Working Papers No. 23

The Original Battle Trolls: How States Represent the Internet as a Violent Place

Ben Kamis/Thorsten Thiel

January 2015

PRIF Peace Research Institute Frankfurt
HSFK Leibniz-Institut Hessische Stiftung Friedens- und Konfliktforschung

Member of the Leibniz Association

The Original Battle Trolls: How States Represent the Internet as a Violent Place

Ben Kamis/Thorsten Thiel

In this paper we argue that the rise of the 'cyber war' metaphor is connected to the spread of the norm of sovereign statehood on the Internet. Although early discourse about the social and political meaning of the Internet prophesied a stateless utopia, the growing importance of digital communication triggered an active proliferation of state-based metaphors. States began not only to seize legal and technical control of the Internet, but also started to shift the discourse on digital affairs, emphasizing typical attributes of statehood, like collective subjectivity, territoriality and hierarchical structuring. This happened through language, and the metaphor of cyber war and the related narrative of sovereign statehood is one of the strongest cases in point. The paper shows how metaphors and narratives work and why they are so important by, firstly, giving an introduction into the role of metaphors in discourse and cognition, then sketching the role metaphors play in the particular discourse on the Internet and finally examining how especially pacific and Internet-friendly states, like Estonia, Hungary and Germany, deploy the cyber war metaphor.

1. Introduction

No one reading this paper will seriously doubt the social and political significance of the Internet. Much of life's dynamic experience is mediated through its communicative and interactive technology, and much of life's static representation is stored in vast, standardized databases. In fact, this space between experience, representation and material technology provides the occasion for this paper, because the Internet's material ontology supports such a broad range of social ontologies. In other words, everyone can agree that the Internet consists of storage media, transmission media and electromagnetic pulses in material terms, but there is much less agreement about what any of that means for human social interaction. The Internet may be a transformative technology, but determining what the Internet *means* is a complicated and politically charged activity.

In order to discern the meaning of the Internet, how people refer to it and speak about it is a logical stating point. Many of the commonly invoked terms highlight its ability to enhance communication and reinforce sociality. Typical examples include 'digital commons', 'information superhighway' and 'world wide web'. What these terms all seem to share, is a techno-utopian predilection: the Internet is represented as a borderless space, where everyone can participate.

Cyber war, then, is a puzzle of hardly comparable significance: war on the Internet. The puzzle lies in the fact that the same cyberspace that hosts countless chats between old friends, where people trade, share, play and find tawdrier pleasures is simultaneously represented as a warzone where armies are constantly engaged in combat. A cyber attack could right now be travelling through the same cable as a cooperative gesture in a multiplayer game or a warm greeting on a social network. Cyber war, then, is a powerful, but slightly counter-intuitive, representation of the Internet. But what does this representation entail and how is it made discursively manifest?

In this paper we assume that the rise of the cyber war metaphor is directly connected to the spread of the norm of sovereign statehood on the Internet. Contrary to much of what is stated in the political science literature on governing the Internet, we posit that states make use of particular discursive structures to justify their regulatory authority and compulsive powers. The sword is not enough; the power of words is needed, too. For the state to thrive on the Internet it must also win the conceptual struggle over what the Internet is imagined to be and how it is described and conceptualized. Only if people accept the statist representation of the Internet will they allow

governance practices that enable the state to act preventively and ubiquitously, thereby rescinding the open and decentralized architecture of the Internet.[1]

We argue that painting the Internet as a dangerous and violent place is an image that helps enable states to reappropriate their traditional privileges. The narrative that only in a world organized around states can war be prevented, and otherwise it would be the default mode of life in anarchy is the oldest argumentative trick in the book on sovereignty and statehood. By invoking the metaphor of cyber war, states shift the discourse and narrative of the Internet. And this is why in the title of this paper we equate their behavior with trolling. Of course, states do not post indecent comments on blogs, but they do indeed behave like trolls in terms of the Internet discourse as a whole. According to Wikipedia, troll behavior consists of uttering 'inflammatory, extraneous, or off-topic messages […] with the deliberate intent of provoking readers into an emotional response. By constantly making threats and shifting the topic from the possibilities of communication to risks and vulnerabilities, states seduce citizens into accepting their depiction of the Internet.[2] Once, this narrative has been accepted, norm-setting and institutional policies follow directly and 'inexpensively' from the justificatory force of the sovereign understanding of order.

