RAEL: Revista Electrónica de Lingüística Aplicada

Vol./Núm.:	19.1
Enero-diciembre	2020
Páginas:	58-77
Artículo recibido:	02/02/2020
Artículo aceptado:	06/05/2020
Artículo publicado	29/06/2020

Url: http://www.aesla.org.es/ojs/index.php/RAEL/article/view/377

Metaphor Co-Creation in Reframing Cybersecurity Issues

La co-creación de metáforas en la reformulación de problemas de ciberseguridad

INNA SKRYNNIKOVA
VOLGOGRAD STATE UNIVERSITY

The paper substantiates the explanatory and interpretative potential of analogical reasoning in resolving the ambiguity of defining cybersecurity. By applying cognitive linguistics and corpus linguistics methods, it presents an attempt to showcase how the metaphor co-creation strategy may be helpful in reframing the discourse around cybersecurity dominated by inapt metaphors. The latter, in their turn, prompt wrong inferences, which ultimately results in false decisions about the nature of cyber vulnerabilities. The comparison of the conversational valence introduced by professional audience and laymen involved in the campaign of co-creating new metaphor-based utterances reveals how it channels the cybersecurity discourse, and is followed by outlining the implications of applying the newly created metaphors.

Keywords: *analogical reasoning, metaphor, co-creation strategy, reframing, cybersecurity discourse*

Este artículo corrobora el potencial explicativo e interpretativo del razonamiento analógico para resolver la ambigüedad de definir la ciberseguridad. Al aplicar los métodos de la lingüística cognitiva y de la lingüística de corpus, se presenta un intento de mostrar cómo la estrategia de co-creación de metáforas puede resultar útil para reformular el discurso en torno a la ciberseguridad dominada por metáforas inadecuadas. Estas últimas, a su vez, provocan inferencias erróneas, que finalmente dan como resultado decisiones equivocadas sobre la naturaleza de las cibervulnerabilidades. La comparación de la valencia conversacional introducida tanto por los profesionales como por los no expertos involucrados en la campaña de co-creación de nuevas expresiones metafóricas revela cómo se canaliza el discurso de seguridad cibernética, describiendo seguidamente las implicaciones que conlleva la aplicación de las metáforas recién creadas.

Palabras clave: *razonamiento analógico, metáfora, estrategia de co-creación, reformular, discurso de ciberseguridad.*

1. INTRODUCTION

The world increasingly relies on technology to far greater extent than ever before, and there is no sign that this trend will slow down. As a result, digital data creation has surged with businesses and governments storing a great deal of data on computers and transmitting them across networks to other computers. Devices and their underlying systems have vulnerabilities that, when exploited, undermine the health and objectives of an organization or a national government. Therefore, the critical role of cybersecurity cannot be underestimated under the circumstances when it is becoming more challenging for cybersecurity experts to keep up with the changing security risks.

Cybersecurity, also known as information security, refers to the practice of ensuring the integrity, confidentiality, and availability (ICA) of information. It comprises an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorized access. Since cybersecurity is a broad umbrella term that encompasses a number of specific practice areas ranging from network and application security to data and operational security, each with its own list of possible vulnerabilities, its current interpretations vary greatly. Some researchers explain it by claiming that "the more inclusive the concept is regarding the domain, the harder it will be to identify what policy is, or should be, surrounding cyberspace"[1] This basic tension is a recurring theme in the cybersecurity strategies of most countries that have attempted to formalize them (Betz & Stevens, 2011: 36). As a result, such conceptual imprecision afflicts cybersecurity (Betz & Stevens, 2013).

The best way to resolve the ambiguity of such a complex concept as "cybersecurity", along with some other encryption-related concepts (e.g. backdoor, phishing, etc.), is to ensure effective communication among different research communities to further objectives and to contribute to meaningful dialogue between professionals and policymakers. However, there is still little consensus on the meaning of "cybersecurity" and "cyberspace", despite attempts to develop common vocabularies (Rauscher & Yaschenko, 2011).

Taking into account the powerful interpretative potential of analogical reasoning, this corpus-based study focuses on co-creation as a new persuasive strategy applied to reframe the cybersecurity discourse through engaging both the professional community and general public. First, the paper provides a short overview of relevant theories followed by the analysis of current cyber metaphors and the inferences they produce in the minds of the target audience. It proceeds by describing our case study of the co-created cyber metaphors and their possible implications for the future of the cybersecurity discourse. Finally, the paper interprets the findings and outlines further line of research.

2. **ANALOGICAL REASONING AND CYBERSECURITY METAPHORS**

2.1. Explanatory potential of analogical reasoning

Previous research has repeatedly focused on analogical reasoning as a powerful interpretative mechanism which proved to be strikingly effective in resolving the mystery of ambiguous or contested concepts.

> Analogical reasoning or argument by analogy can be defined as a specific way of thinking, based on the idea that because two or more things are similar in some respects, they are probably also similar in some further respect. Integrating various human-level reasoning mechanisms, arguing by analogical thinking, use analogies by transferring knowledge from one particular entity (the analogue or source) to another one (the target). Furthermore, it refers to the linguistic form, which corresponds to the process of relating the source and the target. As specific form of inference or reasoning, analogies draw

[1] The quote from a policy making veteran giving a speech at the workshop "Cyber Security: Lacunae of Strategy'" held on 25 October 2011 and 31 January 2012 at King's College London (retrieved from http://www.newpolcom.rhul.ac.uk/npcu-blog/2012/1/26/oloughlin-at-gchq-cyber-security-lacunae-of-strategy.html, 24.12.2019).

> conclusions by applying heuristics to propositions or observations as well as by interpolating logical steps or patterns. Analogies focus on relating specific particularities in two or more cases or things to form the basis for a conclusion (Küpers, 2012:2).

A specific form of analogy is metaphor as a cognitive mechanism (Lakoff & Johnson, 1980) enabling to understand one abstract disembodied entity in terms of another concrete, familiar and embodied one (e.g. ARGUMENT is WAR, IDEAS are FOOD). Metaphors are a common constituent of language, either in their obvious forms as deliberate or novel constructions, or as 'dead metaphors', phrases that through constant repetition and ubiquity have passed into common usage (Lakoff, 1987). Therefore, metaphors may explain and interpret obscure concepts serving as a catalyst of thinking and bringing about a sought-for result or undesirable consequences, when used unwisely.

