Gebrauch einer bestimmten Metapher nicht nur von einem*r Sprecher*in zu einem*einer anderen Sprecher*in unterscheiden kann, sondern auch unter Sprechern verschiedener Sprachen variieren kann. Die konventionalisierten Metaphern in einer Sprache überlappen nicht unbedingt mit den konventionalisierten Metaphern in einer anderen Sprache. Eine Metapher, die in einer Sprache üblich ist, kann als „neue" Metapher (vom Englischen „novel metaphor") in einer anderen Sprache dienen. Die Motivation, die der konzeptuellen Metapher zu Grunde liegt, kann für Zweitspachler*innen möglicherweise undurchsichtig sein (vgl. Charteris-Black 2004:19).

Die Idee, konzeptuelle Metaphern über mehrere Sprachen hinweg zu vergleichen ist nicht neu, und dieses Thema wurde in Werken von mehreren Sprachwissenschaftler*innen behandelt (vgl. Barcelona 2001, Kövecses 2005, Gibbs 2018). Die Schlussfolgerungen der Wissenschaftler*innen sollen in Kürze vorgestellt werden.

Trim (2007) schlug eine vereinfachte Klassifizierung vor:

1. Beide Sprachen teilen eine konzeptuelle Metapher und ihre linguistische Form
2. Beide Sprachen teilen eine konzeptuelle Metapher, nicht aber ihre linguistische Form
3. Eine konzeptuelle Metapher existiert nur in einer Sprache (vgl. Trim 2007: 29)

Dass diese Liste für eine kontrastive Analyse nicht erschöpfend ist und dass sich jede Kategorie in Unterkategorien unterteilen lässt, wird weiter elaboriert.

Gibbs (2018) merkt an, dass es ausreichende linguistische Belege dafür gibt, dass viele Kulturen ähnliche metaphorische Konzepte teilen, so wie DIE ZEIT IST EIN RAUM, EIN WÜTENDER MENSCH IST EIN BEHÄLTER UNTER DRUCK oder DAS LEBEN IST EINE REISE (vgl. Gibbs 2018: 37).

Obwohl es nicht wenige Fälle gibt, in welchen eine konzeptuelle Metapher sprachübergreifend ist, kann sie in jeder Sprache anders linguistisch repräsentiert werden und diese spezifischen Manifestationen können subtile Unterschiede im kulturell-ideologischen Hintergrund offenbaren, in dem konzeptuelle Metaphern funktionieren (vgl. Gibbs 2018: 37). Kövecses (2005) demonstriert das am Beispiel von zwei konzeptuellen Metaphern: die erste ist DIE GESELLSCHAFT IST EINE FAMILIE. Die Familie kann als eine Einheit gesehen werden, die durch eine autoritäre Person geleitet wird und in der alle anderen Familienmitglieder gehorchen sollen oder auch als ein Ort, an dem man Unterstützung und Empathie finden kann (vgl. Kövecses 2005: 118f). In der zweiten

Metapher DIE POLITIK IST EIN SPORT, bedeutet Sport in der im Amerikanischen Englisch American Football oder Baseball, während in der chinesischen Sprache über Tischtennis, Volleyball oder Fußball geredet wird (vgl. Kövecses 2005: 120).

Herkunftsdomänen können eindeutig sein, wie z.B. FEUER und trotzdem Varietäten bei der Interpretation zulassen, wie Kövecses (2005) zeigt: Obwohl die beiden Sprachen Englisch und Zulu FEUER als Herkunftsdomäne für WUT teilen, wird in der Zulu-Sprache die konzeptuelle Metapher WUT IST FEUER in Form von anderen lexikalischen Metaphern als im Englischen realisiert, z.B. auf Zulu kann man die Wut eines Menschen „löschen", indem man diesem Wasser auf den Kopf gießt. Diese abweichenden Interpretationen nennt Kövecses „entailments" (vgl. Kövecses 2005: 127).

Ein weiteres Merkmal, das bei einer kontrastiven Analyse verwendet werden kann, ist der Grad der linguistischen Ausgestaltung (vom Englischen „degree of linguistic elaboration"). Eine konzeptuelle Metapher, die in zwei Sprachen ähnlich ist, kann eine größere oder kleinere Anzahl von lexikalischen Ausdrücken produzieren (vgl. Kövecses 2005: 151). Darüber hinaus kann eine konzeptuelle Metapher in unterschiedlichen Sprachen in Form von einzelnen Wörtern, Mehrwortbenennungen oder komplexen syntaktischen Ausdrücken realisiert werden (vgl. Kövecses 2005: 152).

Andere Kriterien, nach denen konzeptuelle Metaphern verglichen werden können, umfassen den Grad der Konventionalisierung, den Grad der Spezifizität der Herkunftsdomäne oder der Zieldomäne und den Grad inwieweit eine Metapher transparent ist (vgl. Barcelona 2001:139). Kövecses (2005) kommt zum folgenden Schluss:

> Two languages may share a conceptual metaphor and the conceptual metaphor may be expressed by largely overlapping metaphorical expressions, but the expressions can reveal subtle differences in the cultural-ideological background in which the conceptual metaphor functions (Kövecses 2005: 155).

Anhang des Beispiels der konzeptuellen Metapher ZEIT IST RAUM kann demonstriert werden, wie in unterschiedlichen Kulturen räumliche Darstellungen darauf Einfluss haben, wie unterschiedlich in der Alltagssprache Zeit, Zukunft und Vergangenheit thematisiert wird. Boroditsky (2011) weist darauf hin, dass die zeitlichen Ereignisse entweder entlang einer vertikalen (für Mandarin-Sprecher*innen) oder horizontalen Achse (für Englisch-Sprecher*innen) geistig dargestellt und organisiert werden können. Die subjektive Wahrnehmung von Zeit unterscheidet sich auch zwischen den Kulturen: in Mandarin sind Metaphern, die von einem*r Beobachter*in ausgehen, der*die sich entlang einer stationären Zeitlinie bewegt, weniger wahrscheinlich als solche, die von einem*r stationären Beobachter*in und einer sich bewegenden Zeitlinie ausgehen. Es existiert eine

Abhängigkeit davon, ob in einer Kultur die akzeptierte Schreibrichtung von links nach rechts oder von rechts nach links ist, und in welcher Reihenfolge Proband*innen die Ereignisse in ihrer zeitlichen Abfolge sortieren. Für Englisch-Sprecher*innen liegt die Zukunft vor dem*der Beobachter*in und die Vergangenheit hinter dem*der Beobachter*in, was sich in entsprechenden Metaphern widerspiegelt („the future is ahead“). Für Aymara-Sprecher*innen ist dieses Muster umgekehrt und es wird gesagt, dass die Zukunft hinter dem*der Betrachter*in liegt, während die Vergangenheit vor ihm*ihr liegt (vgl. Boroditsky 2011).

Der Fall, in dem es offensichtlich ist, dass zwei Kulturen eine konzeptuelle Metapher nicht teilen, verdient eine genauere Betrachtung. Wie Gibbs (2018) feststellt, können zwei Kulturen manchmal zwei unterschiedliche konzeptuelle Metaphern für eine bestimmte Zieldomäne haben, was zu völlig unterschiedlichen Konzepten für diese Domäne in zwei Sprachen führt (vgl. Gibbs 2018: 39). Beispielsweise wird in der chinesischen Sprache das Herz als das Zentrum des Geistes gesehen, aber im Englischen und in vielen westlichen Kulturen gehört diese Rolle dem Gehirn, während das Herz für Emotionen und Gefühle zuständig ist (2018: 39). Diese unterschiedlichen Perspektiven führen zu zwei unterschiedlichen konzeptuellen Metaphern: DER GEIST IST DAS GEHIRN und DER GEIST IST DAS HERZ. Kövecses (2005) nennt diesen Zustand „alternative Metaphern”: „In alternative conceptualization we have a source domain in one language that is used for a particular target domain and we have a different source for the same target in another language” (vgl. Kövecses 2005: 70). Schematisch kann das wie in Abb.5 zu sehen dargestellt werden.

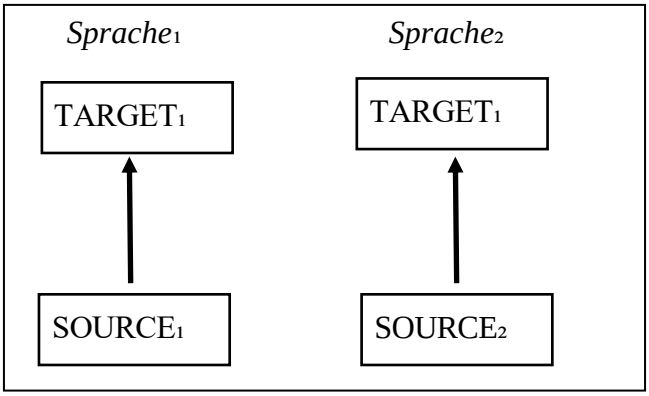

Abbildung 5: Vergleich von zwei konzeptuellen Metaphern mit derselben Zieldomäne und unterschiedlichen Herkunftsdomänen

Einen separaten Fall würde eine Situation darstellen, wenn es in zwei Sprachen für dieselbe Zieldomäne eine gemeinsame konzeptuelle Metapher gibt, es aber auch in einer der Sprachen für dieselbe Zieldomäne eine Metapher gibt, die nur für diese Sprache spezifisch ist wie in Abb. 6 dargestellt. Beispielsweise teilen die englische und die chinesische Sprache die Metapher DAS

GLÜCK IST OBEN, aber die Metapher DAS GLÜCK IST BLUMEN IM HERZEN existiert nur in der chinesischen Sprache (vgl. Kövecses 2005: 70).

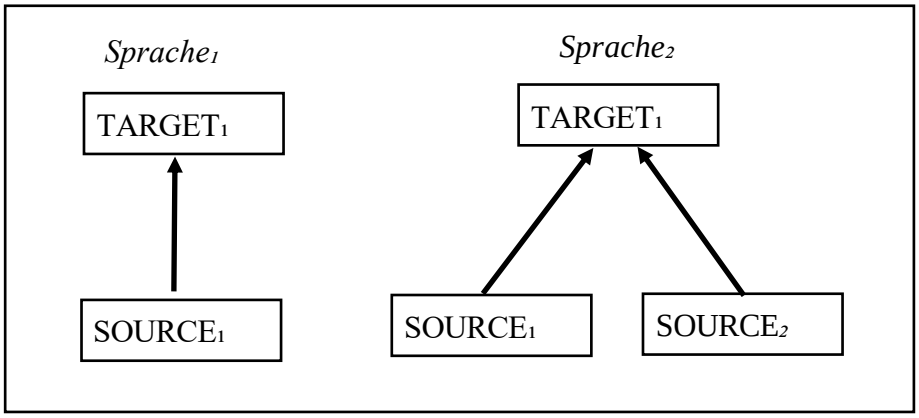

Abbildung 6:Vergleich von zwei konzeptuellen Metaphern mit derselben Zieldomäne und einer unterschiedlichen Anzahl an Herkunftsdomänen

Es finden sich auch Varietäten innerhalb der Herkunftsdomänen wie in Abb. 7 verbildlicht: z.B. GEBÄUDE kann als Herkunftsdomäne für die Zieldomäne Theorien oder Beziehungen im Englischen agieren, aber auch für Kindererziehung im Tunesischen (vgl. Kövecses 2005: 71-75).

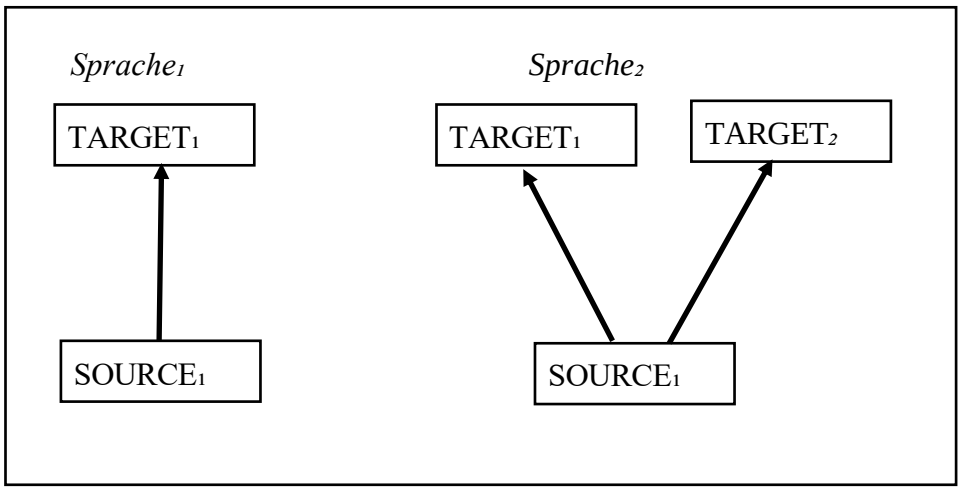

Abbildung 7: Vergleich von zwei konzeptuellen Metaphern mit derselben Herkunftsdomäne und einer unterschiedlichen Anzahl an Zieldomänen

Als einzigartige Metaphern („unique metaphors“) bezeichnet Kövecses solche, deren Herkunftsdomäne und Zieldomäne für eine Sprache einzigartig ist, d.h. für diese Herkunfts- und Zieldomäne gibt es keine konzeptuellen Metaphern in einer anderen Sprache (vgl. Kövecses 2005: 68). Solche Metaphern sind nicht einfach zu finden, wie Kövecses anmerkt, denn:

> most of our source and target domains are deeply entrenched in the conventional conceptual system and we do not easily invent either new sources in terms of which targets are conceptualized or new targets that are the focus of conceptualization by more basic source domains. (Kövecses 2005: 86).

Zusammenfassend lässt sich sagen, dass die komparativen wissenschaftlichen Studien von konzeptuellen Metaphern durch eine deutliche Tendenz gekennzeichnet sind, nämlich, dass viele konzeptuelle Metaphern im Großen und Ganzen universell verbreitet sind, besonders in Fällen, in denen diese Metaphern auf typischer körperlicher Erfahrung basieren (vgl. Gibbs 2018: 39). Es ist nicht verwunderlich, denn Menschen sind sich auf der Ebene, wie der menschliche Körper und das Gehirn funktionieren, wie wir uns bewegen, wie wir Objekte manipulieren usw. ähnlich (vgl. Kövecses 2005: 34). Es gibt keine einzige Lösung, die erklären kann, warum es doch Unterschiede in konzeptuellen Metaphern gibt, jeder Fall sollte separat analysiert werden. Zu einigen Faktoren zählen die physische Umgebung, die soziale Umgebung (Machtverhältnisse, Unterdrückung usw.), der kulturelle Kontext (Sitten und Bräuche, Mentalität), historische Bedingungen, Interessen, um nur einige zu nennen (vgl. Kövecses 2005). Bei der Analyse, in welchen konzeptuellen Metaphern in einzelnen Kulturen bestimmte abstrakte Begriffe thematisiert werden, werden Hypothesen aufgestellt, was Menschen über diesen abstrakten Begriffen denken (vgl. Kövecses 2005, Barcelona 2001, Lakoff & Johnson 2021)

2.5 Konventionalisierte Metaphern

Lakoff und Johnson (2021) teilen Metaphern in konventionalisierte und unkonventionelle auf. Konventionalisierte Metaphern sind Metaphern, die „das gängige Konzeptsystem unserer Kultur strukturieren, das sich seinerseits in unserer Alltagssprache niederschlägt“ (vgl. Lakoff & Johnson 2021: 161). Ihnen werden „neue“ Metaphern gegenübergestellt, die „außerhalb unseres konventionalisierten Konzeptsystems liegen“, „Metaphern, die der individuellen Phantasie und Kreativität entspringen“ (2021: 161). In anderen Worten, Metaphern wie LIEBE IST VERRÜCKTHEIT sind konventionalisiert („verrückt verliebt“), aber z.B. LIEBE IST EIN GEMEINSAM GESCHAFFENES KUNSTWERK ist ein Beispiel von einer neuen, originellen Metapher, weil in der Regel über Liebe nicht wie über ein Bild oder eine Skulptur geredet wird, das man einrahmen kann und auf eine Wand hängen oder auf einem Postament platzieren kann, um von anderen bewundert zu werden.

Charteris-Black meinte (2004), dass alle konventionalisierte Metaphern einmal der Kategorie neuer Metaphern angehörten:

> Conventional metaphors are phrases that exist at some point between literal and metaphorical uses – they reflect a diachronic process whereby use that was originally 'metaphorical' becomes established as 'literal' within a language. (Charteris-Black 2004: 17)

Je mehr eine Metapher in einer Sprache verwendet wird und durch die Sprecher*innen als treffend akzeptiert wird, desto schneller passiert dieser Prozess der Konventionalisierung, bis die Metapher „automatic, effortless and generally established as a mode of thought among members of a linguistic community" ist (vgl. Lakoff & Turner 1989: 55). Nur erfolgreiche Metaphern werden konventionalisiert (vgl. Charteris-Black 2004: 18).

Laut Charteris-Black ist der erfolgreichste Ansatz, um konventionalisierte Metaphern zu identifizieren, in einem umfangreichen Korpus nachzuschlagen. Wie häufig eine Metapher im modernen Sprachgebrauch auftritt, kann den Grad nachweisen, inwieweit eine Metapher in einer Sprache konventionalisiert ist (vgl. Charteris-Black 2004: 19). Tatsächlich kann eine konventionalisierte Metapher als Klischee eingestuft werden:

> Metaphor does not signify an unworldly transcendence from ordinary language, thought, or reality. Instead, what is most clichéd and conventional about reality are those aspects of experience that are primarily constituted by metaphorical thought. (vgl. Gibbs 2018: 3)

In der vorliegenden Arbeit werden die konventionalisierte Metaphern in den Mittelpunkt der Untersuchung gestellt. Es soll angemerkt werden, dass keine klar gezogene Grenze zwischen den „neuen" und „langlebigen", „konventionalisierten" Metaphern existiert. Es gibt ein breites Spektrum an konventionalisierten, neuen, lebendigen und toten Metaphern; die Tatsache, dass eine Metapher als konventionalisiert bezeichnet wird, bedeutet nicht, dass sie gar keine Metapher ist und keine übertragende metaphorische Bedeutung hat (vgl. Charteris-Black 2004: 67).

2.6 Kritik an der konzeptuellen Metapherntheorie

Seit der Vorstellung der konzeptuellen Metapherntheorie im Jahre 1980 wird über den Stellenwert der in Lakoff und Johnson (1980) aufgestellten Thesen gestritten. Einige Kritiker*innen (Strang 1982, Murphy 1997) haben sofort in den 80er Jahren auf die Idee, dass konzeptuelle Metaphern existieren, negativ reagiert und zwar mit der Behauptung, dass es nicht genug Beweise gibt, um deren Existenz zu begründen. So berichtet Strang (1982), dass es einen „gap between evidence and conclusion" gibt

(vgl. Strang 1982: 134). Laut Strang (1982), ist dieses Werk nur eine „series of essays", und hat nur einen wenig wissenschaftlichen Wert: „vast conclusions can be drawn from suggestive, carefully chosen instances" (vgl. Strang 1982: 135). Sie findet die linguistische Evidenz, die Lakoff und Johnson präsentiert haben, als nicht ausreichend, um zu behaupten, dass wir alle Aspekte unseres Lebens, unsere Realität in Metaphern strukturieren und dementsprechend handeln (1982: 135). Murphy (1997) zeigt, dass der Begriff „metaphorisches Konzept" nicht eng genug ausgearbeitet ist (vgl. Murphy, 1997: 100) und dass metaphorische Ausdrücke nur als Beweis für „structural similarity between domains" interpretiert werden können und nicht als Beweis der zu Grunde liegenden konzeptuellen Metaphern (vgl. Murphy, 1996: 173).

Gibbs erkennt die Berechtigung dieser Vorwürfe, und vermerkt dazu: „The fact, that a speaker […] used particular words or phrases does not imply that he was cognitively drawing cross-domain comparisons" (vgl. Gibbs 2018: 8). Beim Ziehen von Schlussfolgerungen über menschliches Denken und menschliche Erfahrung aus der textuellen und sprachlichen Analyse muss man vorsichtig sein. (2018: 8). Ob metaphorische Sprache unbedingt aktives metaphorisches Denken voraussetzt, war im Jahr 1980 schwierig eindeutig zu beantworten. Mittlerweile werden aktiv Studien (Boroditsky 2011, Boulenger et al. 2012) durchgeführt, um festzustellen, ob bei der Verarbeitung von metaphorischer Sprache (z.B. „grasp the idea") im Gehirn dieselben sensomotorischen Bereiche aktiviert werden, wie bei der Verarbeitung von Ausdrücken, die mit dem Manipulieren von Objekten zu tun haben (z.B. „grasp the handle"). In einer Analyse mehrerer schon vorhandener Brain-Imaging-Studien kommt Desai (2021) zu dem Schluss, dass „on a fairly consistent bases, sensory-motor metaphors activate corresponding sensory-motor areas" (2021: 9). Auf der Basis der durchgeführten Studien behauptet er folgendes:

> Evidence from brain imaging, brain stimulation, and lesion studies, on balance, shows that when abstract concepts are expressed as linguistic metaphors to sensory-motor domains, they are understood in terms of those domains (vgl. Desai 2021: 15)

Es soll hervorgehoben werden, dass sich die oben angeführten Forschungsergebnisse nur auf eine begrenzte Auswahl von Metaphern beziehen und nicht als ausschlaggebende Nachweise für alle Arten von Metaphern dienen können. In der gängigen Forschungspraxis wird es trotzdem zugelassen, dass die einzelnen linguistischen Metaphern die zu Grunde liegenden konzeptuellen Metaphern widerspiegeln können, insbesondere wenn mehrere sprachliche Ausdrücke systematisch miteinander verbunden zu sein scheinen (vgl. Gibbs 2018:104). Die Existenz einer konzeptuellen Metapher wird nie nur auf Basis einer einzelnen lexikalischen Metapher postuliert, es werden in der Regel 5-10 oder

sogar mehr zusammenhängende sprachliche Ausdrücke angeführt (vgl. Barcelona 2001, Semino et al. 2004)

In der Literatur werden oft methodologische Schwachstellen der konzeptuellen Metapherntheorie behandelt. Es wird u.a. behauptet, dass die systematische Analyse von konventionalisierten metaphorischen Ausdrücken auf reine Intuition gestützt ist (vgl. Gibbs: 2018:8). Goschler formuliert dieses Problem wie folgt:

> Bei der Zusammenfassung verschiedener Herkunftsbereiche zu konzeptuellen Metaphern oder auch Metaphernmodellen ist der Analysierende bei der Entscheidung, was eine konzeptuelle Domäne ausmacht und wie sie von anderen Domänen abzugrenzen ist, im Wesentlichen auf seine Intuition angewiesen. Daher kommt es in jeder dieser Analysen zu ad-hoc postulierten Metapher. Je nach Intuition oder Geschmack werden viele verschiedene, dann oft sehr spezifische, oder sehr wenige generalisierende zugrunde liegende konzeptuelle Metaphern angenommen. (vgl. Goschler 2009:189)

Menschliche Meinungen, ob eine lexikalische Einheit eine Metapher darstellt, variieren stark. Verschiedene Menschen können denselben Ausdruck unterschiedlich interpretieren und abweichende implizite Metaphern ableiten. Es kann also mehr als nur eine Entsprechung zwischen den linguistischen Metaphern und der konzeptuellen Metapher, die ihr zu Grunde liegt, geben. (vgl. Gibbs: 2018: 115)

Als weiterer Nachteil wird der konzeptuellen Metapherntheorie vorgeworfen, dass sie über keine gültigen Leitlinien für das Identifizieren von konzeptuellen Metaphern verfügt. Es wird diskutiert, welche Kriterien ausreichend sind, um mit Sicherheit zu behaupten, dass bestimmte lexikalische Ausdrücke die Anwesenheit von bestimmten konzeptuellen Metaphern direkt beweisen (vgl. Gibbs: 2018:9). Einige Versuche, ein solches Modell zu erarbeiten, wurden von Steen (vgl. Steen, 1999; Dodge et al. 2015) unternommen und wurden im Kapitel 2.3.5 ausführlich behandelt. Laut Dodge et al. (2015) wird mit ihrem Ansatz der oft geäußerten Kritik begegnet, dass die typische Analysen von konzeptuellen Metaphern idiosynkratisch sind, in denen die Methodik sich von Forscher*in zu Forscher*in unterscheidet, und dass die Forscher*innen einen Top-down-Ansatz verfolgen und sich auf die Analyse von Daten stützen, die durch Introspektion gewonnen wurden und sich auf der Analyse von Metaphern fokussieren, die der*die Forscher*in schon vorher in der Literatur identifiziert hat, in anderen Worten eine Zirkelargumentation (vgl. Dodge et al. 2015: 40). Dodge et al. (2015) schlagen vor:

> Instead of relying on intuitions about how a given target domain is metaphorically conceptualized, it is possible to search a corpus and identify which source domain lemmas and frames are used, and with what relative frequency (vgl. Dodge et al. 2015: 46).

Im Rahmen des Projekts MetaNet wurde eine Analysemethode entwickelt, in der schon vorhandene Erkenntnisse über die konzeptuellen Metaphern in Form von einem Repository von einem zusammenhängenden Netz von Frames und Metaphern integriert sind, und die im Gegensatz zu den Ansätzen der intuitiven, beispielsbasierten Analyse von Metaphern, eine automatisierte rechenbasierte Identifizierung von einer großen Anzahl von metaphorischen Ausdrücken in einem Korpus ermöglicht und laut der Einschätzung von Linguist*innen für die englische und spanische Sprache zuverlässige Ergebnisse liefert (vgl. Dodge et al. 2015: 46). Der Quellcode für den Algorithmus wurde online publiziert; das Repository von Frames und Metaphern steht ebenso online zur Verfügung (vgl. MetaNet GitHub Repository 2017, vgl. MetaNet Wiki 2016).

Die in diesem Kapitel angeführte Kritik an der konzeptuellen Metapherntheorie soll nicht den Eindruck vermitteln, dass sie überwiegend mit Skepsis gesehen wird. Die große Zahl der Studien, die in der Anlehnung an die Theorie durchgeführt werden, beweist das Gegenteil. Die Theorie war „an eye-opener in the worlds of both metaphor studies and cognitive science", so Gibbs (vgl. Gibbs: 2018:148).

3. Aktueller Stand der Forschung

Seit der Veröffentlichung der Theorie von konzeptuellen Metaphern von Lakoff und Johnson (1980), das den Untersuchungsgegenstand aus der interdisziplinären (linguistischen und philosophischen) Sicht behandelt, wird das Thema der konzeptuellen Metaphern von mehreren wissenschaftlichen Disziplinen untersucht. Aus der Perspektive der Psychologie ist eine mögliche Forschungsrichtung psychologische Experimente durchzuführen, um festzustellen, wie die Auswahl einer bestimmten Metapher das Verhalten der Proband*innen bei der Problemlösung beeinflusst (vgl. Thibodeau & Boroditsky 2011). Wie Gibbs (2018) anmerkt, bleibt die Analyse von konzeptuellen Metaphern ein wertvolles Instrument der Erkenntnisgewinnung für Wissenschaftler*innen, die sich für (Zweit)Sprachlehre, pädagogische Praxis, interkulturelle Kommunikation, Werbung und Marketing, die Interaktion zwischen Patient*innen und Ärzt*innen, Psychotherapie, Übersetzungswissenschaft oder Politik interessieren (vgl. Gibbs 2018: 4). Im Fokus von Metaphernforscher*innen stehen die individuelle Kreativität von Literat*innen, schöpferische Traditionen, kulturelle Motive, kommunikative Fähigkeiten in Abhängigkeit von sozialen Verhältnissen, die Wirkung von Metaphern auf Gedanken, Emotionen, bewusste und unbewusste Kognition, so Gibbs (2018: 7). Konzeptuelle Metaphern werden von Vertreter*innen der angewandten Linguistik, kognitiven Linguistik, Übersetzungs- und Terminologiewissenschaft und Philosophie untersucht (vgl. Elitze 2012, Drewer 2003, Özçalskan 2003, Papišta 2017).