Our argument proceeds in three steps. First, we clarify what we mean by metaphor and narrative as theoretical concepts and exactly how we intend to use them. Second, we ask in general terms how the state has managed to apply statehood to the Internet. After a brief period during which the statist narrative appeared unconvincing and superfluous, the growing importance of digital communication in diverse aspects of life triggered an active proliferation of state-based metaphors. States began to seize legal and technical control and to shift the discourse about digital affairs. In order to do this they represented themselves as natural entities and the logic of sovereignty as a prerequisite for commodious social life. Our claim is that 'violence' and 'war' are congenial to a state-based ontology. In the third part of the paper we analyze the use of one special metaphor, that of cyber war. We posit that the concept of 'cyber war' can only be understood metaphorically, but it is not 'just a metaphor', because it suggests further metaphorical representations and privileges some speakers and actors over others. Overall, we hope to contribute to the understanding of how the norm of sovereign statehood spreads and persists in cyberspace.[3]

2. Pictures and Stories, Metaphors and Narratives

Given our claim that cyber war and associated metaphors reinforce a statist narrative of what the Internet is and how it is constituted as a political object, we should first clarify what we mean by 'metaphor' and 'narrative'.

As for metaphor, there are three principal conceptualizations of the term: the rhetorically epiphenomenal, the cognitive, and the discursive. For our purposes the discursive conceptualization is most appropriate because it grants metaphors their due as effectual modes of

1 Of course, this openness is also under threat from private actors, as was also the case with the development of telecoms networks and radios (Wu, 2010; Zittrain, 2009). Nevertheless, in this paper we will only focus on the state side of the equation, not judging which threat is more urgent and not following up on how the two are connected.

2 Despite the treatment of normative topics and questions, this paper is not primarily a normative endeavor. Instead, our goal is to focus on the *How* of the semantic (re)production of order.

3 This study contributes to the literature on the Internet and politics by making use of an innovative and enlightening methodology. While there has been voluminous research on the mechanisms that states have used to arrogate the order of the Internet, on the 'reality' and importance of cyber wars and the normative value of the different understandings of ordering the Internet Deibert and Crete-Nishihata (2012), only lately has the discussion turned towards the finer, more semantic aspects of the 'contested ontology' of order in cyberspace. We contribute to this debate by, first, adding a theoretically richer view on the composition of the statist narrative and the relationship to its contenders as well as by analyzing the especially important metaphor of cyber war as an empirical phenomenon and a theoretical construct used to expand the application of sovereign statehood. This is related to the securitization research program that has been deployed with great success to analyze current shifts in Internet governance (Dunn Cavelty, 2008a, 2008b, 2013; Hansen & Nissenbaum, 2009; Hart, Jin, & Feenberg, 2014; Nissenbaum, 2004, 2005), but it takes narrative and perlocution somewhat more seriously and focuses on atypical, 'hard' cases.

communication and leaves space to consider how metaphors branch out and relate to each other without making strong causal claims about how they work cognitively. With regard to narrative, there are two ways the term is generally used in such studies: as an analytical construct and as a means of representing and organizing objects, subjects and events into a more or less coherent reality. Because we are less concerned with how to present our data than what kind of broader inference we can draw from it, such that we are trying to *read* the story off the data than *write* a story into them, we prefer the latter conceptualization.

