# Analogical reasoning in uncovering the meaning of digital-technology terms: the case of *backdoor*

Inna V. Skrynnikova
Volgograd State University, Russian Federation
Corresponding author: i.skrynnikova@volsu.ru

Received: 18 February 2020 / Accepted: 30 April 2020 / Published: 22 May 2020

*Abstract*
The paper substantiates the critical role of analogical reasoning and figurative languge in resolving the ambiguity of cybersecurity terms in various expert communities. Dwelling on the divergent interpretations of a backdoor, it uncovers the potential of metaphor to serve both as an interpretative mechanism and as a framing tool in the ongoing digital technologies discourse. By combining methods of corpus research and frame semantics analysis the study examines the challenges of unpacking the meaning of the contested concept of the backdoor. The paper proposes a qualitatively new metaphor-facilitated mode of interpreting cybersecurity vulnerabilities based on MetaNet deep semantic metaphor analysis and outlines the merits of this hierarchically organized metaphor and frames ontology. The utility of the method is demonstrated through analyzing corpus data and top-down extracting of metaphors (linguistic metaphor – conceptual metaphor – entailed metaphor – inferences) with subsequent identifying of metaphor families dominating the cybersecurity discourse. The paper further claims that the predominant metaphors prompt certain decisions and solutions affecting information security policies.

***Keywords:*** analogical reasoning, figurative language, conceptual metaphor, metaphor corpus, contested concepts, cyber security, backdoor

## 1. Introduction

Cybersecurity has long been recognized as a pressing issue resulting in a fierce ongoing debate over strong computer encryption of communications and data. The reasons for divergent interpretations of encryption lie in the fact that, on the one hand, it can both ensure security and privacy for individuals but, on the other and, make it challenging for the intelligence and law enforcement communities to perform their surveillance and investigative duties. The most divisive question arising in this context is whether encryption systems should be required to

DOI: https://doi.org/10.4995/jclr.2020.12921

have a "backdoor" to provide the government with special access to encrypted information. Another related problem that recent research has revealed is that users fail to understand the security properties provided by encryption and the related terms. It can be explained by their poor explanations focusing solely on structural mental models consequently yielding ambiguous concepts. Such conceptual imprecision ultimately afflicts cybersecurity (Betz and Stevens 2013), and there is still little consensus on the meanings of concepts like 'cybersecurity', 'cyberspace' and 'backdoor' despite numerous attempts to develop common vocabularies. Therefore, this calls for the need to be sufficiently wary of the ways in which discourse around cybersecurity structures our thinking and to prevent it from channelling us into modalities that are confusing and misleading. Research communities involved should raise the efficiency of their communication to facilitate a meaningful dialogue between professionals and policymakers.

Numerous studies have shown the powerful potential of analogical reasoning in uncovering the essence of ambiguous and contested concepts through explaining abstract and "blurry" entities in terms of concrete, familiar and embodied concepts. Such meaning transference through corresponding inferencing enables us to grasp the intricacies of complex disembodied phenomena. Creating adequate analogies should be seen as a crucial task in constructing cybersecurity discourse and the appropriate use of analogical reasoning should, therefore, be a priority for those involved in cybersecurity, with due attention being paid to metaphor as a specific form of analogy. Rhetoric surrounding cybersecurity is currently dominated by geopolitical and Cold War metaphors that frame the Internet in terms of national security. It is widely applied to justify the militarization of cyberspace and state surveillance (Betz and Stevens 2013) which results in unnecessary militarization contributing to mismanagement in cyber matters. The metaphors that politicians and the media use when talking about cybersecurity both reflect and shape how it is reasoned about and prompt certain decisions affecting not only professional communities but also general public.

Recent years have seen unprecedented growth in national governments' numerous endeavours to gain ubiquitous access to encrypted data which IT specialists and privacy advocates fiercely oppose. The parties to this ongoing conflict, generally referred to as *Crypto Wars*, resort to figurative language to effectively frame the resulting disagreement with their adversaries. Good examples of figurative terms are *Cloud, Big Data, Piracy,* and *Virus,* which have long become common in the debates about digital technologies. It is quite obvious that they are metaphors originating from other fields than technology.

Given the ubiquitous, pervasive and mostly unconscious conceptual nature of metaphor which has been repeatedly shown since Lakoff and Johnson's (1980) seminal book *Metaphors we Live by*, further exploration of the metaphors we use in the cybersecurity domain can be helpful in improving our reasoning about it in several ways. Primarily, deep semantic analysis of metaphors provides our deeper insights into the value and limitations of the concepts we have mapped from other domains into the cybersecurity domain. Another opportunity the study of metaphors presents is coming up with less common or new metaphors which may subsequently feed the creativity of researchers and policy developers. Tested metaphors that "do their work" efficiently might be further translated into a whole set of new models or concepts for addressing cyber security problems. Finally, a metaphor's heuristic function is to serve as an explanatory tool facilitating clearer understanding of abstract cybersecurity concepts by the non-specialists who might not be sufficiently tech-savvy to embrace all the nuances of cyber terms.

The claim the paper is trying to make is that a metaphorical perspective adopted when thinking about cybersecurity can reveal the "weak points" of current approaches in the digital technologies discourse and propose alternative metaphorical narratives suggesting novel creative solutions to cyber issues.

## 2. Related work

### 2.1 Corpus-based metaphor research

A great body of research has examined metaphor across genres, with copious studies being done in English. Manual qualitative analyses dealing with hand annotation of texts as well as corpus methods have been extensively applied to analyze when and how metaphor is used. The Metaphor Identification Procedure (Pragglejaz Group 2007; Steen 1999) is widely used across various genres and discourse (Demjén, Semino, and Koller 2016; Steen, Dorst, Herrmann, Kaal, Krennmayr, and Pasma 2010). Another approach relying on more traditional corpus linguistic methodologies (Stefanowitsch and Gries 2006; Deignan 2005; Lederer 2013; Martin 2006; Philip 2004) use concordances, collocation patterns, frequency counts and keyword analysis to identify potentially metaphoric uses of target words. Computational linguistics major focus is elaborating automated means of metaphor identification across larger or more diverse corpora.

Despite the fact that specific methodologies and goals vary, most natural language processing (NLP) approaches seek for improvements in recall and precision mechanisms when it comes to automated linguistic metaphor identification. Some studies apply statistical cluster methods (Shutova, Teufel and Korhonen 2012; Shutova and Sun, 2013) for metaphor identification. Others (Gutiérrez, Shutova, Marghetis, and Bergen 2016) employ compositional distributional semantic vector space models or use the selectional preference of verbs, and clusters of nodes derived from WordNet senses (Mason 2004). Alternative methods include word sense disambiguation-based approaches (Krishnakumaran and Zhu 2007), neural nets (Do Dinh and Gurevych 2016), maximum entropy classification combined with hand-annotation of metaphoricity (Gedigian, Bryant, Naryanan, and Ciric 2006), knowledge-representation models (Martin 1994), etc. Such automated approaches are undeniably useful as they meet specific research needs and textual genres, and are characterized by high recall and precision in automated metaphor identification which can be explained by their reliance on lexical and semantic resources, e.g. WordNet in Lönneker (2003), SOMO ontology in Dunn (2013). Still, they are not without flaws when one has to address specific questions about the functions of metaphor in a particular language context or cognitive and social domain (David and Matlock 2018).

Unlike all the approaches described above, MetaNet (large-scale automated metaphor identification system), the present paper relies on methodologically, treats semantic frames as central to defining metaphor. A semantic frame is defined as a knowledge schema through which “a word’s meaning can be understood only with reference to a structured background of experience, beliefs, or practices, constituting a kind of conceptual prerequisite for the meaning” (Fillmore and Atkins 1992, 76–77). It emerges as a part of FrameNet (Fillmore, Johnson, and Petruck 2003). MetaNet presents metaphors as frame-to-frame mappings, and therefore uses frame elements and lexeme-to-frame evoking patterns. (David 2016; Stickles et al. 2016).

### 2.2. Cybersecurity discourse studies

Previous studies on cybersecurity discourse (Wolff 2014; Gill 2018) point out that the most common metaphor in cybersecurity is that of the fortress where valuable information is kept within a walled enclosure. It is usually encircled by a moat, accessed by portals, gates or doors, and guarded by watchmen whose task is to keep out the unauthorized. Another pervasive metaphor is that of cops and robbers (vandals) who break into the house and steal valuables. Then the scenario frequently suggests that forensic measures are taken to track them down, after which they are identified and legally prosecuted. A third common metaphorical way of thinking about cybersecurity is in terms of warfare where enemies, using various weapons and tactics, attack, steal or destroy property (or commit espionage) in order to achieve some strategic goal.