Current cybersecurity debates rely heavily on metaphors, models, and related rhetorical devices which initially seem to provide deeper insights into the challenges we face in cyberspace. However, some of them frequently "end up as empty labels or catch phrases used by different people to mean different things" (Lapointe, 2011). If this is the case, then metaphors can impede meaningful discussion rather than be a vehicle for creative thought. Most common cyber metaphors currently shape our discourse, and some of them do not contribute to a clearer vision of future challenges and ensuing measures we have to take to ensure cybersecurity. There are notorious examples of reporting on cybersecurity which have resulted in mistranslation and misrepresentation. Applying some "cyber doom" scenarios appealing to national historical consciousness has given rise to using such analogies as the Pearl Harbor or 9/11 attacks, which, as some researchers argue, are aimed at adding urgency to calls for action (Conway, 2008). Others find these metaphors "unhelpful and dangerous" (Brito & Watkins, 2011: 38; Stohl, 2006). We must be aware and concerned of the inappropriate ways in which the current cybersecurity discourse structures our thinking by misleading and confusing analogies. This fact substantiates the idea that the 'right' application of analogical reasoning should be one of the top priorities for those involved in cyber security. Figurative language that policy makers, privacy advocates and the media use referring to cybersecurity affects the ways it is reasoned about prompting certain decisions. The latter will ultimately affect not only professional communities but also general public.

2.2. Dominant cybersecurity metaphors

The most pervasive analogies dominating the cybersecurity discourse are the burglar metaphor, the war metaphor, and the health metaphor. All of these metaphors do not stress the responsibilities of an individual actor or the function of a specific technological process but rather on the nature of the threat or problems, posed by computer networks (Wolff, 2014). This echoes D. Schön's analysis applying metaphors to framing public policy debates by setting up or generating a mental model of the problem that makes a certain policy solution clearly appropriate. He argues the metaphors used to refer to these issues "select for attention a few salient features and relations from what would otherwise be an overwhelmingly complex reality. They give these elements a coherent organization, and they describe what is wrong with the present situation in such a way as to set the direction for its future transformation" (Schön, 1979). Similarly, the health, war, and burglar metaphors in the cybersecurity discourse frame computer security challenges as more familiar social problems from which we infer that the most appropriate protective measures to be taken are the same as the ones protecting the society from robbers, wars, or diseases.

Elaborating on the burglar metaphor, Hallam-Baker (2008) emphasizes that theft would not be considered an appropriate metaphor for Internet crimes, as many of them literally involve stealing money from people by means of extortion, impersonation, or persuasion. However, the burglary analogy does invoke the notion of breaking and entering into the physical world, the etymology of the word "burglary" (Latin *burgare – to break into a house*, derived from the Latin term *burgus – fortress or castle*). What makes Internet crimes similar to burglary is the idea of breaking into a protected space. It has given rise to numerous explanations that the ways computer networks should be defended should be identical to protecting houses against burglars and fortifying medieval castles. Nonetheless, the burglar metaphor is hardly apt as castles do not perfectly map onto computers. Defensive strategies implied by the metaphor include locks, alarms, guard dogs, fences, and Landwehr et al. (1994) point out several computer security flaws in terms of gates and fences. Domain flaws map onto "holes in fences" because the protections between different pieces of software are porous. Another weakness of the metaphor is that describing defense in terms of fences or gates implies that security flaws will be observable to defenders. However, this assumption is not applicable to computers, where vulnerabilities and access points are not necessarily and clearly manifested. The burglar metaphor captures the financial motivation driving some computer crimes as well as the importance of bolstering barriers to access points with detection-response mechanisms and prosecutorial measures. But it fails to specify the challenges and complexity of identifying computer system access points, combining multiple and different defenses to protect them or figuring out when information has been stolen in a timely fashion. However, the language of the burglary metaphor pervades discussions of cybersecurity, partly because, being familiar, it frames a challenging problem in the context of a much older and better understood one. Another reason is commercial value of the burglar metaphor. The multi-billion dollar business of selling information security products employs marketing materials rife with burglar metaphors with its message that more defence is always better.

The international political arena is increasingly dominated by the war metaphor. For many who employ the language of the war metaphor it is highly problematic to understand when the notion of "cyber war" ceases to be metaphorical. Despite being excessively aggressive, the war metaphor draws certain implications from the burglar metaphor when it comes to the nature of computer systems threats and the appropriate tactics of defense. The war metaphor implies a significant body count and violence. Similar to the notions of breaking and entering in the burglary metaphor which do not apply clearly to computer crimes, the essential elements of war, death and violence are not characteristic of most computer security breaches. While the burglar metaphor implies a set of attackers who are concerned primarily with financial gain by means of theft, the war metaphor presupposes a set of powerful, well-organized malicious actors, including national governments, concerned with promoting political or ideological agendas by means of physical violence (Wolff, 2014). The increased involvement of governments and national militaries in computer security and espionage efforts has spurred the use of the war metaphor. This suggests that the burglar metaphor is increasingly inadequate to describe the full range of actors and motivations involved. The war metaphor has very different defensive implications. One of them is that defense is the responsibility of national armies and governments. Another one is that war implies huge expenses of the defensive measures applied and the collateral damage which are justifiable when presented with the war metaphor as it brings the underlying message that lives are at stake. In the case of cybersecurity, however, those lives are mainly metaphorical, leading some researchers to reject the metaphor due to its inaptness (Wisniewksi, 2013) as no cyber offense meets the war criteria. The metaphoric value of the war metaphor may be observed in suggesting a host of non-violent diplomatic and political measures used to avert or end wars. According to the war metaphor, this sort of diplomatic negotiations could prove useful in averting or putting an end to certain forms of computer security threats. However, it is not always clear where the line is drawn between defensive and offensive measures in this war. Both the burglar and war metaphors point out to the critical importance of gaining a more comprehensive view of the access paths or “terrain” associated with computer systems but offer few clues about the ways in which this might be accomplished.

Where the two metaphors mentioned above ascribe agency for computer security threats to human actors, the health metaphor treats these threats as those caused by a very different type of villain: an infectious disease. The most pervasive element of this metaphor which has become trite is the term “computer virus”. It stresses the disease-like ability of some malware to replicate itself, but extends even further than that. Like microbial diseases and numerous ever-changing viruses, computer security threats can spread rapidly, evolve in response to new and improved defenses (vaccines), and can be addressed with defensive measures ranging from preventative care to treatment and quarantine of active infections. Still, there are some areas where the metaphor seems less apt, when it implies that lives are on the line or edge. Despite this fact, the health metaphor is the most appropriate of the three due to the fact that over the past few decades nations have made more significant progress in treating diseases and improving the state of public health than in preventing theft or war. Charney (2010) supports applying the health metaphor to improve the security of the Internet by claiming that governments and industry could improve and maintain the health of the population of devices in the computing ecosystem through preventative measures, detecting infected devices, notifying affected users, enabling those users to treat devices infected with malware, and ensuring that infected computers do not put other systems at risk. The health metaphor makes it clear that the IT industry and Internet access providers share responsibility for ensuring the health of devices before granting them access to the Internet.