Although the philosophical, linguistic and social scientific literature treating the form, cognition and use of metaphors is vast, the theories can be roughly grouped into three categories: Firstly, the Aristotelian view, according to which metaphors are merely stylistic literary devices used for rhetorical effect (Glucksberg, 2008; McGlone, 2007; Searle, 1979). Here metaphors add rhetorical flourish to a text without affecting the literal semantics or the content of the discourse. Many topics, however, like quantum theory and politics, and many objects, like the state, seem to require more substantively metaphorical language (Chilton & Lakoff, 1989; Glucksberg, 2008). The second is conceptual metaphor theory (CMT), which argues that metaphors are based on our experiences of bodies moving through space and that they reflect how thought and concepts are structured (Chilton & Lakoff, 1989; Lakoff, 1992, 1993; Semino, 2008). The process of analyzing metaphors consists of describing how the source domain, which is the non-literal concept invoked, 'maps' onto the target domain, which is the actual topic of discussion, and how this mapping yields further implicit connotations. This type of analysis has been put to good use in several studies in the social sciences, treating topics such as missile defence (Flanik, 2011), war (Lakoff, 1992), weapons proliferation (Mutimer, 1997), historical learning (Shimko, 1994), terrorism (Spencer, 2012) and law (Winter, 2008).

Discursive metaphor theory analyzes how metaphors are used discursively. Milliken (1999) has suggested that analyzing metaphors in the mode of poststructuralist semiotics is a valuable form of discourse analysis. Alternatively drawing on Wittgenstein, Fierke (2002; 1997) has described the familial metaphors of Cold War rhetoric in terms of language games with attendant grammars that predispose a culture to a particular form of life. Zinken (2003) developed the related concept of intertextual metaphors, which are informed by an author's experience as a consumer of culture, and although they do not necessarily exclude conceptual metaphors informed by bodily experience, he found that such intertextual metaphors are more common than conceptual metaphors in the most important and salient parts of journalistic texts. This approach also allows for the mapping process described by CMT to work in both directions so that in the relation established between the source domain and the target domain, the latter colours the former as well. This third category of how to conceptualize metaphors suggests that discursive metaphors are used in communication, they are effectual, and they can and should be studied.

Fortunately, our argument need not rest on showing how metaphors work cognitively. We claim merely that, although metaphors probably have some cognitive effect, people do in fact tend to *communicate* in metaphorical terms, even if they do not always *think* metaphorically. So for our pragmatic purposes, Semino (2008) provides the most appropriate definition, whereby metaphor is 'the phenomenon whereby we talk and, potentially, think about something in terms of something else'.

Metaphors rarely travel alone, so mapping is useful to analyze what further metaphors a given metaphorical representation would entail, such as the notion that invoking games as a source domain for some practice would likely make winning and losing more salient and coherent as outcomes than they otherwise might be. Further, a given metaphor might make other metaphors more salient and accessible to certain discourses. For example, using evolution as a source domain in a discourse about, say, economic activity might also make other source domains more likely, such as war and sport, where evolution is also a common source domain. We label such connections between source domains and their ability to implicate each other in the discourse about a given target domain 'metaphorical productivity'. How broadly semantic fields such as

these extend in actual discourse, however, is an empirical question, and as we will argue below, 'cyber war' is a very productive metaphor in that it brings many other source domains into the discourse. The metaphors are part of a larger picture, and we make claims about the form of this picture on the basis of the metaphors. Our means of making this inference is the concept of narrative, which we must now explain.

Narrative also has multiple uses in the social sciences. The first conception depicts it as an analytical construct that helps us to interpret data. Narratives then, are a means of organizing data in order to make them intelligible (Abell, 2001, 2009). As with a statistical model, the analyst constructs the narrative by ordering the data in a particular fashion, so the analyst imposes the narrative upon the world as an explanatory device. A second conception sees narratives as features of the world for the observer to find and analyze. Here narratives bring functional details, like characters, their attributes, objects and events, into a temporal order or overarching sequential structure, and these structures follow rules and grammars like sentences, which make them open to comparison as well as internal analysis (Barthes, 1977). The internal rules of narratives have to do with the functions of the representations they contain, and some representations in the narrative bind its future course in a relation of 'narrative necessity' (Bruner, 1991).