Spatial metaphors started their life when the term *cyberspace* was invented in 1982 by science fiction writer William Gibson. It became commonly applied to the Internet and the World Wide Web in the 1990’s. It is a good example of how a metaphor—mapping of one domain (three dimensional space) to another domain (computer networks)—has become so pervasive that we are hardly aware of it as a metaphor any more and use it unconsciously. The newly formed US Air Force Cyber Command describes its mission in ways that imply that cyberspace is just another class of physical spaces called “domains”:

> Cyberspace is a domain like land, sea, air and space and it must be defended. Although we've been operating in cyberspace for a very long time—since the invention of telegraph, radio and radar—we now conduct the full range of military operations in this domain. Just as the sea domain is characterized by use of water to conduct operations, and the air domain characterized by operations in and through the atmosphere, the cyber domain is characterized by use of electronic systems and the electromagnetic spectrum.[1]

According to J. Wolff, most cybersecurity analogies derive from one of three metaphors: the burglar metaphor, the war metaphor, and the health metaphor. These security metaphors do not stress the responsibilities of an individual actor, or the function of a specific technological process), but rather the nature of the threat, or problems, posed by computer networks (Wolff 2014). She argues that comparisons of Internet crime to burglary draw on the notion of breaking into a protected space and apply it to a domain in which both the ideas of “breaking” and “entering” have a much less physical manifestation and are therefore significantly less clearcut.

[1] http://www.afcyber.af.mil/library/factsheets/factsheet.asp?id=10784

Many descriptions and explanations of how computer networks should be defended derive from these analogies to protecting houses against burglars and fortifying medieval castles. However, the burglar metaphor fails to provide meaningful guidance for how to protect computer systems because some of its central assumptions about the nature of theft and the best ways to stop burglars do not map neatly from castles onto computers.

The types of defense implied by the burglary metaphor derive from standard home security tools—locks, alarms, guard dogs, fences. For instance, Landwehr et al. (1994) describe several different computer security flaws in terms of gates and fences: "Providing secure operation of a computer often corresponds to building fences between different pieces of software (or different instantiations of the same piece of software), to building gates in those fences, and to building mechanisms to control and monitor traffic through the gates".

While the commercial market for defense technologies is dominated by the burglar metaphor, the international political arena increasingly prefers the war metaphor. It casts computer security and defense efforts in a very different light than the burglar metaphor. The latter implies a set of attackers who are concerned primarily with financial gain by means of theft, the former - a set of powerful, well-organized malicious actors (including national governments, promoting political or ideological agendas by means of physical violence). Such a contrast suggests the reasons why the war metaphor has become increasingly popular in discussions of cybersecurity and ways in which it is misleading in this context.

The health metaphor likens cyber threats to those caused by a very different type of villain: a disease. The most pervasive lexicalizer of this metaphor is the term *computer virus* coined to capture the disease-like ability of some malware to replicate itself. Like microbial diseases, computer security threats can spread rapidly, evolve in reaction to new and improved defenses, and be addressed with defensive measures ranging from preventative care to treatment and quarantine of active infections. On the other hand, the metaphor sometimes seems less apt. Some of the most crucial defenses against disease have no clear counterpart in computer systems. Hallam-Baker (2008) points out that while the human race is protected from biological diseases by its genetic diversity, most computers run the same few operating systems providing very little diversity in the "computing gene pool." For companies, countries and individuals seeking to protect their own particular computer systems from threats, this analogy provides no useful insight.

More novel and embodied cybersecurity metaphors derive from the field of biology. Broadly speaking, biological metaphors suggest thinking of cyber systems as instances of complex, adaptive systems similar to our biological systems. A more specific example of such systems is the ecosystem, a complex system of interdependent species in populations in a particular kind of environment. The concept drawn from ecosystem studies is that of biodiversity. It prompts the idea that systems with diverse components are likely to be more stable, resilient, and adaptable to change. An alternative example is biological immune systems, the subject increasingly reflected in computer science literature and stressing how the mechanisms of immune processes systems can be imitated in hardware and software systems.

Another related metaphor is that of programmed cell suicide in multicellular organisms. It is particularly helpful in explaining how computers might be programmed to recognize if they have become infected and detach themselves from their network. The human health/infectious diseases metaphor has been pervasive in the encryption discourse. Discussions of computer *hygiene* as a means of preventing the spread of *infection* go back at least to 2007, but hygiene is well on its way to becoming obsolete.

This list of cyber security metaphors is far from exhaustive. It serves as a starting point for further exploration and search for newer and more powerful metaphorical models capable of addressing the digital technologies in a more coherent and effective manner.

## 3. Scope, Method and Data

The aim of the present study is to reveal the role of the *backdoor* metaphor both as an interpretative mechanism enabling to make sense of this obscure term and as a framing tool foregrounding certain intended aspects of this phenomenon while deliberately ignoring other ones. Based on Ch. Fillmore's frame semantics analysis, G. Lakoff's neural theory of language and metaphor (the four-step metaphor analysis procedure), theory of metaphoric neural cascades and drawing evidence in English from two corpora, a general corpus (the GLoWbE corpus: Davies, 2013; Davies and Fuchs, 2015) and a specialized, obtained by random sampling, IT corpus of textual and visual data (IT-related journals, professional security and IT blogs, forums, political debates, cartoons, memes, etc.), the study examines the challenges of unpacking its meaning resulting from the contested nature of the backdoor. The Gigaword corpus in English was chosen due to its availability, sufficient size, representativeness in the domain of cyber security, which is a topic frequently appearing in the newswire data.

The paper proposes a qualitatively new metaphor-facilitated mode of interpreting cybersecurity vulnerabilities in general and backdoor in particular with regard to various, often controversial, aspects and diverging interpretations of backdoors to be highlighted in a specific context. Following the line of the Lakoffian deep semantic analysis and by applying a four-stage top-down metaphor extraction procedure (linguistic metaphor → conceptual metaphor → entailed metaphor → inferences) we extracted metaphors from the specialized corpus, both textual and pictorial (business and technology press as well as from transcripts of expert discussions at CyberFests held between 2015-2019, internet blogs and the websites of IT security professionals). The resulting specialized metaphor corpus comprises 236 textual and 52 pictorial examples of metaphors representing backdoors. The deep semantic analysis of the backdoor metaphor assumes the following three levels: *descriptive* consisting in identifying the frames applied to refer to backdoor; *interpretative* establishing frame-to-frame mappings and *motivational (inferential)* defining certain intentions of cyber security actors.

The approach presented above seems particularly promising not only in revealing possible conceptualizations of this ambiguous phenomenon but also in identifying certain inferences as well as policymakers and cyber security specialists' motivations for resorting to a particular metaphor (which is not possible at the purely linguistic surface level of the semantic analysis). Although the corpus is limited, it may point out to a clear pattern of conceptualization and provide an accurate picture of the cybersecurity natural discourse. In our view, such methodological procedure enables us to reveal some "weak points" in addressing the encryption problems and prompt the novel ways of addressing them more effectively. The analysis of frame-to-frame mappings relies heavily on MetaNet repository, elaborated in International Computer Science Institute at University of California, Berkeley, and FrameNet database. The beauty of the ontology of metaphors and frames in the MetaNet, the current paper mainly relies on, lies in the fact that it applies a computational method which is organized in terms of metaphor cascades, i.e. pre-existing packages of hierarchically organized primary and general metaphors that co-occur. It shows the type of relations between the activated frames which work together to provide a computationally tractable mechanism for automatically discovering new metaphoric expressions in texts (David, Lakoff, and Stickels 2016).

The MetaNet is structured in such a way that the source and target domain frames of metaphors are arranged in an inheritance network relative to each other, where specific frames are subcases of more general ones. For instance, as shown in Figure 1, *Information insecurity* is a specific type of *Social Problem*, while *Disease* is a more specific type of *Physical Affliction*. The hierarchical pattern shows that information insecurity is a disease is a subcase of both social problems are physical afflictions.

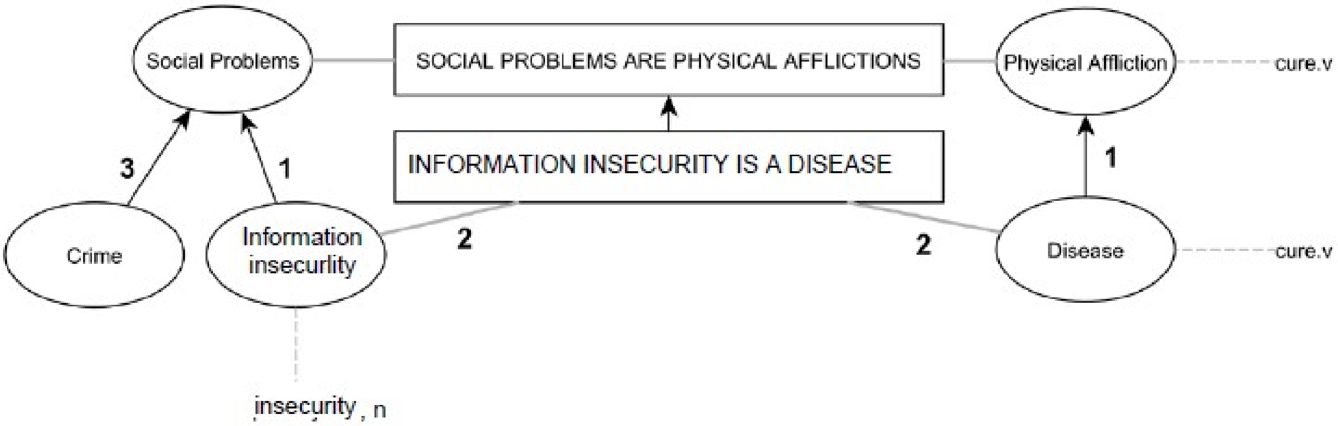


FIGURE 1. METAPHOR INHERITANCE DIAGRAM FOR INFORMATION INSECURITY IS A DISEASE WITH RELATIONS TO LEXICAL ITEMS.