In diesen Studien wurden Metaphern sowohl innerhalb nur einer Sprache als auch sprachvergleichend untersucht. Einige Forschungsergebnisse dieser Studien werden im Folgenden näher betrachtet.

Eine beispielhafte Untersuchung von konzeptuellen Metaphern in der Alltagssprache stellt das Werk von Özçalskan (2003) dar. Sie versuchte die sprachlichen Unterschiede im Bereich von Bewegung im Raum in Bezug auf Metaphern zu identifizieren. Sie führte eine systematische Analyse der linguistischen Metaphern im Englischen und Türkischen durch, die mit dem Konzept von Bewegung verbunden sind. In Anlehnung an die Theorie von konzeptuellen Metaphern hatte sie das Ziel, die Besonderheiten und Gemeinsamkeiten der metaphorischen Strukturen in beiden Sprachen aufzudecken, die für eine bestimmte Zieldomäne in Bewegungsmetaphern konzeptualisiert sind (vgl Özçalskan 2003: 190).

Als Textkorpus verwendete sie 20 Novellen und 10 Zeitschriften, die reich an Metaphern sind (vgl Özçalskan 2003: 193). Sie hat ungefähr 800 Metaphern im Englischen und Türkischen manuell extrahiert (2003: 194). Danach hat sie die Daten in verschiedenen Zieldomänen kategorisiert, z.B.

Zustand, Zeit usw. (2003: 195f). Anschließend hat sie für jede Zieldomäne konzeptuelle Metaphern identifiziert und zwischen den Sprachen verglichen, z.B. TIME IS LOCATION (2003: 197).

Sie ist zu dem Schluss gekommen, dass Zeit, Emotionen und Geisteszustände die größten Zieldomänen sowohl im Türkischen als auch im Englischen sind, die Gebrauch von Bewegungsmetaphern machen, gefolgt von der Domäne von Körperzuständen, z.B. Krankheiten oder Tod (2003: 194). In Zeitungen dienen auch andere abstrakte Konzepte wie Wirtschaft, Bevölkerung, Budget, Staat als Zieldomänen (2003: 194). Am Ende hat sie eine komparative Liste von allen Zieldomänen präsentiert (2003: 195). Beide Sprachen haben eine begrenzte fast identische Liste der Herkunftsdomäne und auch die Projektionen zwischen den Herkunftsdomänen und Zieldomäne (Bewegung) sind gleich (2003: 222).

Drewer (2003) untersuchte die Rolle der konzeptuellen Metaphern in der Fachsprache für die Erkenntnisgewinnung und -vermittlung. Sie verwendet zwar den Begriff „kognitive Metapher", und begründet die Auswahl der Termini, damit dass das Adjektiv „kognitiv" die kognitive Dimension der Metapher unterstreicht, und von „konzeptuell" abgrenzt, denn das sind die konzeptuellen Bereiche („conceptual domains"), die aufeinander projiziert werden, und schließlich die Metapherntheorie, die aus dem Bereich der ***Kognitiven*** Linguistik stammt. (vgl. Drewer 2003: 22). Drewer hat sich auf den Fachbereich der Physik konzentriert und als Zieldomäne Schwarze Löcher ausgewählt (2003: 133). Sie interessierte sich für Unterschiede zwischen Textsorten, die für Lai*innen erstellt sind, fachexterne Kommunikation und Textsorten mit einer höheren Fachlichkeitsstufe, fachinterne Kommunikation (2003: 2). Drewer wählte als Methode eine korpuslinguistische Analyse authentischer Fachtexte um sicherzustellen, dass Metaphern nicht kontextlos, sondern aus dem aktuellen Sprachgebrauch angeführt werden und um „eine intersubjektive Überprüfbarkeit der Daten und Ergebnisse zu gewährleisten" (2003: 136). Als Korpus für fachexterne Kommunikation verwendete sie didaktisierende Fachtextsorten, z.B. Lehrbücher für Schülerinnen und Schüler und popularisierende Fachtextsorten, z.B. populärwissenschaftliche Texte (2003: 155). Zum Korpus der fachinternen Kommunikation gehörten Lehrbücher für Studierende aus dem Fach der Physik, Astrophysik und Astronomie (2003: 170). Die Analyse wurde in drei Schritten realisiert: Die manuelle Identifizierung von Metaphern in Texten, das Filtern von konventionalisierten Metaphern von den kreativen Einzelmetaphern, das Formulieren von konzeptuellen Metaphern. (2003: 138). Jeder konzeptuellen Metapher ist ein eigenes Unterkapitel gewidmet, z.B. SCHWARZE LÖCHER SIND EIN GEHEIMNIS (2003: 260).

Drewer (2003) erarbeitete eine Typologie der Funktionen der Metapher in wissenschaftlichen Textsorten und teilte sie in zwei Gruppen: erkenntnisfördernde Wirkung (Gewinnung, kognitive Verarbeitung, Versprachlichung, perspektivische Präsentation, Vermittlung wissenschaftlicher

Erkenntnisse) und erkenntnishemmende Wirkung (Gefahren durch inadäquaten Metapherngebrauch – unreflektierter Metapherngebrauch, manipulativer Metapherngebrauch usw.) (vgl. Drewer 2003).

Die Analyse von Fachtexten weist nach, dass Metaphern zur Gewinnung neuer Erkenntnisse, Theoriekonstruktion, Hypothesenbildung, Kommunikation von innovativen wissenschaftlichen Erkenntnissen beitragen. Durch den Rückgriff auf das bestehende Wissen, wie körpergebundene Grunderfahrungen, wird die Komplexität der unbekannten Sachverhalte reduziert (vgl. Drewer 2003: 386f.) Abstrakte und komplexe Konzepte kann man am besten über Analogien begreifen (2003: 135).

Als ein Beispiel der sprachvergleichenden Studie für konzeptuelle Metaphern in der Fachsprache kann das Werk von Elitze (2012) dienen. In dieser Arbeit vergleicht sie die prozentuale statistische Aufteilung von Herkunftsdomänen für metaphorische Ausdrücke in der Fachsprache der Börse im Spanischen und Deutschen (sie nennt diesen Teil „Makroanalyse“) und beschreibt für jede Herkunftsdomäne im Detail jede einzelne lexikalische Metapher mit ihrem Hintergrund und mit Kontext, zusammen mit ihrem Äquivalent in der Fremdsprache („Mikroanalyse“) (vgl. Elitze 2012: 65). Die statistischen Forschungsergebnisse hat Elitze in Form von Diagrammen dargestellt. Dabei waren in beiden Sprachen die häufigsten Herkunftsdomänen „Krieg“, „Sport“, „Gebirge“ (2012: 67). Als Korpus untersuchte sie insgesamt 117 Artikel von Börsenberichten und Kommentaren aus der spanischen Tageszeitung El País und dem deutschen Tagesblatt Süddeutsche Zeitung (2012: 48). Aus den Forschungsergebnissen geht hervor, dass die Fachsprache der Börse sowohl im Deutschen als auch im Spanischen stark metaphorisch strukturiert ist und dass die beiden Sprachen großenteils eine große Ähnlichkeit im Metaphernrepertoire aufweisen oder sogar identische Metaphern teilen (2012: 111).

Dodge (2018) setzt die computergestützte Methode, die im Rahmen des Projekts MetaNet (siehe Kapitel 2.3.5) entwickelt wurde, zur Identifizierung von konzeptuellen Metaphern zum Thema „Armut“ („poverty“) ein. Die Metaphern wurden automatisch aus einem großen Korpus mit dem Einsatz des MetaNet Algorithmus zur Metaphernidentifizierung, der MetaNet Metaphernrepository und einer Reihe von typischen Mustern für die Metaphernbildung referenziert, extrahiert (vgl. Dodge 2018: 128).

Die potenziellen metaphorischen Ausdrücke wurden zuerst im Englischen Gigaword Korpus 2011 (vgl. Graff and Cieri 2003) anhand einer Suchanfrage, die die zum Frame *poverty* dazugehörende „lexikalische Units“ verwendet („poverty“, „impoverishment“, „indigence“, „destitution“, „poverty line“, „poverty rate“), ermittelt, insgesamt 17.755 Sätze (vgl. Dodge 2018: 139). Aus den extrahierten Datensätzen wurde ausgerechnet, welche Zieldomäne-Frames am öftesten vorkommen („diseases schema family“, „physical combat“, „position schemas“, „translational motion“, „endangerment schemas“, „motion impediments“, „harmful encounter“). Es wurde

festgestellt, dass im Diskurs zum Thema Armut zwei metaphorische Systeme prävalieren: das eine System verwendet „location/motion network“ („live in poverty“, „fall into poverty“), für das andere System bedeutet Armut „physical harm“ („suffer excruciating poverty“, „crippled by poverty“) (vgl. Dodge 2018: 128). Die jeweiligen Zieldomäne-Herkunftsdomäne Mappings für die beiden konzeptuellen Systeme werden im Detail in jedem Unterkapitel betrachtet. Aus der lexikalischen Analyse geht hervor, dass je nachdem ob von der Armut in Metaphern von Ort/Bewegung oder physischen Schäden gesprochen wird, sich der Standpunkt der Personen unterscheidet, die von der Armut betroffen sind. Da die Menschen in der Regel selbst für das Bleiben an einem Ort oder das Verlassen eines Ortes verantwortlich sind, unterstützen die erste Kategorie von Metaphern die Konzeptualisierung von Armut, in der die Menschen selbst für die Lage verantwortlich sind. Dagegen sind laut der zweiten Kategorie der Metaphern die betroffenen Individuen nicht für den Schaden verantwortlich, der ihnen zugefügt wurde und brauchen Hilfe von den anderen (vgl. Dodge 2018: 159-160). In dieser Arbeit mehrere konzeptuelle Metaphern wie POVERTY IS A BOUNDED REGION, POVERTY IS A DISEASE, ADDRESSING POVERTY IS TREATING A PHYSICAL AFFLICTION formuliert (vgl. Dodge 2018: 130, 145, 161).

Ein computergestützter Ansatz für die Erkennung von Metaphern im Korpus, der sich auf neuronale Netze basiert, wurde von Shutova et al. (2021) in einer Studie von Metaphern im politischen Diskurs verwendet. Ein Datensatz von 85.000 Facebook Posts, die von 412 US-Politikern veröffentlich wurden, wurde in der Studie verarbeitet (vgl. Shutova et al. 2022: 504). Das Model zur Metaphernidentifizierung nimmt als Eingabedaten ein Wortpaar, z.B. Adjektiv + Substantiv, Verb + Subjekt, Verb + Objekt, und gibt eine Punktezahl aus, wie wahrscheinlich das ist, dass dieser Wortausdruck metaphorisch ist (vgl. Shutova et al. 2021: 505).

Der Fokus der Untersuchung lag auf dem Zusammenhang zwischen dem metaphorischen Gebrauch und der Aktivität von Followern. Es wurde festgestellt, dass metaphorische Sprache mehr Engagement unter den Nutzern generiert, und dass es eine direkte Korrelation zwischen dem intensiveren metaphorischen Sprachgebrauch und der aktuellen politischen ungünstigen Position, d.h. Niederlage bei den Wahlen des*der Politiker*in existiert (vgl. Shutova et al. 2021: 510).

4. Methodik

In diesem Kapitel wird die für die vorliegende Arbeit gewählte Forschungsmethodik vorgestellt. Der korpusbasierte Ansatz für die Suche nach Metaphern und die Auswahl von Texten, die sich auf das Thema Cybersicherheit beziehen, wird begründet. Weiter wird das schrittweise Model für die automatische Metaphernidentifizierung von Dodge et al. (2015) zusammen mit ihren Anpassungen an die manuelle Herangehensweise präsentiert. Besondere Aufmerksamkeit wird der Problematik der Anwendbarkeit der ursprünglich für die englische Sprache erarbeiteten Construction Patterns für Metaphern auf die deutsche und russische Sprache gewidmet, sowie den methodischen Herausforderungen für die russische Sprache im Ganzen. Als letzter Schritt wird das Design für die Online-Umfrage, die für die Validierung der Ergebnisse geplant ist, erläutert.

4.1 Korpuserstellung

Das Ziel der vorliegenden Arbeit besteht darin, die bestehenden Metaphern im Bereich der Cybersicherheit zu finden und zwischen den drei Sprachen (Englisch, Deutsch, Russisch) zu vergleichen. Um sich einen fachlichen Überblick über den aktuellen Sprachgebrauch im Bereich Cybersicherheit zu verschaffen, empfiehlt es sich, einen Korpus der relevanten Fachliteratur zu analysieren. Derselbe Ansatz erwies sich als nützlich in den relevanten Studien, die im Detail in Kapitel 3 vorgestellt wurden (vgl. Elitze 2012, Drewer 2003, Özçalskan 2003). Ein wichtiges Argument wird von Gibbs (2018) betont:

> The examination of actual language patterns, as evident from the analysis of large-scale corpora, provides a firmer basis for determining underlying conceptual metaphors that can be provided by analyses that rely on dictionaries, thesauruses, or decontextualized verbal metaphors. Part of the concern here is that standard CMT analyses are too often based on the intuitions of individual analysts, which may be biased, inaccurate, or poor reflections of how metaphors are really used in discourse (Gibbs 2018: 117).

Durch eine korpusgeleitete Analyse kann sichergestellt werden, dass sprachliche Belege für konzeptuelle Metaphern nicht kontextlos angeführt werden und als Quelle nicht die individuelle sprachliche Intuition oder das Vokabular dienen. Laut Drewer (2003) ist eine wichtige Anforderung bei der Korpuserstellung, dass die analysierten Texte von den Autor*innen in ihrer Erstsprache verfasst werden müssen und keine Übersetzungen enthalten, um auszuschließen, dass Metaphern aus

einer Fremdsprache in den Text übernommen wurden (vgl. Drewer 2003: 137). Dies würde die Abgrenzung von Systemen von konzeptuellen Metaphern in drei Sprachen erschweren. Aus den oben angeführten Gründen ist die Textauswahl auf vergleichbare Texte begrenzt um einen Vergleichskorpus zu erstellen. Das sind Artikel und Blogeinträge auf den offiziellen Webseiten der Unternehmen, die professionelle Leistungen im Bereich Cybersicherheit erbringen. Um sicher zu stellen, dass es sich bei einem Text nicht um eine Übersetzung handelt, werden ausschließlich die Artikel berücksichtigt, die nur in einer Sprache verfügbar sind. Die mehrsprachigen Versionen derselben Texte sind von der Recherche ausgeschlossen, weil nicht sichergestellt werden kann, was die ursprüngliche Sprache des Textes war und daher auch nicht ob die gefundenen Metaphern eine Übersetzung aus einer Ausgangssprache in die Zielsprache darstellen und sonst nicht in der natürlichen Zielsprache vorkommen. Um die Vergleichbarkeit der vorgestellten Korpora zu gewährleisten, wurden Texte herangezogen, die vergleichbare Subbereiche der Cybersicherheit für die Sprachen Deutsch, Englisch und Russisch abdecken, nämlich die allgemeinen Informationen zum Thema Cybersicherheit, Faktoren der Cybersicherheit für private Personen und Unternehmen, Arten von Malware, Lösungen zum Schutz und Beseitigung von Computerviren, Netzwerkschutz (VPN und Firewalls), IT-Sicherheitsaudit und Testen der IT-Sicherheit im Unternehmen, Schutz vor Datenabfluss, Phishing-Attacken, Ransomware (Erpressersoftware), Verhalten bei einem IT-Sicherheitsvorfall, Insider-Attacken, die letzten Trends in der Cybersicherheit-Industrie wie die Gewährleistung der Cybersicherheit beim Remote Arbeiten, DDoS-Attacken, Attacken auf die kritische Infrastruktur, Schulung von Mitarbeiter*innen im Bereich IT-Sicherheit, Best Practices in der Industrie, Berichte über signifikante Sicherheitsverletzungen wie die Verbreitung von WannaCry-Malware und Hackerangriff-Vorkehrmaßnahmen. Online-Quellen wurde aufgrund ihrer Zugänglichkeit Vorzug gegeben, und zwar den Quellen, die bei der Google-Suche nach Schlüsselwörtern „Dienstleistungen Cybersicherheit IT-Sicherheit“ (auf Deutsch), „services cybersecurity it-security“ (auf Englisch), „услуги кибербезопасность информационная безопасность“ (auf Russisch) auf einer hohen Position in den Suchergebnisseiten erscheinen. Zu den Firmen, welche Internetressourcen für die Recherche herangezogen wurden, zählen Thinking Objects, Albfinanz, Perseus Technologies, Cyqueo, Gme, Suresecure, CBT Training & Consulting, YesDefend, SCHNEIDER INTERCOM, BLUE Consult, Vindler, G DATA CyberDefense, Kaspersky, CASA, Langguth, BRANDMAUER (in Deutschland), ARCEO Cybersecurity, Certitude Consulting, CyberCure, CYBERCONTACT-CERT, CYBERTRAP, IT-Native, ProxySec, TUFO Cyber Security, Werbeagentur Cybercrime, Itpmcc (in Österreich), ROHDE & SCHWARZ, T-Systems (mit Büros sowohl in Österreich als auch in Deutschland), SecurityScorecard, CyberUnit, Ricoh, Wizlynx, GE Digital, eSudo, CarefulSecurity, AuroraIT, Fortinet, Lieberman Technologies,

Courant, Defendify, Whittakerassociates, Datacast Technologies, Onsite Logic, Conversant Group, Lifars (in den USA), NetStar, ActionFraud, Redscan Cyber Security, IntruderSystems, ATG (in Großbritannien), Cipher, HackerOne, Nomios, Foresite, Opswat (EU), Nucleustechnologies, Cyberint (mit Büros sowohl in den USA als auch in Großbritannien), XBase (Canada), Смарт-Софт (Smart-Soft), АРинтег (ARinteg), СНС-Контрол (SNS-Control), Арудит Секюрити (Arudit Security), Лаборатория Касперского (Kaspersky Lab), КлаудКлан (CloudClan), Кодебай (Codeby), ДатаФорт (DataFort), Т1 Клауд (T1 Cloud), Гарда Технологии (Gardatechnologies) (in Russland), ВирусДетект (VirusDetect) (in der Ukraine).

Die analysierten Artikel werden kopiert und im Word-Dokument für die weitere Verarbeitung (die Aufzählung der Sätze/Seiten) separat pro Sprache zusammengesetzt. Die empfohlene Seitenzahl für einen Korpus für größere Abschlussarbeiten im Bereich konzeptueller Metaphern beträgt 300 Seiten (vgl. Drewer 2003), für kleinere Studien – ungefähr 100 (vgl. Özçalskan 2003). Für die vorliegende Arbeit beträgt der zusammengestellte Korpus ungefähr 65 Seiten pro Sprache (Schriftart Times New Roman, Schriftgröße 12), oder 50 Artikel. Die Quellen für die untersuchten Webseiten sind im Literaturverzeichnis angeführt.

Jede konzeptuelle Metapher soll ausreichend mit lexikalischen Beispielen belegt werden. Auf das Verfahren für die Metaphernanalyse soll nachstehend näher eingegangen werden.

4.2 Metaphernidentifizierung

Für die Metaphernidentifizierung wird in der vorliegenden Arbeit eine manuelle Variante der Methode des Projekts MetaNet von Dodge et al. (2015) angewendet. Die Methode zeigte eine hohe Präzision für Englisch (85 %) und Russisch (90 %) (vgl. Dodge et al. 2015: 46). Es kann erwartet werden, dass für eine mit Englisch verwandte germanische Sprache wie Deutsch vergleichbare zuverlässige Ergebnisse erzielt werden können. Als potenzielle weiterführende Forschungsrichtung wäre es auch möglich, die verfügbaren Quelldateien von MetaNet zu installieren, Texte aus dem Korpus in maschinenlesbarem Format zu parsen und automatisch Metaphern zu extrahieren, um diese mit den manuell erzeugten Ergebnissen zu vergleichen.

Um den Verlauf des Algorithmus von MetaNet manuell zu reproduzieren, sind folgende Schritte notwendig:

1. **Die Suche im Korpus nach Schlüsselwörtern**. Die Schlüsselwörter beschreiben die Herkunftsdomäne Cybersicherheit.

Schlüsselwörter für die englische Sprache: security, cyber(security), network, hacker usw.

Schlüsselwörter für die deutsche Sprache: Sicherheit, Cyber(sicherheit), Netzwerk, Hacker usw.
Schlüsselwörter für die russische Sprache: безопасность, кибер(безопасность), сеть, хакер, хакерский usw.

2. **Die Identifizierung von Kandidaten im Text**, die den geeigneten grammatikalischen Mustern für Metaphernbildung wie T-subj_S-verb, T-subj_S-verb-conj usw., entsprechen (siehe Kapitel 2.3.5). Ein Beispiel der Verwendung des CoreNLP Tools (vgl. CoreNLP 2022) für die Identifizierung von Construction Patterns ist in Abb. 8 dargestellt:

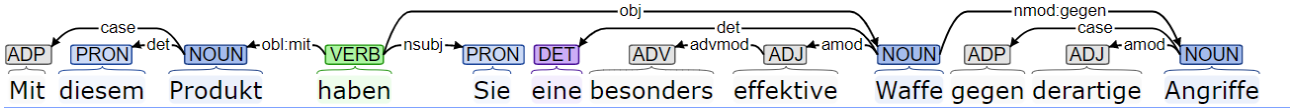

Abbildung 8: Die Identifizierung von Construction Patterns im Text mit Hilfe von CoreNLP Tool (vgl. CoreNLP 2022)

3. **Die Einschätzung der Wahrscheinlichkeit der Metapher**. Die Metaphernkandidaten werden analog mit der Framestruktur aus dem MetaNet-Verzeichnis analysiert. Die Beziehungen zwischen den Frames können nicht-metaphorisch sein, wenn die Frames direkt verlinkt werden können, z. B. „cure cancer“ (siehe Abb. 9) oder nur durch eine konzeptuelle Metapher verlinkt werden können, z.B. „cure poverty“ (siehe Abb. 10) (vgl. Dodge et al. 2015: 42, 45).

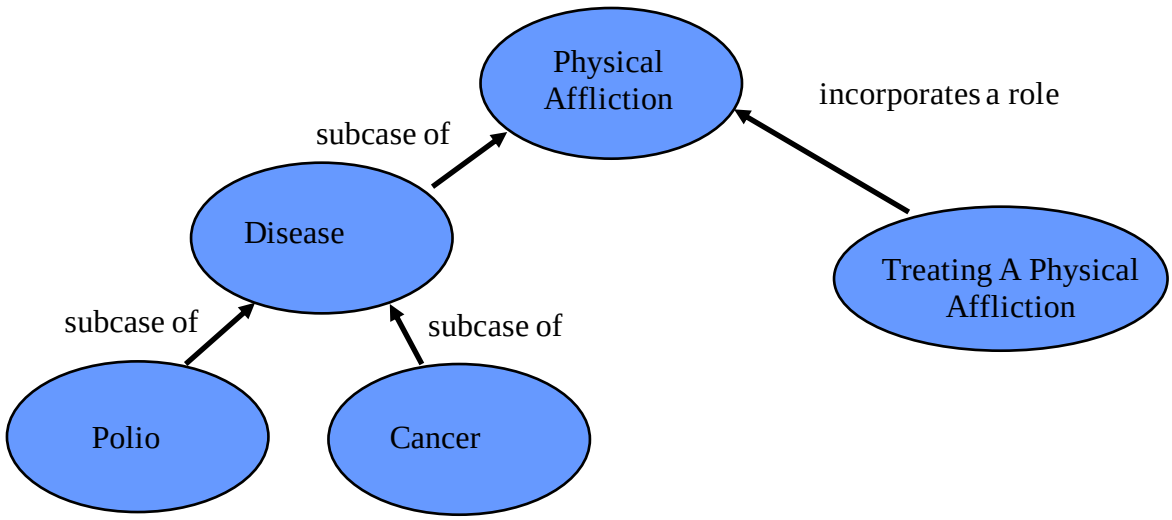

Abbildung 9: Nicht-metaphorische Beziehungen zwischen Frames „cure“ und „cancer“ (vgl. Dodge et al. 2015: 42)

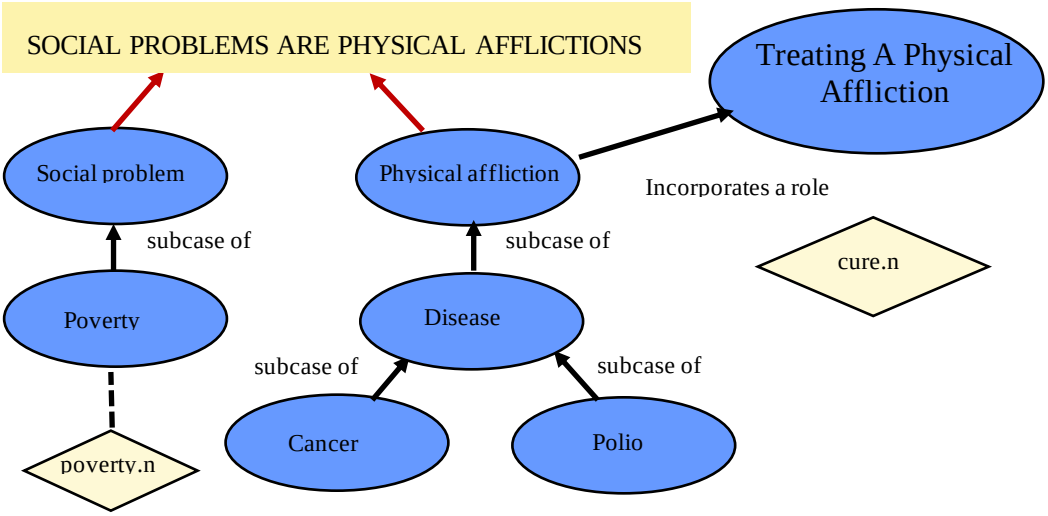

Abbildung 10: Metaphorische Beziehungen zwischen Frames „cure“ und „poverty“ (vgl. Dodge et al. 2015: 45)

Für die deutsche Sprache wird das FrameNet des Deutschen der Heinrich-Heine-Universität Düsseldorf (vgl. FrameNet des Deutschen 2022), für die englische Sprache wird das FrameNet der Internationale Informatik Institute (International Computer Science Institute) in Berkeley referenziert (vgl. FrameNet des Englischen 2022). Die farbmarkierten Schlüsselwörter in den Framedefinitionen, die Frameelemente, die lexikalischen Units, die im Frame enthalten sind, dienen als Hinweis auf die Metaphorizität der sprachlichen Ausdrücke. Die Metaphern, die denselben oder verwandten Frames angehören, z.B. Frame „attack“ und „hostile encounter“, werden zusammen analysiert und anschließend in Gruppen aufgeteilt. Auf der Basis der erhobenen Daten werden die folgenden Tabellen aufbereitet: eine Tabelle mit der Anzahl von Metaphern pro Gruppe pro Sprache, einschließlich der gesamten Anzahl von Metaphern für alle drei Sprachen; eine Tabelle mit der Anzahl der Metaphern mit der gesamten Anzahl der Sätze (für die sprachübergreifende Analyse); eine Tabelle mit den metaphorischen Mappings, die im Prozess der Metaphernidentifizierung aufgedeckt wurden und zwar separat pro Gruppe und pro Sprache; eine Tabelle mit den metaphorischen Beispielen und zugehörigen Frames separat pro Gruppe und pro Sprache für die Zwecke der sprachspezifischen Analyse; eine Tabelle mit den Constructions Patterns für die Metaphernbildung und ihre Häufigkeit pro Sprache.

4. **Ableiten von konzeptuellen Metaphern** aus den lexikalischen Darstellungen von konzeptuellen Metaphern und Analyse der Beziehungen zwischen den Ziel- und Herkunftsdomänen. Es werden mehrere mögliche Varianten für jede konzeptuelle Metapher formuliert, aus denen während der Validierung der Ergebnisse durch IT- und Cybersicherheit-

Expert*innen nur eine passende Formulierung ausgewählt werden soll. Zu diesem Zweck werden die einzelnen ausgewählten lexikalischen Metaphern nach den konzeptuellen Metaphern gruppiert und für die Validierung in Form einer Umfrage erfasst. Die detaillierte Vorgehensweise zum Umfrageprozess ist in Kapitel 4.4 beschrieben.