Although these social narratives also serve to organize the experience of reality just like the analytical narratives, they are posited to exist as objects in society that the analyst discovers and interprets (Bevir & Rhodes, 2006). That is, the story of social reality contained in the narrative not only describes what is and how it came to be, but also what counts as improvement and progress and what as corruption and deterioration (Cover, 1983-1984). That narratives, therefore, are morally laden also implies that they are politically charged and subject to dispute and negotiation. The fight for narrative hegemony is not just a weak echo of the struggle over material realities, such as 'realist' positions claim that disprove the 'utopias' of net-utopians all the time (Drezner, 2004; Morozov, 2011). We assume that these narratives have a life of their own and are relevant in and of themselves. Capacity-building practices and the possibility to think and act in certain ways result from these narratives and the horizon of possibilities they reveal.

It is also important to note that narratives are not created *ex nihilo*. Rather, they can only persist when they fit the interplay of material factors and technical infrastructures. This implies that the ontology of the Internet is a complex affair, consisting both of more or less 'objective facts', like the quantity and capacity of subsea cables, as well as the meaning attached to them through the construction of metaphors and their integration into stories of progress and calamity. These two aspects inform each other, with the materiality of the Internet making some metaphors and narratives more salient and the metaphors and narratives informing the apprehension of the status quo and the development of new material capacities. Although we acknowledge this ontological complexity, our discursive approach also naturally focuses more on the meaning of the Internet than on its nuts and bolts or hardware and software.

The tasks below, then, are to consider the narrative into which the metaphor of cyber war fits as well as to examine its metaphorical productivity empirically. The first will require an examination of how the Internet developed and the technical possibilities it opened, how these developments have been represented through time, as well as how these representations fit together in a larger narrative. Although the social meaning of the Internet is likely to be roughly stable day-to-day, its historical novelty and ontological complexity also imply that there has been considerable discursive space for competing representations. As described below, the initial techno-utopian narrative based on the frantic and disorderly growth of the new technology quickly yielded to a statist narrative characterized by domestic political hierarchy and international anarchy, which the war metaphor concretizes, justifies and reinforces. The second task will involve examining the metaphorical representation of cyber war and the other metaphors that it generates.

3. The Setting and the (competing) Narrative(s)

Using these concepts, we now illustrate the main characteristics of the statist narrative and contrast it with its main challenger in the discourse on order in cyberspace. Once the main differences between the two competing narratives have been depicted and the antagonistic relationship explained, we will further examine the basic justificatory narrative that is proposed to advance the norm of sovereign statehood in the Internet, namely: violence and war.

From its very beginnings the Internet promised to diverge from centralized, territorial statism. Its decentralized and non-proprietary structure makes it a generative system that allows for an indefinite number and open development of possibilities. Even if it started out as a state-funded endeavour, the open architecture of Internet communication sparked the imagination of a new kind of networked order that could free itself from controlling influences and allows new ways of connecting people. Fittingly, the history of the founding fathers (and the very few mothers) of the Internet is deeply intertwined with counterculture, a playful, anarchical spirit and a strong belief in technology and its benefits (Turner, 2006). During the rise of the mass Internet from the eighties onwards there was a strong sense that cyberspace must be understood as a space of its own, a strange kind of place where normal rules and routines do not apply and state governance is neither needed nor possible.[4]

What, though, makes the networked order so different from the logic of statehood? Ever since the invention of the national state, the question of how best to set up an effective and lasting collective order seemed settled. Sovereign statehood expanded across the entire globe and left nothing untouched. Even in times of global governance, the state is still the basic anchor, or at least the ever-present background condition for all modes of collective action. It regulates social organization and enables as well as limits the way we interact and associate.