The presented methodological approach differs from the existing corpus-based methods to metaphor in such a way that lexical items do not map to metaphors as proposed by Stefanowitsch (2006) but are associated with frames, which in their turn are associated with metaphors. Another crucial difference is that metaphoricity of a phrase is determined by a cascade exploiting frame inheritance networks and frame-to-frame relationships (Dodge et al. 2015). This method can be further expanded to cover other languages since lexical items are associated with the existing frame and metaphor structures.

## 4. The Symbolism of *door*

### 4.1. The power of the door metaphor

The door metaphor in general is pervasive across languages suggesting:

- entering another world
- bringing changes
- presenting opportunities
- giving hope
- an invitation to somewhere
- keeping a mystery (when closed or locked)
- giving choices (when you are in front of several ones)

Doors are known to be ways in or ways out of or to something. However, we commonly do not attach much significance to doors and their symbolism when we get to it – unless it is a particularly eye-catching one.

However, doors are entrances for coming people and opportunities and exits for going to other places or worlds which were formerly unknown. They may be open to welcome a person, shut or even locked suggesting unwillingness of hosts of the house to see or welcome someone. Being unlocked they stand for the insecurity or vulnerability of people inside a house in contrast to locked doors which make people outside feel unwanted, insecure or excluded from one's immediate circle. In this way, doors separate and connect, demark and open, denoting passage and movement. Similarly, doors only have meaning in relation to the people that move through them, otherwise they are meaningless.

In terms of their location, we distinguish between front doors, back doors and side doors. The former are public, official and formal, mostly used by strangers and serve as the main entrance, where you expect to be welcomed. The latter are more intimate and casual, designed for family and friends, so they are unofficial, immediate, however, they may sometimes be neglected. Back doors are used to refer to an indirect way of achieving something, so that people do not know about it and thus cannot object to it.

Such linguistic expressions as "a foot in the door", "knock on doors" and "open up doors" illustrate the idea of generating opportunities, while the idea of closing opportunities is conveyed in such expressions as "show someone the door", "have the door slammed in ones face", and "shut the door".

### 4.2. The case of *backdoor*

The most pervasive and yet contested term (Jenner 2018) within a long series of conflicts and power struggles over encryption technologies between national security agencies and privacy advocates is the *backdoor*. The former claim that having a backdoor in encrypted systems might provide enhanced information security while the latter treat backdoors as a means of unauthorized access to personal data. Such a discrepancy in interpretations cannot contribute to better understanding of the term, and this is where apt metaphors as the most powerful framing tools employed in the digital discourse serve to perform the explanatory, interpretative as well as transformative and manipulative functions (Kupers 2013; Skrynnikova et al. 2017) in uncovering the essence of abstract and frequently ambiguous concepts. Therefore, the following research questions inevitably arise:

Q1 - What normative or political baggage do they carry?

Q2 - How does this vocabulary shape the emerging digital society?

Q3 - What are the assumptions and meanings of metaphors in the digital era?

But before delving deeper into the conceptual and figurative underpinnings of the term we find it appropriate to look more closely into its origins.

Originally, the term "backdoor" started its life along with "trapdoor" in the 1980s and was used to refer to secret accounts and/or passwords created to enable someone unknown access into a system. Such a state of affairs raised serious public concern about instances when a malicious programmer or system administrator was able to leave behind a trapdoor and subsequently use it to get into a system after they were officially working on it. Later on, in early days of the crypto wars (throughout the 1990s) privacy advocates repeatedly referred to the government's key proposals (stating that the government or private companies would keep copies of people's decryption keys) as a "backdoor" into encryption.

Such use of the term "backdoor" clearly suggests that it can broadly refer to any mechanism someone designs into a system enabling for access via bypassing normal security measures. And although historically the word "backdoor" was frequently applied to refer to secret ways to access a system, a backdoor does not need to be secret. An early, good but notorious example is the American government's ability to bypass the Clipper Chip's security (a dedicated chip for encrypting telephone communications on lines where secrecy and privacy were important, for example in R andD or at an embassy, made by the Mykotronx company under the direction of the NSA) openly in the 1990s. But it was still a backdoor, a mechanism designed to allow access through bypassing security features. There is no need for a backdoor to stop being a backdoor just because it is well-known and public. The most famous backdoor in recent cryptographic affairs is the Dual EC DRBG standard secretly designed by the NSA to include a deliberate mathematical flaw which only they could exploit using a secret backdoor key to spy on anybody using it. Although it became known to the public, we still call it a backdoor.

Unlike other vulnerabilities, known today, the backdoor is unique for several reasons. This concept seems to be quite simple to state, however, a closer look leads us to conclude that pinning down a comprehensive definition may be a challenging task. Similar to the back door of a house, a crypto backdoor (generally written as a single word) is a way to circumvent the locks and protections of the main entrance in order to get in unhindered and make oneself comfortable. A backdoor can be found in a phone, laptop, router, security camera and other devices.

But backdoors appear to be fundamentally different from other means of bypassing traditional security distinguishing it from a bug or administrative access:

- backdoors operate without the consent of the computer system's owner;
- the actions performed by backdoors are at odds to the stated purpose of the system;
- backdoors are under the control of undisclosed actors unlike viruses and worms which operate more or less autonomously, harvesting information or spamming your contacts.

Backdoors that track the original definition of the word—i.e., secret accounts or passwords—are still widely used. Researchers found built-in, secret ways of accessing some D-Link routers, Juniper and Fortinet firewalls, among other products. Interestingly enough, but what the FBI is trying to force Apple to do in the current case does not share all of the features of classic backdoors. It prompts the public to question how well the term applies here. Some point to the fact that the government's attempt to undermine security in this case is not illegal while others claim that the software in question would be developed subsequently rather than ahead of time. Still others suggest that the true backdoor is Apple's ability to approve software updates changing a locked device's security properties but not erasing its encryption keys. Such lack of unanimity derives from absence of a clear definition of a backdoor, the term which have both influenced and been influenced by popular culture and the fact that government officials did not learn the lessons of the first crypto war – that it is technically impossible to design a "backdoor" that doesn't compromise security. This is where the role of analogical reasoning and metaphor as a powerful interpretative mechanism is becoming critical in resolving the mystery of backdoor and its underlying meaning.

### 4.3. The deep semantic analysis procedure

The four-stage deep semantic analysis procedure of the door metaphor is exemplified below.

Surface linguistic metaphor example:

(1) The ceasefire agreement has opened distant doors to further talks between the two parties.

Conceptual metaphor:

PRESENTING OPPORTUNITIES is OPENING A DOOR

This conceptual metaphor is a specific case of the more generic OPPORTUNITIES are PORTALS metaphor

Entailed metaphors:

OPPORTUNITIES are PORTALS (DOORS)