4.3 Methodische Herausforderungen für die Russische Sprache

Der im Kapitel 4.2 vorgestellte methodische Ansatz lässt sich nur mit bestimmten Schwierigkeiten für die russische Sprache anwenden. Zum Zeitpunkt des Erstellens der vorliegenden Masterarbeit existiert noch kein erarbeitetes FrameNet für die russische Sprache, das nützliche Informationen bezüglich der Framedefinitionen, Frameelementen, lexikalischen Units, Beziehungen zwischen Frames liefern könnte. Darüber hinaus gibt es keinen entsprechenden POS-Tagger oder Dependency-Parser für die russische Sprache, die frei zugänglich sind. Die Analyse beruht daher auf den Übersetzungen der jeweiligen Frames aus dem FrameNet des Englischen ins Russische, die Wortarterkennung und das Dependency Parsing wird manuell durchgeführt. Es sollte angemerkt werden, dass das FrameNet des Deutschen schließlich auch nur eine Übersetzung aus dem Englischen darstellt (vgl. FrameNet des Deutschen 2022). Laut Einschätzung von Erk et al. (2003) kann die Frameidentifizierung mit der manuellen Annotation im Korpus mit relativ hoher Präzision durchgeführt werden. Der Grad des Konsensus zwischen Linguist*innen bezüglich der Framezuordnung lag durchschnittlich bei 96-97% (vgl. Erk et al. 2003: 5). In anderen Aspekten unterscheidet sich die Vorgehensweise für das Formulieren von konzeptuellen Metaphern auf der Basis der lexikalischen Metaphern nicht von der für die deutsche und englische Sprache.

4.4 Validierung der Ergebnisse

Für die Validierung der Ergebnisse wird eine Umfrage durchgeführt. Die Zielgruppe sind IT-Expert*innen, vorzüglich mit Kenntnissen im Bereich Cybersicherheit. Zuerst wird zu Beginn der Umfrage eine kurze Einführung in konzeptuelle Metaphern dargestellt. Die anschließenden Fragen enthalten eine Liste mit metaphorischen Ausdrücken und eine Auswahlliste mit möglichen konzeptuellen Metaphern. Die Aufgabe besteht darin, eine konzeptuelle Metapher aus der vorgegebenen Liste auszuwählen, die die aufgelisteten sprachlichen Ausdrücke vereinigt. Es bleibt die Möglichkeit, die Liste zu ergänzen und anstatt der vorgegebenen konzeptuellen Metaphern eine

eigene zu formulieren. Zuerst wird eine kleine Pilotstudie mit einer Testperson pro Sprache durchgeführt und dann auf der Basis der Rückmeldungen die Umfrage mit den ergänzten Informationen aktualisiert und verbessert. Die Hauptaufgabe ist, die Subjektivität der in der selbstständigen Recherche erhobenen Daten zu reduzieren. Die Umfrage wird mittels Online-Tool LimeSurvey (vgl. LimeSurvey 2022) durchgeführt und wird separat für die deutsche, englische und russische Sprache angefertigt. Der Text der Umfrage ist im Anhang ersichtlich.

5. Forschungsergebnisse

Nach der durchgeführten Online-Recherche und der manuellen Suche nach metaphorischen Ausdrücken gilt es die erbrachten Forschungsergebnisse zu strukturieren und anschaulich präsentieren.

Im folgenden Kapitel wird in Form von Tabellen die Zahl der ermittelten Cybersicherheitsmetaphern pro Gruppe pro Sprache dargestellt und die Zahl wird zwischen den Sprachen verglichen, um zu demonstrieren, inwieweit Metaphern die Fachsprache der Cybersicherheit jeweils für Deutsch, Englisch und Russisch prägen. Die Ergebnisse einer sprachspezifischen Detailanalyse pro Gruppe werden ebenso tabellarisch aufsummiert. Welche grammatikalische Construction Patterns für welche Sprache eingesetzt werden, kann mittels einer entsprechenden Vergleichstabelle geschätzt werden. Jeder im Korpus gefundene metaphorische Ausdruck wurde seiner Herkunftsdomäne zugeordnet. Die Metaphern mit einer ähnlichen Herkunftsdomäne wurden ein eine Gruppe aufgenommen. Am Ende der Korpusrecherche wurden mehrere grob umrissene Gruppen deutlich. Der Kürze halber werden die Gruppen der Metaphern nach ihren Herkunftsbereich als „Kriegsmetaphern“, „Erkrankungsmetaphern“, „Innen/Außen-Metaphern“ (das sind die Metaphern, die die Cybersicherheit als einen geschlossenen Raum betrachten), „Jagdmetaphern“ und „Angelnmetaphern“ bezeichnet. Die konkrete Auslegung der Metaphern-Gruppen mit Beispielen erfolgt in einem entsprechenden Unterkapitel.

5.1 Sprachübergreifende Analyse

Ein statistischer Vergleich zwischen den Sprachen Deutsch, Englisch und Russisch mit einer Sortierung nach Metaphern-Gruppen zeigt, dass die ersten drei Gruppen Kriegsmetaphern, Erkrankungsmetaphern und Innen/Außen-Metaphern die Mehrheit aller Cybersicherheits-Metaphern darstellen (siehe Tabelle 2). Die Gruppe der Jagdmetaphern ist am wenigsten stark repräsentiert, mit nur etwa 5-6 Beispielen in allen Sprachen. Das „**Angeln**“ dient nur für die russische Sprache als Herkunftsdomäne und die Anzahl solcher Metaphern ist sehr gering, da nur 4 Beispiele identifiziert wurden. In Bezug auf gesamte Anzahl der Metaphern nimmt die englische Fachsprache der Cybersicherheit den ersten Platz mit insgesamt 41 identifizierten Beispielen ein, gefolgt von der deutschen Sprache mit 36. Der russische Korpus enthält am wenigsten metaphorische Ausdrücke, nur 31.

Metaphern-Gruppen	Deutsch	Englisch	Russisch	Die gesamte Anzahl
Kriegsmetaphern	11	12	7	30
Erkrankungsmetaphern	11	11	6	28
Innen/Außen-Metaphern	9	12	8	29
Jagdmetaphern	5	6	6	17
Angelnmetaphern	0	0	4	4
Gesamt	36	41	31	108

Tabelle 2. Anzahl der Metaphern pro Metaphern-Gruppe pro Sprache

Der Korpus für jede Sprache wurde insgesamt aus ca. 50 Artikeln zum Thema Cybersicherheit erstellt, daraus ergeben sich 1237 Sätze für die deutsche Sprache, 1138 Sätze für die englische Sprache und 1375 Sätze für die russische Sprache (siehe Tabelle 3). Die Links für die bei der Korpuserstellung benutzten Online-Quellen sind im Literaturverzeichnis enthalten.

Sprache	Anzahl der Sätze	Anzahl der Metaphern
Deutsch	1237	36
English	1138	41
Russisch	1375	31

Tabelle 3. Anzahl der analysierten Sätze im Verhältnis zu gefundenen Metaphern

5.2 Vergleich der metaphorischen Mappings

Die metaphorischen Mappings stellen die Beziehungen zwischen den Herkunfts- und Zieldomänen dar. Nicht alle Eigenschaften oder Erfahrungen aus einer Herkunftsdomäne werden in Metaphern abgebildet. So werden bei der Herkunftsdomäne „**Krieg**“ die Begriffe „Armee“, „Defensive“, „Kampffeld“ für die metaphorische Bilder verwendet, der Begriff „Kampfführer“ aber nicht. In nachfolgenden Tabellen (siehe Tabellen 4 – 8) werden pro Metaphern-Gruppe die metaphorischen Mappings vorgestellt, die auf der Basis der gefundenen metaphorischen Ausdrücke erstellt wurden.

Kriegsmetaphern	
Deutsche Sprache	
Zieldomäne	**Herkunftsdomäne**

virtuelle Attacke	Attacke in realer Welt
Cyber-Angreifer	Angreifer in realer Welt
Handlungen der Cyber-Angreifer	Offensive im Kampf
Handlungen der (potenziellen) Opfer von Cyber-Angreifer	Defensive im Kampf
durch eine Cyberattacke betroffene Partei	Opfer des Angriffs
sich für eine Cyberattacke vorbereitende Partei	Verteidigende im Kampf
Maßnahmen gegen einen Cyberangriff	Waffen
Kampffeld	Angriffsfläche
Englische Sprache	
Zieldomäne	**Herkunftsdomäne**
attack online	physical attack
the person carrying out cyber attack	assailant (in physical attack)
computers/persons being attacked	victims of (physical attack)
malware	weapon
protection measures against a cyber attack	arsenal, armoury
destructive effect of malware	physical hit
spreading of malware	advancing into area of the enemy
defending from cyber-attack	defending from physical attack
cyber-attack offense	physical attack
Russische Sprache	
Zieldomäne	**Herkunftsdomäne**
действия киберпреступников	физическое нападение („körperlicher Angriff“)
защита от киберпреступников	оборона при физическом нападении („Abwehr von Cyberkriminellen“)
политика безопасности	оружие („Waffe“)
техники, применяемые хакерами	арсенал оружия („Waffenarsenal“)
большое количество ботов	армия („Armee“)
поиск возможностей взломать сеть	разведка („Geheimdienstführung“)

Tabelle 4. Vergleich der metaphorischen Mappings für Kriegsmetaphern

Aus der angeführten Liste der metaphorischen Mappings in Tabelle 4 wird ersichtlich, dass es bestimmte Ähnlichkeiten zwischen allen drei Sprachen gibt, nämlich, dass sich in allen Metaphern die Elemente einer physischen aggressiven Auseinandersetzung wie „Attacke“, „Waffe“, „Defensive“ und „Offensive“ widerspiegeln. Dagegen ist es nur für die russische Sprache charakteristisch, auch „Armee“ und „Geheimdienst“ im metaphorischen Sinne zu gebrauchen. Es lässt sich eine deutliche Tendenz erkennen: Es gibt eine große Anzahl von metaphorischen Ausdrücken, die die Konfrontation zwischen den Cyberkriminellen und ihren Angriffszielen in Begriffen von einem bewaffneten Konflikt, und sogar einem Krieg fassen.

Erkrankungsmetaphern	
Deutsche Sprache	
Zieldomäne	**Herkunftsdomäne**
Beschädigung der IT-Strukturen	menschliche Infektion
sich replizierende Schadprogramme	menschliche Viren
mit Schadsoftware betroffene IT-Systeme	kranker Mensch
mit Schadsoftware betroffene IT-Systeme	mit Krankheiten verseuchter Ort
gut geschützt gegen Cyberangriffe	immun gegen Krankheiten
Maßnahmen gegen Cyberangriffe	Heilmittel gegen Krankheiten
Isolierung von potenziell schädlicher Software	Quarantäne für potenzielle Kranken
Englische Sprache	
Zieldomäne	**Herkunftsdomäne**
computer malware	human infection
computer/network	human being
disable network access to the IT-System with malware in it to prevent its spreading	isolate sick person to prevent spreading of the infection
strong security	strong immunity
level of protection against cyberattacks	physical health
handling a cybersecurity incident	treating a disease
getting rid of cyber threat	curing a disease
Russische Sprache	
Zieldomäne	**Herkunftsdomäne**

вредоносное ПО	вирус („Virus“)
несанкционированное сохранение и запуск вредоносного ПО	инфицирование („Infizierung“)
использующий ресурсы компьютера в своих целях	паразитный („parasitär“)
распространнение вредоносного ПО	эпидемия („Epidemie“)
устранение проблем в скомпрометированной системе безопасности	лечение („Behandlung“)

Tabelle 5. Vergleich der metaphorischen Mappings für Erkrankungsmetaphern

Eine große Zahl der Metaphern, die für Cybersicherheit relevant sind, stammt aus der Beobachtung, dass der Schaden, der durch Cyberattacken angerichtet wird, ähnlich den Konsequenzen einer menschlichen Krankheit ist (siehe Tabelle 5). Ähnlich wie ein Krankheitserreger, der für die Übertragung und Verbreitung einen Wirt braucht, kann eine Schadsoftware einen PC befallen („infizieren“), wenn sein „Immunsystem“ nicht ausreicht, und muss auch behandelt werden.

Das besondere Interesse stellen fehlende Mappings zwischen den Frames „Erkrankung“ und „Cybersicherheit“ dar. Wenn die betroffenen IT-Systemen frei von der schädlichen Software sind, spricht man in der Regel auf Deutsch nicht von „Heilung“, sondern von „Säuberung“ und gerettete IT-Systeme sind nicht „gesund“, sondern „sauber“ („eine saubere Datei“) (vgl. Kaspersky[1] 2022). Im Unterschied zum Englischen oder Deutschen wird im Russischen oft im Kontext von Beseitigung von Schadsoftware über „Heilung“ oder „Behandlung“ gesprochen: „вылечить зараженные сайты“ (die verseuchten Websites heilen) (vgl. Virus-Detect[1] 2022).

Für alle drei Sprachen gilt, dass die mit einer Erkrankung verbundene Begriffe wie „Symptom“, „Patient“ oder „Arzt“ in der Verbindung mit Cybersicherheit nicht in metaphorischen Mappings repräsentiert sind.

Innen/Außen-Metaphern	
Deutsche Sprache	
Zieldomäne	**Herkunftsdomäne**
IT-Systeme	geschlossener Raum
Bedrohung für die Cybersicherheit verhindern	eine Öffnung schließen, damit der geschlossene Raum wieder isoliert ist
Sicherheit zu verletzen	in einen geschlossenen Raum einzubrechen

Teil des Netzwerks, in dem eine Cyberattacke begonnen wurde Grenze zwischen dem eigenen Netzwerk und äußeren Netzwerk innerhalb eines Heimnetzwerks außerhalb eines Heimnetzwerks	der Ort, an dem mit Gewalt Zugang in den geschlossenen Raum erlangt wurde Grenze zwischen dem Innenraum und Außenraum innerhalb eines geschlossenen Raums außerhalb eines geschlossenen Raums
Englische Sprache	
Zieldomäne	**Herkunftsdomäne**
error in security/security hole get access to network through a security hole get access to network through a security hole **by force** securing the network no connection to a network being secure being unsecure	gap/opening in closed space enter a closed space through an opening enter a closed space through an opening **by force** closing of the space boundary of a closed space being inside of the closed space being outside of the closed space
Russische Sprache	
Zieldomäne	**Herkunftsdomäne**
информационная безопасность угрозы информационной безопасности плохо защищенная часть сети, представляющая угрозу для информационной безопасности граница между защищенным и не защищенным участком сети действия киберпреступников устранение потенциальных рисков для информационной безопасности	замкнутое пространство („begrenzter Raum“) отверстия в оболочке, ограничивающем замкнутое пространство („Löcher in der Hülle, die den begrenzten Raum umgibt“) входные ворота в замкнутое пространство („Eingangstor zum begrenzten Raum“) периметр („Perimeter“) нарушение границ замкнутого пространства („Grenzverletzung des begrenzten Raumes“) герметизация закрытого пространства („Dichtmachung des begrenzten Raumes“)

Tabelle 6. Vergleich der metaphorischen Mappings für Innen/Außen-Metaphern

Die Gruppe der metaphorischen Mappings zwischen der Cybersicherheit und einem virtuellen abgeschlossenen Raum ist in allen drei Sprachen Deutsch, Englisch, Russisch präsent (siehe Tabelle 6). Die Verletzung von dessen „Geschlossenheit", oder „Sicherheitslücken", ist eine Gefahr für die Cybersicherheit und diese Lücken müssen geschlossen werden, nur dann gilt dieser Raum als sicher. Wie bereits erwähnt, basieren die metaphorischen Ausdrücken auf menschliche Erfahrung. In diesem Zusammenhang kann das Image Schema CONTAINMENT als die mögliche Ursprungsquelle angeführt werden, das zu räumlichen Orientierungen ein unmittelbares Verhältnis hat und sich mit solchen Ideen befasst, wie sich befinden innerhalb und außerhalb einer Grenze und Bewegung in und außer eines begrenzten Raumes (vgl. Hedblom et al. 2018).

Jagdmetaphern	
Deutsche Sprache	
Zieldomäne	**Herkunftsdomäne**
suchen nach virtuellen Daten, von denen man profitieren kann	suchen nach einem wertvollen greifbaren Objekt
Die Fähigkeit der Cyberkriminellen, bei einem Cyberverbrechen unauffällig agieren	die Fähigkeit, sich bei einer Verfolgung unauffällig machen
Bei einem Cyberangriff die Gegenseite auszutricksen	Beute in die Falle locken
Techniken, die verwendet werden, um die Gegenseite beim Cyberverbrechen zu betrügen	Köder in einer Falle
Beweise von einem Cyberangriff	Spuren (Fuß-/Fingerabdrücke) von einem Menschen
Englische Sprache	
Zieldomäne	**Herkunftsdomäne**
cyber criminal	hunter
cybersecurity expert	hunter
commit cyber crime	to catch (somebody)
to look out for ways to violate somebody's security	to hunt
to look out for ways to prevent security violations	to hunt
victim of cyber criminals	hunter's prey
techniques, used by cyber criminals	hunter's trap

means, by which the victim of cyber criminals is attracted	hunter's bait
Russische Sprache	
Zieldomäne	**Herkunftsdomäne**
действия киберпреступников, нацеленные на поиск возможности скомпрометировать чужую информационную безопасность	охота („Jagd“)
свидетельства пребывания киберпреступников в сети	следы животного на охоте („Spuren von einer Beute auf der Jagd“)
уловка киберпреступников, которая заставит пользователя скомпрометировать свою информационную безопасности	ловушка на охоте („Falle“)
зараженный файл, который привлекает внимание пользователя	приманка в ловушке („Köder in einer Falle“)

Tabelle 7. Vergleich der metaphorischen Mappings für Jagdmetaphern

Die früher angeführten metaphorische Mappings für die Kriegs-, Erkrankungsmetapher und die Metapher, die sich auf den abgeschlossenen Raum beziehen, existieren in allen drei untersuchten Sprachen: Deutsch, Englisch, Russisch (siehe Tabelle 7). Es ist bemerkenswert, inwieweit die metaphorische Sprache in der Fachsprache der Cybersicherheit in allen drei Sprachen Gemeinsamkeiten aufweist. Die Gruppe der Jagdmetapher ist keine Ausnahme. In allen drei Sprachen wird die Herangehensweise von Cyberkriminellen mit einer Jagd assoziiert. Dieselben Jagdattribute wie „Köder“, „Falle“, „Spuren“ wurden in allen drei Sprachen in die metaphorischen Mappings aufgenommen.

Angelnmetaphern	
Russische Sprache	
Zieldomäne	**Herkunftsdomäne**
киберпреступник	рыбак („Fischer“)
уловки киберпреступников	рыболовная удочка, крючок („Angelleine“, Angelhaken“)
жертва киберпреступников	рыба („Fisch“)
попасться на уловки киберпреступников	клюнуть на наживку („den Köder verschlucken“)

не дать киберпреступникам себя обмануть	сорваться с крючка („vom Haken befreien“)

Tabelle 8. Vergleich der metaphorischen Mappings für Angelnmetaphern

Die letzte Gruppe der metaphorischen Mappings existiert dagegen nur in der russischen Sprache und war bei der Recherche im englischen und deutschen Korpus nicht zu entdecken. Aus den metaphorischen Mappings (siehe Tabelle 8) geht hervor, dass das Angeln bestimmte Merkmale mit der Jagd teilt: beide Aktivitäten setzen Fangen von einer Beute mittels bestimmter Werkzeuge voraus. In der russischen Sprache können dieselben Angelnmetaphern nicht nur für Cyberkriminalität verwendet werden, sondern für alle Arten von Betrug.

5.3 Sprachspezifische Detailanalyse für Metaphern-Gruppen

In den nachfolgenden Tabellen (siehe Tabellen 9 – 21) sind die Frames und ihre Definitionen aufgelistet, die während der Korpus-Recherche gefunden wurden, zusammen mit den zugehörigen Metaphern. Die Zuordnung zwischen den Metaphern und den Frames passierte auf Basis der Schlüsselwörter in Framedefintionen, den in der Framebeschreibung angeführten lexikalischen Units, Frameelementen, Rollen und Beziehungen zwischen den Frames. Jede Tabelle ist mit einem ausführlichen Kommentar versehen.

5.3.1 Deutsche Sprache

5.3.1.1 Kriegsmetaphern

Frame	***Angriff***
Framedefinition	Ein Angreifer greift ein Opfer (das normalerweise, aber nicht immer empfinden kann) physisch an und verursacht oder beabsichtigt den physischen Schaden des Opfers. Eine Waffe, die vom Angreifer verwendet wird, kann neben dem üblichen Ort, der Zeit, dem Zweck, der Erklärung, etc. auch erwähnt werden (vgl. FrameNet des Deutschen 2022).
Beispiele	Hackerangriff (auch Hacker-Angriff) (vgl. Rohde & Schwarz² 2022).

	Hackerattacke (auch Hacker-Attacke) (vgl. Rohde & Schwarz[2] 2022). Cyberangriff (auch Cyber-Angriff) (vgl. Thinking Objects[2] 2022) Cyberattacke (auch Cyber-Attacke) (vgl. Thinking Objects[1] 2022) Waffe gegen Angriffe (vgl. Proxysec[1] 2022). Gewappnet gegen Cyberangriffe (vgl. Proxysec[2] 2022). Angriffsfläche für Cyber-Kriminalität (vgl. Schneider Intercomp 2022).
Frame	***Abwehren***
Framedefinition	Ein Verteidiger wehrt erfolgreich den aggressiven Versuch einer Übernahme durch einen Feind ab (vgl. FrameNet des Deutschen 2022).
Beispiele	den Angriff abwehren (vgl. T-Systems 2022).
Frame	***Verteidigen***
Framedefinition	Ein Verteidiger reagiert auf den Angriff eines Angreifers auf ein Opfer, indem er ihm direkt und in der Regel gewaltsam entgegenwirkt (vgl. FrameNet des Deutschen 2022).
Beispiele	sich gegen Cyberattacken zu verteidigen (vgl. CBT Training & Consulting 2022).
Frame	***Feindliche Begegnung***
Framedefinition	Dieser Frame wird von Wörtern evoziert, die eine feindliche Begegnung zwischen gegensätzlichen Kräften (Seite_1 und Seite_2, die kollektiv als Seiten benannt werden können) über eine umstrittene Angelegenheit und/oder zur Erreichung eines bestimmten Zwecks beschreiben (vgl. FrameNet des Deutschen 2022).
Beispiele	Angreifer und Verteidiger (vgl. T-Systems 2022). Opfer von Hackerangriffen (vgl. Rohde & Schwarz[2] 2022).

Tabelle 9. Metaphern in der deutschen Sprache. Gruppe der Kriegsmetaphern

Im Rahmen der Gruppe der Kriegsmetaphern in Tabelle 9 wird die Tätigkeit von Cyberkriminellen und Gegenmaßnahmen ihrer Opfer in Begriffen von aggressiver Auseinandersetzung betrachtet. Im Mittelpunkt der aggressiven Auseinandersetzung steht der Akt der Gewalt, oder im Fall von Cybersicherheitsverletzung – der Hackerangriff, die Hackerattacke, der Cyberangriff, die Cyberattacke. Die Frameelemente aus der Definition des Frames „**Angriff**" nämlich „Angreifer", „Opfer", „Waffe", „Ort" können sehr genau auf Cybersicherheit projiziert werden. Wenn ein „Angriff" in der realen Welt dem „Cyber-Angriff" entspricht, so besteht dieselbe metaphorische Beziehung zwischen „Angreifer" und „Cyber-Angreifer".

Die mit dem Frame „Angriff" verwandten Frames „Abwehren" und „Verteidigen" produzieren ebenso eine Reihe an metaphorischen Ausdrücken, wie „den Angriff abwehren" und „sich gegen Cyberattacken zu verteidigen". „Den Angriff abwehren" enthält streng genommen keine Andeutungen auf die Zieldomäne Cybersicherheit und nur aus dem Kontext wird klar, worum es sich handelt (der bevorstehende Satz lautete „Unser Hauptaugenmerk liegt auf der Cyberangriff-Soforthilfe für Unternehmen") (vgl. Proxysec[1] 2022). Wie später zu sehen sein wird, ist es keine Ausnahme, dass in einem Ausdruck die Zieldomäne nicht direkt referenziert wird und es sich trotzdem um eine Metapher handelt, weil die Zieldomäne eindeutig aus dem Kontext erschlossen werden kann.

Ein weiteres Frameelement des Frames „Angriff", „Waffe" wurde in die metaphorische Sprache übernommen. Software-Produkte werden oft als (digitale) Waffe vermarktet (vgl. Proxysec[1] 2022). Ein bewaffneter Konflikt kann mit einem Krieg gleichgestellt werden. Das Konzept der herkömmlichen Waffen wird auf die virtuellen Waffen übertragen. Es kann an dieser Stelle angemerkt werden, dass Waffen bei Cybersicherheit nicht als Pistolen, Bomben oder Raketen bezeichnet werden, es wird immer nur der Überbegriff „Waffen" verwendet.

Der „Ort" im Frame „Angriff" wird bei Cybersicherheitsangriffen als „Angriffsfläche" bezeichnet. Laut Pohlmann (2022) bedeutet Angriffsfläche alle Schwachstellen im Netzwerk, IT-System, Anwendungen usw., die Angreifer für einen Angriff ausnutzen können. In diesem Begriff können Ähnlichkeiten mit einem Kampffeld gesehen werden: obwohl Angriffsfläche prinzipiell nur eine Zeile Code sein kann, wir sie trotzdem als „Fläche" bezeichnet, ähnlich wie ein Feld, ein Stück flacher Erde.

Der Frame „Verteidigen" enthält eine Erwähnung des Frameelements „Feind" und es kann eine Verbindung zum Frame „feindliche Begegnung" nachverfolgt werden. Wie in jedem Konflikt existieren im Cybersicherheits-Konflikt mindestens zwei Seiten: die eine, die angreift und die andere, die sich verteidigt. Das entspricht dem Frameelement „Seite 1" (Angreifer) und „Seite 2" (Opfer von Hackerangriffen, Verteidiger) (vgl. FrameNet des Deutschen 2022). Im Unterschied zu einem realen

Kampf, ist es nicht einfach die Gegenseite zu identifizieren; der Kampf wird in einem virtuellen Raum geführt, auf einer Seite fungiert entweder eine Person oder organisierte Banden, die lieber anonym bleiben, während die Vertreter*innen auf der anderen Seite jeder von privaten Personen bis hin zu ganzen Unternehmen, Einrichtungen oder Regierungen sein können.

Obwohl Cybersicherheits-Bedrohungen oft in Begriffen von Angriff oder Krieg thematisiert werden, ist dieses Phänomen nicht mit dem Cyber-Krieg (aus dem Englischen „Cyberwar", „Cyberwarfare") zu verwechseln. Bei einem Cyber-Krieg handelt es sich um eine Erweiterung des herkömmlichen bewaffneten Konflikts von der militärischen Ebene auf Cyberspace. Dazu gehören Cyber-Angriffe auf die Infrastruktur des Gegners (vgl. IT-Native 2022).

Der Frame „Krieg" fehlt zurzeit im FrameNet des Deutschen. Im Online-Wörterbuch Wiktionary wird „Krieg" als ein „bewaffneter Konflikt zwischen mindestens zwei Parteien wie Staaten" und „übertragen: Auseinandersetzungen und Streit zwischen Parteien/Partnern" bezeichnet (vgl. Wiktionary[1] 2022). Hier sind Ähnlichkeiten mit dem Frame „**Angriff**" offensichtlich – es gibt auch zwei Seiten und eine Auseinandersetzung. Der Frame „**Krieg**" wird aktiv für nicht-konventionalisierte Metaphern verwendet, wie „ist auf der Cyberfront schon passiert", „wir finden Ihre offenen Flanken!" usw. (vgl. IT-Native 2022, vgl. Tufo 2022). Diese Metaphern werden nur ab und zu in Fachtexten zum Thema Cybersicherheit von Cybersicherheits-Dienstleistungsfirmen verwendet, gehören aber zur selben Herkunftsdomäne „Krieg".