The health is not devoid of flaws either. To demonstrate that Hallam-Baker (2008) stresses that the protection mechanisms used by humans and operating systems differ greatly. The humans are protected from biological diseases due to their genetic diversity unlike most computers which run the same few operating systems lacking diversity in the “computing gene pool.” It means that the diverse genetics is no defense for individuals, but rather ensures the species’ survival. For those seeking to protect their own computer systems from threats, this analogy does not prove to be in explaining the ways cyber threats should be addressed. The limitations of applying a health metaphor are considerable despite its ability to capture the evolution of threats. The strongest argument against this metaphor is that computers are not biological organisms while viruses are the product of human nature. The health metaphor fails to capture the fact that there is a thinking human agent driving every step of computer security threats. It also implies certain mysteriousness and elusive character of the problem as it is the case with cancer metaphors. Trying to grasp the essence of ‘radical’ or ‘absolute’ evil like cyber threats we desperately search for adequate metaphors which frequently result in oversimplification or justification of harsh measures.

As can be seen from a short overview of the currently applied cyber metaphors, they have very little to offer in terms of guiding our information security activities or strengthening computer security. Such state of affairs calls for the need to reframe the cyber security discourse and propose new metaphoric solutions to address cyber-related issues. One of the possible reframing strategies, as the present paper proposes, is metaphor co-creation which has been previously proved effective in promoting new solutions to challenging societal problems.

3. METAPHOR CO-CREATION IN CYBERSECURITY DISCOURSE

The rapid growth and adoption of the Internet undoubtedly creates an unprecedented opportunity for innovation and socio-economic growth but also makes securing cyberspace more difficult. To address this challenge, many countries organize cybersecurity awareness campaigns, which aim to educate governments, private industry, educators, and individual citizens about potential problems they can encounter online and to understand their individual roles and responsibilities for creating a safer cyberspace (Stop. Think. Connect Initiative in the USA, Be CyberStreetWise in the UK**,** Qatar's National Cyber Security Strategy**,** etc.). Classic cybersecurity campaigns aim to persuade their audience by using fear appeals to make them scared and aware of possible threats the Internet may bring. These appeals frequently remain unheard and ineffective, leading to a call for alternative methods of cyberspace behavior change (Ruiter et al., 2014).

The present paper responds to this call by focusing on a new persuasive strategy of metaphor co-creation as applied to reframing the cybersecurity discourse through engaging both the professional community and general public. Involving the public and the stakeholders in co-creation has previously been reported to be effective as they do not passively receive but actively participate in the creation of value (i.e. an idea, a product, testing, promotion, self-revelation, etc.) (Zwass, 2010). Numerous studies and extensive application of co-creation can be found in the context of commercial marketing (Bacile, Ye, & Swilley, 2014; Gebauer, Füller, & Pezzei, 2013; Zwass, 2010). One of the ways to implement co-creation strategies is asking consumers of a company to define and solve problems jointly through active dialogues, which eventually results in a co-created product or service meeting consumers' demands and improving the company image (Prahalad & Ramaswamy, 2004). Consequently, advantages of co-creation include reduced costs, improved products or services, gained time, a better profile of the consumer and enhanced consumer-company relationship (Hoyer et al., 2010). To the best of our knowledge, there is still no evidence as to the way co-creation exactly works in cybersecurity awareness campaigns.

The question of whether and how metaphor co-creation works in cybersecurity campaigns remains open. It is still unknown if co-creation can potentially assist in boosting the impact of such campaigns or reframe the cybersecurity discourse dominated by inapt metaphors leading to false inferences and assumptions about the current cyber vulnerabilities. The goal of this study is to show how a professional audience and laymen involved in the campaign co-create new metaphor-based slogans and utterances to channel the cybersecurity discourse into the 'right' direction and to outline the implications of applying the newly created metaphors to reinforce the future campaign messages. Therefore, we investigate from a corpus-linguistic perspective how contributions from professional audience members who co-create a cybersecurity campaign resonate with or deviate from the ones co-created by general public.

4. THEORETICAL FRAMEWORK

Analogies and metaphors have long been viewed as representing admixtures of emotional and instrumental utility. The same words may be used in different ways and in different contexts, and be received differently by different audiences. In the field of security the "choice of a metaphor carries with it implications about contents, causes, expectations, norms, and strategic choices" (Bobrow, 1996: 436). Metaphors serve to shape discourse and become the premises on which decisions are made. In a very real sense, metaphors play a central role in 'structuring political reality for manipulative purposes' (Hook, 1984: 259).

Why metaphors are so helpful in structuring the cyber discourse derives from the fact that, according to Lakoff and Johnson (1980), metaphorical language used to describe and communicate can serve as a window into conceptual systems that power human understanding and, ultimately, actions. Not only can metaphors limit our vision and understanding of the world, but they can also constrain our possible avenues of action. Therefore, we should be cautious and reflexive about our use of metaphors because they "carry with them, although covertly and insidiously, natural 'solutions" (Ortony, 1979: 5–6). Another strong point of metaphors is that they do not just work individually or in isolation but collectively and systematically help to bridge the gap between individual human cognition and collective understanding and action. This is particularly true of cyber metaphors employed in the common language concerning cybersecurity today, which is criticized for being automatically and excessively militarized. This militarization takes place at two levels. At the first level, the discourse unfolds around protecting our "networks" or "systems" or "critical infrastructure" by keeping others out of them thus forming the deterrence model. At the second level, cybersecurity is seen as a national security interest giving rise to the corresponding view of possible ways of addressing the issue. Since these metaphors work together in systems, they come with entailments. This means that a root metaphor can bring with it other related metaphors. In the case of the cyber war metaphor, notions of "attack," "offense," "defense," "battlefields," and "domains of war" are all entailments of the war metaphor (Lapointe, 2011; Lawson, 2012; Wolff, 2014). Sticking to the war metaphor vividly, this shows how it constrains current actions to counter cyber threats leading us to consider searching for alternative scenarios of framing the cybersecurity discourse.

This study delves into the importance of acknowledging an overlooked role of metaphorical framing in the construction of cybersecurity discourse, therefore explaining the essence of the frame approach adopted here is important. Since the early days of cognitive semantics, the structural organization of knowledge configurations, 'frames' and 'domains', has been repeatedly stressed. Relying on the conceptual metaphor theory, this study treats metaphor as an extended type of frame that assists in understanding the coherent structure and organization of the digital environment. It follows the definition of the frame proposed by Charles Fillmore: "Any system of concepts related in such a way that to understand any of them you have to understand the whole structure in which it fits; when one of the things in such a structure is introduced into a text, or into a conversation, all of the others are automatically made available (Fillmore, 1982: 111). The array of frames found in the cybersecurity discourse brings with them a certain "emotional charge" reflected in the conversational valence of metaphoric utterances to refer to cyber issues.