Statehood as an organizing principle is based on some common elements – namely state territory, state people and state power. From these follow more intrinsic characteristics that reflect the historical development of the national state. In our context the most important one is the need to organize state power in a hierarchical fashion, meaning on the domestic level that the state has to establish a certain kind of authority structure in order to reach decisiveness and coherence, two elements best captured in the concept of sovereignty. Only if ordered in a sovereign fashion can the state create the requisite level of control and controllability leading to security and prosperity. At the international level sovereignty implies an anarchical system of co-existence, where the state exists among equal, sovereign entities and, in principle, ascribes the same autonomy and self-regulating capacities to them all.[5]

As a contrasting view, the network architecture of the Internet allows us to imagine workable forms of social order and collective action that are more situational, overarching and spontaneous. Connective action (Bennett & Segerberg, 2013) emerges as a new and promising form of acting together that does not rely on the shadow of hierarchy to be successful. Ideas of participatory democracy and more flexible, less permanent political entities become thinkable. Anonymity and decentralization also inspire a reconfiguration of political space and run contrary to the high-modernist ideology of the state that tries to organize and discipline its citizens in an effective manner. At least three influential variants of the newly emerging social imaginary of the Internet

4 This revolutionary spirit is present in all the early writings on the Internet and was in a more commercial style reinvented when from 2000 on the discourse of the social Internet took hold. Even if this new version is not so much based on a technical-structural description but on the social capabilities of many-to-many communications the rhetoric of connectedness and cooperation runs equally strong. The attractiveness of the vision and the belief in its force is not even hampered by the fact that today's social networks are better described as strongly hedged and highly regulated commercial enterprises than as utopian playfields.

5 One has to keep in mind that sovereignty has always been a "weak evolutionary stable strategy" (Krasner, 2001, p. 231). Sovereignty does not have to be encompassing, nor does it need to constantly reassert itself even if it is in theory an unstable idea. What counts is that sovereignty is widely recognized as the central organizational principle and that the keepers of sovereign power preserve their capacity to decide along their stated will at crucial moments.

can be identified, but each is based on a different configuration of the connection between freedom, horizontality/democracy and openness: a communitarian variant, where the capacities for cooperation and community-building are highlighted (Rheingold, 1993, 2002; Shirky, 2008), a more anarchic version that stresses newly emerging self-organizational capacities and shifts in the modes of production (Benkler, 2006, 2013; Kelty, 2005) and a libertarian version that emphasizes the expansion of the means to self-expression and the possibilities to realize personal autonomy (Dahlberg, 2010; Schmidt & Cohen, 2013).[6]

The real utopias developing out of these trajectories, then, spill over from the Internet discourse to the broader domain of social life, where new ways of communication have changed how we interact, trade and organize (Benkler, 2013). Since our thinking and behavior in the long run might adapt to these reconfigured entities, the Internet has been described as some kind of meta-power able to change how we represent ourselves and the narratives into which those narratives are organized (Castells, 2010; Singh, 2013). Many Internet pioneers, therefore, presented the statist, hierarchical order as a waning narrative that would inevitably succumb to the superiority of networked forms. Over time the state would become redundant.[7] The motivation for this view is the conviction that it would be impossible for the state to control unbounded end-to-end communication, which would eventually lead states to accept their own inexpediency and bow to the facticity of newly emerging self-organizing communities.

As is always the case, these utopian predictions came to nought, revealing technological determinism and the uncontrollability of cyber affairs as a fantasy. Over time states have developed the technical capabilities, such as filtering mechanisms and virtually ubiquitous access to many forms of network communication, as well as the legal means to gain control over many aspects of Internet communications. From a regulatory point of view, the Internet can no longer be treated as a separate identity, something that has its own substance, logic and rules as imagined by the Internet pioneers. Instead, governing the Internet by and through states has increasingly become something not only thought of as possible, but even as 'normal' or 'desirable'. This general trend of the 'etatisation' of the Internet – the state becoming a dominant actor in all things cyber – has often been described (Deibert, Palfrey, Rohozinski, & Zittrain, 2012; Goldsmith & Wu, 2006) and is not only related to the factual rise of censorship and filtering, but to the whole arrangement of organizing life on the Internet. States are not only able but also willing to regulate and interfere in all things cyber.[8]

While the structural and material realities swiftly changed, or always had been misjudged by the utopians, the struggle for narrative supremacy continues. Neither *de jure* nor even *de facto* control has overcome the overall challenge the rise of the Internet poses to the norm of statehood. Though sovereignty might be based on territory, population and power, it also depends on a certain kind of unquestioned recognition as a social reality, as a necessary setting for any given political narrative. With hindsight, one can see that in the realm of cyberspace the biggest challenge does not lie in technical control but in the much loftier issue of recognition. As long as the main principle of statehood is questioned, states will have to work on making themselves indispensable and appearing natural, and to this question we now turn.