5.3.1.2 Erkrankungsmetaphern

Frame	***Erkrankung***
Framedefinition	Wörter in diesem Frame nennen Beschwerden oder Erkrankungen, an denen ein Patiens leidet, die behandelt werden, von denen er geheilt werden kann oder an denen er stirbt. Die Beschwerde oder Erkrankung kann auf verschiedene Weise beschrieben werden, einschließlich des von der Erkrankung betroffenen Teils oder Bereichs des Körpers (Körperteil) (z.B. Leberkrebs, Herz-Kreislauf-Erkrankungen), der Ursache der Erkrankung (z.B. bakterielle Meningitis, Viruspneumonie) […] (vgl. FrameNet des Deutschen 2022)
Beispiele	(Computer)Virus (vgl. Blue Consult 2022). Infektion mit Schadsoftware (vgl. Grüner[2] 2018). mit einer Schad-Software infizieren (vgl. Grüner[1] 2018).

	Infektionsquelle (vgl. Rohde & Schwarz[3] 2022). Viren infizieren Daten (vgl. Blue Consult 2022). das virenfreie (Programm) (vgl. Grüner[1] 2018). infizierte Systeme (vgl. Perseus 2022). verseuchte Websites (vgl. Grüner[1] 2018). immun gegen Cyberangriffe (vgl. YesDefend 2022). Allheilmittel gegen Cyberangriffe (vgl. Wallner 2022). Quarantäne für Angriffe (vgl. Rohde & Schwarz[1] 2022).

Tabelle 10. Metaphern in der deutschen Sprache. Gruppe der Erkrankungsmetaphern

In diese Gruppe der Metaphern in Tabelle 10 sind solche Metaphern aufgenommen, die aus dem Frame „Erkrankung" ihren Ursprung nehmen. Das bekannteste Beispiel ist natürlich der „Computervirus". Im Großen und Ganzen kann eine Beziehung zwischen „menschlichen Infektion" und der „Beschädigung der IT-Strukturen" nachverfolgt werden. Während „Infektion" ein Überbegriff ist, der mehrere Cybersicherheitsbedrohungen miteinschließt, existieren auch Unterarten von „Infektionen", wie z.B. Viren. Die Benennung „Virus" kommt auch in der Beschreibung des Frames „**Erkrankungen**" vor („Viruspneumonie").

Die „Krankheit", die Netzwerke und PCs dank Bemühungen von Cyberkriminellen befällt, hat keinen einzigen Namen wie die menschlichen Krankheiten „Grippe" oder „Windpocken" und wird oft als Überbegriff „Infektion" bezeichnet. Im Begriff „Infektionsquelle" wird die Zieldomäne „Cybersicherheit" nicht direkt referenziert und ist nur durch den Kontext „schadhafte Links" feststellbar (der komplette Satz lautete „E-Mails mit schadhaften Links sind die primäre Infektionsquelle") (vgl. Rohde & Schwarz[1] 2022). In dem Fall, in dem ein Substantiv durch ein Pronomen ersetzt wird, waren für die Analyse noch zusätzliche Schritte notwendig, z.B. wenn im Text „dieses ist virenfrei" steht, muss der ganze Satz analysiert werden („Starten Sie kein Programm aus dem Internet oder von Freunden, von dem Sie nicht sicher sind, dass dieses vollkommen virenfrei ist") (vgl. Grüner[1] 2018). Es ergibt sich, dass sich „dieses" auf „Programm" bezieht, und wenn „dieses" mit „Programm" ersetzt wird, kann in „virenfreies Programm" das Construction Pattern S-adj_mod_T-noun leicht erkannt werden. Dafür waren aber zusätzliche Schritte notwendig (Ersetzen des Pronomens „dieses" mit dem früher genannten Substantiv und Verwandlung des Ausdrucks in seine Grundform).

Das Frameelement „der von der Erkrankung betroffene Teil oder Bereich des Körpers (Körperteil)" kann im Frame „**Erkrankungen**" als „infiziert" bezeichnet werden, wenn es um den

ganzen Menschen geht. Wenn aber ein Platz als ungünstig für die Gesundheit eingestuft wird, kann er als „verseucht“ bezeichnet werden. Dieselben Adjektive werden auch in Fachtexten zum Thema „Cybersicherheit“ verwendet („infizierte Systeme“ und „verseuchte Websites).

Als ein Frameelement des Frames „Erkrankungen“ muss „Gesundheitszustand“ erwähnt werden. Erstens kann das Angriffsziel der Cyberkriminellen entweder „immun“ oder „nicht immun“ gegen Cyberattacken sein. „Immun gegen Cyberangriffe“ kann als ein Fall einer doppelten Metapher gesehen werden; auf der einen Seite stammt „immun“ aus der Herkunftsdomäne „Erkrankung“, während „Angriff“ aus der Herkunftsdomäne „Krieg“ stammt, und das Construction Pattern wäre S^1-adj_prep_T-noun_S^2-noun. Trotzdem lassen sich die beiden Metaphern gut kombinieren.

Eine Krankheit kann mit Heilmitteln behandelt werden („Allheilmittel gegen Cyberangriffe“). Es können auch Vorbeugungsmaßnahmen eingesetzt werden, wie Quarantäne. Für „Quarantäne für Angriffe“ gilt auch dieselbe Kombination der Herkunfts- und Zieldomäne, wie bei „Immun gegen Cyberangriffe“: „Erkrankung“ und „Krieg“, dabei ist die Zieldomäne „Cybersicherheit“ nicht präsent und nur aus dem Kontext erschließbar („Der virtuelle Browser schließt die Sicherheitslücke „Internet“, indem er eine digitale Quarantäne für Angriffe ermöglicht“) (vgl. Rohde & Schwarz[1] 2022).

5.3.1.3 Innen/Außen-Metaphern

Frame	***Begrenzter Bereich***
Framedefinition	Außen, Oberfläche, Grenze und Innen stechen relativ zu einem (Hinter-)Grund hervor. Dieser (Hinter-)Grund kann entweder nur die Grenze besetzen (in diesem Fall bildet das Innen einen negativen Raum), oder der (Hinter-)Grund kann das Innen füllen (vg. FrameNet des Deutschen 2022).
Beispiele	Sicherheitslücke (vgl. Arceo Cybersecurity 2022). in Computersysteme einzudringen (vgl. Arceo Cybersecurity 2022). in ein Netzwerk einzubrechen (vgl. Cybertrap[1] 2022). Einfallstor von Cyberattacken (vgl. Proxysec[1] 2022). die Schadsoftware sucht einen Einstiegspunkt (vgl. Rohde & Schwarz[1] 2022). Sicherheitsperimeter (vgl. Vindler 2022). Sicherheitsbarriere (vgl. Wallner 2022).

	Angriffe von innen wie von außen (vgl. Thinking Objects[3] 2022). Absaugen von Daten nach außen (vgl. Rohde & Schwarz[4] 2022).

Tabelle 11. Metaphern in der deutschen Sprache. Gruppe der Innen/Außen-Metaphern

Die Gruppe der Innen/Außen-Metaphern in Tabelle 11 basiert auf dem Frame „Begrenzter Bereich", oder dem Image Schema CONTAINMENT (vg. FrameNet des Deutschen 2022, vgl. Hedblom et al. 2018). Die IT-Systeme gleichen einem abgeschlossenen Innenraum, die Bedrohungen für die Sicherheit befinden sich hingegen draußen. Wenn Sicherheit nicht mehr gewährleistet wird, ist dieser begrenzte Bereich nicht mehr isoliert, und man kann über eine „Sicherheitslücke" sprechen.

Ein unbefugter Zugang in einen geschlossenen Raum kann mit einem Eindringen oder Einbruch verglichen werden („in Computersysteme eindringen", „in ein Netzwerk einbrechen").

Es ist bemerkenswert, wie viele Ausdrücke, die für die Verletzung der Sicherheit relevant sind, das Präfix „ein" enthalten („eindringen", „einbrechen", „Einfallstor", „Einstiegspunkt"). Das Präfix „ein" unterstreicht die Abgrenzung zwischen der sich im geschlossenen Raum befindenden Entität und der Entität, die sich außerhalb der Grenzen von diesem Raum befindet.

„Grenze" und „Innen/Außen" sind beides Frameelemente des Frames „Begrenzter_Bereich" (vgl. FrameNet des Deutschen 2022). Diese Idee spiegelt sich in einer Reihe von aufeinanderfolgenden lexikalischen Metaphern wider („Sicherheitsperimeter", „Sicherheitsbarriere", „Angriffe von innen wie von außen", „Absaugen von Daten nach außen"). Die innen-außen Orientierung, und entsprechende Präpositionen und Adverbien wie „in", „ein", „aus", „außerhalb" usw., wurden von Lakoff und Johnson (2021) als ein Zeichen von so genannten „CONTAINER" Image Schema identifiziert (vgl. Lakoff & Johnson 2021: 39). Ein CONTAINER oder ein geschlossener Raum wird mit dem Heimnetzwerk der Benutzer assoziiert. Sich außerhalb dieses Netzwerkes zu befinden entspricht sich außerhalb eines CONTAINERS/Raumes zu befinden.

5.3.1.4 Jagdmetaphern

Frame	***Suchen***
Framedefinition	Ein Kognizierendes_Agens versucht, eine Gesuchte_Entität zu finden, indem er einen Bereich absucht. Der Erfolg oder Misserfolg dieser Handlung (das Ergebnis) kann dabei angezeigt werden (vg. FrameNet des Deutschen 2022).
Beispiele	Daten auf dem Computer ausspähen (vgl. Rohde & Schwarz[3] 2022).

Frame	***Jagen***
Framedefinition	Ein Jäger versucht, Nahrung zu beschaffen, indem er ein lebendiges Wesen überlistet oder verfolgt. Der Jäger hofft, dass der Versuch im Fangen und Töten des Lebewesens, das für den menschlichen Verzehr bestimmt ist, resultiert (vg. FrameNet des Deutschen 2022).
Beispiele	Tarnung von Malware (vgl. Sysware 2022). Phishing-Emails locken in die Falle (vgl. G-Data 2022). Angreifer in die Falle locken (vgl. G-Data 2022). Cyberkriminelle ködern (ihr Opfer) (vgl. IT-Native 2022). Angreifer folgen Köder (vgl. Cybertrap[2] 2022). Spuren von Schadcode (vgl. Kaspersky[1] 2022).

Tabelle 12. Metaphern in der deutschen Sprache. Gruppe der Jagdmetaphern

In die vierte Gruppe der sogenannten „Jagdmetaphern“ in Tabelle 12 wurden metaphorische Ausdrücke aufgenommen, die auf die Bemühungen von Cyberkriminellen, ihre Opfer auszutricksen, Bezug nehmen. Es wurden die Metaphern kombiniert, die Bezug auf die Frames „**Suchen**“ und „**Jagen**“ nehmen. Bei einem Cyber-Betrug geht es darum, so lang wie möglich unbemerkt zu bleiben, während die Daten von Benutzer*innen abgesucht werden, mit dem Zweck festzustellen, ob man davon irgendwie profitieren kann (wie im Beispiel „Daten ausspähen“). Genauso wie wenn jemand an etwas/an jemandem Interesse hat und nicht will, dass das Objekt der Verfolgung das erfährt, kann ein/eine Cyberkriminelle/r die virtuelle Daten nach etwas Wertvollem durchsuchen, ohne dass das jemand merkt.

Um einen Schadcode unauffällig erscheinen zu lassen, z.B., wenn man ein Werbebanner auf einer Webseite harmlos aussehen lassen will, das aber einen schädlichen Code enthält, kann die Erkennung von Malware mit „Tarnung“ verhindert werden. Die Tarnung, als die Fähigkeit, sich bei einer Verfolgung unauffällig zu machen, wird in eine Analogie zu der Fähigkeit der Cyberkriminellen, bei einem Cyberverbrechen unauffällig zu agieren, gesetzt. Es kann postuliert werden, dass ursprünglich „Tarnung“ zum Frame „**Jagen**“ gehört, weil es bei einer Jagd eine große Rolle spielt, unbemerkt zu bleiben. Tatsächlich ist bei der Korpus-Recherche aufgefallen, wie oft im Kontext von Cyberkriminalität mit einer Jagd verbundene Ausdrücke vorkommen, wie z.B. „in die Falle locken“, dabei können entweder die Cyberkriminellen ihre Opfer in die Falle locken, oder umgekehrt die Cybersicherheit-Expert*innen können die Cyberkriminellen in die Falle locken und

einen Angriff abwehren (vgl. Cybertrap[1] 2022). Die Anwender*innen können eine Strategie für die Abwehr von Cyberattacken einsetzen, indem im Netzwerk spezielle „Köder" platziert wurden, die in eine Simulation einer echten Produktivumgebung führen und die Angreifer*innen falsche Informationen zurückbekommen, die aber echt aussehen (vgl. Cybertrap[1] 2022). Der Ursprung dieser Metapher ist die Ähnlichkeit zwischen dem Locken der Beute in die Falle und der Aktivität der Cyberkriminellen und ihrer Opfer, indem sie versuchen einander auszutricksen.

Obwohl die Cyberkriminelle versuchen, unbemerkt zu bleiben, gelingt es nicht immer. In diesem Fall redet man von „Spuren von Schadcode", ähnlich wie Spuren auf der Erde bei einer Jagd. Die Firma „Perseus" verwendet ein mit „Spuren" verwandten Begriff – „Spurensicherung", um die Aktivität von Cyberexpert*innen nach einer Cyberattacke zu beschreiben, die Netzwerkprotokolle, Log-Dateien und Datenträger untersuchen, wie einen virtuellen Tatort (vgl. Perseus 2022).

5.3.2 Englische Sprache

5.3.2.1 Kriegsmetaphern

Frame	***Attack***
Framedefinition	An Assailant physically attacks a Victim (which is usually but not always sentient), causing or intending to cause the Victim physical damage. A Weapon used by the Assailant may also be mentioned […] (vgl. FrameNet des Englischen 2022).
Beispiele	cyber attack (vgl. ATG 2019). attacker (vgl. Andrew 2020). victim to cybersecurity attack (vgl. Shpirer 2018).
Frame	***Hostile encounter***
Framedefinition	This frame consists of words that describe a hostile encounter between opposing forces (Side_1 and Side_2, collectively conceptualizable as Sides) over a disputed Issue and/or in order to reach a specific Purpose (vgl. FrameNet des Englischen 2022).
Beispiele	weapon of cybercriminals (vgl. Foresite[1] 2022). cybersecurity arsenal (vgl. Aurora IT 2022). cybersecurity armoury (vgl. Wallis 2021). ransomware strikes (vgl. Careful Security 2022). ransomware hits (vgl. Cyberunit[2] 2022).

	Wannacry infiltrated (vgl. Wallis 2021).
Frame	***Defending***
Framedefinition	A Defender responds to an Assailant's attack on a Victim by directly, and usually violently, countering it. […](vgl. FrameNet des Englischen 2022).
Beispiele	defense against (cyber) criminals (vgl. Ricoh USA[2] 2022). cybersecurity defense (vgl. Wizlynxgroup 2022). cybersecurity offense (vgl. Wizlynxgroup 2022).

Tabelle 13. Metaphern in der englischen Sprache. Gruppe der Kriegsmetaphern

Die Gruppe der Kriegsmetaphern in Tabelle 13 für die englische Sprache umfasst dieselbe Frames wie für die deutsche Sprache, nämlich „**attack**“, „**hostile encounter**“ und „**defending**“. Es war zu erwarten, dass in der Cybersicherheits-Fachsprache im Englischen Ausdrücke vorkommen, die für den Kampf relevant sind, da sich in allen Ländern und Sprachräumen Cyberkriminelle und die zivilisierte Gesellschaft ständig in einer Konfrontation befinden. Im Unterschied zur deutschen Sprache, wo es zwei Synonyme gibt: „Cyberattacke“ und „Cyberangriff“, gibt es im Englischen nur eine Variante, und zwar „cyber attack“. Der Ausdruck „cyber assailment“ kommt im englischsprachigen Korpus nicht vor. Es unterscheidet sich die linguistische Realisierung dieser Metapher im Deutschen und Englischen: ein 1:1 Äquivalent für „under attack“ („unter Attacke“) existiert im Deutschen nicht, es wird öfter als „ein Objekt wurde angegriffen“ formuliert.

Zu den Frameelementen des Frames „**attack**“ gehören laut dem FrameNet „Assailant“, „Victim“ und „Weapon“ (vgl. FrameNet des Englischen 2022). Die Frameelemente „Assailant“ und „Victim“ können auch im Fall einer Cyber-Attacke identifiziert werden. Der Angreifer wird oft „attacker“ genannt („the attacker erased the database's tables“) (vgl. Andrew 2020), und Opfer als „victims to cybersecurity attack“ (vgl. Foresite[1] 2022). Es wäre einfacher für die Metaphernidentifizierung, wenn in einem metaphorischen Ausdruck sowohl die Herkunftsdomäne als auch die Zieldomäne dargestellt werden, aber die Adjektiv-Substantiv-Verbindung „cyber attacker“ kommt in Fachtexten zur Cybersicherheit nicht vor und wird einfach mit „attacker“ ersetzt und soll deswegen in die Sammlung von Metaphern aufgenommen werden. „Attacker“ und „victim“ können auch als Seite_1 und Seite_2 im übergeordneten Frame „**hostile encounter**“ gesehen werden.

„Weapon“, als ein Frameelement des Frames „attack“ wird im FrameNet wie folgt definiert: „An entity used by the Assailant to cause damage to the Victim” (vgl. FrameNet des Englischen 2022). Einzelne Angriffsmethoden werden als „weapon“ im Kontext der Cybersicherheit bezeichnet,

während die Gesamtheit von Waffen als „arsenal“ oder ein Synonym, „armoury“ referenziert wird. Der Ausdruck „weapon“ wird ähnlich als eine materielle Waffe, die man in der Hand halten kann und mit der man jemanden anderen attackieren kann, auf die Schadprogramme („malware“), in diesem Fall „ransomware“ (Software für Erpressung) übertragen. An dieser Stelle ist allerdings zu beachten, dass „weapon“ in der Regel nur im Zusammenhang mit Cyberkriminellen verwendet wird, von denen die Aggression ausgeht, während die angegriffenen Menschen oder Unternehmen nicht freiwillig an diesem Kampf teilnehmen und streng genommen keine Waffen besitzen, sondern Schutzmaßnahmen ergreifen müssen, und diese Schutzmaßnahmen vor einem Cyberangriff werden nicht als „weapon“ bezeichnet, sondern als „cybersecurity arsenal“.

Die Frames im FrameNet des Englischen sind ausführlicher elaboriert als im FrameNet des Deutschen, d.h. es gibt für jeden Frame nicht nur eine Definition und die dazugehörige Frameelemente, sondern auch Frame-Beziehungen zu anderen Frames und eine Liste der lexikalischen Ausdrücke, durch die ein Frame realisiert wird (vgl. FrameNet des Englischen 2022). Zu solchen lexikalischen Ausdrücken für den Frame „**attack**“ gehören z.B. „assail“, „ambush“, „charge“, „fire“, „infiltrate“, „hit“, „offensive“, „strike“ usw. Einige davon sind in Fachtexten zum Thema Cybersicherheit leicht zu finden („ransomware strikes“, „ransomware hits“, „WannaCry infiltrated“) von einer organisierten Attacke, die 2017 durch eine Hackergruppe durchgeführt wurde, wo die Benutzerdaten verschlüsselt wurden und eine Zahlung in Bitcoins für die Entschlüsselung aufgefordert wurde (vgl. Whittaker 2019). Was „infiltrate“ betrifft, kann vermutet werden, dass dieser Ausdruck aus der militärischen Fachsprache stammt, wo „infiltrieren“ sich in das Territorium des Gegners unentdeckt fortzubewegen bedeutet (vgl. Bowyer 2007). Aus dieser Sicht entspricht das heimliche Eindringen in das Territorium des Gegners einer Verbreitung der Schadsoftware.

„Defend/defense/defensive“ und „offense/offensive“ sind eng mit dem Frame „**attack**“ verbunden. Die Wörter „offensive“ sind in der Liste von dazugehörigen lexikalischen Units zum Frame „attack“ aufgelistet, während Frame „defending“ laut FrameNet eine direkte Beziehung zum Frame „attack“ hat, deswegen sind die Metaphern „defense against (cyber) criminals“, „cybersecurity defense“, „cybersecurity offense“ auch in die Liste der Kriegsmetaphern aufgenommen (vgl. FrameNet des Englischen 2022).

Der Frame „**war**“ ist im FrameNet des Englischen nicht repräsentiert, ebenso wenig wie im FrameNet des Deutschen, obwohl es auf dem MetaNet Metaphor Wiki Portal konzeptuelle Metaphern gibt, die direkt diesen Frame referenzieren, z.B. ARGUMENT IS WAR, CANCER TREATMENT IS WAR usw. (vgl. FrameNet Wiki 2022).

5.3.2.2 Erkrankungsmetaphern

Frame	***Medical condition/disease***
Framedefinition	Words in this frame name medical conditions or diseases that a patient suffers from, is being treated for, may be cured of, or die of […](vgl. FrameNet des Englischen 2022).
Beispiele	computer virus (vgl. ActionFraud[1] 2022). infect computer (vgl. ActionFraud[1] 2022). block infections (vgl. ActionFraud[1] 2022). isolate infected systems (vgl. Careful Security 2022). computer is immune (vgl. Courant 2014). immune to cybersecurity treats (vgl. Lieberman Technologies 2022). cybersecurity health (vgl. Defendify 2022). security hygiene (vgl. GE Digital 2022). virus infestations (vgl. Gibson 2003).
Frame	***cure***
Framedefinition	This frame deals with a Healer treating and curing an Affliction (the injuries, disease, or pain) of the Patient, sometimes also mentioning the use of a particular Treatment or Medication. This frame differs from Medical_intervention in that this frame deals only with cases in which the Patient is cured of the Affliction, not just treated for the Affliction (vgl. FrameNet des Englischen 2022).
Beispiele	cure a virus (vgl. Rawat 2022).
Frame	***recovery***
Framedefinition	These words describe the recovery or healing of a Patient from an Affliction without reference to the influence of any Treatment or Healer (see the Cure frame) (vgl. FrameNet des Englischen 2022).
Beispiele	recover from a cyber attack (vgl. ATG 2019).

Tabelle 14. Metaphern in der englischen Sprache. Gruppe der Erkrankungsmetaphern

Die nächste Gruppe der „Erkrankungsmetaphern“ in Tabelle 14 wird von Metaphern geformt, die den Frames „**Medical_condition**“, „**cure**“ und „**recovery**“ gehören. Das Netzwerk oder der PC wird als ein Lebewesen gesehen, das durch Schadsoftware wie durch einen menschlichen Virus infiziert werden kann. Der Begriff „computer virus“ wurde im Kontext von Cybersicherheit zuerst in der englischen Sprache durch den Cybersicherheit-Experten Fred Cohen in 1980-er Jahren geprägt, der außerdem viel zur Entwicklung der modernen Cybersicherheitsschutzmethoden beigetragen hat (vgl. Middleton 2017). Zum Frame „**Medical_conditions**“ gehören auch die Frameelemente „patient“, „symptom“, „Body_part“, „cause“, „degree“, „duration“ und viele medizinische lexikalische Units, darunter Krankheitsnamen wie „influenza“, „cancer“, „infection“ usw. (vgl. FrameNet des Englischen 2022). Der Frame „**disease**“ ist nur auf der Webseite von FrameNet Wiki dargestellt, und zwar ohne einer ausgearbeiteten Definition, aber mit einer großen Liste relevanter lexikalischer Units wie „infection“, „virus“, „immune“, „health_state“ (vgl. FrameNet Wiki 2022). Die Nutzung von „virus“ sowie „infection“ und vom gleichen Wortstamm abgeleiteten Wörtern ist in solchen Metaphern wie „computer virus“, „infect computer“, „block infections“ ersichtlich. Für „Block infections“, da keine Zieldomäne Cybersicherheit oder IT-Systeme direkt referenziert wird, soll der komplette Kontext angeführt werden: „Make sure your computer has a firewall and reputable anti-virus software. Without these, your computer has no defence to block infections.“ (vgl. ActionFraud[1] 2022). In diesem Ausdruck werden sogar zwei Herkunftsdomäne referenziert: „defence“ aus der Gruppe der Kriegsmetaphern und „infections“, aus der Gruppe der Erkrankungsmetaphern

Genau so wie ein kranker Mensch infiziert ist, und eine Gefährdung für die Mitmenschen darstellt, können auch infizierte Systeme gefährlich für die noch nicht betroffenen Systeme sein und müssen „isoliert“ werden („Isolate or disable the infected systems and triage for recovery“) (vgl. Careful Security 2022). Wie aus dem Lexikon der Infektionskrankheiten folgt, gehört die Isolierung der Kranken zu den wichtigsten Strategien des Ausbruchsmanagements (vgl. Darai et al. 2012) und muss auch als Metapher betrachtet werden. Im diesem Satz ist das Wort „triage“ besonders interessant. In der Medizin wird dieser Begriff verwendet, um die „medizinische Einstufung und Festlegung der Behandlungsbedürftigkeit“ zu bezeichnen (vgl. Peters 2010: 415). Es kann vermutet werden, dass hier gemeint wurde, dass die Aufgabe der Cybersicherheits-Expert*innen darin besteht, zu entscheiden, welches betroffene IT-System die höchste Priorität hat und schnellstmöglich funktionsfähig sein muss. Das ist aber keine konventionalisierte Metapher, gehört aber derselben Herkunftsdomäne – „Infektion/Krankheit“ an.

Wenn ein Computer als ein Lebewesen gesehen wird, das infiziert und krank werden kann, kann durch Analogieschlüsse vermutet werden, dass, wenn ein IT-System keinen starken Cybersicherheit-Schutz hat, dass es dann ein schwaches Immunsystem hat. Während der Ausdruck

„Immunität“ in Cybersicherheitsfachtexten nicht vorkommt, kommt das Adjektiv „immun“ vor („no computer is immune“) (vgl. Courant 2014).

Die Wörter „health“ und „hygiene“ können auch im Zusammenhang mit Cybersicherheit verwendet werden („cybersecurity health“ und „security hygiene“). Die lexikalische Unit „hygiene“ ist noch in keinem Frame im FrameNet aufgenommen, hat aber eine unmittelbare Beziehung zur Gesundheit, als Gesamtheit von Gewohnheiten und Regeln nach denen man Gesundheit fördern kann.

Die Definition des Frames „**Medical_condition**“ setzt voraus, dass eine Krankheit behandelt werden kann („treated for“). Deswegen wurde der Frame „**cure**“ auch in diesem Zusammenhang für die Analyse herangezogen. Die Terminologie „treat“ und „cure“ wurde auch in die Fachsprache der Cybersicherheit aufgenommen („treat computer virus infestations“) (vgl. Gibson 2003), „cure a virus-infected file“) (vgl. Rawat 2022). Das Wort „recover“ kann nicht immer eindeutig zur Herkunftsdomäne „Erkrankung“ zugeordnet werden, weil es nicht nur „Genesung“, sondern auch „Wiederherstellung“ bedeuten kann. An dieser Stelle soll nur angemerkt werden, dass „recover/recovery“ im Zusammenhang mit Cyber-Attacken verwendet wird, wie „triage for recovery“, oder den Folgen einer Cyber-Attacke, wie Datenverlust („recover data“). Angesichts der Tatsache, dass die Genesung von einer Infektion („recover from flu“) und der Wiederherstellung der Cybersicherheit in den gleichen Begriffen thematisiert wird, kann der metaphorische Ausdruck „recover from a cyber attack“ als Metapher eingestuft werden.