LOST OPPORTUNITIES are CLOSED (LOCKED) PORTALS

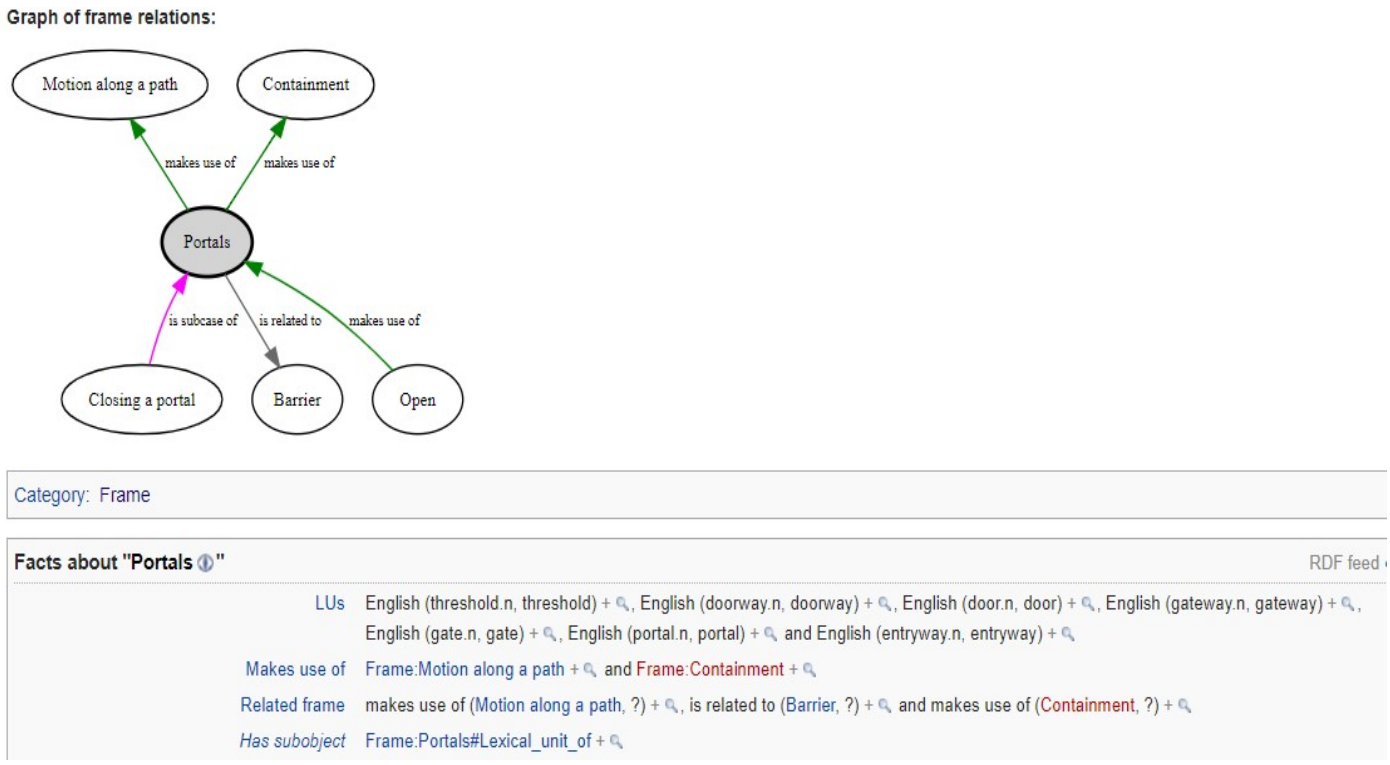
PRESENTING OPPORTUNITIES is OPENING A PORTAL (A DOOR)

FINDING NEW OPPROTUNITIES is CROSSING A THRESHOLD OF A DOOR

Metaphorical inferences:

- Entering new doors may present someone with an opportunity to see and learn something new or formerly unknown.
- Looking for opportunities one should be careful while choosing a door to enter as a wrong door may imply certain dangers or complexities.
- Some opportunities may sometimes be hidden, so seeing a closed door, be sure to knock and check if it can be opened.

The relations of the Portal frame with other frames, facts about portals and its lexical units, are shown in Figure 2 in the way they appear in the MetaNet repository.



Category: Frame

Facts about "Portals"

RDF feed

| | |
|---|---|
| LUs | English (threshold.n, threshold) +, English (doorway.n, doorway) +, English (door.n, door) +, English (gateway.n, gateway) +, English (gate.n, gate) +, English (portal.n, portal) + and English (entryway.n, entryway) + |
| Makes use of | Frame:Motion along a path + and Frame:Containment + |
| Related frame | makes use of (Motion along a path, ?) +, is related to (Barrier, ?) + and makes use of (Containment, ?) + |
| *Has subobject* | Frame:Portals#Lexical_unit_of + |

FIGURE 2. GRAPHIC REPRESENTATION OF THE PORTALS FRAME RELATIONS (adopted from MetaNet repository).

## 5. Defining a backdoor

Far from being fully grasped by laymen, interpretations of the term *backdoor* may vary even within the IT community ranging from 1) an undocumented portal for an administrator to enter the system to troubleshoot in software or a computer system to 2) a secret portal for hackers and intelligence agencies to gain illicit access; to 3) a technique in which a system security mechanism is bypassed undetectably to access a computer or its data. Such divergence cannot but contribute to a myriad of conceptualization patterns and give rise to considerable confusion urging both the cyber people and policy makers to seek for unanimity in addressing the security issues and general public to be more aware of possible personal information leaks.

I argue that diverging interpretations of the backdoor derive from the lack of the clear and comprehensive definition of the term and propose a three-layer structure of the backdoor metaphor. At its core lies the original and most basic understanding of the *back door* as the rear door to a building. Further metaphoric extension, exemplified in the phrase *by the back door,* consists in stressing indirect and illicit means of achieving something. The latter, in its turn, results in understanding the backdoor as a mechanism for bypassing security, and more narrowly encryption.

The twofold usage of the term *backdoor* in the following headline by British technology news website *The Register* from 30 November 2016 should not be dismissed as merely a mediocre pun. The headline's wordplay sheds some light on the multiple layers of metaphorical meaning the IT term *backdoor* carries.

(2) UK's new Snoopers' Charter just passed an encryption backdoor law by the backdoor (The Register, November 2016)

Our corpus data suggest that the interplay of the literal and metaphoric meaning of backdoor highlights the multiple facets of metaphoricity encoded in the backdoor as viewed by IT security experts. The illicit or undisclosed manner of obtaining data stressed by this cyber security term is then extended to other types of activities going far beyond the field of digital technologies and making the way for the term in other types of discourse as shown in (3) and (4)

(3) Valley lands rare 'backdoor capital raise' with latest acquisition (American Banker, June 2019).

(4) Lawmakers need to reject this backdoor attempt to arm teachers (Penncapital Star, May 2019).

## 6. METAPHOR LAYERS

Let us consider each layer of the backdoor metaphor more closely starting from the core layer treating back door as a rear door to a building. Although when used within the realm of IT, the term *backdoor* refers to a highly technical and complex concept, it still borrows its meaning from everyday life. Another argument we put forward is that relating the backdoor in encryption to the back door of a building immediately creates some sort of an image enabling basic understanding of this technical concept, making it easier for those less advanced in information technology to grasp the meaning of the backdoor. This makes the backdoor metaphor particularly useful and powerful, serving as an interpretative tool. However, interpretations may vary depending on a position someone takes concerning the encryption mechanisms applied. From a network administrator's perspective, for example, backdoors are seen as a program or application used for troubleshooting or official use. This results in a positive view of the phenomenon treated as an alternative way for insiders to solve some unauthorized access-related issues. Network administrators may also use backdoors to easily access different devices on the network for the same purpose. At the conceptual level, this view is supported by the following metaphor:

Conceptual metaphor

SOLVING AN ENCRYPTION PROBLEM is ENTERING THROUGH A BACK DOOR

Entailed metaphors

ENCRYPTION MECHANISMS are DOOR LOCKS
NETWORK ADMINISTRATORS are DOOR LOCK INSTALLERS
PROTECTING A NETWORK is USING A BACK DOOR
INFLICTED INSECURITY is BROKEN DOOR LOCKS

Inferences

- Backdoors should be left to ensure a user to access and control a computer or mobile device, usually remotely over a network or the Internet.
- Having a backdoor is gaining control of a system as it exploits undocumented processes or features in an operating system or installed program.

However, the metaphor may be also potentially misleading, as it creates imperfect analogy which may result in false inferences and assumptions, oversimplification or even an instrumentalisation of the term. In contrast to a front door, a back door can be understood as an alternative, unofficial point of entry. If we go back in time, we can well remember that in past centuries back doors were used by servants. In rural areas, family members and frequently visiting neighbours entered through the back door to avoid carrying dirt through the front door, which was reserved for more formal visits. A more recent example that comes to mind today is the back door to a restaurant, where goods are received and waiters take a quick smoke break. Another example is a popular nightclub, where renowned musicians are ushered in through the back door while underage fans try to bypass the security person. These examples all point to one implied characteristic of the back door: it is meant to be used only by people who are somehow legitimised to do so. This authorisation is often enforced by controlled access to the keys.

According to many IT specialists, this is where the backdoor metaphor fails to adequately describe the technical reality. A backdoor into one "building" would inevitably be a backdoor into all other similar "buildings". In this view, the backdoor metaphor is misleading if it is not used in combination with the idea of a "master key". The master key metaphor was also used by Apple CEO Tim Cook in 2016 when the FBI and Apple clashed over the encrypted iPhone. The technique required to open the San Bernardino shooter's iPhone "would be the equivalent of a master key, capable of opening hundreds of millions of locks" argued Cook in an open letter in response to the FBI's demands.

Still, the master key metaphor, in its turn, is not without its problems. IT security experts suggest the dilemma that governments fail to acknowledge goes as followed: "We cannot build a backdoor that only works for a particular type of government, or only in the presence of a particular court order. Either everyone gets security or no one does. Either everyone gets access or no one does." (Bruce Schneier, Washington Post, February 18, 2016) This reasoning goes against the most basic understanding of a back door as an alternative entry point, which can only be accessed by authorized parties in possession of a key.

When analysing the term *backdoor* in the context of encryption, it is not sufficient to think only about the physical back door. It leads us to argue the presence of the middle layer of the backdoor metaphor exemplified in the linguistic expression *by the back door.* Long before any disputes over locked iPhones, the term was already being used metaphorically to describe "a secret, furtive, or illicit method, manner, or means". This is also the case in the aforementioned headline:

(5) An encryption backdoor law is passed by the backdoor.