---

6 While the latter might be the most mundane in terms of utopian spirit and basically understands the Internet as an extension of the market side of the market-state dichotomy, it still plays an important role in that it is connected with the forces that drove the enormous development of the Internet and backed by Silicon Valley's mighty entrepreneurs, providing resources and political influence to uphold certain structural features of the Internet as we know it.

7 The situation is, of course, very different in non-western regions of the world, where the normative vision of a free and open Internet never had the opportunity to prosper and where state powers are more centralized and less reliant on public support. There states tried to limit or control the Internet early on and often erected parallel structures to be able to control external influence and have intermediaries under strict control.

8 This does not necessarily mean that states had to abandon all of the new arrangements that have arisen out of the efforts to self-regulate the Internet. Quite often states have at least partially adapted to the network logic (Mueller, Schmidt, & Kuerbis, 2013).

What makes states unique and on what basis can they claim that their organizational capacities outrival the self-organizing capabilities of the net? In order to re-establish sovereignty and to reinvigorate the old hierarchical structure the state needs to reinforce its own narrative, which depends on its ability to muster accepted metaphors, understandings of progress and decay, and narratives of origin and destination. It is important to note, however, that this effort need not be part of a concerted, or even conscious, strategy. 'Need' here does not refer to a desire, but an evolutionary requirement in the face of competing narratives. Just as the prophets of the net utopia told a story of historical necessity to which many agents contributed knowingly or not, the state represents a different teleology whose story can be told by an omniscient narrator but enacted by unwitting players.

Social contract theory, according to which the state arises as the only possible collective guarantor of certain public goods, is especially prominent in justifying sovereign statehood. The three most prominent variants are the Hobbesian version, which is centered around the security of the individuals; the Lockean version, where the protection of property and the evolution of individual freedom is central; and the Rousseauean variant, which identifies republican freedom or, in modernized versions, justice and democracy, as crucial goods. All three narratives appear in attempts to justify a strong role for the state in cyber matters, but the Hobbesian logic appears to offer the most pressing solution as well as the logic most strongly opposed to networks.

So how does this justificatory narrative work? Hobbes's basic argument is that there is a structural insecurity inherent in horizontal ordering. Even without the contested anthropology, his argument leads to a couple of conjectures. The first is that societies can be represented as some kind of higher organism. Understanding societies as organisms results not only in the adequacy of centralizing power and establishing representational relationships but reveals the interdependence of individual and collective security. The vulnerability of the 'body politick' as a whole is then directly connected to the safety of each individual.[9] The second assumption is that fear is the strongest motivation for people to cooperate. Fear is understood as such a strong natural reaction that it renders all other deliberations moot. Avoiding fear then explains how collectives can overcome the initial costs of organizing in a hierarchical structure and empowering a certain force to keep fear at bay. So, the fear of internal divisions and external dangers in an apocryphal past become the main driver for the creation of states.

This leads us directly to the role of violence and war in state building. Appealing to violence entails appealing to an absolute and universally shared experience. Violence is characterized by immediacy and physicality, and though there are more dimensions and uses of the word 'violence', they all originate in the imagination and language of physical violence, something archaic and directly threatening. If threatened with violence or trapped at the brink of chaos, every individual has a reason to accept the necessity to create a sovereign structure. To cut a long story short, sovereignty is in the Hobbesian view "not a political choice but the necessary reaction to an anarchical condition" (Der Derian, 1993, p. 154).