5.3.2.3 Innen/Außen-Metaphern

Frame	***Bounded Entity***
Framedefinition	This is an abstract frame for bounded areas […] (vgl. FrameNet des Englischen 2022).
Beispiele	gaps in security (vgl. Netstar 2022) security holes (vgl. Intruder 2022). close the security gap (vgl. Datacast Technologies 2022). entry for cybercriminals (vgl. Cyberunit[3] 2022). break into network (vgl. ActionFraud[2] 2022). close systems to cyber threats (vgl. Cyberunit[1] 2022).
Frame	***opennes***
Framedefinition	A Useful_location is accessible to some (possibly generic) Theme despite a potential Barrier, or is not accessible because of the Barrier (vgl. FrameNet des Englischen 2022).
Beispiele	gateway to your network opens (vgl. SecurityScorecard 2022).

Frame	***boundary***
Framedefinition	This frame contains words that describe a Boundary between two Entities […] (vgl. FrameNet des Englischen 2022).
Beispiele	network perimeter (vgl. RedScan² 2022). boundaries of a (network) perimeter (vgl. RedScan² 2022).
Frame	***Part_inner_outer***
Framedefinition	This frame concerns Parts of objects that are defined relative to the center or edge of the object […] (vgl. FrameNet des Englischen 2022).
Beispiele	inside and outside cybersecurity threats (vgl. OnsiteLogic 2022). data stays inside (vgl. Foresite² 2022). infiltrators stay outside (vgl. Foresite² 2022).

Tabelle 15. Metaphern in der englischen Sprache. Gruppe der Innen/Außen-Metaphern

Die vier Frames „**bounded entity**“, „**openness**“, „**boundary**“ und „**part_inner_outer**“ hängen eng zusammen. Der Frame „boundary“ benutzt unmittelbar den Frame „bounded entity“, also die beiden Frames sind in FrameNet mit der Beziehung „is used by“ verbunden (vgl. FrameNet des Englischen 2022). Die Frames „openness“ und „boundary“ enthalten beide synonyme lexikalische Units wie „boundary“ und „perimeter“. Der Frame „**part_inner_outer**“ ist durch einen Zwischenframe „part whole“ mit dem Frame „bounded entity“ verbunden.

In der dritten Gruppe der lexikalischen Metaphern in Tabellen 15 wird die Idee vorgestellt, dass der Cyberraum, oder Netzwerke von untereinander verbundenen Maschinen, ein begrenzter geschlossener Innenraum ist. Wenn dieses Konzept des „begrenzten Raumes“ als Herkunftsdomäne betrachtet wird, und Cybersicherheit als Zieldomäne, können die Ausdrücke „gaps in security“ und „security holes“ als metaphorisch eingestuft werden, indem eine Öffnung im geschlossenen Raum („gap/opening in closed space“) mit dieselben Assoziationen verknüpft ist, wie ein Fehler in der Sicherheit, der einen unbefugten Zugang in ein Netzwerk erlaubt („error in security/security hole“).

Der Frame „**boundary**“ spielt eine große Rolle im Bereich Cybersicherheit im Ganzen und insbesondere bei der Kommunikation zwischen den Netzwerken. Wie Levis und Burke (2019) anmerken, „all networks have a boundary“, und „if a network wants to communicate with devices, nodes or networks outside of that boundary, they require the functionality of a gateway“, dabei „gateways serve as an entry and exit point for a network“ (vgl. Levis & Burke 2019). Die Schlüsselwörter „gateway“ und „entry“ sind in Cybersicherheit-Metaphern zu finden („the gateway

to your network opens for cybercriminals to exfiltrate data“ (vgl. SecurityScorecard 2022), „it only takes one point of entry for a cybercriminal to gain access into your systems“ (vgl. Cyberunit[1] 2022). Ein Cyberkrimineller kann durch diesen Eingang („entry“) den Zugang zum Netzwerk bekommen, ähnlich wie ein Mensch durch eine Tür einen geschlossenen Raum betreten kann. Bei einem gewaltsamen Zugang spricht man von „breaking into computers and computer networks“ (vgl. ActionFraud[2] 2022). Es wird in dieser Metapher hervorgehoben, dass der Eintritt nicht freiwillig, nicht erlaubt war und dass Schaden angerichtet wurde.

Das Beispiel „gateway to your network opens“ impliziert, dass der Zugangspunkt zum Netzwerk geöffnet werden kann; das Gegenteil ist aber auch wahr, d.h. die Lücke kann „geschlossen“ werden („close your systems off to those potential malicious cyber threats“) (vgl. Cyberunit[1] 2022). Ein Netzwerk abzusichern, bedeutet das Netzwerk abzuschließen („close“).

Wie ein geschlossener Raum („bounded entity“) eine Grenze („boundary“) haben kann, kann auch ein Netzwerk eine Abgrenzung vom Außenbereich haben, d.h. es existiert kein Anschluss an ein anderes Netzwerk und das Netzwerk gilt als gut abgesichert und deswegen abgeschlossen („closed“). Für diese Abgrenzung konnten im Korpus solche metaphorischen Ausdrücke wie „network perimeter“ or „boundaries of perimeter“ gefunden werden.

In diese Gruppe der Innen/Außen-Metaphern, die die Netzwerksicherheit als einen geschlossenen Raum betrachten, wurden auch lexikalische Metaphern aufgenommen, die das Befinden innerhalb dieses Raums im Gegensatz zum Außen gegenüberstellen („inside and outside cybersecurity threats“) (vgl. OnsiteLogic 2022), „data stays inside and […] infiltrators stay outside“ (vgl. Foresite[2] 2022).

5.3.2.4 Jagdmetaphern

Frame	***hunting***
Framedefinition	A Hunter tries to gain Food by way of outsmarting or tracking a living. The Hunter hopes the attempt will result in the catching and killing of the living entity […] (vgl. FrameNet des Englischen 2022).
Beispiele	endpoint protection can catch viruses, spyware, worms (vgl. Ricoh USA[1] 2022). hunt for threats (vgl. RedScan[1] 2022). hackers hunt (vgl. Champion 2019). hacker’s bait (vgl. ActionFraud[3] 2022).

	hacker's prey (vgl. Cyberunit[4] 2016). hacker's trap (vgl. Stasmayer 2022).

Tabelle 16. Metaphern in der englischen Sprache. Gruppe der Jagdmetaphern

Die Jagdmetaphern sind in der Fachsprache der Cybersicherheit am wenigsten stark repräsentiert. Trotzdem existieren bestimmte Übereinstimmungen zwischen dem Jagdvokabular und der Fachsprache der Cybersicherheit, die in Tabelle 16 angeführt werden, z.B. das Wort „catch", wie aus der Definition des Frames „**hunting**" „the hunter hopes the attempt will result in the catching" (vgl. FrameNet des Englischen 2022) und einer Beschreibung der typischen Cyberattacken auf Remote-Arbeiten hervorgeht: „There are, of course, other cyberattacks including viruses, spyware, worms and others. Strong endpoint protection can catch most of these" (vgl. Ricoh USA[1] 2022). Anstatt „hunt" kann „on the hunt" verwendet werden, wie „hackers are on the hunt" (vgl. Lifars 2021). Aus diesen lexikalischen Metaphern („hunt for threats") geht hervor, dass nicht nur die Aktivität der Cyberkriminellen als eine Jagd betrachtet wird, sondern auch insofern die Gegenmaßnahmen von Benutzer*innen auch in Begriffen von Jagd bezeichnet werden. Hier ist ein Unterschied zu einer realen Jagd offensichtlich – in der Regel können die Jäger und die Beute nicht Plätze tauschen. Der Frame „**Hunting**" hat im FrameNet nur drei lexikalischen Units: „hunt", „fish", „seal" und ist in diesem Sinne nicht detailliert ausgearbeitet (vgl. FrameNet des Englischen 2022). Im Glossar von Maine Department of Inland Fischeries & Wildlife können folgende Jagdbezogene Termini gefunden werden, die auch in Bezug auf die Cybersicherheit aktiv verwendet werden: „trap", „bait", „prey" (vgl. Maine Department of Inland Fisheries & Wildlife 2022), die in solchen Metaphern abgebildet sind wie „hacker's bait", „hacker's prey", „hacker's trap". Die mit Jagd verbundenen Ausdrücke werden nicht nur im Zusammenhang mit Hacker*innen, sondern mit allen Cyberkriminellen verwendet z.B.: „Cyber criminals use fake messages as bait to lure you into clicking on the links" (vgl. ActionFraud[3] 2022).

5.3.3 Russische Sprache

5.3.3.1 Kriegsmetaphern

Frame	***Атака (die Attacke)***
Framedefinition (Übersetzung)	Надапающий физически атакует Жертву (которая не всегда наделена разумом), причняя или намереваясь причинить Жертве физический вред. Также может быть упомянуто

	Оружие, используемое Нападающим […] (vgl. FrameNet des Englischen 2022, Übersetzung aus dem Englischen).
Beispiele	хакерская аттака (Hackerattacke) (vgl. SafenSoft[2] 2022). кибернападение (Cyberangriff) (vgl. T1 Cloud 2018). оборона (корпоративной) сети (Defensive des (Firmen)netzwerkes) (vgl. Pentest[2] 2022). взять на вооружение политику безопасности (eine starke Sicherheitspolitik zur Bewaffnung nehmen) (vgl. Ilyin 2015). арсенал хакеров (Hackerarsenal) (vgl. Pentest[3] 2020). армии ботов (Bot-Armeen) (vgl. Kaspersky[4] 2018). первый шаг хакера – разведка (Der erste Schritt des Hackers ist Geheimdienstführung) (vgl. Pentest[4] 2020). сетевая разведка (digitale Geheimdienstführung) (vgl. Gardatech 2022).

Tabelle 17. Metaphern in der englischen Sprache. Gruppe der Kriegsmetaphern

Die Gruppe der Kriegsmetaphern in Tabelle 17 umfasst die Ausdrücke, die in der Fachsprache verwendet werden, um die Bedrohungen für die Cybersicherheit in Begriffen von aggressiven kriegerischen Handlungen zu beschreiben. Angesichts des fehlenden FrameNets auf Russisch besteht keine Möglichkeit, die Framebeschreibungen, die ursprünglich für die russische Sprache entwickelt wurden, für die Analyse heranzuziehen und als Alternative wird die Übersetzung von Frames aus dem englischen FrameNet ins Russische verwendet. Mithilfe dieser Frames können im Russischen folgende metaphorische Ausdrücke identifiziert werden: „хакерская аттака“ (Hackerattacke), „кибернападение“ (Cyberangriff), „оборона“ („Defensive“) und „вооружение“ („Bewaffnung“). Sie sind als fester Bestandteil eines bewaffneten Konflikts in den Metaphern repräsentiert. Die anderen mit der kriegerischen Thematik verbundenen Termini wie z.B. „арсенал“ („Arsenal“) oder „армия“ („Armee“) haben auch ihren Weg in die Fachsprache der Cybersicherheit im Russischen gefunden. Die verschiedenen Techniken, die von Hackern eingesetzt werden, werden mit einem Waffenarsenal verglichen, während eine große Menge von Bots, die unmittelbar Hackerattacken durchführen (z.B. Maschinen, die mit einem Virus infiziert wurden), mit einer Armee assoziiert sind.

Dass es sich im Fall von Cybersicherheitsverletzungen nicht nur um einen Kampf handelt, sondern um einen regelrechten Krieg, lässt sich noch an folgenden Metaphern demonstrieren: „Geheimdienstführung“ und „digitale Geheimdienstführung“. Die Ausspähung nach Möglichkeiten,

in ein fremdes Netzwerk einzudringen, korreliert mit der Aktivität des Geheimdiensts, genauso wie dies während eines Krieges der Fall sein würde.

5.3.3.2 Erkrankungsmetaphern

Frame	***Болезнь (Erkrankung)***
Framedefinition (Übersetzung)	Слова в этом фрейме относятся к болезни, от которой страдает пациент/пациентка, от которой он/она получает лечение, может вылечиться или умереть (vgl. FrameNet des Englischen 2022, Übersetzung aus dem Englischen).
Beispiele	компьютерный вирус (Computervirus) (vgl. Kaspersky² 2022). инфицирование компьютеров (Infizierung von Computern) (vgl. Arinteg² 2022). паразитный трафик (der parasitäre Datenverkehr) (vgl. Arinteg¹ 2022). эпидемия трояна-шифровальщика (die Epidemie des Verschlüsselungs-Trojaner) (vgl. Perekalin 2017). вылечить зараженные сайты (die verseuchten Websites heilen) (vgl. Virus-Detect¹ 2022). „лечение“ системы безопасности (Behandlung für Sicherheitssysteme) (vgl. Pentest¹ 2020)

Tabelle 18. Metaphern in der englischen Sprache. Gruppe der Erkrankungsmetaphern

In diese Gruppe der Metaphern in Tabelle 18 wurden die metaphorischen Ausdrücke aufgenommen, die aus dem Bereich Medizin und Heilkunde stammen und die für die Bezeichnung von Schadsoftware, ihrer Wirkung und Beseitigung genutzt werden. Um genauer einzugrenzen, wird die durch ein bösartiges Programm verursachte Gefahr mit einer Krankheit verglichen. Ein bestimmter Typ von selbst replizierenden Programmen wird „компьютерный вирус“ („Computervirus“) genannt, mit dem ein Computer „инфицирован“ („infiziert“) werden kann. Der Ausdruck „компьютерный вирус“ („Computervirus“) wird im Russischen mit einem Adjektiv und einem Substantiv gebildet, im Unterschied zum Englischen „computer virus“, der aus zwei aufeinanderfolgenden Substantiven besteht. Der Virus bezieht sich auf Schadsoftware, während die Infizierung die geheime Abspeicherung einer böswilligen Datei und ihre Ausführung bezeichnet.

Im Unterschied zum Deutschen oder Englischen, wo aus der Reihe der Krankheiten ausschließlich virale Krankheiten und Viren als Prototyp für das unerwünschte Eindringen und Replizieren dienen, werden im Russischen auch einige Ausdrücke aus dem Vokabular von Parasiteninfektionen entlehnt, wie z.B. das Adjektiv „паразитный“ („parasitär“). Die Konstruktion „паразитный трафик“ („der parasitäre Datenverkehr“) beschreibt die das Netzwerk überlastende unerwünschte Anfragen, die von durch Malware betroffenen Computern ausgehen (vgl. Arinteg[1] 2022). Die Programme, die die Computerressourcen ohne Erlaubnis für ihre Zwecke verbrauchen und Schaden anrichten, werden mit Parasiten verglichen.

Wenn eine große Anzahl von Menschen von einer Krankheit befallen wird, spricht man von einer Epidemie. Dieser Begriff wurde erfolgreich in die Fachsprache der Cybersicherheit aufgenommen: „эпидемия трояна-шифровальщика“ („die Epidemie des Verschlüsselungs-Trojaner“) (vgl. Perekalin 2017).

Zu den Beispielen der Metaphern mit dem Stamm „леч“ („cure“) zählen „вы**леч**ить сайты“ („Webseiten heilen“) und „**леч**ение” системы безопасности“ („Behandlung für Sicherheitssysteme“). Im zweiten Beispiel wird diese Metapher im Originaltext in Anführungszeichen angeführt, was darauf hindeuten könnte, dass diese Metapher noch nicht komplett konventionalisiert ist.

5.3.3.3 Innen/Außen-Metaphern

Frame	***Замкнутое пространство (abgeschlossener Raum)***
Framedefinition (Übersetzung)	Это абстрактный фрейм для замкнутых пространств (vgl. FrameNet des Englischen 2022, Übersetzung aus dem Englischen).
Beispiele	дыры в безопасности (Sicherheitslücke) (vgl. Ilyin 2015). брешь в безопасности (Sicherheitslücke) (vgl. Cloud Clan 2022). ворота для киберугроз (Eingangstor für Cyberbedrohungen) (vgl. Kaspersky[5] 2022). периметр безопасности (Sicherheitsperimeter) (vgl. SafenSoft[3] 2022). хакеры по ту сторону интернета (Hacker jenseits des Internets) (vgl. Pentest[5] 2022).

	хакерское вторжения (Hackereinbruch) (vgl. SafenSoft[1] 2010). вторжение хакеров (Hackereinbruch) (vgl. Virus-Detect[3] 2022). закрыть уязвимость (die Sicherheitsschwachstelle schließen) (vgl. Virus-Detect[1] 2022).

Tabelle 19. Metaphern in der englischen Sprache. Gruppe der Innen/Außen-Metaphern

In die Gruppe der Innen/Außen-Metaphern in Tabelle 19 wurden Metaphern ausgewählt, die die Cybersicherheit als einen geschlossenen Raum konzeptualisieren, in dem eine Öffnung einer Sicherheitsverletzung entspricht. Wenn es Risse oder offene Lücken im Äußeren dieses geschlossenen Raumes gibt: „дыры в безопасности“ (wörtliche Übersetzung: „Löcher in Sicherheit“) oder als Synonym „брешь в безопасности“ (wörtliche Übersetzung: „Lücken in Sicherheit“), dann ist die Sicherheit nicht mehr gegeben, bevor die Lücken geschlossen sind („закрыть уязвимость“, „die Sicherheitsschwachstelle schließen“). Es wird ein metaphorisches Mapping erzeugt, indem ein geschlossener Raum, der mit einer dichten Umgrenzung umgeben wird, mit IT-Sicherheit assoziiert wird. Lücken in dieser Umgrenzung entsprechen Sicherheitsbedrohungen. Das Schließen einer Lücke und das Dichtmachen von einem virtuellen Raum wird im übertragenen Sinne für die Beseitigung von potenziellen Risiken für die Sicherheit genutzt.

Eine potenzielle Sicherheitslücke, mittels derer tatsächlich ein Cyberangriff passieren könnte, wird auch als „ворота для киберугроз“ („Eingangstor“ für Cyberangriffe) bezeichnet. Dieser metaphorische Ausdruck deutet auf die ähnliche Idee hin, dass der geschlossene Raum, der die Sicherheit repräsentiert, von Sicherheitsbedrohungen durch eine Öffnung, in diesem Fall ein virtuelles Eingangstor, betreten werden kann. In diesem Sinne wird das Eingangstor mit einem schlecht vor einem unbefugten Zugriff geschützten Teil des Netzwerks assoziiert.

Ein wichtiges Attribut des geschlossenen Raumes ist die Umgrenzung zwischen diesem Raum und der restlichen Umgebung. Aus dem Korpus kann ermittelt werden, dass diese Grenze als „периметр безопасности“ („Sicherheitsperimeter“) referenziert wird.

Ein weiterer Ausdruck, in dem sich eine ähnliche Idee wie im Beispiel „Sicherheitsperimeter“ widerspiegelt wird, ist, dass es eine Abgrenzung von einem sicheren Raum und der restlichen Umgebung in Form von einer spürbaren Grenze gibt, und dass die Bedrohungen für die Sicherheit, (z.B. Hackerattacken) unter anderem von dort ausgehen: „хакеры по ту сторону интернета“ („Hacker jenseits des Internets“). Die IT-Sicherheit und geschlossene Räume weisen bestimmte

Ähnlichkeiten auf: Es gibt eine Grenze, in der Lücken existieren können, und dass man sich draußen oder drinnen befinden kann.

Zwischen einem Eindringen oder Einbruch in geschützte Informationssysteme können Parallele mit einem unbefugten Überqueren einer Grenze gezogen werden. So werden Sicherheitsverletzungen als „хакерские вторжения“/„вторжения хакеров“ („Hackereinbrüche“) bezeichnet.

5.3.3.4 Jagdmetaphern

Frame	***Jagen***
Framedefinition (Übersetzung)	Охотник пытается добыть Пропитание, перехитрив или выследив живое существо. Охотник надеется, что ему удастся поймать и убить живое существо. (vgl. FrameNet des Englischen 2022, Übersetzung aus dem Englischen).
Beispiele	хакеры охотятся (Hacker jagen) (vgl. Kaspersky³ 2022). следы злоумышленников (Spuren der Cyberkriminellen) (vgl. Smart-Soft 2020). запутать следы (Spuren verwischen) (vgl. Smart-Soft 2020). ловушки киберпреступников (Fallen von Cyberkriminellen) (vgl. Bezmalyi 2014). документы-приманки (Köderdateien) (vgl. Kaspersky ICS Cert 2022). код прячется (der Code versteckt sich) (vgl. Virus-Detect² 2022).

Tabelle 20. Metaphern in der englischen Sprache. Gruppe der Jagdmetaphern

Die vierte Gruppe der lexikalischen Metaphern in Tabelle 20 umfasst Redewendungen, die die Aktivität von Cyberkriminellen als eine Art Jagd betrachten. Es wird von der Annahme ausgegangen, dass solche lexikalischen Units wie „jagen“, „Falle“, „Köder“, „Spuren (verwischen)“, „sich verstecken“ aus verwandten semantischen Feldern stammen und zum selben Frame „Jagd“ gehören.

Das erste Beispiel „хакеры охотятся“ („Hacker jagen“) zeigt, wie die Suche von Hacker*innen nach einer passenden Möglichkeit die Cybersicherheit von anderen zu ihrem Vorteil zu kompromittieren, mit einer Jagd verglichen werden kann.

Die Firma Smart-Soft bietet Dienstleistungen im Bereich Cyber-Forensics an, indem sie Ermittlungen gegen Cyberkriminelle einleitet. Dabei wird erwähnt, dass die Cyberkriminelle oft ihre Spuren verwischen: „затем смотрят ПО, стремясь найти следы злоумышленников“ („Danach wird die Software untersucht, um die Spuren der Cyberkriminellen zu finden“) und „Вычислить происхождение атаки […] можно по косвенным признакам, которые можно подделать, чтобы запутать следы“ („Man kann die Herkunft des Angriffs mittels indirekter Beweise ermitteln, die gefälscht werden können, um die Spuren zu verwischen“) (vgl. Smart-Soft 2020). Es können klare Parallelen zwischen der Ausspähung von einer Beute (eines Tieres) durch einen Jäger mittels seiner Spuren und der Aufklärung von einer Straftat im Cyberbereich durch Spuren, z.B. Änderungen im Netzwerkeinstellungen oder Logeinträgen, die durch Cyberkriminellen hinterlassen wurden, gesehen werden.

Unabdingbare Attribute einer traditionellen Jagd wie Fallenaufstellung und Nutzung von Ködern sind auch in der Fachsprache der Cybersicherheit repräsentiert: „ловушки киберпреступников“ („Fallen von Cyberkriminellen“), „документы-приманки“ („Köderdateien“). Was „документы-приманки“ („Köderdatei“) betrifft, gehört in diesem Kompositum das Wort „Datei“ streng genommen nicht unbedingt der Zieldomäne „Cybersicherheit“ an, sondern eher einem Oberbegriff „IT-Systeme“ und nur aus dem vollen Kontext, dass es sich um Cyberkriminelle und Trojaner handelt, wird ersichtlich, dass die sogenannten „Köderdateien“ für Cyberverbrechen verwendet werden (z.B. eine PDF-Datei mit einem interessanten Inhalt, die man nichtsahnend öffnet, und ein Virus im Hintergrund geladen wird) (vgl. Kaspersky ICS Cert 2022). Das Material, das die Neugierde bei Opfern weckt, würde in diesem Fall einem Köder in der Falle entsprechen.

Die letzte Metapher, die im Zusammenhang mit der Jagd angeführt werden konnte, kann nur indirekt mit der Jagd assoziiert werden, dennoch umfasst der Prozess des Jagens das Verfolgen und das Verstecken, genauso wie Cyberkriminelle ihre „Fallen“ verstecken: „код прячется“ („der Code versteckt sich“). Diese Metapher ist für die Fachsprache der Cybersicherheit besonders relevant, weil Cyberkriminelle für ihre Zwecke die Kunst des Versteckens und der Tarnung meistern müssen. Benutzer*innen merken, dass etwas nicht stimmt, wenn es schon zu spät ist, und der Schaden schon angerichtet wurde, z.B. dass eine Software für den Diebstahl von Kryptowährung auf dem PC läuft, eine Variante von Cyberattacken, vor der Smart Soft (2020) gewarnt hat (vgl. Smart-Soft 2020).

5.3.3.5 Angelnmetaphern

Frame	***Angeln***

Framedefinition (Übersetzung)	Акт ловли рыбы (vgl. Wiktionary[2] 2022).
Beispiele	крючок злоумышленников (Angelhaken der Cyberkriminellen) (vgl. Dedenok 2021). попасться на удочку киберпреступников (mit einer Angelleine der Cyberkriminellen gefangen werden) (vgl. Hugh 2021). клюнуть на наживку (Köder verschlucken) (vgl. Mash 2019). сорваться с крючка (vom Haken befreien) (vgl. Mash 2019).

Tabelle 21. Metaphern in der englischen Sprache. Gruppe der Angelnmetaphern

Die letzte Gruppe der Metaphern in Tabelle 21 hat zwar direkte Beziehungen zur Gruppe der Jagdmetaphern, wurde aber separat behandelt, weil diese Art von Metaphern nur für die russische Sprache relevant ist. Es geht um die Metaphern aus der Herkunftsdomäne „Angeln".

„Крючок злоумышленников" („Angelhaken der Cyberkriminellen") und „попасться на удочку киберпреступников" („mit einer Angelleine der Cyberkriminellen gefangen werden") vermitteln das Bild, dass Cyberkriminelle als Fischer agieren, und die Tricks, die eingesetzt werden, mit Angelzubehör verglichen werden können, und dass die Opfer der Cyberkriminellen als nichtsahnende Fische betrachtet werden können. Die weiteren Metaphern „клюнуть на наживку" („Köder verschlucken"), „сорваться с крючка" („vom Haken befreien") können nur durch den Kontext identifiziert werden, weil das Wort „Cyberkriminelle" das Subjekt in diesem Satz ist: „Интернет-мошенникам приходится следить, чтобы клюнувшие на наживку не срывались с крючка" („Cyberkriminelle müssen aufpassen, dass diejenige, die den Köder geschluckt haben, sich nicht vom Haken befreien" (vgl. Mash 2019). Im Kontext von Cybersicherheit kann „клюнуть на наживку" („Köder schlucken") bedeuten, dass das Opfer auf einen Trick der Cyberkriminellen reingefallen ist und „сорваться с крючка" („vom Haken befreien"), dass das Opfer es doch gelungen ist, sich vor dem Betrug zu schützen.

5.4 Construction Patterns

Im Anschluss an die Vorstellung von mehreren Metaphern-Gruppen im Deutschen, Englischen und Russischen gilt es die für die gefundenen Metaphern vorhandenen Construction-Patterns zu bestimmen. Sie sind in Tabelle 22 jeweils pro Sprache aufgelistet. In der Tabelle wird ersichtlich,

dass eine viel größere Anzahl von unterschiedlichen Construction Patterns existieren könnte, als nur die Zwölf von Dodge et al. (2015) vorgeschlagenen. Ein Pattern kann aus mehr als nur 3 Bestandteilen bestehen und auch andere Wortarten enthalten als nur Substantiv, Verb, Adjektiv, z.B. Adverb. In einem metaphorischen Ausdruck können lexikalische Unis aus mehreren Herkunftsdomänen enthalten sein, wie z.B. S^1-adj_prep_T-noun_S^2-noun „immun gegen Cyberangriffe“, wo der Teil „immun“ zur Herkunftsdomäne „Infektion“ gehört und der Teil „Angriff“ zur Herkunftsdomäne „Krieg“. Zu den Construction Patterns, die am häufigsten im Korpus vorkommen, zählen T-noun_mod_S-noun mit 17 Beispielen, darunter 8 in der deutschen Sprache, 8 in der englischen Sprache und 1 in der russischen Sprache, und S-noun_Genitive_T-noun mit 10 Beispielen in der russischen Sprache. Aus den 40 identifizieren Patterns kommen mehr als 10 nur einmal vor. In Beispielen mit nur einer Herkunftsdomäne ist die Zieldomäne trotzdem aus dem Kontext ersichtlich.