The idea that conversational valence (i.e., how negatively or positively people speak about pressing societal issues) influences predictors of people's behaviors is not new (Hendriks, van den Putte, & de Bruijn, 2014). This conversational valence can in turn be affected by the metaphorical utterances produced. Previous studies show that exposure to a certain metaphor indirectly affects intentions and subsequent decisions people make about an issue discussed (Lawson, 2012). Campaigns aimed at raising public awareness of complex controversial issues generally prompt people to talk negatively about unhealthy behaviors that include people's ignorance of cyber security threats. Nonetheless, the question arises whether the audience will also take up this negative conversational valence in their conversations about the imprudent web behavior when cyber security campaigns let the audience co-create the campaign.

5. RESEARCH QUESTIONS

The aforementioned observations lead us to address the following research questions.

RQ1: How does the conversational valence as introduced by the professional audience resonate with or deviate from the campaigns' conversational valence toward the proposed cyber space behavior?

Cybersecurity co-creation campaigns can stimulate the dialogue between professionals and laymen and promote their fruitful communication resulting in subsequent change of social norms by using co-creation. By doing so, they invite the target audience to co-construct a slogan or motto to be further promoted to the public. In this way, the campaign organizers can produce the first words of a sentence that enables the target audience to produce the remainder of the sentence. The procedure works in such a way that as soon as a co-constructed sentence is established, the first fragment becomes an environment for the second, capable of shaping its implicated meaning. Moreover, the second fragment creates a new context for the first, potentially unfixing its former meaning and giving it a new one. This is referred to as "backframing" (Du Bois, 2014). The beauty of co-creation lies in the fact that the open-ended character of language guarantees the limitless potential for engagement in co-constructing a sentence. This makes it easy and interesting for a target audience to co-construct a sentence and provides it with a script to talk about the issue of concern in their own way, mediated by cultural context: practices, norms, and meanings (Akaka, Schau, & Vargo, 2013).

RQ2: How does the professional audience co-construct a metaphoric utterance about the cybersecurity issue, being previously exposed to certain metaphors and how does this correspond to or deviate from the way the campaign participants formulate them?

Nowadays, it has become quite common to communicate online. Microblogging, for example, is a frequently used online tool for sharing opinions about brands. Moreover, due to the rise of social networking sites (SNS) (e.g., *Facebook, Twitter, Telegram*), the use of co-creation has been made easier (Van den Heerik et al., 2017). These sites provide unlimited means for Internet users to consume, contribute, and create content (Muntinga, Moorman & Smith, 2011). Consumers engage in co-creation on distinct social media channels to varying degrees For example, *Facebook* and *Twitter* pronounce more negative sentiment than *YouTube* regarding user-generated content (Esbrí-Blasco et al., 2019). Moreover, people often use *Twitter* to initiate or engage in discussions and spread news. (Smith, Fischer & Yongjian, 2012). These facts make us wonder if a target audience also engages differently in the co-creation of a cyber security campaign depending on the SNS, leading us to the third research question:

RQ3: How does the target audience co-create on *Twitter* and *Facebook*?

The patterns of engaging in co-creation within the cyberecurity awareness campaigns may vary for professional audience and general public. The audience is unevenly and to varying degrees involved in different SNS. Moreover, it may follow different co-creation routes depending on its professional background and awareness of the cyber threats as well as the character of co-creation campaigns.

6. METHODOLOGY

6.1 Case study

The *Facebook* Hacktober campaign and CyberFest workshops held between 2015 and 2019 serve as a case study to answer our research questions. The former campaign is a *Facebook* annual, monthlong initiative to build and maintain a security-conscious culture through contests, workshops, and expert talks as a part of National Cyber Security Awareness Month, a campaign to keep people involved in cyber security and play their part in making the Internet safer and more secure for everyone. The latter is a series of workshops for cyber security professionals initiated by national security laboratories in the USA and Europe aimed at elaborating innovative solutions to cyber threats through applying co-creation strategies. Both campaigns stress that addressing a variety of possible approaches for improving cyber security in the future will facilitate a deeper understanding of cyber defense and result in some creative novel solutions in the field. Both events were distributed through mass media and online social networks. The crucial part of brainstorming activities was to elicit creative thinking about the problems of cyber security through a specific type of co-creation: namely, contributing to the campaign by coming up with apt cyber security metaphors reflecting the participants' views of the current digital vulnerabilities.

The major assumption underlying the cyber security research is that exploration of the metaphors we use in the cyber security domain may help improve our thinking and discussion in four important ways. Firstly, it enables us to gain a deeper understanding of the value and limitations of the concepts we have mapped from other domains into the cyber security domain. Secondly, introducing less common or novel metaphors may feed the imagination of researchers and policy developers. Thirdly, metaphors that will prove to "work" particularly well might be further developed into holistic new models or sets of concepts for addressing cyber security problems. Finally, a metaphor serves a heuristic purpose of bringing deeper insights of abstract concepts from the field of cyber security into domains which a non-specialist may be more familiar with. Metaphor co-creation activities were preceded by considering four major scenarios illustrating current threat-related problems (information confidentiality, integrity, and availability). These scenarios included exploitation of a software vulnerability leading to loss of information services in a large company, large-scale theft of proprietary information by a company employee, loss of a valuable oil exploration submersible traced to design and test errors traced to flawed hardware and software, and an unattributable network attack leading to disasters in an air traffic control system. The scenarios were intended to illustrate not only a set of security issues, but also the influence that implicit metaphors and issue framing can have on problem definitions and solutions.

The discussions of the aforementioned scenarios exposed the campaign and workshop participants to a wide range of metaphors pervading the current cyber security discourse. They range from those relating to military and other types of conflict, biological, health care, markets, three-dimensional space, and physical asset protection. The evoked metaphors discussed include fortress (castle), cops and robbers, warfare, complex adaptive systems, ecosystem biodiversity, immune systems, programmed cell death, disease prevention and health care, market incentives, risk management, outer space, the global environment, banking, games, martial arts, and military deterrence. The subsequently produced metaphors from the two events do show how these co-creation routes lead to different possible solutions ensued.

6.2 Procedure and method

Identifying conceptual metaphors in a corpus presents a certain challenge since conceptual mappings are not restricted to a specific set of linguistic forms but rather to different sets. The study applies a specific technique consisting in search of topic/ target domain vocabulary which helps to figure out the nature of the conceptual mapping it belongs to. The first step is to select the lexical items referring directly to topic/target domain concepts. Then those occurrences of the topic/target domain which indicate a metaphorical status are identified to reveal the metaphorical mappings.

We collected a corpus of 454 metaphoric utterances both from Hacktober campaign and CyberFest workshop which were co-created by the target audience, including laymen and professionals. Some were found online by random sampling on the Hacktober campaign websites to include 83 metaphoric utterances from the campaign advertisements collected from its *Facebook* and *Twitter* pages. The remaining 371 examples were obtained from a list of metaphors co-constructed by the expert audience at the CyberFest.