What follows is that in order to end violence the state has to establish itself as a superior power, a power that is able to counter violence with violence or even preventing violence from happening altogether by controlling risks ahead of the violent event. While Hobbes concentrated on the reasons to monopolize violence in order to pacify internal relationships between citizens, he was also aware that outside of the state, in the sovereign relationship between states, the risk is perhaps even graver. The potential for violence between states in the form of war, therefore, becomes the

9 By contrast, networks are more resilient because of their different logic of connection. The framing of vulnerability and dependency, therefore, is something more akin to the statist imaginary. Fittingly, in a highly enlightening juxtaposition Helen Nissenbaum (2005) has contrasted the concepts of computer security, defined by availability, integrity and confidentiality, with cyber security. The former is born of a technically spirited perspective, while the second focuses more on the vulnerability of modern societies due to their reliance on computers and networks with concomitant demands preventive security measures. This shows that advocating a less state-based view does not necessarily imply freedom from the pitfalls of open networks and communications.

other main force in convincing citizens of the necessity of the state. Thus, just as violence was the imputed origin of the state-based organization of society, the statist narrative also includes violence as the potential future corruption against which the continuation of this state organization could be represented as progress.

So what does this mean for cyberspace and the discourse on order and the Internet? If the state is to prove its own indispensability, it has to show that the Internet is at least potentially a dangerous and violent place, a place that has to be ordered. As long as life in cyberspace does not appear to be 'solitary, poor, nasty, brutish, and short', but full of possibilities and opportunities, the state is of little use. But once the state has convincingly made the case that societies need security from the perils of war, it becomes not only a keenly desired authority but also one that has to be equipped with exceptional powers and preventive capacities. Further, violence and especially the possibility of war entail a self-enforcing logic in the form of a security dilemma. The accumulation of resources to act collectively, decisively and preventively leaves other states few options but to colonize cyberspace themselves and, thereby, confirming the necessity of sovereign involvement and regulatory structures. This argument appears all too frequently in relation to other states as well as cyber-terrorism and the related expansion of surveillance capacities. This is where cyber war comes in, to which we will now turn.

4. The Characters

The argument until now has been that narrative is a form of discourse that structures social reality, and that metaphors are important and effective discursive objects. Further, there is a prominent Hobbesian narrative that supports organizing society around states on the basis of an apocryphal violent past and a potential future safe from violence and social disintegration. This narrative appears to be prevailing in relation to the Internet over a narrative of decentralized and horizontally arranged social actors. Given that the materiality of the Internet would seem to resist representations of war and violence, we seek to understand the metaphors that support the statist narrative. We focus in particular on the metaphor of 'cyber war', which we now analyze empirically.

The first step in the empirical analysis is to explain what sources we examined and why. The first criterion was to focus on official statements by agents of state. In practice, this included white papers and security policy statements as well as official, planned speeches directed at 'cyberspace' or that explicitly invoked cyber war.[10] Other studies have considered the popular discourse as well (Dunn Cavelty, 2013), but, as discussed above, the Hobbesian narrative suggests that we should be considering how states represent the Internet.

Although we focused states' own representations, we opted to present our theory with a 'hard case', reasoning that if the theory obtains even under conditions that work against it, it should apply *a fortiori* in the more congenial cases. Therefore, we opted to analyze the representations of states that are the most Internet-friendly to maximize the chance that they would depict the Internet in positive terms and the least militarist to minimize the chance that they would include a strong element of violence and war in their narrative justifications of social order. In practice, this involved ranking states with according to the relative freedom of their Internet policies, as rated by Freedom House (2012), then ranking them inversely according to their military expenditure as a

10 We should mention that, although we acquired sufficient text to analyze German discourse, we were unable to find more than one oral statement in English in which any agent of the German state invoked cyber war, but this one case bears comment. The statement is from an interview between the German foreign minister, Guido Westerwelle, with the Financial Times newspaper (Westerwelle, 2010), which would have borne analysis because it is also published in English on the website of the German foreign ministry. In the interview, the journalist invokes 'computer war' and asks Westerwelle how to deal with it, to which Westerwelle answers that he considers this to be NATO's domain and remarks how easily one can invoke 'war' in English, even in the case of a 'war against climate change'. As enlightened as this sounds, the website of the German ministry of defence contains 42 documents invoking 'cyber war' as an Anglicism, but the texts are unfortunately all in German.

proportion of GDP, using the figures from SIPRI (2012). Weighting these two factors equally, we examined the top three states of our index, which are Hungary, Germany and Estonia, using documents from the period of 2001 to 2013.[11]

5. Analysis

In presenting the results of our survey, the challenge is in selecting what to include or exclude because the texts were so rich in metaphorical language. In fact, we often generated nearly as much paper in filling out the coding frame as the original text materials used. Therefore, what follows is a selection based on ubiquity and salience. That is, we focus here on metaphors that were especially common across the materials or that stand out for showing some critical aspect of how the metaphor of 'cyber war' inspires further discursive moves.