Construction Patterns	**Deutsch**	**Englisch**	**Russisch**
T-noun_mod_S-noun	Hackerangriff Hackerattacke Cyberangriff Cyberattacke Computervirus Sicherheitslücke Sicherheitsperimeter Sicherheitsbarriere	cybersecurity arsenal cybersecurity armoury cybersecurity defence cybersecurity offense computer virus cybersecurity health security hygiene network perimeter	кибернападение
	8	8	1
S-noun_S-verb	den Angriff abwehren		
	1		
prep_T-noun _mod_S-noun_S-verb	sich gegen Cyberattacken zu verteidigen		
	1		

S-noun_conj_S-noun	Angreifer und Verteidiger		
	1		
S-noun		attacker	разведка
		1	1
S-noun_prep_T-noun	Infektion mit Schadsoftware Infektionsquelle für Malware Allheilmittel gegen Cyberangriffe Tarnung von Malware Spuren von Schadcode	defense against (cyber)criminals entry for cybercriminals	дыры в безопасности брешь в безопасности ворота для киберугроз
	5	2	3
S-noun_prep_T-noun_mod_S-noun	Opfer von Hackerangriffen Angriffsfläche für Cyber-Kriminalität	victim to cybersecurity attack boundaries of network perimeter	
	2	2	
S-noun_prep_S-noun	Waffe gegen Angriffe		
	1		
S-verb_prep_T-noun_mod_S-noun	gewappnet gegen Cyberangriffe		
	1		
S-verb_prep_T-noun		break into network	
		1	
S-noun_S-verb-conj_T-dobj	Viren infizieren Daten		
	1		
S-adj_mod_T-noun	virenfreies Programm	cyber attack	

	infizierte Systeme verseuchte Websites		
	3	1	
S¹-adj_mod_conj_T-noun_ S²-noun		inside and outside cybersecurity threats	
		1	
S¹-adj_prep_T-noun_S²-noun	immun gegen Cyberangriffe		
	1		
S¹-noun_prep_ S²-noun	Quarantäne für Angriffe Angriffe von innen Angriffe von außen		
	3		
prep_T-noun_S-verb	in Computersysteme einzudringen in ein Netzwerk einzubrechen mit einer Schadsoftware infizieren		
	3		
S-noun_prep_T-noun_ mod_S-noun	Einfallstor von Cyberattacken Einstiegspunkt für Cyberattacken		
	2		
S-noun_prep_T-noun_prep_S-noun	Absaugen von Daten nach Außen		
	1		
T-subj_S-verb	Cyberkriminelle ködern	ransomware strikes ransomware hits Wannacry infiltrated	хакеры охотятся код прячется

		hackers hunt	
	1	4	2
T-subj_S-verb-S-adverb		data stays inside infiltrators stay outside	
		2	
T-subj_S-verb_prep_S_noun	Phishing-Emails locken in die Falle		
	1		
T-subj_S-verb(_S-dobj)	Angreifer folgen (Köder)		
	1		
S^1-obj_prep_S^2-noun_ S^2-verb	Angreifer in die Falle locken		
	1		
S-noun_of_T-noun		weapon of cybercriminals	
		1	
S-verb_T-dobj		infect network cure a file catch spyware hunt threats	взять на вооружение политику безопасности закрыть уязвимость
		4	2
T-dobj _S-verb	Daten ausspähen		
	1		
S-verb_prep_S-dobj			клюнуть на наживку сорваться с крючка
			2

S-verb_T-noun_mod_S-noun_S-noun		treat computer virus infestations	
		1	
S-verb_S-dobj		block infections	запутать следы
		1	1
S-verb_ S-adj_T-noun		isolate infected systems	вылечить зараженные сайты
		1	1
T-noun_cop_S-adj		computer is immune	
		1	
S^1-adj_prep_T-noun-mod_T-noun_ S^2-noun		immune to cybersecurity threats recover from a cyber attack	
		2	
S-verb_ T-adj_mod_S-noun		close the security gap	
		1	
S-noun_prep_T-noun_S-verb		gateway to the network opens	
		1	
T-noun_poss_S-noun		hacker's bait hacker's prey hacker's trap	
		3	
T-adj_mod_S-noun			хакерская аттака сетевая разведка паразитный трафик хакерское вторжения
			4

S-noun_ Genitive_T-noun			оборона сети арсенал хакеров армии ботов эпидемия трояна-шифровальщика лечение системы безопасности периметр безопасности вторжение хакеров следы злоумышленников ловушки киберпреступников крючок злоумышленников
			10
T-noun_prep_det_S-noun- Genitive_T-noun			хакеры по ту сторону интернета
			1
T-noun_S-noun			документы-приманки
			1
S-verb_prep_S-dobj_ Genitive _T-noun			попасться на удочку киберпреступников
			1

Tabelle 22. Construction Patterns für Metaphernbildung

5.5 Ergebnisse der Umfrage

Als Ergebnis der durchgeführten Umfrage, in der die IT-Expert*innen die Formulierungen für konzeptuelle Metaphern abstimmen sollten, wurden aus der Liste der vorgeschlagenen 2-3 Kandidaten für jede konzeptuelle Metapher folgende endgültige Varianten mit Mehrheit der Stimmen gewählt.

- Deutsche Sprache
    - CYBERKRIMINALITÄT IST EIN KRIEG
    - BEDROHUNG DER CYBERSICHERHEIT IST EINE INFEKTION
    - SICHER IST INNEN, UNSICHER IST AUßEN
    - CYBERKRIMINALITÄT IST EINE JAGD
- Englische Sprache
    - CYBERCRIME IS WAR
    - THREAT TO CYBERSECURITY IS AN INFECTION
    - SECURITY IS A CLOSED SPACE
    - CYBERCRIME IS A HUNT
- Russische Sprache
    - БОРЬБА ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ – ВЕДЕНИЕ ВОЙНЫ („KAMPF UM CYBERSICHERHEIT IST KRIEGFÜHRUNG“)
    - НАРУШЕНИЕ КИБЕРБЕЗОПАСНОСТИ – БОЛЕЗНЬ („SICHERHEITSVERLETZUNG IST EINE KRANKHEIT“)
    - ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ЗАКРЫТОЕ ПРОСТРАНСТВО („CYBERSICHERHEIT IST EIN GESCHLOSSENER RAUM“)
    - КИБЕРПРЕСТУПНОСТЬ – ОХОТА („CYBERKRIMINALITÄT IST JAGD“)
    - КИБЕРПРЕСТУПНОСТЬ – РЫБАЛКА („CYBERKRIMINALITÄT IST ANGELN“)

An der Abstimmung über die Formulierung der konzeptuellen Metaphern haben 20-25 IT-Expert*innen aus der Firma Deutsche Telekom mit Deutsch, Englisch und Russisch-Sprachkenntnissen teilgenommen (die genaue Anzahl ist nicht bekannt, weil die Umfrage anonym durchgeführt wurde und dieselbe Person zwei oder drei Mal teilnehmen könnte, einmal für jede Sprache, der/die er/sie beherrscht). Die Proband*innen sind Kolleg*innen der Autorin der vorliegenden Masterarbeit. Die absolute Mehrheit der deutsch- und russischsprachigen Kolleg*innen

sind Erstsprachler*innen, für die englische Sprache wurde die Beherrschung der Sprache von der Mehrheit der Teilnehmer*innen auf der fortgeschrittenen Stufe eingestuft, damit gilt die für die Teilnahme an der Umfrage erforderliche sprachliche Kompetenz der Teilnehmer*innen als gegeben.

Die Umfrage bestand aus 3 Teilen, jeweils pro Sprache. Im Rahmen eines Pilot-Versuchs wurde die Umfrage an 3 Personen ausgesendet und auf der Basis des eingetroffenen Feedbacks überarbeitet. Von einem IT-Experten wurde der Vorschlag gemacht, eine kurze Information, was konzeptuelle Metaphern sind, in der Einführung zu ergänzen. Die Fragen selbst waren absichtlich so formuliert, um den Begriff „konzeptuelle Metaphern" auszulassen, um diejenigen, die keine Erfahrung mit konzeptuellen Metaphern haben, nicht zu verwirren. Dies erwies sich als nützlich, denn 100% der Befragten haben die Frage: „Haben Sie Erfahrung mit konzeptuellen Metaphern? (wenn ja, welche)" mit „Nein" beantwortet. Es wurde auch darauf aufmerksam gemacht, dass in der Frage „Welche der folgenden Aussagen repräsentiert diese Beispiele am besten" das Wort „Aussagen" in Großbuchstaben geschrieben wurde, um zu unterstreichen, dass die konzeptuellen Metaphern immer in Großbuchstaben geschrieben werden.

Die anderen Proband*innen der Pilotstudie empfanden die Aufgabe als intuitiv klar und hatten keine weiteren Anmerkungen. Nach dieser Überarbeitung wurde die Umfrage wieder für alle freigeschaltet.

Angesichts der Tatsache, dass unter den Teilnehmer*innen ein großer Teil nur zwei Sprachen beherrscht: entweder Deutsch als Erstsprache und Englisch als Zweitsprache oder Russisch als Erstsprache und Englisch als Zweitsprache (also es mehr potenzielle Teilnehmer*innen gibt, die die Umfrage für die englische Sprache beantworten können) wurde die Umfrage mit der deutschen und russischen Sprache gestartet, um die Anzahl der Befragten für alle drei Sprachen gleich zu halten. Pro Sprache wurden jeweils 10 Teilnehmer*innen befragt.

Zuerst wurde der Teil mit konzeptuellen Metaphern für die deutsche Sprache unter den deutschsprachigen Kolleg*innen, die alle Erstsprachler*innen sind, verteilt. Nach 10 abgesendeten Antworten wurde die Umfrage geschlossen. Danach wurde die Umfrage für die russisch-sprachigen Kolleg*innen-Muttersprachler*innen ausgesendet.

Abschließend wurden ebenso 10 Antworten für die Umfrage für englische konzeptuelle Metaphern gesammelt.

Was die Befragten betrifft, gehörten die meisten zu der Altersgruppe 31-45 (50% der Befragten), etwa 25% gehören der Kategorie 46-65 an und weitere 25% der Kategorie zwischen 18-30. Es gab nur eine*n Teilnehmer*in, der*die als Bildungsniveau „Schule" angegeben hat, alle anderen haben einen Universitätsabschluss. Nur wenige Teilnehmer*innen haben angegeben, einige Erfahrung im Bereich Cybersicherheit zu haben (4 Proband*innen). Nur 2 der Befragten waren

Frauen, was darauf zurückzuführen ist, dass die Mehrheit des Personals in technischen Unternehmen Männer ausmachen.

Für die Sprachen Deutsch und Englisch wurden Formulierungen für 4 konzeptuelle Metaphern angeboten, für die Sprache Russisch – 5 konzeptuelle Metaphern. Obwohl in der Umfrage eine Option angeboten wurde, eine eigene Formulierung für die konzeptuelle Metapher vorzuschlagen, wurde diese Möglichkeit von niemandem wahrgenommen. Es kann beobachtet werden, dass die konzeptuellen Metaphern, die die Mehrheit der Stimmen bekommen haben, in drei Sprachen übereinstimmen, außer der Metapher über die Cybersicherheit als abgeschlossener Raum. Für die deutsche Sprache bestand die Wahl aus drei Varianten: (1) SICHERHEIT IST EIN GESCHLOSSENER RAUM, (2) SICHER IST INNEN, UNSICHER IST AUßEN und (3) FREMDES NETZWERK IST EIN GESCHLOSSENER RAUM. Die zweite Variante bekam die meisten Stimmen, während für die englische Sprache die Variante SECURITY IS A CLOSED SPACE mehr Stimmen erhielt, 6 von 10, (und nicht SECURITY IS INSIDE, INSECURITY IS OUTSIDE, die nur 4 Stimmen erhielt). Die Stimmen-Differenz ist aber minimal. Das Feedback zur Umfrage war insgesamt positiv, einige Kolleg*innen haben sogar telefonisch Kontakt aufgenommen, um mehr über die Forschung und die Endergebnisse der Umfrage zu erfahren.

Was den Aufbau der Umfrage betrifft, wurde für jede konzeptuelle Metapher 3 bis 5 Beispiele angeführt. Für die deutsche Sprache, wurde die Gruppe der „Kriegsmetaphern“ mit 3 Beispielen (eins davon enthält 2 Metaphern, „Angriff auf die Cybersicherheit abwehren“ enthält „Angriff“ und „abwehren“), die Gruppe der „Erkrankungsmetaphern“ mit 5 Beispielen, die Gruppe der „Metaphern über den geschlossenen Raum“ mit 4 Beispielen, und die Gruppe der „Jagdmetapern“ mit 5 Beispielen. Für die englische Sprache wurde für jede Gruppe 4 Beispiele angeführt. Für die Russische Sprache wurde für die Gruppe der „Angelnmetaphern“ 3 Beispiele angeführt, für die vier anderen Gruppen jeweils 4 Beispiele. Wie viele Stimmen jede einzelne konzeptuelle Metapher erhielt, lässt sich in folgender Tabelle ablesen:

deutsche Sprache	
Kriegsmetaphern	
Formulierung für konzeptuelle Metapher	Anzahl der Stimmen
WAHRUNG DER CYBERSICHERHEIT IST EIN KRIEG	3
CYBERKRIMINALITÄT IST EIN KRIEG	7
SICHERHEITSVERLETZUNG IST EINE FEINDLICHE BEGEGNUNG	0
Erkrankungsmetaphern	

SICHERHEITSVERLETZUNG IST EINE KRANKHEIT	4
CYBERKRIMINALITÄT IST EINE INFEKTION	1
BEDROHUNG DER CYBERSICHERHEIT IST EINE INFEKTION	5
CYBERKRIMINALITÄT IST EINE VERSEUCHUNG	0
Metaphern über den geschlossenen Raum	
SICHERHEIT IST EIN GESCHLOSSENER RAUM	2
FREMDES NETZWERK IST EIN GESCHLOSSENER RAUM	2
SICHER IST INNEN, UNSICHER IST AUßEN	6
Jagdmetapern	
CYBERKRIMINALITÄT IST EIN SPIEL	0
CYBERKRIMINALITÄT IST EINE JAGD	7
AKTIVITÄT DER CYBERKRIMINELLEN IST EINE JAGD	3
englische Sprache	
Kriegsmetaphern	
VIOLATION OF CYBERSECURITY IS PHYSICAL COMBAT	1
CYBERCRIME IS WAR	8
PROTECTION OF CYBERSECURITY IS PARTICIPATING IN PHYSICAL COMBAT	1
Erkrankungsmetaphern	
THREAT TO CYBERSECURITY IS A DISEASE	4
THREAT TO CYBERSECURITY IS AN INFECTION	5
COMPUTER IS A LIVING ENTITY	1
Metaphern über den geschlossenen Raum	
BEING SECURE IS BEING INSIDE OF A CLOSED SPACE	0
SECURITY IS A CLOSED SPACE	6
SECURITY IS INSIDE, INSECURITY IS OUTSIDE	4
Jagdmetapern	
CYBERCRIME IS A HUNT	7
CYBER CRIMIALS ARE HUNTRES	2
DECEIVING PEOPLE THROUGH CYBER CRIME IS GOING ON A HUNT	1
russische Sprache	
Kriegsmetaphern	

БОРЬБА ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ – ВЕДЕНИЕ ВОЙНЫ („KAMPF UM CYBERSICHERHEIT IST KRIEGFÜHRUNG“)	7
ДЕЙСТВИЯ КИБЕРПРЕСТУПНИКОВ – ВОЙНА („HANDLUNGEN DER CYBERKRIMINELLEN IST EIN KRIEG“)	2
ДЕЙСТВИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЗАЩИТА ОТ ВОЕННОГО НАПАДЕНИЯ („CYBERSICHERHEITSMAßNAHMEN SIND EIN ABWEHR VON EINEM ANGRIFF“)	1
Erkrankungsmetaphern	
НАРУШЕНИЕ КИБЕРБЕЗОПАСНОСТИ – БОЛЕЗНЬ („SICHERHEITSVERLETZUNG IST EINE KRANKHEIT“)	6
ВРЕДОНОСНОЕ ПО – БОЛЕЗНЬ („MALWARE IST EINE KRANKHEIT“)	4
ВТОРЖЕНИЕ ВРЕДОНОСНОГО ПО В СИСТЕМУ – ВТОРЖЕНИЕ БОЛЕЗНИ В ОРГАНИЗМ („EINDRINGEN VON EINER MALWARE INS SYSTEM IST EINDRIGEN VON EINER ERKRANKUNG INS KÖRPER“)	0
Metaphern über den geschlossenen Raum	
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ЗАКРЫТОЕ ПРОСТРАНСТВО („CYBERSICHERHEIT IST EIN GESCHLOSSENER RAUM“)	8
НАХОЖДЕНИЕ В СЕТИ, ЗАЩИЩЕННОЙ ОТ КИБЕРУГРОЗ – НАХОЖДЕНИЕ В ЗАМКНУТОМ ПРОСТРАНСТВЕ („BEFINDEN IN EINEM VOR CYBERSICHERHEITSBEDROHUNGEN GESCHÜTZTEM NETZWERK IST BEFINDEN IN EINEM GESCHLOSSENEN RAUM“)	1
ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – СОХРАНЕНИЕ НЕПРОНИЦАЕМОСТИ ЗАКРЫТОГО ПРОСТРАНСТВА („SICHERSTELLEN DER CYBERSICHERHEIT IST IMPENETRABILITÄT EINES GESCHLOSSENEN RAUMS“)	1
Jagdmetapern	
КИБЕРПРЕСТУПНОСТЬ – ОХОТА („CYBERKRIMINALITÄT IST JAGD“)	8
КИБЕРПРЕСТУПНИК – ОХОТНИК („CYBERKRIMINELLER IST EIN JÄGER“)	2

ЖЕРТВА КИБЕРПРЕСТУПНИКОВ – ДОБЫЧА ОХОТНИКА („OPFER DER CYBERKRIMINELLEN IST EINE BEUTE DER JÄGER“)	0
Angelnmetaphern	
КИБЕРПРЕСТУПНОСТЬ – РЫБАЛКА („CYBERKRIMINALITÄT IST ANGELN“)	9
КИБЕРПРЕСТУПНИК – РЫБАК („CYBERKRIMINELLER IST FISCHER“)	1

Tabelle 23. Statistische Daten der Umfrage

6. Diskussion

Im Ergebniskapitel wurden jeweils pro Sprache Deutsch, Englisch, Russisch aus den einzelnen Metaphern die ihnen zu Grunde liegenden konzeptuellen Metaphern abgeleitet. Es wurde demonstriert, dass in allen drei Sprachen ähnliche Gruppen der Metaphern existieren, nämlich, die den Kampf um die Cybersicherheit als einen Krieg thematisieren; die Cybersicherheitsbedrohungen als eine Infektion oder Erkrankung bezeichnen; die das Sich-Befinden in einem abgesicherten Netzwerk als das Sich-Befinden in einem abgeschlossenen Raum, außerhalb dessen Grenzen die Cybersicherheitsbedrohungen existieren ansehen; und die die andauernden Versuche der Cyberkriminellen ihre Opfer auszutricksen, mit einer Jagd vergleichen. Für die russische Sprache ist noch eine zusätzliche Gruppe der Metaphern relevant, nämlich die die illegalen Aktivitäten von Cyberkriminellen in Begriffen von Angeln betrachten. Die universelle Verbreitung von metaphorischen Ausdrücken in ausgewählten Texten lässt die Annahme zu, dass konzeptuelle Metaphern in der Fachsprache präsent sind und sie prägen. Es gibt mehr Herkunftsdomänen für konzeptuelle Metaphern als ursprünglich angenommen. Eine der vorgeschlagenen Herkunftsdomänen „Medizin“ hat sich als ein zu grob umrissener Bereich erwiesen und wurde mit „Infektion“ ersetzt. Zu den zwei Herkunftsdomänen, die nicht ursprünglich als die Quellen von konzeptuellen Metaphern vorausgesetzt wurden, deren Existenz aber während der Recherche festgestellt wurde, zählen „Jagd“ und „geschlossener Raum“. Auf der einen Seite überlappen sich im Großen und Ganzen die Metapherngruppen („Kriegsmetaphern“, „Erkrankungsmetaphern“, „Jagdmetapern“, „Metaphern über den geschlossenen Raum“) in allen drei Sprachen, unabhängig davon ob diese Sprachen verwandt sind (wie Deutsch und Englisch) oder zu unterschiedlichen Sprachfamilien gehören (wie Deutsch und Russisch). Auf der anderen Seite ist die Gruppe der „Angelnmetaphern“ nur für die russische Sprache charakteristisch. Die Wahl von Angeln als ein Herkunftsbereich für Metaphern ist vermutlich auf die Popularität des Angelns und die passenden klimatischen und geographischen Bedingungen wie Anzahl der Seen und Flüssen in Ländern des russischsprachigen Raums zurückzuführen, und wenn Russland ein Land mit einem Wüstenklima wäre, würde Angeln weniger wahrscheinlich als Quelle für metaphorische Redewendungen herangezogen werden.

Ziel dieser Masterarbeit war es, die konzeptuellen Metaphern in der Cybersicherheits-Fachsprache zu identifizieren und zwischen den drei Sprachen zu vergleichen. Die vier konzeptuellen Metaphern im Deutschen, die vier konzeptuellen Metaphern im Englischen, die fünf konzeptuellen Metaphern im Russischen lassen die Schlussfolgerung zu, dass die Mehrheit der konzeptuellen Metaphern in der Cybersicherheits-Fachsprache sprachübergreifend universell ist. Die Präsenz der

oben genannten konzeptuellen Metaphern und deren Herkunftsbereichen „Krieg“, „Infektion“, „Jagd“, „abgeschlossener Raum“ lässt sich auch bei Namen der IT-Sicherheitsfirmen ablesen: „YesDefend“, „Defendify“, „Dr Web“ („Doctor Web“), „CyberTrap“, „Intruder“.

Die für die vorliegende Forschungsarbeit ausgewählte Methode der Metaphernidentifizierung mittels der Construction Patterns für Metaphern und der Assoziationen zwischen Herkunft- und Zieldomänen auf der Basis von FrameNet kann als fruchtbar angesehen werden, da mit ihrer Hilfe mehr als 100 metaphorische Ausdrücke und 13 konzeptuelle Metaphern gefunden werden konnten.

Die von Dodge et al. (2015) vorgeschlagenen Construction Patterns erwiesen sich in den meisten Fällen als ausreichend. Besonders für die englische Sprache stimmten die Construction Patterns der im Korpus gefundenen Metaphern fast immer mit denen in Tabelle 22 angeführten überein. Einige neu entdeckte Construction Patterns für die englische Sprache beinhalten die von Dodge (2015) ursprünglich vorgeschlagene, wie z.B. S-verb_S-adj_mod_T-noun im „isolate infected systems“ enthält S-adj_mod_T-noun oder S-noun_prep_T-noun_mod_S-noun im „Opfer von Hackerangriffen“ enthält S-noun_prep_T-noun. Einige der angeführten metaphorischen Beispiele bestehen aus mehr als zwei Elementen (z. B. ein Verb, ein Substantiv und ein Adjektiv), während die Construction Patterns in der Typologie von Dodge et al. (2015) in der Regel nur zwei Bausteine voraussehen.

Die Frames aus dem FrameNet für die englische Sprache sind relativ gut ausgearbeitet. Es existieren Verbindungen zu verwandten Frames und eine Liste von lexikalischen Units für jeden Frame. Für die deutsche Sprache stellt das FrameNet des Deutschen zwar eine Übersetzung aus dem Englischen dar, aber die angeführten lexikalischen Units und die Frameelementen wurden manuell korrigiert und an die deutsche Sprache angepasst (vgl. FrameNet des Deutschen 2022). Es existiert zurzeit kein FrameNet im Russischen und für die Analyse wurden die Übersetzungen aus dem englischsprachigen FrameNet herangezogen.

Es konnte beobachtet werden, dass in mehreren lexikalischen Ausdrücken Metaphern aus zwei Herkunftsdomänen kombiniert werden können, z.B. „perimeter ausspähen“ kann als eine Zusammensetzung aus den Herkunftsdomänen „abgegrenzter Raum“ und „Jagen“ gesehen werden, bei „Angreifer in die Falle locken“ können die zwei Herkunftsdomänen „Krieg“ und „Jagen“ erkannt werden, bei „immune to cybersecurity threats“ – die Herkunftsdomänen „Infektion“ und „Krieg“, „inside and outside cybersecurity threats“ – die Herkunftsdomänen „abgegrenzter Raum“ und „Krieg“ . Die Anzahl der Herkunftsdomänen ist begrenzt auf „Krieg“, „Infektion“, „abgegrenzter Raum“, „Jagen“, aber sie können frei aneinandergereiht werden. Die Zieldomäne „Sicherheit“ muss nicht immer direkt genannt werden und kann auch nur impliziert werden („Waffe gegen Angriffe“, „immun gegen Angriffe“), es fehlen also im metaphorischen Ausdruck die Schlüsselwörter oder

Präfixe („Cyber“), die auf die Zieldomäne hindeuten können, und die metaphorischen Beziehungen zwischen den Herkunfts- und Zieldomäne können nur mit Hilfe des Kontexts nachverfolgt werden. Das Construction Pattern T-noun_mod_S-noun wird im Englischen und Deutschen anders realisiert („Hackerattacke“ – „hacker attack“). Komposita werden im Deutschen zusammengeschrieben, während im Englischen entsprechende grammatikalische Konstruktionen separat geschrieben werden. Für die russische Sprache wird ein entsprechender metaphorischer Ausdruck aus einem Adjektiv und einem Substantiv gebildet („хакерская аттака“), und das grammatikalische Muster entspricht dann T-adj_mod_S-noun. Die Zusammensetzung von zwei Substantiven T-noun_mod_S-noun ist für die russische Sprache zwar auch möglich, im Korpus wurden ausschließlich nur solche Metaphern mit einem Präfix „кибер“ („cyber“) gefunden, wie „кибернападение“ („Cyberangriff“), „кибервойна“ („Cyberkrieg“). Die besitzanzeigende Form wird im Englischen oft mit Apostroph gebildet: T-noun_poss_S-noun („hacker’s arsenal“), im Russischen ist die Wortreihenfolge umgekehrt, also S-noun_Genitive_T-noun, und es wird der Genitiv Kasus verwendet („арсенал хакеров“). Dasselbe gilt für die Konstruktion S-noun_of_T-noun, die im Russischen ohne die Präposition, nur mit Genitiv und entsprechenden Wortendungen als Construction Pattern S-noun_Genitive_T-noun gebildet wird: „оборона сети“ („Defensive des Netzwerkes“).

Die Unterschiede in Construction Patterns zwischen den Sprachen spiegeln die Unterschiede in der linguistischen Realisierung von denselben konzeptuellen Metaphern in verschiedenen Sprachen wider. So wird der Ausdruck „in ein Netzwerk einzubrechen“ nach dem Pattern prep_T-noun_S-verb gebildet, dabei zeigt sowohl die Präposition „in“ als auch das Präfix „ein“, dass es sich um eine begrenzte Entität handelt; der entsprechende Ausdruck im Englischen „break into the network“ wird nach einem symmetrischen Pattern S-verb_prep_T-noun geformt. Dies könnte dadurch bedingt sein, dass angesichts der Verbreitung des Englischen als Lingua Franca insgesamt für die IT-Sprache und der Entlehnung der Fachausdrücke aus dem Englischen in andere Sprachen, die entsprechenden Ausdrücke nach den in der Zielsprache geltenden grammatikalischen Regeln angepasst sind. Für einige Ausdrücke aus dem Englischen wie „ransomware strikes“ oder „ransomware hits“ („strikes“ und „hits“ sind in diesem Fall Verben) wurden keine direkten entsprechenden Entlehnungen im deutschen Korpus gefunden, es wird eher das Substantiv „Ransomware-Angriffe“ verwendet. Die Construction Patterns sind nicht für jede Sprache identisch und müssen eindeutig für jede Sprache erstellt und analysiert werden. Auch wenn mehrere Sprachen dieselbe konzeptuelle Metapher teilen, gibt es einige linguistische Feinheiten für jede Sprache, die z. B. durch die akzeptierte Wortfolge oder bestehender Sprachgebrauch bedingt sind. Die metaphorischen Mappings zwischen der Herkunfts- und Zieldomäne können gleich sein und zu gleichen Metaphern in der Sprache führen, wie z.B. „hackers hunt“, „хакеры охотятся“ im

Deutschen und im Russischen. Es ist auch eine umgekehrte Situation möglich: ein Teil der Herkunftsdomäne wird in einer Sprache referenziert, in einer anderen Sprache dagegen nicht. So wird sowohl im Russischen als auch im Deutschen über Schad-Software als eine virale Infektion gesprochen („Virus“, „вирус“), aber nur im Russischen spricht man auch von einer „parasitären Infektion“ in Bezug auf Datenverkehr, der durch Malware initiiert wird und das Netzwerk belastet („паразитный трафик“ – „der parasitäre Datenverkehr“).