Applying corpus-linguistic analysis (WordSmith Tools 5.0), the following coding categories from the data were derived: conversational valence, type of utterance, and the domain that cyber (in)security was compared with. The first was to analyze conversational valence of the collected metaphorical utterances and examine whether cyber (in)security was compared with something bearing a positive or negative connotation. To maximize the objectivity, we annotated an utterance as having a positive or negative valence only when the words used made this valence explicit. Therefore, we searched for words that had a clear positive or negative connotation (positive: "good," "winning," and "reliable"; negative: "bad," "bully," and "stealing", "hacking", "violating"). We also analyzed whether the metaphoric utterances included any form of negation ("not," "never", "hardly") to indicate that cyber (in)security was being compared with something negative. We also attend to emoticons (☺/L) and punctuation marks (. . ., ((, ?!) as markers of positivity or negativity. Utterances were marked as a comparison, a metonymy or an attribution. Finally, for the comparisons, we annotated the domain which cybersecurity was compared to. Then we defined the most frequently used values and systematically grouped the utterances under these domains. Eventually, utterances of different categories were compared based on keywords, content, and the interpretation of the underlying context to merge some domains and distinguish 11 domains (see Table 1). It is worth mentioning that utterances could be categorized under more than one domain, i.e. a generic term for background knowledge structure in cognitive semantics.

Table 1. Domains, concepts and conceptual metaphors

Domains	***Domain contents***	***Cyber insecurity is***
PUBLIC HEALTH	*Activities, roles and responsibilities in healthcare and related institutions*	*a catching disease (viruses, worms)* *impeding wellness* *disrupted check-ups* *impaired body integrity* *deceiving a patient*
ECOSYSTEM	*Activities to stimulate biodiversity, manage unpredictable processes, deal with formerly unknown phenomena*	*challenging biodiversity* *inability to manage change* *bringing about calamities/disasters* *killing/endangering species*
COOKING FOOD	*Processes of preparing or buying food, its quality and consequences for someone who eats it*	*underbaking a pie* *serving raw food* *being poisoned*
MARKET PLACE	*Relations among market participants, buying and selling, competing, business practices*	*preventing market innovation* *failed customer support* *unfair competition* *unbalanced economic forces* *suffering severe damage*

BATTLEFIELD	*Warfare activities involving general command, tactics and strategies a waging a war, resulting wounded/ killed soldiers, victims and ruined territories*	*fighting an unknown enemy* *militarizing software* *Internet battlefield* *wounded soldiers* *invading one's terrotory* *waging a Cold War*
COMMON SPACE	*Things, processes and activities arising in a shared space, maintaining its security, providing access to it for law-abiding citizens*	*circumscribing a physical space* *intruding global commons* *entering through a back door* *trespassing someone's field*
PHYSICAL ASSET PROTECTION	*Guarding activities and tools aimed at preventing stealth or robbery of one's house, keeping valuables in a secure place, possessing a host's key, letting in only familiar people*	*failed property guard* *unauthorized access to a fortress (castle)* *stealing valuables from a house* *picking up keys to someone else's locks* *enabling stealing*
COMPETITIVE GAME	*Sports or leisure activities involving competing players and based on healthy competition and fair play practices, resulting in someone's winning thanks to outmaneuvering another player*	*doing martial arts* *playing poker/chess/checkers* *offending an opponent* *cheating in a game*
EMOTIONS	*Activities resulting in evoking people's feelings about smb/smth arising from previous (mis)deeds of other people or institutions they interact with*	*instilling fear/panic* *feeling unsafe* *experiencing uncertainty*
SOCIAL NORM	*Behavior that is seen as (in)decent by the general norm*	*controlling individual/social morality* *preventing illegal activities*
SEX/RELATION	*Activities and situations that have to do with sexual/romantic relations and sexual inclination*	*having casual and unsafe sex with a stranger* *changing sexual partners* *marrying one's own sister or brother*

7. FINDINGS

The analysis yielded both quantitative and qualitative results. They are interesting in terms of the correspondence and deviation between the campaign utterances produced by laymen on *Twitter* and *Facebook* and professional audience utterances co-created at the workshop. In this way we answer RQ3 by comparing the utterances of the two events throughout the analysis of valence, types of utterance, and domains.

7.1 Valence of the Utterances

To answer RQ1, we examined the valence of the campaign and professional audience metaphoric utterances on *Twitter* and *Facebook.* Table 2 shows the number of campaign utterances and target audience utterances on *Twitter* and *Facebook* with a negative or positive valence. This table shows that, overall, both campaign and target audience slogans displayed negative valence more often than positive valence. However, the target audience slogans expressed valence significantly more often on *Twitter,* both positive (e.g., "ensuring cybersecurity is like being friends with @someone"), and negative (e.g., "ensuring cybersecurity is like opening a back door to a stranger"), compared with the overall corpus. The campaign utterances revealed negative valence less frequently compared with the general distribution of conversational valence in the corpus. The valence of the utterances produced by the target audience thus mostly corresponds to the valence of the campaign utterances, but deviates on *Twitter.*

7.2 Type of Utterance

To answer RQ2, we took a closer look whether the campaign and target audience resort to a comparison, an attribution, or metonymy. As you can see from Table 2, most campaign utterances and target audience utterances were comparisons. Nevertheless, on *Facebook*, the professional audience preferred metonymy ("cybersecurity is so 1998 . . .") and attribution ("cybersecurity is so yuck!") significantly more frequently with fewer comparisons identified, both in comparison with the overall distribution of the corpus. By way of contrasting, on *Twitter*, the use of metonymy and attribution by the target audience was significantly reduced compared with the general distribution of the corpus, while the use of comparisons appeared to be more preferable ("providing cybersecurity is so much like knowing exes of your boyfriend"). The professional audience thus co-constructed a metaphoric sentence about cybersecurity measures using different types of utterances that corresponded with the campaign on *Twitter* but deviated from the campaign on *Facebook*.

7.3 Domains of the Comparisons

To elaborate further into the ways the professional audience co-constructed the current cyber security measures and threats, we focused on the domains they were compared with. Table 2 below shows how the metaphoric utterances from the campaign and professional audience were categorized into domains.