In different contexts, the Trump administration has inspired several headlines making use of this metaphor. For instance, the Los Angeles Times wrote that Donald Trump was plotting "another backdoor effort to gut Obamacare's consumer protections" while the Huffington Post commented on "Trump's Backdoor Muslim Ban". When referring to the law making process, the phrase is often used to highlight and criticise a supposedly intentional lack of transparency that impedes public scrutiny. In this sense, the middle layer adds a negative connotation to the term by suggesting the government is working against its citizens. Thus, government officials have reasons to steer clear of the term *backdoor* in IT issues and often do.

The idea of gaining access to private or sensitive data by hackers and intelligence agencies is commonly communicated through the secret portal metaphor. Interestingly enough, this metaphorical model places intelligence agencies along with hackers undermining the image of the former in the eyes of wide public. Therefore, it would be logical to differentiate between conceptualizing a backdoor as intervening people's privacy by intelligence agencies and as breaking a physical object by hackers. The critical public view of the government stance of backdoors is obvious in the following example.

<u>Surface linguistic metaphor:</u>

(6) This mass transformation of the private self to the networked self suggests that even a state-mandated backdoor to all iPhones would not lead to a qualitative shift in our lives.

(7) The law didn't require it to create a "backdoor" to enable the government to unlock its customers' encrypted devices

<u>Conceptual metaphor</u>

INTERVENING PRIVACY is OPENING SOMEONE'S BACKDOOR

<u>Entailed metaphors</u>:

ACCESSING PRIVATE DATA is SEEING THINGS KEPT SECRETLY BEHIND THE BACKDOOR

OBTAINING SECRET DATA is SNEAKING INTO SOMEONE'S TERRITORY UNNOTICED

RIGHTS are TERRITORIES

<u>Inferences:</u>

- Encryption laws should be abolished or banned.
- People's privacy must not be violated.
- Government powers to access personal data should be effectively controlled.
- Secret access of public authorities to personal data is violation of citizens' rights to privacy.

The government stance on the issue promotes an opposite view facilitated by MAINTAINING PUBLIC SECURITY is BEING ABLE TO ENTER A BACKDOOR metaphor, which inevitably activates the resulting entailed metaphors and produces corresponding inferencing.

Entailed metaphors:

ABILITY TO MAINTAIN PUBLIC SECURITY is POSSESSING KEYS TO ALL DOORS

INTELLIGENCE AGENCIES are KEY POSSESSORS

Inferences:

- Passing encryption laws should be seen as a merit.
- Personal data and sensitive information should be accessible for security reasons.
- Governments and businesses are expected to share a single decryption key for personal data and sensitive information.

Thus, in our view, this case study can serve as a useful testing ground for effectiveness of the applied method. Specific metaphoric expressions some of which are typical of each viewpoint involved in the debate characterize the backdoor debate rhetoric.

As the corpus data show, one of the pervasive metaphorical patterns to refer to hackers' illicit access to personal data is ILLICIT ACCESSING DATA is BREAKING A BACKDOOR which makes use of the more generic metaphor ACCESSING DATA is ENTERING A PORTAL.

Surface linguistic metaphor:

(8) Some 2.3 million customers were broken through that backdoor, blamed on hackers who reportedly targeted tech giants.

(9) Hackers pushed a secret backdoor in Asus's update software.

Conceptual metaphor:

ILLICIT ACCESSING DATA is BREAKING A BACKDOOR

Entailed metaphors:

DATA is a PHYSICAL OBJECT

ILLEGAL ACTIVITIY is BREAKING A PHYSICAL OBJECT

GAINING ILLICIT ACCESS TO DATA is BREAKING A HOUSE DOOR

CAUSING MORAL DAMAGE IS CAUSING PHYSICAL PAIN

DAMAGED DATA is a BROKEN OBJECT

Inferences:

- Illegal activities must be prosecuted.
- Data need to be adequately protected.
- Personal data integrity is a prerequisite for information security.
- Software should be improved to withstand an ever-expanding range of hacker attacks.

Since illegal activities are conceptualized as crimes, ILLICIT ACCESSING DATA is BREAKING

A BACKDOOR metaphor is a part of the CRIME scenario. The graphic representation of frame-to-frame inheritance relations within this scenario is shown in Figure 3 below.

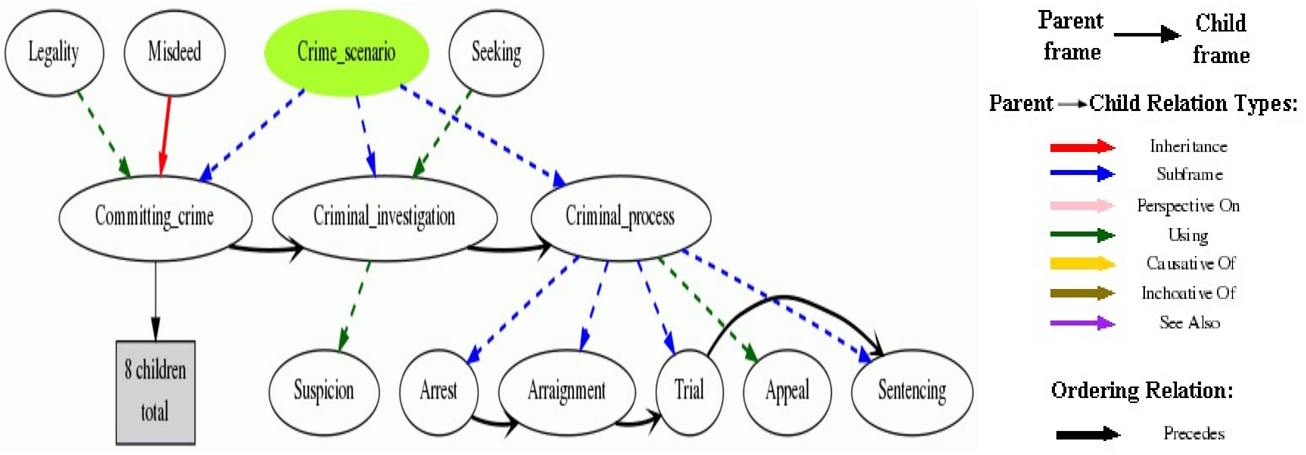
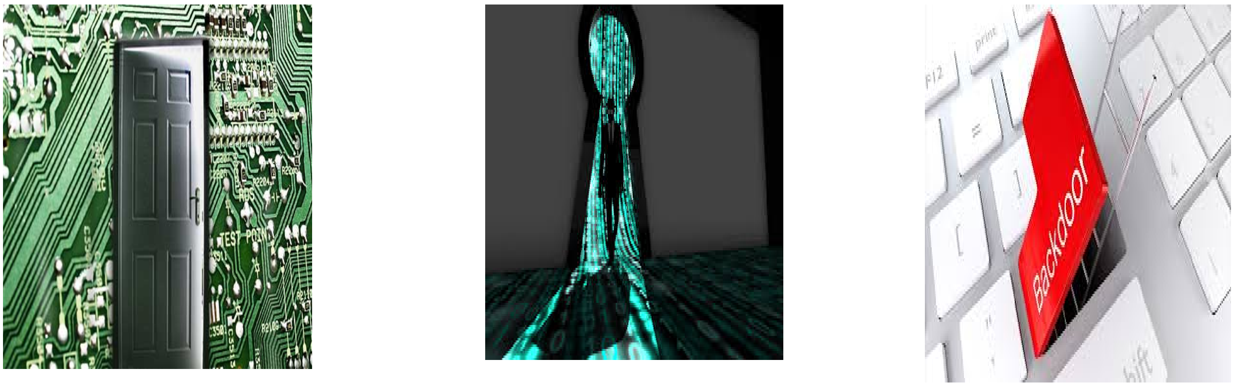


FIGURE 3. FRAME-TO-FRAME INHERITANCE RELATIONS WITHIN THE CRIME SCENARIO.

The outer layer of the backdoor metaphor is manifested in the use of backdoor as an IT term. Technical definitions of the term *backdoor* remain somewhat ambiguous themselves in two regards. Firstly, general definitions of the backdoor in computing remain notoriously vague. A specific backdoor needs to be *hidden*; it can only remain an alternative entry point if its technical properties are not widely known. Secondly, definitions vary with regard to the purpose and the typical users of backdoors. Some definitions focus solely on backdoors as a tool used by *attackers* or *hackers* with malicious intent. But there are also examples for broader definitions: "A backdoor in software or a computer system is generally an undocumented portal that allows an administrator to enter the system to troubleshoot or do upkeep. But it also refers to a secret portal that hackers and intelligence agencies use to gain illicit access". This definition distinguishes between but also includes both *legitimate* and *illegitimate* backdoors. Interestingly, the definition mentions hackers and intelligence agencies in the same breath.

Owing to the multimodal nature of metaphor, it is strikingly effective in providing not only linguistic but also visual representations of obscure unfamiliar terms. The three pictures below feature visual metaphoric representations corresponding to three possible interpretations of a backdoor in IT.