Die Umfrage erwies sich als ein nützliches Hilfsmittel, um die technische Expertise von IT-Expert*innen im Hinblick auf die erhobenen linguistischen Daten einzusetzen und durch eine interdisziplinäre Arbeit zwischen den Linguist*innen und den IT-Expert*innen die Ergebnisse zu validieren. Die Übereinstimmung in den Formulierungen von konzeptuellen Metaphern in allen drei Sprachen war hoch.

Für die konzeptuellen Metaphern stellen das besondere Interesse die konventionalisierten Metaphern dar, die streng genommen nicht als Metaphern wahrgenommen werden und im Fließtext verwendet werden. Wenn im Korpus eine Metapher identifiziert wurde, die in Anführungszeichen angeführt wurde, wurde sie in der Regel als nicht-konventionalisierte, also Autormetapher interpretiert und nicht in die Analyse aufgenommen, wie z. B. „поймать за руку вредоносный код“ („die Hand der Schad-Software greifen“). Das Ziel war, die Metaphern aus dem in der Fachsprache der Cybersicherheit akzeptierten Sprachgebrauch für die Analyse heranzuziehen. Die Ausdrücke, die sowohl mit als auch ohne Anführungszeichen im Text vorkommen, wie „дыры“ („Lücken“) oder „лечить“ („heilen“), wurden als konventionalisierte Metaphern eingestuft, wenn sie nur in einem Text und nicht in allen in Anführungszeichen gesetzt wurden, und deren üblicher Gebrauch ohne Interpunktionszeichen als Zeichen des hohen Grades der Konventionalisierung betrachtet. Es könnte trotzdem diskutiert werden, inwiefern ein metaphorischer Ausdruck konventionalisiert wird und es erscheint sinnvoll für die Beantwortung solcher Fragen einen weitaus größeren Korpus für eine umfassendere Analyse zu erstellen, was aber den Rahmen dieser Masterarbeit sprengen würde. Im Zweifelsfall, wenn nicht eindeutig belegt werden konnte, ob ein Ausdruck tatsächlich eine Metapher aus der ausgewählten Herkunftsdomäne darstellt, wurde dieser aus der Analyse ausgeschlossen. So kann bestritten werden, ob „anti-virus“ der Herkunftsdomäne „Infektion“ angehört, da es z.B. für Menschen „antivirals“ eingesetzt werden und die menschlichen Medikamente werden nicht als „anti-viruses“ bezeichnet.

Eine weitere Einschränkung der vorliegenden Studie war die Abwesenheit von entsprechenden Online-Werkzeugen für Part-Of-Speech Tagging und Dependency Parsing für die russische Sprache. Zum Zeitpunkt der Erfassung dieser Masterarbeit gab es kein frei zugängliches Tool und auch eine Recherche für ein Tool mit einer Lizenz hat nichts ergeben. Die Wortarten und

grammatikalische Abhängigkeiten mussten manuell definiert werden. Es gibt auch Softwarefehler im Part-Of-Speech Tagging und Dependency Parsing Tool für die deutsche und englische Sprache CoreNLP, so wurde im Satz „to proactively hunt for and shut down threats“ das Wort „hunt“ als Substantiv identifiziert, obwohl es sich um ein Verb handelt. Diese Fehler mussten manuell korrigiert werden (vgl. CoreNLP 2022).

Eine interessante Erweiterung dieser Studie wäre, die konzeptuellen Metaphern in der Cybersicherheits-Fachsprache neben Deutsch, Englisch und Russisch auch in anderen Sprachen zu untersuchen. Da es kaum möglich ist, dass nur eine Person für eine fundierte Untersuchung die notwendigen Sprachkenntnisse auf einem hohen Niveau beherrscht, ist als eine mögliche Form der Untersuchung eine Zusammenarbeit von mehreren Linguist*innen mit unterschiedlichen Sprachkenntnissen, auch aus unterschiedlichen Universitäten aus mehreren Ländern, vorstellbar.

7. Schlussfolgerungen

Die im Kapitel über den aktuellen Stand der Forschung beschriebenen umfangreichen Forschungsarbeiten decken die Existenz einer Vielzahl von konzeptuellen Metaphern in verschiedenen Sprachen, sowohl in der Alltags- als auch in den Fachsprachen, auf, die eine wichtige Rolle darin spielen, komplexe abstrakte Sachverhalte mithilfe von metaphorischen sprachlichen Ausdrücken zu kommunizieren. Die zentrale Erkenntnis dieser Arbeit ist, dass sich in der Fachsprache der Cybersicherheit mehrere klar definierbare Gruppen von metaphorischen Ausdrücken identifizieren lassen, auf deren Basis man die zu Grunde liegenden konzeptuellen Metaphern formulieren kann und dass diese Formulierungen in Sprachen wie Deutsch, Englisch und Russisch praktisch identisch oder mindestens synonym sind. Die ursprüngliche Annahme, dass Krieg und Medizin die bedeutendsten Herkunftsdomänen für konzeptuelle Metaphern darstellen, wurde teilweise bestätigt, allerdings wurden noch weitere Herkunftsdomänen festgestellt, nämlich räumliche Dimension – geschlossener Raum, Jagd und Angeln. Während der Korpusrecherche von Fachartikeln und Blogeinträgen auf den offiziellen Webseiten von Firmen, die professionelle Dienstleistungen im Bereich Cybersicherheit anbieten, konnte nachgewiesen werden, dass die Herkunftsdomänen für Deutsch, Englisch und Russisch bis auf eine einzige Ausnahme, und zwar Angeln, die nur für die russische Sprache relevant ist, übereinstimmen.

Konzeptuelle Metaphern repräsentieren metaphorische Verbindungen zwischen der Herkunftsdomäne (Medizin, Krieg usw.) und der Zieldomäne (Cybersicherheit). Für gewöhnliche Menschen existieren sie auf der Ebene des Unbewussten, als kognitive Mechanismen, die mentale Repräsentation von abstrakten Konzepten erleichtern und nur in Forschungsarbeiten von Linguist*innen aufgedeckt, systematisiert und explizit artikuliert werden. Auf der sprachlichen Ebene werden konzeptuelle Metaphern in sprachlichen Ausdrücken realisiert, die in jedem Fachtext allgegenwärtig sind. Es wird schwierig sein, einen Text zum Thema Cybersicherheit zu finden, der Cyber-Bedrohungen nicht mit „Kriegs"-Begriffen thematisiert, den man abwehren muss, oder der die Schadsoftware nicht als eine Infizierung eines PCs bezeichnet, oder der ein Netzwerk nicht als einen geschlossenen Raum betrachtet, in den man einbrechen kann oder gewiefte Cyberkriminelle nicht als diejenige vorstellt, die Fallen mit Ködern stellen und darauf achten, keine Spuren zu hinterlassen, genauso wie es ein Jäger tun würde. Es wurde demonstriert, dass grammatikalische Strukturen, nach denen diese sprachlichen Ausdrücke gebildet sind, nicht willkürlich sind, sondern bestimmten Construction Patterns folgen. Sie bestehen aus mindestens zwei Elementen, in der Regel gehört das eine der Herkunftsdomäne („source domain", S) und das andere der Zieldomäne („target domain", T), die mit einer Präposition verbunden werden können. wie z.B. „Infektion mit Schadsoftware" dem

Pattern S-noun_prep_T-noun entspricht. Durch diese Construction Patterns werden metaphorische Mappings zwischen der Herkunftsdomäne und Zieldomäne realisiert (aus dem Englischen „source-to-target domain mappings“), dass per Definition sowohl eine Herkunftsdomäne als auch eine Zieldomäne erfordert. Es war aber unmöglich, mehrere Fälle zu ignorieren, in denen nur die Herkunftsdomäne direkt referenziert wurde, und die Zieldomäne nur aus dem Kontext erschlossen werden konnte, wie z.B. in „Waffe gegen Angriffe“ (Pattern S-noun_prep_S-noun, Herkunftsdomäne „Krieg“) oder die ein Zusammenspiel zwischen mehreren Herkunftsdomänen darstellen, wie z.B. „immun gegen Cyberangriffe“ (Pattern S^1-adj_prep_T-noun_S^2-noun, Herkunftsdomänen „Medizin“ und „Krieg“). Eine weitere methodische Herausforderung bestand darin, dass konzeptuelle Metaphern für einige Sprachen wie z.B. Russisch noch nicht ausreichend erforscht wurden, und die für das Erschließen von konzeptuellen Metaphern notwendigen Online-Tools, wie z.B. FrameNet oder Dependency Parser Core NLP nur für eine kleine Anzahl der Sprache vorhanden sind. Als Ergebnis kann festgestellt werden, dass es noch keine etablierte Vorgehensweise für solche Arten von Forschungsarbeiten gibt und die Ansätze verschiedener Autor*innen erheblich variieren. In diesem Sinne kann die in der vorliegenden Arbeit erprobte Methodik als Orientierung für zukünftige ähnliche Forschungsarbeiten dienen, da auf der Grundlage einer Korpusrecherche mit ihrer Hilfe mehrere konzeptuelle Metaphern für die klar abgegrenze Zieldomäne „Cybersicherheit”, aus mehr als nur zwei urspünglich vermuteten Herkufntsdomänen identifiziert werden konnten, die im Anschluss während einer Umfrage von IT-Expert*innen verifiziert wurden.

Die vorliegende Masterarbeit umfasst nur einen kleinen Teil der metaphorischen Vielfalt in der Fachsprache und zeigt nur ihren gegenwärtigen Stand. Es wäre interessant, die historische Entwicklung und Verbreitung von konzeptuellen Metaphern parallel mit der Entstehung der Cybersicherheit als Wissenschaft und der Einführung von neuen Konzepten, wie Cyberattacken, Computerviren usw. nachzuverfolgen. Weiterhin kann im Laufe eines Sammelreviews von schon vorhandenen Forschungsarbeiten untersucht werden, welche Herkunftsdomäne die Hauptquelle für die Mehrheit der konzeptuellen Metaphern sind, wie z.B. „Krieg“, der als Herkunftsdomäne für Metaphern aus dem Bereich Business, Politik, Sport, Verlauf von schweren Krankheiten wie Krebs usw. dienen kann. Des Weiteren besteht die Möglichkeit, basierend auf der in der vorliegenden Arbeit vorgestellten Methodik konzeptuelle Metaphern anhand von mehr als nur ein paar Sprachen zu analysieren, wobei eine Kooperation zwischen mehreren Autor*innen mit verschiedenen Sprachkenntnissen sinnvoll erscheint.

8. Literaturverzeichnis

ActionFraud[1] (2022). Malware and computer viruses. https://www.actionfraud.police.uk/a-z-of-fraud/malware (Stand: 01.10.2022).

ActionFraud[2] (2022). Computer hacking. https://www.actionfraud.police.uk/a-z-of-fraud/computer-hacking (Stand: 01.10.2022).

ActionFraud[3] (2022). Phishing. https://www.actionfraud.police.uk/a-z-of-fraud/phishing (Stand: 01.10.2022).

Andrew, Daniel (2020). 9 minutes to breach. https://www.intruder.io/blog/9-minutes-to-breach-the-life-expectancy-of-an-unsecured-mongodb-honeypot (Stand: 01.10.2022).

Arceo Cybersecurity (2022). https://arceo.at/index.php (Stand: 01.10.2022).

Arinteg[1] (2022). Защита от ddos-атак. https://arinteg.ru/services/ddos-attack.php (Stand: 01.10.2022).

Arinteg[2] (2022). Информационная безопасность в интернете. https://arinteg.ru/articles/informatsionnaya-bezopasnost-v-internete-28201.html (Stand: 01.10.2022).

ATG (2019). How to recover from a cyber attack. https://www.atg-it.co.uk/cyber-security/recover-from-cyber-attack/ (Stand: 01.10.2022).

Aurora IT (2022). SECURITIES AND EXCHANGE COMMISSION TO INTRODUCE NEW CYBERSECURITY DISCLOSURE RULES. https://aurorait.com/2022/07/12/securities-and-exchange-commission-to-introduce-new-cybersecurity-disclosure-rules/ (Stand: 01.10.2022).

Barcelona, Antonio (2001). On the systematic contrastive analysis of conceptual metaphors: case studies and proposed methodology. In: Barcelona, Antonio; Taylor, John R; Dirven, René; Geeraerts, Dirk; Langacker, Ronald W (Hg.) *Applied Cognitive Linguistics, II, Language Pedagogy*. Berlin/Boston: De Gruyter, Inc., 117-146.

Bezmalyi, Vladimir (2014). Чем вдохновляются интернет-мошенники. https://www.kaspersky.ru/blog/avoid-news-related-phishing/4994/ (Stand: 01.10.2022).

Blue Consult (2022). Ransomware Protection. https://blue-consult.de/loesungen/it-security/ransomware-protection/ (Stand: 01.10.2022).

Boulenger, Veronique; Shtyrov, Yury; Pulvermüller, Friedemann (2012). When do you grasp the idea? MEG evidence for instantaneous idiom understanding. *NeuroImage* 59 (4), 3502-3513.

Boroditsky, Lera (2011). How Languages Construct Time. In: Dehaene, Stanislas; Elizabeth M. Brannon (Hg.) *Space, Time and Number in the Brain*. London: Academic Press, Elsevier, 333-341.

Bowyer, Richard (2007). *Dictionary of military terms*. London: A & C Black.

Branch, Jordan (2021). What's in a Name? Metaphors and Cybersecurity. *International Organization* 75 (1), 39-70.

Busse, Dietrich (2012). *Frame-Semantik. Ein Kompedium.* Berlin / Boston: Walter der Gruyter GmbH & Co. KG.

Careful Security (2022). https://www.carefulsecurity.com/build-cybersecurity/prevent-ransomware/ (Stand: 01.10.2022).

CBT Training & Consulting (2022). EC Council. https://www.it-informationssicherheit.de/seminaruebersicht/hersteller/ec-council.html (Stand: 01.10.2022).

Champion, Savannah (2019). Horror Movies & Cyber Security. https://conversantgroup.com/horror-movies-cybersecurity/ (Stand: 01.10.2022).

Charteris-Black, Johnathan (2004). *Corpus approaches to critical metaphor analysis*. Basingstoke: Palgrave Macmillan.

Cloud Clan (2022). Информационная безопасность. https://cloudclan.ru/professional-services/sec/ (Stand: 01.10.2022).

Cooper, Martin (2021). The Big Interview: Language and Cybersecurity. *Oxford University Press* 63 (1), 37 – 39.

CoreNLP (2022). https://corenlp.run (Stand 01.10.2022).

Courant (2014). How did I get this computer virus? https://gocourant.com/get-computer-virus/ (Stand 01.10.2022).

Csatár, Péter (2020). Innovationen in der kognitiv-linguistischen Metaphernvorschung. In: Mikuláš, Roman (Hg.) *Metaphernforschung in interdisziplinären und interdiskursiven Perspektiven*. Paderborn: Brill | mentis, 423 – 439.

Cybertrap¹ (2022). https://cybertrap.com/ (Stand 01.10.2022).

Cybertrap² (2022). Lösungen. https://cybertrap.com/loesungen/ (Stand 01.10.2022).

Cyberunit¹ (2022). Here Is Why You Need To Keep Your Systems Updated. https://www.cyberunit.com/blog/here-is-why-you-need-to-keep-your-systems-updated (Stand 01.10.2022).

Cyberunit² (2022). Signs Of A Ransomware Attack And What You Should Do Next. https://www.cyberunit.com/blog/signs-of-a-ransomware-attack-and-what-you-should-do-next (Stand 01.10.2022).

Cyberunit³ (2022). How To Reduce Your Attack Surface. https://www.cyberunit.com/blog/how-to-reduce-your-attack-surface (Stand 01.10.2022).

Cyberunit⁴ (2016). Casual Connect 2016: From the Hackers' Perspective. https://cyberint.com/blog/techtalks/casual-connect-2016-from-the-hackers-perspective/ (Stand 01.10.2022).

Datacast Technologies (2022). https://datacasttech.com/cybersecurity (Stand 01.10.2022).

Darai, Gholamreza; Handermann, Michaela; Sonntag, Hans-Günther; Zöller, Lothar (2012). *Lexikon der Infektionskrankheiten des Menschen: Erreger, Symptome, Diagnose, Therapie und Prophylaxe*. Berlin, Heidelberg: Springer Berlin Heidelberg.

DAXX (2021). Wie viele Softwareentwickler gibt es in Deutschland, den USA und auf der Welt? https://www.daxx.com/de/blog/entwicklungstrends/anzahl-an-softwareentwicklern-deutschland-weltweit-usa (Stand 04.06.2022).

Dedenok, Roman (2021). Фишинг от имени хостинг-провайдера Как и зачем злоумышленники охотятся на учетные данные от личных кабинетов хостинг-провайдеров.. https://www.kaspersky.ru/blog/hosting-provider-phishing-web-page/30129/ (Stand 01.10.2022).

Defendify (2022). Cybersecurity Risk Assessment Tool. https://www.defendify.com/cybersecurity-assessment-tool (Stand 01.10.2022).

Desai, Rutvik (2021). Are metaphors embodied? The neural evidence. *Psychological research* 11.

Dodge, Ellen; Hong, Jisup; Stickles, Elise (2015). *MetaNet: Deep semantic automatic metaphor analysis. Proceedings of the 3rd Workshop on Metaphor in NLP*. Denver, Colorado: NAACL HLT, 40-49.

Dodge, Ellen (2018). A deep semantic corpus-based approach to metaphor analysis. In: Petruck, Miriam (Hg.) *MetaNet*. Amsterdam, Philadelphia: John Benjamins Publishing Company, 127-166.

Drewer, Petra (2003). *Die kognitive Metapher als Werkzeug des Denkens: zur Rolle der Analogie bei der Gewinnung und Vermittlung wissenschaftlicher Erkenntnisse*. Tübingen: Narr.

Elitze, Katrin (2012). *Metaphern in der Börsenfachsprache: eine kontrastive Analyse des Spanischen und Deutschen*. Hamburg: Kovac.

Erk, Katrin; Kowalski, Andrea; Padó, Sebastian; Pinkal Manfred (2003). Towards a Resource for Lexical Semantics: A Large German Corpus with Extensive Semantic Annotation. In: *Proceedings of the 41st Annual Meeting of the Association for Computational Linguistics*. Stroudsburg: Association for Computational Linguistics, 537-544.

Foresite¹ (2022). The motivation of Cyber Threat Actors: Who's after your stuff? https://foresite.com/blog/the-motivation-of-cyber-threat-actors-whos-after-your-stuff/ Stand 01.10.2022.

Foresite² (2022). Fence Holes and Cybersecurity. https://foresite.com/blog/fence-holes-and-cybersecurity/ Stand 01.10.2022.

FrameNet des Englischen (2022). https://framenet.icsi.berkeley.edu/fndrupal/frameIndex. Stand 01.10.2022.

FrameNet des Deutschen (2022). https://gsw.phil.hhu.de/framenet/. (Stand 01.10.2022).

FrameNet Wiki (2022). https://metaphor.icsi.berkeley.edu/pub/en/index.php/Category:Metaphor (Stand 01.10.2022).

Gardatech (2022). ЗАЩИТА ОТ СЕТЕВЫХ АТАК. https://gardatech.ru/articles/smi/zashchita-ot-setevykh-atak/ (Stand 01.10.2022).

G-Data (2022). Der Spiegel: Grüße von der falschen Chefin. https://www.gdata.de/g-data-in-der-presse/2022/03/37319-spiegel-gruesse-von-der-falschen-chefin (Stand 01.10.2022).

GE Digital (2022). Maintaining Security Hygiene. https://www.ge.com/digital/blog/maintaining-security-hygiene (Stand 01.10.2022).

Gibbs Jr. Raymond W. (2008). *The Cambridge Handbook of Metaphor and Thought*. New York: Cambridge University Press.

Gibbs, Jr. Raymond W. (2018). *Metaphor Wars: Conceptual Metaphors in Human Life*. New York: Cambridge University Press.

Gibson, Jami (2003). Viruses and Worms. https://whittakerassociates.com/viruses-and-worms/ (Stand: 01.10.2022).

Graff, David & Cieri, Christopher (2003). *English Gigaword LDC2003T05*. Web Download. Philadelphia: Linguistic Data Consortium.

Goschler, Juliana (2009). Drewer, Petra 2003. Die kognitive Metapher als Werkzeug des Denkens. Zur Rolle der Analogie bei der Gewinnung und Vermittlung wissenschaftlicher Erkenntnisse. *Zeitschrift für Rezensionen zur germanistischen Sprachwissenschaft* 1 (2), 187-191.

Grüner[1], Tina (2018). Was ist eigentlich Ransomware? https://blog.to.com/was-ist-eigentlich-ransomware/ (Stand: 01.10.2022).

Grüner[2], Tina (2018). Was ist eigentlich eine DDoS-Attacke? https://blog.to.com/was-ist-eigentlich-eine-ddos-attacke/ (Stand: 01.10.2022).

Johnson, Mark (1987). *The body in the mind: the bodily basis of meaning, imagination, and reason.* Chicago: University of Chicago Press.

Hedblom, Maria; Gromann, Dagmar; Kutz, Oliver (2018*). In, out and through: formalising some dynamic aspects of the image schema containment. Proceedings of the 33rd Annual ACM Symposium on applied computing*, 918-925.

Hoffman, Lothar (1984). *Kommunikationsmittel Fachsprache: Eine Einführung.* Berlin: Akademie-Verlag.

Holt, Thomas J.; Lee, Jin Ree; Freilich, Joshua D.; Chermak, Steven M.; Bauer, Johannes M.; Shillair, Ruth & Ross, Arun (2020). An Exploratory Analysis of the Characteristics of Ideologically Motivated Cyberattacks. *Terrorism and political violence* 8, 1-16.

Hugh, Aver (2021). QR-код, да не тот Рассказываем, как не попасться на удочку киберпреступников при сканировании QR-кодов. https://www.kaspersky.ru/blog/qr-code-threats/30648/ (Stand: 01.10.2022).

Ilyin, Yuri (2015). Профилактика киберугроз: рекомендации для предприятий. https://www.kaspersky.ru/blog/profilaktika-kiberugroz-rekomendatsii-dlya-predpriyatij/14982/ (Stand: 01.10.2022).

Intruder (2022). External Vulnerability Scanner. https://www.intruder.io/external-vulnerability-scanner (Stand: 01.10.2022).

IT-Native (2022). Cyberwar vs. Cybercrime. https://it-native.com/blog/cyberwar-vs-cybercrime/ (Stand: 01.10.2022).

Kaspersky[1] (2022). Was ist Cybersicherheit? https://www.kaspersky.de/resource-center/definitions/what-is-cyber-security (Stand: 01.10.2022).

Kaspersky[2] (2022). Компьютерные вирусы и вредоносное ПО: факты и часто задаваемые вопросы. https://www.kaspersky.ru/resource-center/threats/computer-viruses-and-malware-facts-and-faqs (Stand: 01.10.2022).

Kaspersky[3] (2022). Русскоязычные хакеры охотятся за клиентами швейцарских, австрийских и немецких банков. https://www.kaspersky.ru/about/press-releases/2015_russkoyazichniye-hakeri-okhotyatsya-za-klientami-shweitsarskikh-austriyskikh-i-nemetskikh-bankov (Stand: 01.10.2022).

Kaspersky[4] (2018). Бизнес-инкубатор «Лаборатории Касперского» подводит итоги конкурса Kaspersky Start Russia. https://www.kaspersky.ru/about/press-releases/2018_incubator-results (Stand: 01.10.2022).

Kaspersky[5] (2022). Kaspersky Security для интернет-шлюзов. https://www.kaspersky.ru/small-to-medium-business-security/internet-gateway (Stand: 01.10.2022).

Kaspersky ICS Cert (2022). APT-атаки на промышленные компании во второй половине 2021 года. https://ics-cert.kaspersky.ru/publications/reports/2022/02/28/apt-attacks-on-industrial-companies-in-h2-2021/ (Stand: 01.10.2022).

Kövecses, Zoltán (2005). *Metaphor in culture : universality and variation*. Cambridge: Cambridge University Press.

Kövecses, Zoltán (2017). Conceptual metaphor theory. In: Semino, Elena; Demjén, Zsófia (Hg.) *The Routledge Handbook of Metaphor and Language*. London: Routledge, 13 – 27.

Kövecses, Zoltán (2020). *Extended conceptual metaphor theory*. Cambridge: Cambridge University Press.

Lakoff, George & Johnson, Mark (1980): *Metaphors We Live By*. Chicago: University of Chicago Press.

Lakoff, George & Turner Mark (1989). *More Than Cool Reason: A Field Guide to Poetic Metaphor*. Chicago: University of Chicago Press.

Lakoff, George (1993). The contemporary theory of metaphor. In: A. Ortony (Hg.) *Metaphor and Thought*. Cambridge: Cambridge University Press. 202-251.

Lakoff, George & Johnson, Mark (2021): *Leben in Metaphern: Konstruktion und Gebrauch von Sprachbildern*. Übersetzung von Hildenbrand, Astrid. Heidelberg: Carl-Auer-Systeme.

Levis, Sarah & Burke, John (2019). Gateway. Definition. https://www.techtarget.com/iotagenda/definition/gateway (Stand: 01.10.2022).

Lieberman Technologies (2022). Cybersecurity 101: Monitor, Protect & Fix. https://ltnow.com/blog/cybersecurity-101-monitor-protect-fix/ (Stand: 01.10.2022).

Lifars (2021). Former Hacker Gives Advice on How to Protect Yourself from Cyber Crime. https://www.lifars.com/2021/12/former-hacker-gives-advice-on-how-to-protect-yourself-from-cyber-crime/ (Stand: 01.10.2022).

LimeSurvey (2022). https://www.limesurvey.org/ (Stand: 17.09.2022).

Maine Department of Inland Fisheries & Wildlife (2022). Definitions and Descriptions. https://www.maine.gov/ifw/hunting-trapping/trapping/laws-rules/definitions-descriptions.html (Stand: 17.09.2022).

Mash, Marina (2019). Мошенники на Airbnb расширяют аудиторию. https://www.kaspersky.ru/blog/airbnb-landlordz-scam/22724/ (Stand: 17.09.2022).

MetaNet GitHub Repository (2017). https://github.com/orgs/TheMetaNetProject (Stand: 05.07.2022).

MetaNet Frame Relation Type (2017). https://metaphor.icsi.berkeley.edu/pub/en/index.php/Glossary:Frame_Relation_Type (Stand: 05.07.2022).

MetaNet Wiki (2016). https://metaphor.icsi.berkeley.edu/pub/en/index.php/Category:Frame (Stand: 05.07.2022).

Middleton, Bruce (2017). *A History of Cyber Security Attacks*. Boca Raton: CRC Press.

Monti, Enrico (2009). Translating The Metaphors We Live By: Intercultural negotiations in conceptual metaphors. *European journal of English studies* 13 (2), 207-221.

Murphy, Gregory L. (1996). On metaphoric representation. *Cognition* 60 (2), 173 – 204.

Murphy, Gregory L. (1997). Reasons to doubt the present evidence for metaphoric representation. *Cognition* 62 (1), 99 – 108.

Netstar (2022). IT-Security Checklist. https://www.netstar.co.uk/it-security-checklist/ (Stand: 01.10.2022).