Table 2. ***Distribution of valence, type, and domain of the utterances***[2]

	Campaign n (%)		Target audience				Total		Statistics s
			Twitter n (%)		Facebook n (%)				
Valence of slogan									
Positive	4	5.1%	20^b	15.0 %	14	6.1%	38	8.6%	$\chi^2(2) = 10.05$, $p < 0.01$, Cramer's V = 0.15
Negative	26^a	32.9%	73^b	54.9 %	111	48.5%	210	47.6%	$\chi^2(2) = 9.74$, $p < 0.01$, Cramer's V = 0.15
Type of utterance									
Metonymy and attribution	4	5.1%	2^a	1.5%	40^b	17.5 %			$\chi^2(2) = 25.92$, $p < 0.001$, Cramer's V = 0.24
Comparison	75	94.9%	131^b	98.5%	189^a	82.5%			
Domain of the comparison									
Public health	30	38.0%	61	45.9%	91	39.7%	182	41.3%	$\chi^2(2) = 1.45$, $p = 0.48$
Ecosystem	27^b	34.2%	17^a	12.8%	41	17.9%	85	19.3%	$\chi^2(2) = 14.98$, $p < 0.01$, Cramer's V = 0.20
Cooking food	6	7.6%	25	18.8%	31	13.5%	62	14.1%	$\chi^2(2) = 4.57$, $p = 0.10$
Market place	9	11.4%	19	14.3%	26	11.4%	54	12.2%	$\chi^2(2) = 0.26$, $p = 0.88$
Battlefield	6	7.6%	15	11.3%	31	13.5%	52	11.8%	$\chi^2(2) = 3.82$, $p = 0.15$
Physical asset protection	15^b	19.0%	18	13.5%	7^a	3.1 %	40	9.1%	$\chi^2(2) = 18.48$, $p < 0.001$, Cramer's V = 0.22
Common space	6	7.6%	15	11.3%	16	7.0%	37	8.4%	$\chi^2(2) = 1.02$, $p = 0.60$
Competitive game	6	7.6%	14	10.5%	15	6.6%	35	7.9%	$\chi^2(2) = 0.81$, $p = 0.67$
Emotions	1	1.3%	11	8.3%	4	1.7%	16	3.6%	Not enough cases for reliable statistical testing
Social norm	6	7.6%	2	1.5%	8	3.5%	16	3.6%	Not enough cases for reliable statistical testing
Sex/relation	0	0.0%	7	5.3%	0	0.0%	7	1.6%	Not enough cases for reliable statistical testing

As can be seen, the utterances from both groups corresponded to a large extent to the domains to which cyber insecurity was compared. The domains, cybersecurity was predominantly compared to, were "public health", "ecosystem", "cooking food", "market place" and "battlefield". When considering the comparisons made within these domains, we see that the professional audience's utterances were sometimes literally the same as campaign utterances. For example, within the domain "physical asset protection" both the campaign and professional audiences utterances focus on outdated methods of cyber security comparing it with old hardware and software (flash memory cards) or old-fashioned computer devices or programs, such as "Windows XP".

Still, Table 2 also reveals significant differences with regard to the use of certain domains. The domain "ecosystem" was significantly more frequent in the campaign utterances ("cybersecurity is like a greenhouse effect") and significantly less frequent in the target audience utterances on *Twitter* when compared with the general distribution of the corpus. Similarly, the domain "physical asset protection" was significantly more frequent in the campaign ("providing cybersecurity is locking all the doors") and unexpectedly less frequent in the professional audience utterances on *Facebook.*

Moreover, in some cases the professional audience, probably due to their being more tech-savvy, was more daring and provoking than the campaign. This becomes clear when examining slogans that have to do with "public health" and "common space". For example, the target audience came up with "maintaining cybersecurity is treating AIDS with penicillin" whereas the campaign introduced "maintaining cybersecurity is speed dating" and "cybersecurity is unlocking toilet doors". So, whereas coming up with analogies from the same domain, the professional audience sometimes co-constructed the utterances in a somewhat more creative or deviating manner.

[2] Note: The superscript *a* means "less than expected" and *b* "more than expected" based on standardized residuals. Utterances could be annotated as positive, negative or neither, and categorized under more than one domain. Metonymy and attribution were combined into one category for statistical testing as separately they did not have enough cases for a statistical test to be reliably performed.

Another distinction which can be made is between comparisons with objects or behaviors that evaluate cyber security measures as outdated and those that evaluate them as a negative behavior. The campaign participants more frequently resort to the domains "ecosystem" and "physical asset protection" than the target audience which are most exemplary of outdatedness. However, the professional audience preferred other comparisons, comparing current cyber security measures to something unpleasant ("current cybersecurity is trespassing someone's property"), bad ("entering through a backdoor (a type of vulnerability)/ a hole in the fence, disgusting ("being vulnerable is like sharing your dinner with an enemy"), or socially immoral ("maintaining cybersecurity is so much dancing at someone's funeral"). With these kinds of metaphoric utterances, the professional audience co-constructed the ones that deviated from the campaign utterances, but still attached a negative valence to cyber security measures, thus calling for decisive steps to be taken to counter ever-changing cyber threats.

7.4 Implications of newly co-created metaphors

The analysis of co-created metaphors reveals that the health, burglar and war scenarios of maintaining cybersecurity are still pervasive as the proportion of battlefield, physical asset protection and public health metaphors in the corpus is still high. However, the co-creation procedure has enabled us to elicit new metaphorical models prompting the alternative solutions to addressing cyber crimes and malicious attempts.

For instance, the ecosystem metaphor, one of the most frequent in the selected corpus, can be applied to cyberspace in a number of different ways. First of all, it implies complex interconnection and functional interdependency between the bodies and entities involved in the cyber world, which is similar to interpedendence of diverse species in the ecosystem. Secondly, the advantage of this metaphor lies in the fact that an ecosystem is able to accommodate a new entity or to change in response to shifts in the environment. This adaptive aspect has been shown to be explicit in several papers on the technological ecosystems (Gediminas, 2004; Iansiti & Richards, 2005) stressing that "like its biological counterparts, the IT ecosystem is characterized by a large number of participants who depend on each other for their mutual effectiveness and survival". The appeal of the ecosystem metaphor in the cyber discourse is in the focus on the diversity or interrelationship of cyber constituents. The familiarity of the concept of ecosystem might be another factor. Along with these factors, its productivity in the corpus can be attributed to the positive connotation of the prefix *eco* -. Characterizing the Internet as an ecosystem contributes to rebranding cyberspace as a living environment organism deserving of conservation and care, thus also involving a notion of cyber ecosystem health. The image of such a green, non-threatening cyber ecosystem seems particularly appealing.

The market-related metaphors found in the corpus suggest that the Internet with all its advantages and hidden threats can be seen as a vast marketplace in which goods and services are continuously bought and sold. Despite the lack of the physical attributes of traditional marketplaces, hardware and software systems are also bought and sold. But in our view, such direction of metaphorical exploration is aimed at identifying the ways market and economic principles might be applied to lacking secure systems, changes in economic incentives might change that trend towards more secure operations. This implies creating incentives to harness the self-interest of the market participants in the ways that would result in greater security. On the one hand, such a perspective might be useful in reducing the profits from the development and use of malware by cybercriminals. Moreover, purchasers of computers and software would be empowered to demand that manufacturers guarantee some level of security in their products, and also willing to pay higher prices for greater security.

The idea of "baking cybersecurity" implies careful consideration and thoughtful development of software able to counter various kinds of threats. This approach sounds more sensible than continuing by adding on security measures after new software and hardware are developed and fielded. The inference to be made is that developers should be "skillful cooks" able to prepare a secure dish, which, if being undercooked, can be poisonous for those who eat it. This metaphoric route may stimulate increased selectivity in choosing appropriate and safe strategies of maintaining cybersecurity.