**an undocumented portal** **a secret portal for hackers** **a technique of bypassing security**

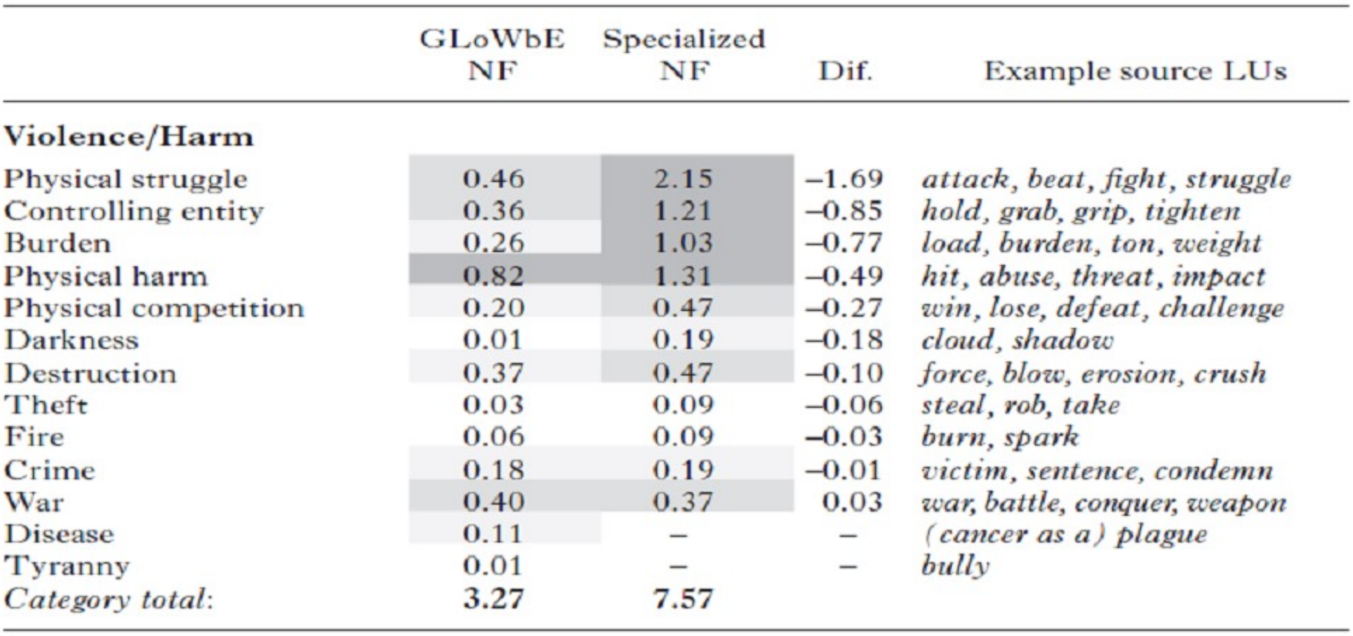
FIGURE 4. VISUAL METAPHORIC REPRESENTATIONS OF *BACKDOOR*.

## 7. THE BACKDOOR METAPHOR ACROSS TWO CORPORA

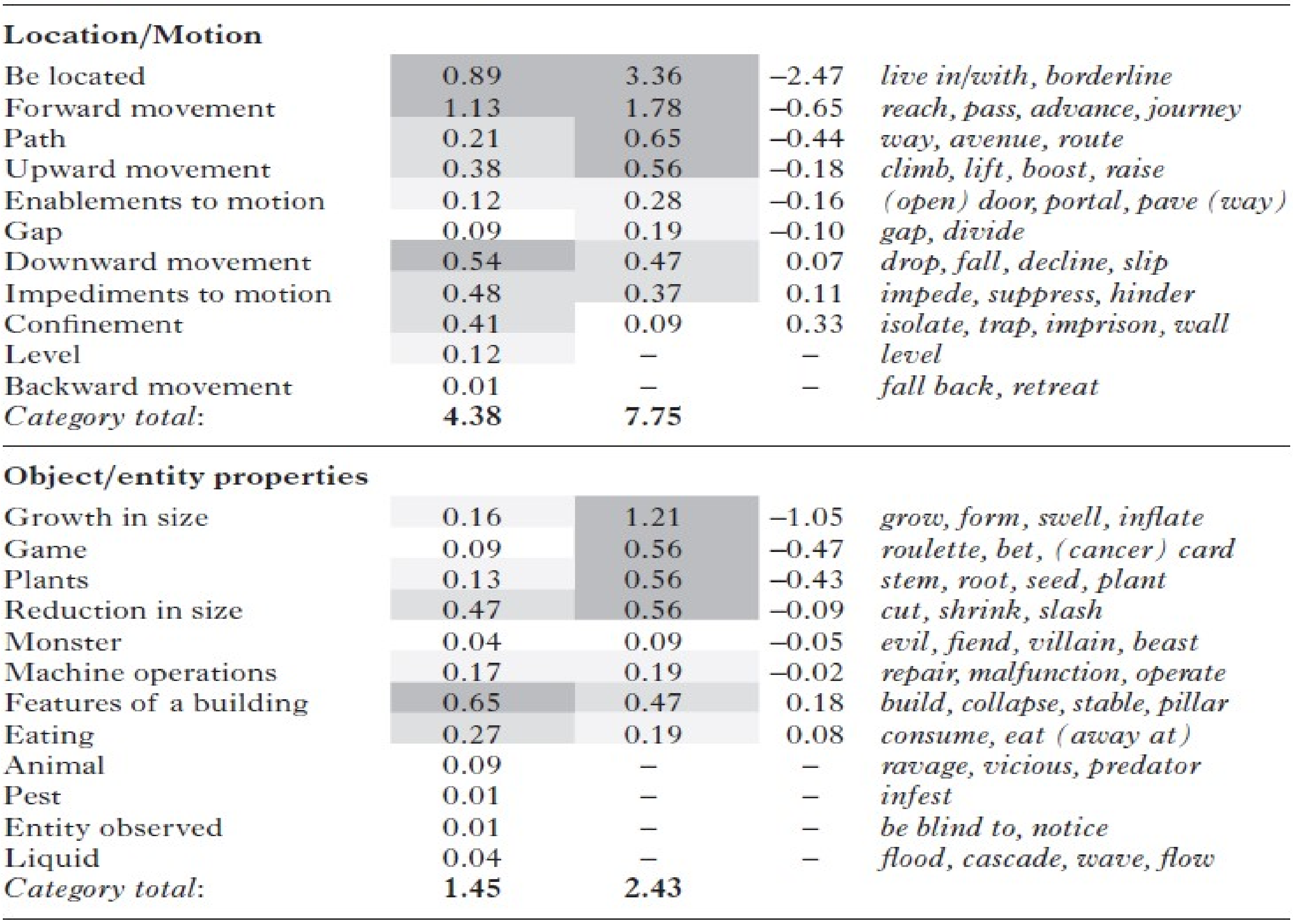
Metaphors are objects the system uses to create a link between the target and source domain frames, with the latter bringing a set of associated lexical items. These metaphors are nested in more complex hierarchical networks of metaphor. Each target-evoking word and phrase is associated with frames that are associated with target domain frame slots of one or more metaphors. At a high level, metaphors can be grouped into three broad categories that have something in common semantically among the source domain frames – Violence/Harm, Location/Motion, and Properties of Objects and Entities. Using this system and inheriting the primary metaphor networks, we identify patterns emerging for backdoor metaphors. It should be specified that the Gigaword corpus is based mainly on newswire sources, which are expected to include more discussion of societal issues, including information security and encryption while the specialized corpus rests on professional discussions in forums and blogs.

Using the source domain semantic categories, we supply a within-genre cross-corpus comparison between a general corpus and a specialized corpus with only blog and forum data. Table 1 summarizes results surrounding the topic of backdoor in English. The results are presented in order of actual, rather than relative, difference in normalized frequencies between the GLoWbE corpus and the specialized corpus. The presence of mostly negative values for the specialized corpus in the 'Dif.' column indicates that the specialized corpus contains a higher quantity of most metaphors for backdoor.