Özçalskan, Seyda (2003). Metaphorical Motion in Crosslinguistic Perspective: A Comparison of English and Turkish. *Metaphor and Symbol* 18 (3), 189-228.

OnsiteLogic (2022). Insider Threats: Spotting Indicators and Warning Signs. https://onsitelogic.com/insider-threats-spotting-indicators-and-warning-signs/ (Stand: 01.10.2022).

Papišta, Žolt A. (2017). Brennende Gefühle: die Strukturmetapher EMOTION IST FEUER in deutschen, serbischen und ungarischen Phraseologismen. *Zbornik za jezike i književnosti Filozofskog fakulteta u Novom Sadu* 6 (6), 193-211.

Patterson, Wayne & Winston-Proctor, Cynthia E. (2019). *Behavioral Cybersecurity Applications of Personality Psychology and Computer Science*. Boca Raton: CRC Press.

Pentest¹ (2020). Защита бизнеса: опасность халатного отношения к безопасности внутренней сети. https://pentest.codeby.net/inf-bezopasnost/audit-vnutrennej-seti/ (Stand: 01.10.2022).

Pentest² (2022). Аудит безопасности внешнего периметра компании. https://pentest.codeby.net/audit-vneshnego-perimetra/ (Stand: 01.10.2022).

Pentest³ (2020). Как избавиться от слабых мест в системе безопасности СКУД. https://pentest.codeby.net/inf-bezopasnost/kak-izbavitsya-ot-slabyh-mest-v-skud/ (Stand: 01.10.2022).

Pentest⁴ (2020). Как защитить от взлома веб-приложения — круговая оборона. https://pentest.codeby.net/inf-bezopasnost/kak-zashhitit-ot-vzloma-veb-prilozheniya-krugovaya-oborona/ (Stand: 01.10.2022).

Pentest⁵ (2022). Аудит системы безопасности: Wi-Fi и СКУД. https://pentest.codeby.net/audit-wi-fi-skud/ (Stand: 01.10.2022).

Perekalin, Alex (2017). Эпидемия шифровальщика WannaCry: что произошло и как защититься. https://www.kaspersky.ru/blog/wannacry-ransomware/16147/ (Stand: 01.10.2022).

Peters, Mike (2010). Triage - (medizin-)rechtliche Implikationen. *Zeitschrift für Evidenz, Fortbildung und Qualität im Gesundheitswesen* 104 (5), 413-416.

Perseus (2022). Remote-Protokolle. https://www.perseus.de/2022/04/25/remote-protokolle/ (Stand: 01.10.2022).

Pohlmann, Norbert (2022). *Cyber-Sicherheit. Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Wiesbaden: Springer Vieweg.

Prasad, Ramjee; Rohokale, Vandana (2020). *Cyber Security: The Lifeline of Information and Communication Technology*. Cham: Springer International Publishing.

Proxysec¹ (2022). https://www.proxysec.com/ (Stand: 01.10.2022).

Proxysec² (2022). Cyber-Services. https://www.proxysec.com/cyber-services (Stand: 01.10.2022).

Quigley, Kevin; Burns, Calvin; Stallard, Kristen (2015). 'Cyber Gurus': A rhetorical analysis of the language of cybersecurity specialists and the implications for security policy and critical infrastructure protection. *Government information quarterly* 32 (2), 108 – 117.

Rawat, Manischa (2022). Recover virus infected excel files. https://www.nucleustechnologies.com/blog/recover-virus-infected-excel-files/ (Stand: 01.10.2022).

RedScan¹ (2022). https://www.redscan.com/ (Stand: 01.10.2022).

RedScan² (2022). SECURING REMOTE WORKERS. https://www.redscan.com/solutions/securing-remote-workers/ (Stand: 01.10.2022).

Ricoh USA¹ (2022). Cybersecurity best practices for a remote workforce to protect your business. https://www.ricoh-usa.com/en/insights/articles/cybersecurity-best-practices-for-remote-workforce-to-protect-business (Stand: 01.10.2022).

Ricoh USA² (2022). Cybersecurity Services. https://www.ricoh-usa.com/en/services-and-solutions/cloud-it-services/ricoh-cyber-security-services (Stand: 01.10.2022).

Roche, Jorg (1992). Fachsprachen, Lesekurse und Computer. *Die Unterrichtspraxis* 25 (1), 22 – 28.

Roelcke, Thorsten (2014). Zur Gliederung von Fachsprache und Fachkommunikation. *Fachsprache 3-4*/2014, 154-178.

Rohde & Schwarz¹ (2022). Sicherer Webbrowser. https://www.rohde-schwarz.com/at/produkte/cybersicherheit/sicherer-webbrowser_232366.html (Stand: 01.10.2022).

Rohde & Schwarz² (2022). Kritische Infrastrukturen im Visier von Cyberkriminellen. https://www.rohde-schwarz.com/at/loesungen/cybersicherheit/about-us/news/news_kritische_infrastrukture_attackiert_255789.html (Stand: 01.10.2022).

Rohde & Schwarz³ (2022). Neue Ransomware-Variante: Hive-Gruppe erpresst Media Markt und Saturn. https://www.rohde-schwarz.com/at/loesungen/cybersicherheit/about-us/news-media/news/neue-ransomware-variante-hive-gruppe-erpresst-media-markt-und-saturn_255289.html (Stand: 01.10.2022).

Rohde & Schwarz⁴ (2022). Schutz vor Datenabfluss. https://www.rohde-schwarz.com/at/loesungen/cybersicherheit/about-us/news-media/news/20220603_news_protection_data-leakage_255766.html (Stand: 01.10.2022).

SafenSoft¹ (2010). Решение компании SafenSoft по безопасности банкоматов TPSecure было номинировано в категории «Новейший подход в области защиты от вредоносного ПО/антиспама. http://sns-control.ru/archiv/n/17/1418 (Stand: 01.10.2022).

SafenSoft² (2022). Защита данных в коммерческих организациях от утечки, http://sns-control.ru/security.phtml?c=805 (Stand: 01.10.2022).

SafenSoft³ (2022). Защита конфиденциального, финансового, коммерческого, маркетингового документооборота, электронной переписки в крупных компаниях и корпорациях. http://sns-control.ru/security.phtml?c=844 (Stand: 01.10.2022).

Schneider Intercomp (2022). CYBER-SICHERHEIT EINE FRAGE DES VERTRAUENS. https://www.schneider-intercom.de/technologie/cyber-security-eine-frage-des-vertrauens.html (Stand: 01.10.2022).

SecurityScorecard (2022). What is Data Exfiltration and How Can You Prevent It? https://securityscorecard.com/blog/what-is-data-exfiltration-how-to-prevent-it (Stand: 01.10.2022).

Semino, Elena; Heywood, John & Short, Mick (2004). Methodological problems in the analysis of metaphors in a corpus of conversations about cancer. *Journal of pragmatics* 36 (7), 1271-1294.

Sharifian, Farzad; Dirven, René; Yu, Ning & Niemeier, Susanne (2008). *Culture, Body, and Language: Conceptualizations of Internal Body Organs Across Cultures and Languages*. Berlin/Boston: De Gruyter, Inc.Sh

Shutova, Ekaterina; Rei, Marek; Prabhakaran, Vinodkumar (2021). *How metaphors Impact Political Discourse: A Large-Scale Topic-Agnostic Study Using Neural Metaphor Detection*. In Proceedings of the 15th International AAAI Conference on Web and Social Media [o.O.], 503-512.

Shpirer, Ronen (2018). Fortinet Covers Industrial Operation Technology and Internets of Things Security at Mobile World Congress. https://www.fortinet.com/blog/business-and-technology/fortinet-covers-industrial-operation-technology-and-internets-of-things-security-at-mobile-world-congress (Stand: 01.10.2022).

Smart-Soft (2020). Кибербезопасность в B2B: как бизнесу защититься от хакеров. https://www.smart-soft.ru/blog/kiberbezopasnost-v-b2b-kak-biznesu-zaschititjsja-ot-hakerov/ (Stand: 01.10.2022).

Stasmayer (2022). Bill the paralegal cybersecurity. https://stasmayer.com/bill-the-paralegal-cybersecurity/ (Stand: 01.10.2022).

Steen, Gerard (1999). From linguistic to Conceptual Metaphor in Five Steps. In: Gibbs, Jr. Raymond W.; Steen, Gerard (Hg.) *Metaphor in cognitive linguistics: selected papers from the Fifth International Cognitive Linguistics Conference, Amsterdam, July 1997*. Amsterdam: John Benjamins, 57 – 78.

Stolze, Radegundis (2009). *Fachübersetzen - ein Lehrbuch für Theorie und Praxis*. Berlin: Frank & Timme.

Strang, Barbara (1982). George Lakoff and Mark Johnson, "Metaphors We Live By" (Book Review). *The Modern Language Review* 77 (1), 134.

Sysware (2022). Endpoint Security. https://www.giepa.de/wp-content/uploads/2013/03/7385.endpoint_security.pdf (Stand: 01.10.2022).

T1 Cloud (2018). Сетевая информационная безопасность: как защититься от DDoS-атак. https://t1-cloud.ru/blog/informatsionnaya-bezopasnost/kak-zashchititsya-ot-ddos-atak/ (Stand: 01.10.2022).

Thibodeau, H. Paul & Boroditsky Lera (2011). Metaphors We Think With: The Role of Metaphor in Reasoning. *PLoS One* 6 (2).

Thinking Objects¹ (2022). IT-Sicherheit im Krankenhaus. https://security.to.com/themen/it-sicherheit-im-krankenhaus (Stand 01.10.2022).

Thinking Objects² (2022). Einführung eines ISMS. https://security.to.com/loesungen/einfuehrung-eines-isms (Stand 01.10.2022).

Thinking Objects³ (2022). Security Intelligence mit SIEM. https://security.to.com/loesungen/security-intelligence-mit-siem (Stand 01.10.2022).

Trim, Richard (2007). *Metaphor networks: the comparative evolution of figurative language*. Basingstoke: Palgrave Macmillan.

T-Systems (2022). 5 Hacks, mit denen Sie sich vor Identitätsdiebstahl schützen. https://blog.t-systems-mms.com/digital-stories/5-hacks-mit-denen-sie-sich-vor-identitaetsdiebstahl-schuetzen (Stand: 01.10.2022).

Tufo (2022). Tufo Cyber Security. https://tufo.at/ (Stand: 01.10.2022).

Universal Dependencies (2022). https://universaldependencies.org/u/pos/ (Stand: 01.10.2022).

Vindler (2022). https://www.vindler.de/de/services/ (Stand: 01.10.2022).

Virus-Detect¹ (2022). Лечение сайта от вирусов. https://virus-detect.ru/zakazat-lechenie-sajta.html (Stand: 01.10.2022).

Virus-Detect² (2022). КАСПЕРСКИЙ БЛОКИРУЕТ САЙТ? КАК УДАЛИТЬ САЙТ С АНТИВИРУСНОЙ БАЗЫ КАСПЕРСКОГО. https://virus-detect.ru/stati/kaspersky-blokiruet-sajt.html (Stand: 01.10.2022).

Virus-Detect³ (2022). КАК УДАЛИТЬ ВИРУС С САЙТА? ОЧИСТКА САЙТА ОТ ВИРУСОВ. https://virus-detect.ru/stati/kak-udalit-virus-s-sajta.html (Stand: 01.10.2022).

Wallis, Chris (2021). How to Keep on Top of Emerging Cyber Threats. https://www.intruder.io/blog/how-to-keep-on-top-of-emerging-cyber-threats (Stand: 01.10.2022).

Wallner Gerald (2022). CYBERANGRIFF AUF KÄRNTEN – WAREN DIE SICHERHEITSVORKEHRENGEN TATSÄCHLICH AUSREICHEND? KANN MAN SICH GEGEN ANGRIFFE WIE IM FALL BLACKCAT SCHÜTZEN? https://cybertrap.com/blog/cyberangriff-auf-kaernten-waren-die-sicherheitsvorkehrengen-

tatsaechlich-ausreichend-kann-man-sich-gegen-angriffe-wie-im-fall-blackcat-schuetzen/ (Stand: 01.10.2022).

Wang, Huili; Runtsova, Tamara & Chen, Hongjun (2013). Economy is an organism – a comparative study of metaphor in English and Russian economic discourse. *Text & talk*, 33 (2), 259-288.

Weber, Arne M. (2017). *Die Körperliche Konstitution Von Kognition*. Wiesbaden: Springer.

Weber, Karsten; Christen Markus & Herrman Dominik (2020). Bedrohung, Verwundbarkeit, Werte und Schaden. *TATuP – Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis* 29 (1), 10-43.

Whittaker, Zack (2019). Two years after WannaCry, a million computers remain at risk. https://techcrunch.com/2019/05/12/wannacry-two-years-on/?guccounter=1 (Stand: 01.10.2022).

Wizlynxgroup (2022). Cyber Security Incident Response Team https://www.wizlynxgroup.com/us/cyber-security-usa/cyber-incident-response-service (Stand: 01.10.2022).

Wiktionary[1] (2022). Krieg. https://de.wiktionary.org/wiki/Krieg (Stand: 01.10.2022).

Wiktionary[2] (2022). Fishing. https://en.wiktionary.org/wiki/fishing (Stand: 01.10.2022).

YesDefend (2022). https://yesdefend.de/ (Stand: 01.10.2022).

9. Abstract (Deutsch)

Die vorliegende Masterarbeit ist eine sprachvergleichende Analyse konzeptueller Metaphern in der Fachsprache der Cybersicherheit für die Sprachen Deutsch, Englisch und Russisch. Das Ziel dieser Masterarbeit ist es, die konzeptuellen Metaphern in der IT-Sprache am Beispiel von Cybersicherheit zu finden und zu analysieren, und zwar wie weit die Konzeptsysteme mit den zu Deutsch verwandten und nicht-verwandten Sprachen Ähnlichkeiten und Unterschiede aufweisen, und konzeptuelle Metaphern aufzudecken, die über Kulturen hinweg konsistent sind. Zu diesem Zweck wurde auf der Basis der konzeptuellen Metapherntheorie von Lakoff und Johnson in einem Korpus der relevanten Fachliteratur für die Sprachen Deutsch, Englisch und Russisch konzeptuelle Metaphern unter Verwendung der Methodik der Construction Patterns von Dodge et al. identifiziert. Für die Validierung der Ergebnisse wurde eine Umfrage unter IT-Expert*innen durchgeführt. Die zentrale Erkenntnis dieser Arbeit ist, dass sich in der Fachsprache der Cybersicherheit mehrere klar definierbare Gruppen von metaphorischen Ausdrücken identifizieren lassen, auf deren Basis man die zu Grunde liegenden konzeptuellen Metaphern formulieren kann und dass diese Formulierungen in Sprachen wie Deutsch, Englisch und Russisch praktisch identisch oder mindestens synonym sind.

10. Abstract (Englisch)

This master thesis is a linguistic comparative analysis of conceptual metaphors in the technical language of cybersecurity for the languages German, English and Russian. The goal of the master thesis is to find and analyze conceptual metaphors in IT language with focus on cybersecurity, to what extent the conceptual systems have similarities and differences with the languages related and unrelated to German, and to uncover conceptual metaphors that are consistent across cultures. For this purpose, based on the Conceptual metaphor theory by Lakoff and Johnson and methodology of Construction Patterns by Dodge et al. a corpus of relevant specialized literature in languages German, English and Russian was used to identify conceptual metaphors. A survey among IT-Experts was carried out to validate the results. The central finding of this master thesis is that several clearly definable groups of metaphorical expressions can be identified in the technical language of cybersecurity, on the basis of which one can formulate the underlying conceptual metaphors and that these formulations are practically identical or at least synonymous in languages such as German, English and Russian.

11. Anhang

11.1. Fragebogen Deutsch

Sehr geehrte Teilnehmer*innen,
Ich schreibe eine Masterarbeit zum Thema "Konzeptuelle Metaphern in der Fachsprache der Cybersicherheit" und brauche Ihre Hilfe für die Validierung der Ergebnisse.
Diese Umfrage dauert ungefähr 10 Minuten.
Alle erhobenen Daten werden ausschließlich anonymisiert und nur für den Zweck der Masterarbeit ausgewertet.
Vielen Dank für Ihre Teilnahme.
Kseniia

A conceptual metaphor is understanding one domain of experience (that is typically abstract) in terms of another (that is typically concrete)
Beispiele:
- *seine Ideen haben schließlich Früchte getragen*
- *eine Idee im Keim erstickt*
- *diese Theorie ist ausgereift*
- *ich möchte dir diese Gedanken ins Herz pflanzen*

Konzeptuelle Metapher: IDEEN SIND PLFANZEN

Demographische Daten
Alter
- unter 18
- 18 – 30
- 31 – 45
- 46 – 65
- über 65

Geschlecht
- männlich
- weiblich
- divers

Bildungsgrad
- Schule
- Fachhochschulabschluss
- Hochschule (Diplom/Bachelor)
- Hochschule (Magister)
- Hochschule (Promotion)
- Sonstiges

Berufliche Tätigkeit
- Studierende
- IT-Expert/in

Haben Sie Erfahrung im Bereich Cybersicherheit?
- Ja
- Nein

Wenn ja, wie viele Jahre?

Haben Sie Erfahrung mit konzeptuellen Metaphern? (wenn ja, welche)

Wie schätzen Sie Ihre Deutschkenntnisse ein?

- Muttersprachniveau
- fortgeschrittenes Kompetenzniveau
- Selbständige Sprachverwendung

Welche der folgenden AUSSAGEN repräsentiert diese Beispiele am besten?
Beispiele:
- *Cyber-Angriff*
- *Angriff auf die Cybersicherheit abwehren*
- *effektive Waffe gegen Cyberangriffe*

Wählen Sie eine passende Aussage oder formulieren Sie selbst
(Sonstiges)

- WAHRUNG DER CYBERSICHERHEIT IST EIN KRIEG
- CYBERKRIMINALITÄT IST EIN KRIEG
- SICHERHEITSVERLETZUNG IST EINE FEINDLICHE BEGEGNUNG
- Sonstiges

Welche der folgenden AUSSAGEN repräsentiert diese Beispiele am besten?
Beispiele:
- *verseuchte Websites*
- *virenfreie Software*
- *mit einer Schad-Software infiziert*
- *Allheilmittel gegen Cyberangriffe*
- *immun gegen Cyber-Angriffe*

Wählen Sie eine passende Aussage oder formulieren Sie selbst
(Sonstiges)

- SICHERHEITSVERLETZUNG IST EINE KRANKHEIT
- CYBERKRIMINALITÄT IST EINE INFEKTION
- BEDROHUNG DER CYBERSICHERHEIT IST EINE INFEKTION
- CYBERKRIMINALITÄT IST EINE VERSEUCHUNG
- Sonstiges

Welche der folgenden AUSSAGEN repräsentiert diese Beispiele am besten?
Beispiele:
- *Sicherheitslücke*
- *in Computersysteme einzudringen*

- *in ein Netzwerk einzubrechen*
- *Angriffe von außen*

Wählen Sie eine passende Aussage oder formulieren Sie selbst
(Sonstiges)

- o SICHERHEIT IST EIN GESCHLOSSENER RAUM
- o FREMDES NETZWERK IST EIN GESCHLOSSENER RAUM
- o SICHER IST INNEN, UNSICHER IST AUßEN
- o Sonstiges

Welche der folgenden AUSSAGEN repräsentiert diese Beispiele am besten?
Beispiele:

- *alle Daten auf dem Computer ausspähen*
- *Opfer zu ködern*
- *Spuren von Schadcode*
- *Angreifer im Netzwerk in die Falle locken*
- *Tarnung von Malware*

Wählen Sie eine passende Aussage oder formulieren Sie selbst
(Sonstiges)

- o CYBERKRIMINALITÄT IST EIN SPIEL
- o CYBERKRIMINALITÄT IST EINE JAGD
- o AKTIVITÄT DER CYBERKRIMINELLEN IST EINE JAGD
- o Sonstiges

Feedback:
Wie ist es Ihnen bei der Zuordnung von Beispielen zu Aussagen (konzeptuellen Metaphern) ergangen?

Haben Sie Anmerkungen zum Inhalt oder Aufbau dieser Umfrage oder Rückmeldungen zum Thema an sich?

11.2. Fragebogen Englisch

Dear participants, I am writing a master thesis on the topic of "Conceptual metaphors in the professional language of cybersecurity" and I need your help for the validation of research results. This survey takes about 10 minutes All collected data will be anonymized and evaluated only for the purpose of the master thesis. Thank you for participating. Kseniia

A conceptual metaphor is understanding one domain of experience (that is typically abstract) in terms of another (that is typically concrete)
Examples:
- *his ideas finally bore fruit*
- *an idea nipped in the bud*
- *this theory is ripe*
- *I want to plant these thoughts in your heart*

Conceptual metaphor: IDEAS ARE PLANTS

Demographical data

Age
- o <18
- o 18 – 30
- o 31 – 45
- o 46 – 65
- o > 65

Gender
- o male
- o female
- o diverse

Education
- o school
- o college
- o university (Bachelor)
- o university (Master)
- o university (PhD)
- o other

Professional experience
- o student
- o IT-Expert

Do you have experience in cybersecurity?
- o Yes
- o No

If yes, how many years?

Do you have experience with conceptual metaphors? If yes, what kind of experience?

How do you estimate your level of English?

- Native speaker
- Upper-intermediate
- Intermediate

Which of the EXPRESSIONS below best sums up these examples?
Examples:
- *cyber attacks*
- *weapon of cybercriminals*
- *cybersecurity arsenal*
- *cybersecurity defense and offense*

Choose the appropriate expression or write your own (Other)

- VIOLATION OF CYBERSECURITY IS PHYSICAL COMBAT
- CYBERCRIME IS WAR
- PROTECTION OF CYBERSECURITY IS PARTICIPATING IN PHYSICAL COMBAT
- Other

Which of the EXPRESSIONS below best sums up these examples?
Examples:
- *computer virus*
- *infected computer*
- *cybersecurity health*
- *treat computer virus infestations*

Choose the appropriate expression or write your own (Other)

- THREAT TO CYBERSECURITY IS A DISEASE
- THREAT TO CYBERSECURITY IS AN INFECTION
- COMPUTER IS A LIVING ENTITY
- Other

Which of the EXPRESSIONS below best sums up these examples?
Examples:
- *security gap*
- *break into network*
- *network perimeter*
- *inside and outside security threats*

Choose the appropriate expression or write your own (Other)

- BEING SECURE IS BEING INSIDE OF A CLOSED SPACE
- SECURITY IS A CLOSED SPACE
- SECURITY IS INSIDE, INSECURITY IS OUTSIDE

- Other

Which of the EXPRESSIONS below best sums up these examples?
Examples:
- *catch computer viruses*
- *hunt for cyber threats*
- *bite the hacker's bait*
- *hacker's trap*

Choose the appropriate expression or write your own (Other)

- CYBERCRIME IS A HUNT
- CYBER CRIMIALS ARE HUNTRES
- DECEIVING PEOPLE THROUGH CYBER CRIME IS GOING ON A HUNT
- Other

Feedback:
What was your experience while matching the metaphorical expressions to the conceptual metaphors?

Do you have any remarks regarding the content or the structure of the survey or any general feedback on the topic of conceptual metaphors?

11.3. Fragebogen Russisch

Уважаемые участники исследования,
Я пишу магистерскую работу на тему "Концептуальные метафоры в профессиональном языке кибербезопасности" и мне нужна ваша помощь для валидации результатов исследования. Длительность данного исследования 10 минут
Все собранные данные обрабатываются анонимно и исключительно в целях научного исследования. Большое спасибо за ваше участие. Ксения

Концептуальная метафора это концептуализирование одной области восприятия (как правило абстрактной) в понятиях другой (как правило конкретной)
Примеры:
- *его идеи наконец принесли плоды*
- *идея, подавленная в зародыше*
- *это зрелая теория*
- *я хочу посеять эти мысли в твоем сердце*

Концептуальная метафора: ИДЕИ – РАСТЕНИЯ

Демографические данные
Возраст
- <18
- 18 – 30
- 31 – 45
- 46 – 65
- > 65

Пол
- муж.
- жен.
- другой

Образование
- школа
- Среднее профессиональное
- Высшее образование (специалист/бакалавр)
- Высшее образование (магистр)
- Высшее образование (аспирантура/докторантура)
- другое

Профессиональная деятельность
- студент
- IT-эксперт

Есть ли у вас опыт в сфере информационной безопасности?
- Да
- Нет

Если да, сколько лет?

Есть ли у вас опыт в области концептуальных метафор? Если да, то какой?

Как вы оцениваете свой уровень владения русским языком?

- носитель языка
- выше среднего
- средний

Какое ВЫСКАЗЫВАНИЕ лучше всего подходит к данным примерам?
Примеры:
- *кибернападения*
- *оборона корпоративной сети*
- *арсенал хакеров*
- *армия ботов*

Выберите подходящее высказывание или предложите свой вариант (Другое)

- БОРЬБА ЗА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ – ВЕДЕНИЕ ВОЙНЫ
- ДЕЙСТВИЯ КИБЕРПРЕСТУПНИКОВ – ВОЙНА
- ДЕЙСТВИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – ЗАЩИТА ОТ ВОЕННОГО НАПАДЕНИЯ
- Другое

Какое ВЫСКАЗЫВАНИЕ лучше всего подходит к данным примерам?
Примеры:
- *дыры в безопасности*
- *входные ворота для киберугроз*
- *периметр информационной безопасности*
- *хакеры по ту сторону интернета*

Выберите подходящее высказывание или предложите свой вариант (Другое)

- ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ЗАКРЫТОЕ ПРОСТРАНСТВО
- НАХОЖДЕНИЕ В СЕТИ, ЗАЩИЩЕННОЙ ОТ КИБЕРУГРОЗ – НАХОЖДЕНИЕ В ЗАМКНУТОМ ПРОСТРАНСТВЕ
- ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – СОХРАНЕНИЕ НЕПРОНИЦАЕМОСТИ ЗАКРЫТОГО ПРОСТРАНСТВА
- Другое

Какое ВЫСКАЗЫВАНИЕ лучше всего подходит к данным примерам?
Примеры:
- *компьютерный вирус*
- *инфицирование компьютеров*
- *эпидемия трояна-шифровальщика*
- *зараженные сайты*

Выберите подходящее высказывание или предложите свой вариант (Другое)

- НАРУШЕНИЕ КИБЕРБЕЗОПАСНОСТИ – БОЛЕЗНЬ

- ВРЕДОНОСНОЕ ПО – БОЛЕЗНЬ
- ВТОРЖЕНИЕ ВРЕДОНОСНОГО ПО В СИСТЕМУ – ВТОРЖЕНИЕ БОЛЕЗНИ В ОРГАНИЗМ
- Другое

Какое ВЫСКАЗЫВАНИЕ лучше всего подходит к данным примерам?
Примеры:
- *хакеры охотятся*
- *следы злоумышленников*
- *маскировать ловушки*
- *документы-приманки*

Выберите подходящее высказывание или предложите свой вариант (Другое)

- КИБЕРПРЕСТУПНОСТЬ – ОХОТА
- КИБЕРПРЕСТУПНИК – ОХОТНИК
- ЖЕРТВА КИБЕРПРЕСТУПНИКОВ – ДОБЫЧА ОХОТНИКА
- Другое

Какое ВЫСКАЗЫВАНИЕ лучше всего подходит к данным примерам?
Примеры:
- *попасться на крючок злоумышленников*
- *интернет-мошенникам приходится следить, чтобы клюнувшие на наживку не срывались с крючка*
- *попасться на удочку киберпреступников*

Выберите подходящее высказывание или предложите свой вариант (Другое)

- КИБЕРПРЕСТУПНОСТЬ – РЫБАЛКА
- КИБЕРПРЕСТУПНИК – РЫБАК
- Другое

Фидбэк:
Как вы считаете у вас получилось соотнести метафорические выражения и концептуальные метафоры?

Есть ли у вас какие-то замечания по содержанию или структуре исследования или какие-либо примечания по теме?