Thus, metaphors provide us with novel and useful insights into cyberspace, but we cannot reasonably rely on metaphors to suggest the entirety of the challenge the Internet offers us. The more undifferentiated aspects of the internet a metaphor is intended to cover, the greater the likelihood is that it will either circumscribe our thinking or dwindle to little more than an empty catch phrase (Karas, Moore & Parrott, 2008). When these things happen, an originally useful metaphor no longer contributes to constructive debate, and may even complicate it.

8. CONCLUSIONS AND DISCUSSION

Our corpus-linguistic analysis of metaphoric utterances from the cybersecurity campaign was aimed at substantiating the application of co-creation as a way to reframe the cybersecurity discourse. To this end, we posed three research questions concerning the valence of the produced utterances, their co-construction, and the differences between slogans on different SNSs. RQ1 concerned the conversational valence of the campaign and professional audience utterances. The prior exposure to evoked metaphors prompted the campaign audience to talk about current cybersecurity measures with a negative valence. The professional audience also elicits more negative than positive valence in their utterances. However, the campaign is less negative compared with the overall valence in the collected corpus of metaphoric utterances. A possible explanation for this may be the fact that the professional audience is more explicit and daring in their evaluation of cybersecurity measures on SNSs and make more use of attributions. Moreover, they do not necessarily compare current measures to counter cyber threats with something outdated, but also with something unpleasant, disgusting, or socially immoral. These types of comparisons often make valence more explicit. As for *Twitter*, the professional audience attached both relatively more negative and positive valence to their utterances compared with the general distribution of the corpus. In our view, this positive valence can occasionally be the consequence of comparing cybersecurity with something possessing a positive valence. The professional audience thus seems to create ironic slogans that eventually do follow the campaigns' negative valence and compare cybersecurity with something negative. However, since this study focuses solely on the content of the utterances and lacks any information about the position of the metaphoric utterance creator, it is hardly possible to decide whether they are actually meant to be ironic.

In regard to RQ2, we have analyzed how the professional audience co-constructed the cybersecurity-related utterance by filling in the second part of the sentence, in comparison with the campaign participants. The campaign predominantly produced utterances that can be categorized as comparisons, while the professional audience on *Facebook* introduced fewer comparisons but more attributions and metonymies compared with the general distribution of the corpus. Highly creative attributive utterances of the professional audience do not meet the campaign's intentions to compare cybersecurity measures with something outdated only, thus suggesting some new framing scenarios. Nevertheless, the form in which they talk about it does not correspond to the comparisons that the campaign participants use in a conversation about cybersecurity. Interestingly enough, but on *Twitter*, the opposite is true: the professional audience employs more comparisons and fewer attributions and metonymies in comparison to the overall use of these types of utterances.

Further analysis of the co-created utterances revealed which domains the campaign and the professional audience compared cybersecurity to. The first part of the utterance gives the professional audience a myriad of possibilities for finishing the sentence. However, it mostly followed the domains that were previously introduced by the campaign. In this respect, we can classify the co-construction as presupposed resonant in Du Bois's terms (2014). It should also be mentioned that the professional audience deviates from the campaign participants in the use of the domains "ecosystem" and "physical asset protection". These domains were more often found in the campaign utterances compared with the general distribution of the corpus. An explanation for this difference can be attributed to the fact that the professional audience may deviate from the comparison of cybersecurity measures with something outdated and, as a result, less frequently resort to the domains that are closely associated with this comparison. General public might not understand why current cybersecurity measures are treated as something outdated, as they are not aware of the previous state of affairs in the field and might therefore focus on cyber vulnerability as something bad or unpleasant in general.

Another characteristic of the professional audience's utterances is their provocative nature. This serves as an indicator of the campaign opting for utterances containing generally accepted social norms, whereas the professional audience challenges them with utterances that are more daring and promoting views which are not online with generally shared social norms. Besides, the professional audience creations appeared to include insiders' jokes ("providing cybersecurity is falling down the stairs"), personal preferences and dislikes ("providing cybersecurity is having your favourite tomato juice"), and irony ("current cybersecurity is agreeing on CO2 emissions cap"). In this respect the campaign co-created utterances were designed to be understood and accepted by a broader public which is not tech-savvy, whereas the professional audience contributed to reframing the current discourse by creating more creative slogans. This shows how the co-created metaphoric utterances are mediated by professional context, along with social and cultural ones.

The study findings enabling us to answer RQ3 are in line with previous research (Smith et al., 2012) and suggest that the professional audience engages in co-creation with the cyberecurity awareness campaign unevenly and to varying degrees on different SNS. The differences found between the utterances can be explained by following the different co-creation routes regarding *Facebook* and *Twitter*. The *Facebook* slogans were created during the campaign events, where participants were photographed with their co-created slogan on a whiteboard, with the pictures subsequently being posted on the *Facebook* page. The *Twitter* slogans, on the contrary, were directly posted by the professional audience. *Facebook* features the slogans of the professional audience, frequently focusing solely on the negative valence and direct meaning of the attribution or metonymy-based slogan. The slogans of the professional audience on *Twitter* were more expressive in terms of valence and more creative concerning the type of utterances.

The study, nevertheless, has certain limitations. Since the campaign was targeted at general public and distributed through mass media and social networks inviting anyone willing to contribute, data collected from social media about the users is limited. Another issue of concern is that people may create alternative or multiple identities online making it impossible to identify a creator of slogans. Other difficulties include annotating certain categories, coding the data when some utterances contained urban or professional language or referred to specific cultural knowledge.

To sum up, this case study has enabled us to identify both promising strategies of reframing pressing and controversial issues and challenges of cybersecurity metaphor co-creation. It has exemplified an alternative strategy of (re)framing issues of public concern opening new opportunities for further research. One possible line of research along these lines is to test the behavioral effects of co-creation campaigns by measuring whether the co-construction of metaphoric utterances eventually affects the line of policies pursued by policy-makers and the cybersecurity community. Further research might also shed some light on people's motivations to participate in co-creation events and the reasons behind their preference for certain domains when looking for analogies.

REFERENCES

Adomavicius, G., Bockstedt, J.C., Gupta, A., & Kauffman, R.J. (2004). An Ecosystem Model of Technology Evolution. Retrieved from http://misrc.umn.edu/workingpapers/fullpapers/2004/0429_112404.pdf , December 12, 2019.

Akaka, M. A., Schau, H. J., & Vargo, S. L. (2013). The co-creation of value in cultural context. In R. W. Belk, L. Price, & L. Peñaloza (Eds.), *Consumer culture theory* (Vol. 15, pp. 265–284). Bingley, England: Emerald.