TABLE 1. RESULTS FOR BACKDOOR METAPHORS IN ENGLISH GENERAL AND SPECIALIZED CORPORA COMBINED (PER 10 RESULTS) (QUARTILE RANGES: 0.5–4, 0.2–0.5, 0.1–0.2, 0-0.1);
NF: NORMALIZED FREQUENCY; LU:LEXICAL UNIT; DIF.: ACTUAL DIFFERENCE.



| | GLoWbE NF | Specialized NF | Dif. | Example source LUs |
|---|---|---|---|---|
| **Violence/Harm** | | | | |
| Physical struggle | 0.46 | 2.15 | –1.69 | *attack, beat, fight, struggle* |
| Controlling entity | 0.36 | 1.21 | –0.85 | *hold, grab, grip, tighten* |
| Burden | 0.26 | 1.03 | –0.77 | *load, burden, ton, weight* |
| Physical harm | 0.82 | 1.31 | –0.49 | *hit, abuse, threat, impact* |
| Physical competition | 0.20 | 0.47 | –0.27 | *win, lose, defeat, challenge* |
| Darkness | 0.01 | 0.19 | –0.18 | *cloud, shadow* |
| Destruction | 0.37 | 0.47 | –0.10 | *force, blow, erosion, crush* |
| Theft | 0.03 | 0.09 | –0.06 | *steal, rob, take* |
| Fire | 0.06 | 0.09 | –0.03 | *burn, spark* |
| Crime | 0.18 | 0.19 | –0.01 | *victim, sentence, condemn* |
| War | 0.40 | 0.37 | 0.03 | *war, battle, conquer, weapon* |
| Disease | 0.11 | – | – | *(cancer as a) plague* |
| Tyranny | 0.01 | – | – | *bully* |
| *Category total*: | **3.27** | **7.57** | | |



| | | | | |
|---|---|---|---|---|
| **Location/Motion** | | | | |
| Be located | 0.89 | 3.36 | –2.47 | *live in/with, borderline* |
| Forward movement | 1.13 | 1.78 | –0.65 | *reach, pass, advance, journey* |
| Path | 0.21 | 0.65 | –0.44 | *way, avenue, route* |
| Upward movement | 0.38 | 0.56 | –0.18 | *climb, lift, boost, raise* |
| Enablements to motion | 0.12 | 0.28 | –0.16 | *(open) door, portal, pave (way)* |
| Gap | 0.09 | 0.19 | –0.10 | *gap, divide* |
| Downward movement | 0.54 | 0.47 | 0.07 | *drop, fall, decline, slip* |
| Impediments to motion | 0.48 | 0.37 | 0.11 | *impede, suppress, hinder* |
| Confinement | 0.41 | 0.09 | 0.33 | *isolate, trap, imprison, wall* |
| Level | 0.12 | – | – | *level* |
| Backward movement | 0.01 | – | – | *fall back, retreat* |
| *Category total*: | **4.38** | **7.75** | | |
| **Object/entity properties** | | | | |
| Growth in size | 0.16 | 1.21 | –1.05 | *grow, form, swell, inflate* |
| Game | 0.09 | 0.56 | –0.47 | *roulette, bet, (cancer) card* |
| Plants | 0.13 | 0.56 | –0.43 | *stem, root, seed, plant* |
| Reduction in size | 0.47 | 0.56 | –0.09 | *cut, shrink, slash* |
| Monster | 0.04 | 0.09 | –0.05 | *evil, fiend, villain, beast* |
| Machine operations | 0.17 | 0.19 | –0.02 | *repair, malfunction, operate* |
| Features of a building | 0.65 | 0.47 | 0.18 | *build, collapse, stable, pillar* |
| Eating | 0.27 | 0.19 | 0.08 | *consume, eat (away at)* |
| Animal | 0.09 | – | – | *ravage, vicious, predator* |
| Pest | 0.01 | – | – | *infest* |
| Entity observed | 0.01 | – | – | *be blind to, notice* |
| Liquid | 0.04 | – | – | *flood, cascade, wave, flow* |
| *Category total*: | **1.45** | **2.43** | | |

The colour concentration in the table above illustrates how genres dedicated to cybersecurity debate reveal greater frequency of the two metaphor families VIOLENCE/HARM and LOCATION/MOTION which dominate the discussion. Motion metaphors mainly concentrate around discussions of moving across the threshold (*crossing the doorway, opening a door/portal*) or imepeding access (*hindering or preventing one's entering a backdoor*). Along with the two dominant metaphor groups, there are also some examples in the source domain of object states, especially changes in object size. This might be due to the common description of information security threats as spreading entities inside the body or more broadly in society.

This latter finding is of particular importance for the present study in terms of conceptual categorization in the backdoor metaphor as it points out to a split in the target domain into several levels: the social one where information security policies and improvement are of paramount importance; the individual level, in which backdoor as a type of illicit behaviour is reified as a burglar that applies destructive force (*breaks, cuts, pushes a backdoor*) and does damage to another person's security; and the physiological level, at which backdoors are seen as lurking, invading, intruding or attacking within the body causung the loss of physical integrity. The following examples illustrate these different perspectives.

(10) The administrator's task here is to to take measures *to eradicate* backdoor-like behaviour.

(societal) (IT_spec_152)

(11) Hackers won't miss another chance *to push a backdoor* into my computer system. (personal) (IT_spec_42)

(12) Backdoors are like tumors growing inside my body swallowing my privacy. (physiological) (glo_3114)

This difference points out to the presence of different metaphor systems for the domain of information security depending on a stance in this heated debate which leads us to consider the political implications of the backdoor rhetoric.

## 8. Political dimension of the backdoor

The deconstruction of the backdoor metaphor into layers or levels does not seem to fully explain the way in which the term is used in public discourse. Therefore, it is worth mentioning what political baggage the metaphor applied in public discourse carry.

Like numerous ambiguous and highly complex terms, the backdoor has also become a contested term within the so-called *Crypto Wars*. While security agencies seem to avoid applying the term to describe their efforts to gain access to computer systems or encryption, technology and privacy experts keep pushing the term *backdoor* to the forefront. In this sense, *uncovering* something as a backdoor seems to have become an argument of its own.

Some layers of the backdoor seem to promote its use as a rhetorical tool against governmental intrusion. As shown below, the backdoor metaphor has associations with illicit means, malicious intent and security threats. Definitions of the IT term go as far as lumping together hackers and intelligence agencies.

However, some aspects of the backdoor metaphor could in turn also be leveraged by governments and their security agencies to strengthen their pro-backdoor argument in discourse. Both the core and the outer layer of the metaphor leave room for claiming and positively framing the term *backdoor* as a tool used by legitimized state actors and likening the act of accessing iPhones in the name of national security to some form of *troubleshooting* or *maintenance*.

From this perspective, the backdoor metaphor as such does not exclusively play to the advantage of either side. The fact that, within the crypto wars, the term is avoided by governments and utilized by the tech scene can ultimately be understood as the result of a power struggle over its meaning. It might be the case that the tech-savvy people and privacy advocates have not won the war, but the term currently represents a powerful rhetorical weapon in their hands.

## 9. Conclusion

The presented deep semantic corpus-based metaphor analysis has identified divergent, to varying degrees, strategies for dealing with computer systems security threats depending on a particular stance of the information security debate actors. These strategies may by no means be mutually exclusive, despite the ambiguity of terms and their application resulting in considerable confusion in their interpretation. This is where the role of analogical reasoning and metaphoric framing should not be underestimated since metaphor, as the present study shows, serves as an interpretative and explanatory tool prompting novel solutions to the cybersecurity issues by creating corresponding inferences. Each of the extracted metaphors has some relevant lessons to offer. For instance, the health metaphor suggests that preventative measures may be much easier and cost-effective to implement than after-the-fact care. The crime metaphor highlights the importance of identifying and securing access points, while the war metaphor stresses that the international diplomatic negotiations and maneuvering might be helpful in mitigating some of the more aggressive and political dimensions of these issues. However, each of these metaphors has considerable limitations when it comes to protecting computer systems. One might argue that one of these metaphors may serve a better or worse purpose than others, but what is more important is that each one carries very strong implications for the causes, motivations, and most appropriate protective measures to deal with cybersecurity threats. Since we do not seem to have made considerable progress in combating the ever-growing range of information security threats, the further search for apt analogies is highly critical both for policy-makers and IT experts commmunity to adequately structure the IT discourse. Such a state of affairs calls for the need to reframe the ongoing debate which means we have to search for new analogies and create new narratives. Experimenting with alternative metaphors can yield different perspectives on the problem and may eventually stimulate creativity in various ways of dealing with it.

This study seems to have illustrated the effectiveness of an automated method for finding a large number and broad variety of metaphoric expressions across various domains of interest and can be expanded to other languages. These findings have become possible due to the presence of primary metaphors in the metaphor database that feeds the automated identification system. Backdoor metaphors were extracted by means of primary metaphors in the higher levels of the metaphor networks, of which more specific metaphors are subcases. Although the repository may not provide sufficiently broad coverage found in some other automated metaphor identification systems, it can be used to inquire certain target domains or domains of knowledge when a researcher seeks to observe distributions of metaphoric language both in one language and cross-linguistically. Without claiming the absolute indisputability of the obtained results and being aware of the limitations of the corpus approach to the study of metaphor (the corpus represents solely the corpus reality and the sample might not be representative enough), we assume the results provide insights that could lead to further quantitative and qualitative analyses. They may serve as a good starting point for understanding conceptual similarities and differences in the domain(s) of interest. Subsequently, other domains can be added to the core primary metaphor network as subcase metaphors and additional lexical items or frames. The iterativity of this process is based on a computationally operationalized version of primary metaphor networks and semantic frames as the source and target domains of conceptual metaphors. By presenting results from one particular domain we have demonstrated the ways in which such a system may appear a valuable contribution to metaphor analysts' computational linguistic tools. The research outcome clearly suggests how conceptual metaphor research can benefit from advances in discourse analytic and corpus linguistic methodologies available today, keeping in mind recent developments in NLP technologies.