Bacile, T. J., Ye, C., & Swilley, E. (2014). From firm-controlled to consumer-contributed: Consumer co-production of personal media marketing communication. *Journal of Interactive Marketing*, 28, 117–133. doi:10.1016/j.intmar.2013.12.001

Betz, D. J., & Stevens, T. (2013). Analogical reasoning and cyber security. *Security Dialogue*, *44*(2), 147–164. Retrieved from: https://doi.org/10.1177/0967010613478323, November 29, 2019.

Betz, D.J., & Stevens, T. (2011). *Cyberspace and the State: Toward a Strategy for Cyber-Power*. Abingdon: Routledge.

Bobrow, D.B. (1996) Complex insecurity: Implications of a sobering metaphor: 1996 presidential address. *International Studies Quarterly* 40(4): 435–450.

du Bois, J. W. (2014). *Towards a dialogic syntax. Cognitive Linguistics*, 25, 359–410. doi:10.1515/cog-2014-0024

Brito, J., & Watkins, T. (2011). Loving the cyber bomb? The dangers of threat inflation in cybersecurity policy. *Working Paper, 11-24. Arlington, VA: Mercatus Center, George Mason University*.

Charney, S. (2010). Collective Defense: Applying Public Health Models to the Internet. Microsoft. Retrieved from: http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/internethealth.aspx October 20, 2019.

Conway, M. (2008). Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. In: Dunn Cavelty, M. and Kristensen, K.S. (Eds.)

Securing 'the Homeland': Critical Infrastructure, Risk and (In)security (pp. 109–129) London: Routledge.

Esbrí-Blasco, M., Girón-García, C. & Renau, M.L. (2019). Metaphors in the digital world: The case of metaphorical frames in 'Facebook' and 'Amazon'. *Series: Applications of Cognitive Linguistics*, nº 39. Mouton de Gruyter

Fillmore, C.J. (1982). Frame semantics. In The Linguistics Society of Korea (Ed.), *Linguistics in the Morning*. Seoul: Hanshin, 111–137.

Gebauer, J., Füller, J., & Pezzei, R. (2013). The dark and the bright side of co-creation: Triggers of member behavior in online innovation communities. *Journal of Business Research*, 66, 1516–1527. doi:10.1016/j.jbusres.2012.09.013

Gozzi, R. Jr. (1994). The Free Library by Farlex, July 1994. Retrieved from: http://www.thefreelibrary.com/The+cyberspace+metaphor.-a015543199 October 21, 2019.

Hallam-Baker, P. (2008). *dotCrime Manifesto: How to Stop Internet Crime*. Upper Saddle River, NJ: Addison-Wesley.

Hendriks, H., van den Putte, B., & de Bruijn, G. (2014). Changing the conversation: The influence of emotions on conversational valence and alcohol consumption. *Prevention Science*, 15, 684–693. doi:10.1007/s11121-013-0418-2

van den Heerik, R. M., van Hooijdonk, Ch.M. J., Burgers, Ch. & Steen, G. J. (2017). "Smoking Is Sóóó ... Sandals and White Socks": Co-Creation of a Dutch Anti-Smoking Campaign to Change Social Norms, *Health Communication*, 32:5, 621-628, doi:10.1080/10410236.2016.1168000

Hook, G.D. (1984). The nuclearization of language: Nuclear allergy as political metaphor. *Journal of Peace Research* 21(3): 259–275.

Hoyer, W. D., Chandy, R., Dorotic, M., Krafft, M., & Singh, S. S. (2010). Consumer cocreation in new product development. *Journal of Service Research*, 13, 283–296. doi:10.1177/1094670510375604

Iansiti, M., & Richards, G.L. (2005). Information Technology Ecosystem Health and Performance. Retrieved from: http://www.hbs.edu/research/pdf/06-034.pdf, October 20, 2019.

Küpers, W. (2012). Analogical Reasoning. In: Seel N.M. (eds.) *Encyclopedia of the Sciences of Learning*. Springer, Boston, MA.

Karas, T. H., Parrott, L.K., Moore, J.H. (2008). Metaphors for Cyber Security, Sandia National Laboratories, Albuquerque, NM 87185-0839.

Lakoff, G. (1987). The death of dead metaphor. *Metaphor & Symbolic Activity* 2(2): 143–147.

Lakoff, G., Johnson, M. (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*., 26, 3, 211-254.

Lapointe, A. (2011). When Good Metaphors Go Bad: The Metaphoric 'Branding' of Cyberspace. *Center for Strategic and International Studies*. Retrieved from: https://www.csis.org/analysis/when-good-metaphors-go-bad-metaphoric-branding-cyberspace, Novemmer 3, 2019.

Lawson, S. (2012). Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, Volume 17, Number 7 - 2 July 2012. Retrieved from: https://firstmonday.org/ojs/index.php/fm/article/view/3848/3270, November 17, 2019. doi:10.5210/fm.v17i7.3848.

Muntinga, D. G., Moorman, M., & Smit, E. G. (2011). Introducing COBRAs: Exploring motivations for brand-related social media use. *International Journal of Advertising*, 30, 13–46. doi:10.2501/IJA-30-1-013-046

Ortony, A. (Ed.). (1979). *Metaphor and thought*. New York: Cambridge University Press.

Prahalad, C. K., & Ramaswamy, V. (2004). Co-creation experiences: The next practice in value creation. *Journal of Interactive Marketing*, 18, 5–14. doi:10.1002/dir.20015

Rauscher, K.F., & Yaschenko, V. (2011). *Critical Terminology Foundations*. New York: East West Institute.

Ruiter, R. A., Kessels, L. T., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, 49, 63–70. doi:10.1002/ijop.12042

Schön, D. A. (1979). Generative metaphor: A perspective on problem-setting in social policy. In A. Ortony (ed.) *Metaphors and Thought*, pp. 254-283. Cambridge: Cambridge University Press.

Smith, A. N., Fischer, E., & Yongjian, C. (2012). How does brand-related user-generated content differ across YouTube, Facebook, and Twitter? *Journal of Interactive Marketing*, 26, 102–113. doi:10.1016/j.intmar.2012.01.002

Stohl, M. (2006). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point, or patriot games? *Crime, Law & Social Change* 46(4–5): 223–238.

Wisniewski, C. (2013). Comment: There's No Such Thing as Cyber War. *Infosecurity Magazine*. Retrieved from http://www.infosecurity-magazine.com/view/33755/comment-theresno-such-thing-as-cyber-war-/, June 19, 2019.

Wolff, J. (2014). Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors. Paper presented at TPRC Conference, March 31, 2014. Retrieved from: http://dx.doi.org/10.2139/ssrn.2418638, May 30, 2019.

Zwass, V. (2010). Co-creation: Toward a taxonomy and an integrated research perspective. International Journal of Electronic Commerce, 15 (1), 11–48. doi:10.2753/JEC1086-4415150101