## References

Betz, David and Stevens, Tim. 2013. "Analogical Reasoning and Cyber Security." *Security Dialogue 44, No. 2: 147-164 (2013).* https://doi.org/10.1177/0967010613478323

David, Oana and Matlock, Teenie. 2018. "Cross-linguistic automated detection of metaphors for poverty and cancer." *Language and Cognition* 10 (2018), 467–493. UK Cognitive Linguistics Association. https://doi.org/10.1017/langcog.2018.11

David, Oana. 2016. Metaphor in the grammar of argument realization. Unpublished doctoral dissertation, University of California, Berkeley.

David, Oana, Lakoff, George, and Stickles, Elise. 2016. "Cascades in metaphor and grammar: A case study of metaphors in the gun debate." Constructions and Frames 8. https://doi.org/10.1075/cf.8.2.04dav

Davies, Mark. 2013. "*Corpus of Global Web-Based English: 1.9 billion words from speakers in 20 countries*." Available at: http://corpus.byu.edu/glowbe/

Davies, Mark. and Fuchs, Robert. 2015. "Expanding horizons in the study of World Englishes with the 1.9 billion word Global Web-based English Corpus (GloWbE)." *English World-Wide* **36**(1), 1–28. https://doi.org/10.1075/eww.36.1.01dav

Deignan, Alice. 2005. *Metaphor and corpus linguistics*. Amsterdam/Philadelphia: John Benjamins. https://doi.org/10.1075/celcr.6

Demjén, Zsófia, Semino, Elena, and Koller, Veronika. 2016. "Metaphors for 'good' and 'bad' deaths." *Metaphor and the Social World* **6**(1), 1–19. https://doi.org/10.1075/msw.6.1.01dem

Dodge, Ellen. K., Hong, Jisup, and Stickles, Elise. 2015. "MetaNet: deep semantic automatic metaphor analysis." *Proceedings of the Third Workshop on Metaphor in NLP,* 40–49. Denver, Colorado, 5 June 2015. Association for Computational Linguistics. https://doi.org/10.3115/v1/W15-1405

Do Dinh, Erik-Lân and Gurevych, Iryna. 2016. "Token-level metaphor detection using neural networks." *Proceedings of the Fourth Workshop on Metaphor in NLP* (June), 28–33. https://doi.org/10.18653/v1/W16-1104

Dunn, Jonathan. 2013. "What metaphor identification systems can tell us about metaphorinlanguage." *Proceedings of the First Workshop on Metaphor in NLP, Atlanta Georgia, 13 June 2010,* 1–10. Available at: http://www.aclweb.org/anthology/W13-0901

Fillmore, Charles J. and Atkins, Beryl. T. 1992. "Toward a frame-based lexicon: the semantics of RISK and its neighbors." In *Frames, fields, and contrasts: new essays in semantic and lexical organization,* edited by A. Lehrer and E. F. Kittay, 75–102. New York/London: Routledge.

Gedigian, M., Bryant, J., Narayanan, S., and Ciric, B. 2006. "Catching metaphors." *Proceedings of the Third Workshop on Scalable Natural Language Understanding ScaNaLU 06* (June), 41–48. https://doi.org/10.3115/1621459.1621467

Gill, Lex. 2018. "Law, Metaphor, and the Encrypted Machine." *Osgoode Hall Law Journal* 55.2: 440-477. Available at: https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/3

Gutiérrez, E. Dario, Shutova, Ekaterina, Marghetis, Tyler, and Bergen Benjamin. 2016. "Literal and metaphorical senses in compositional distributional semantic models." In *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics, Berlin, Germany, August 7–12, 2016,* 183–193. https://doi.org/10.18653/v1/P16-1018

Hallam-Baker, Phillip. 2008. *dotCrime Manifesto: How to Stop Internet Crime*. Addison-Wesley.

Jenner, Leontine. 2018. "Backdoor: how a metaphor turns into a weapon." Available at: https://www.hiig.de/en/backdoor-how-a-metaphor-turns-into-a-weapon/

Krishnakumaran, Saisuresh and Zhu, Xiaojin. 2007. "Hunting elusive metaphors using lexical resources." In *Proceedings of the Workshop on Computational Approaches to Figurative Language,* 13–20. Association for Computational Linguistics. https://doi.org/10.3115/1611528.1611531

Kupers, Wendelin M. 2013. "Embodied transformative metaphors and narratives in organisational life-worlds of change." *Journal of Organizational Change Management*, Vol. 26 Issue: 3, 494-528. https://doi.org/10.1108/09534811311328551

Lakoff, George. 1993. "The contemporary theory of metaphor". *In Metaphor and thought,* edited by *A. Ortony*, 202-251. New York, NY, US: Cambridge University Press. https://doi.org/10.1017/CBO9781139173865.013

Lakoff, George, and Johnson, Mark. 1980. *Metaphors we live by*. Chicago, IL: University of Chicago Press.

Landwehr, C., Bull, A. R., McDermott, J. P., and Choi, W. S. 1994. "A Taxonomy of Computer Program Security Flaws, with Examples." *ACM Computing Surv.,* vol. 26, no. 3, 211-254. https://doi.org/10.1145/185403.185412

Lederer, Jenny. (2013). "Assessing claims of metaphorical salience through corpus data." In *Proceedings of the 37th Annual Meeting of the Cognitive Science Society,* editored by D. C. Noelle, R. Dale, A. S. Warlaumont, J. Yoshimi, T. Matlock, C. D. Jennings and P. P. Maglio, 1255–1260. Austin, TX: Cognitive Science Society.

Lönneker, Birte. 2003. "Is there a way to represent metaphors in WordNets? Insights from the Hamburg Metaphor Database." *Proceedings of the ACL 2003 Workshop on Lexicon and Figurative Language – Volume 14,* 18–27. https://doi.org/10.3115/1118975.1118978

Martin, James H. 1994. "MetaBank: a knowledge-base of metaphoric language conventions." *Computational Intelligence* **10**(2), 134–149. https://doi.org/10.1111/j.1467-8640.1994.tb00161.x

Martin, James H. 2006. "A corpus-based analysis of context effects on metaphor comprehension." In *Corpus-based approaches to metaphor and metonymy* edited by S. T. Gries and A. Stefanowitsch, 214–236. Berlin: Mouton de Gruyter.

Mason, Z. J. 2004. "CorMet: a computational, corpus-based conventional metaphor extraction system." *Computational Linguistics* **30**(1), 23–44. https://doi.org/10.1162/089120104773633376

Philip, G. 2004. "Locating metaphor candidates in specialized corpora using raw frequency and keyword lists." In *Metaphor in use: context, culture, and communication* edited by F. MacArthur, J. L. Oncins-Martínez, M. Sánchez-García and A. M. Piquer-Píriz, 85–105.Amsterdam: John Benjamins.

Pragglejaz Group. 2007. "MIP: a method for identifying metaphorically used words in discourse." *Metaphor and Symbol* 22(1), 1–39. https://doi.org/10.1080/10926480709336752

Shutova, Ekaterina, Teufel, Simone, and Korhonen, Anna. 2012. "Statistical metaphor processing." C*omputational Linguistics* **39**(2), 301–353. https://doi.org/10.1162/COLI_a_00124

Shutova, Ekaterina and Sun, Lin. 2013. "Unsupervised metaphor identification using hierarchical graph factorization clustering." In *Proceedings of NAACL-HLT 2013, Atlanta, Georgia, 9–14 June 2013,* 978–988. Available at: http://www.aclweb.org/anthology/N13-1118

Skrynnikova, Inna, Astafurova, Tatiana, and Sytina, Nadezhda. 2017. "Power of metaphor: cultural narratives in political persuasion." Proceedings of the 7th International Scientific and Practical Conference "Current issues of linguistics and didactics: The interdisciplinary approach in humanities" (CILDIAH 2017). https://doi.org/10.2991/cildiah-17.2017.50

Steen, Gerard J., Dorst, Aletta, Berenike, Herrmann J., Kaal, Anna A., Krennmayr, Tina, and Pasma, Trijntje. 2010. *A method for linguistic metaphor identification: from MIP to MIPVU*. Amsterdam: John Benjamins. https://doi.org/10.1075/celcr.14

Steen, Gerard, J. 1999. "From linguistic to conceptual metaphor in five steps." In *Metaphor in cognitive linguistics*, edited by R. W. Gibbs and G. J. Steen (Eds.), 57–77. Amsterdam/Philadelphia: John Benjamins. https://doi.org/10.1075/cilt.175.05ste

Stefanowitsch, Anatol, and Gries, Stefan Th., eds. 2006. *Corpus based approaches to metaphor and metonymy*. Berlin/New York: Mouton de Gruyter. https://doi.org/10.1515/9783110199895

Stickles, Elise, David, Oana, Dodge, Ellen K., and Hong, Jisup. 2016. "Formalizing contemporary conceptual metaphor theory." *Constructions and Frames* **8**(2), 166–213. https://doi.org/10.1075/cf.8.2.03sti

Wolff, Josephine. 2014. "Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors." Paper presented at TPRC Conference, March 31, 2014. https://doi.org/10.2139/ssrn.2418638