The principal metonymies

Although the metaphors in the documents produced by the three states in question differed markedly in many respects, to our surprise given that we chose them based on criteria that we expected would offer little variation, they all invoked two metonymies in very similar ways and fairly consistently.

The first consistently invoked metonymy is the prefix of 'cyber' itself. Although the term's origins lie in ancient Greek and science fiction and military research from the 20th century, the etymology seems to be of little interest to most of the state agents who use it ubiquitously. And given the wide variety of nouns attached to 'cyber' as a prefix in state documents, including 'space', 'domain,' 'crime', 'attack', 'security', 'terrorism', 'war(fare)', 'threats', 'defence', 'policy', 'response', 'freedom', 'culture' and 'world', it is startling how little effort is devoted to explicating what the term denotes. Only one Estonian document mentioned the lack of clarity as a potential problem (Estonia, 2008), only rarely are any of these portmanteaus defined, and the definitions that do appear are woefully imprecise. For example, a German document defines cyberspace as 'the virtual space of all IT systems linked at data level on a global scale' (Germany, 2011a, p. 15), and a Hungarian document defines it as 'the combined phenomenon of globally interconnected, decentralised and ever-growing electronic information systems as well as the societal and economic processes appearing in and through these systems in the form of data and information' (Hungary, 2013, p. § 3). Terms such as 'virtual space' and 'data level' make the first nearly impossible to interpret, and by including 'societal and economic processes appearing in and through these systems', the Hungarian definition would seem to include, for example, not only the data transmitted electronically during a Skype conversation or the equipment involved, but the people involved as well.

Indeed, it is because 'cyber' is so vague that it functions as a metonymy at all. If it had a roughly precise and consistent literal meaning, it would not function metaphorically. But as it is used in fact, 'cyber' serves as a stand-in for a conceptual domain of indefinite content and extent. Although using terms like 'cyber' as a kind of conceptual shorthand can be legitimate, as all concepts somehow simplify and compartmentalize a more complex reality, the imprecision in this instance is troubling. Two interpretations for why state agents use such vague language suggest themselves, though neither is very complimentary. The first is that the vagueness is a function of ignorance or carelessness, such that the agents invoking the term are uttering mere jargon without care or reflection on what it means, perhaps in the hope of imparting an impression of sophistication,

11 We should also note that we ignored dead metaphors, like 'grey area', strictly etymological metaphors, like 'cyber' as a prefix originating in ancient Greek, and many prepositional metaphors, like 'going forward' in a temporal sense. In cases of doubt, we used the PRAGGLEJAZ identification procedure described in Semino (2008). Finally, we restricted our analysis to official English translations because we are not competent to assess the semantics and syntax of Hungarian or Estonian, but also because metaphors have a different value in German, which is replete with metaphorical semantics in its indefinite quantity of compound words.

much like the prestige and status associated with the use of anglicisms.[12] The second interpretation is that a precise definition could constrain executive powers, and state agents are deliberately trying to preserve their freedom of action. For example, the same Hungarian document that provided the vague definition of cyberspace quoted above also suggests taking 'political, legal, economic, educational, awareness-raising and technical measures to manage risks in cyberspace that transforms the cyberspace [sic] into a reliable environment for the smooth functioning and operation of societal and economic processes by ensuring an acceptable level of risk in cyberspace' (Hungary, 2013, p. § 5). As a call to legislative action coming from the executive, this statement not only identifies cyberspace, which can include almost all remote communication and those involved, as a risky environment in need of transformation, it also seems to be calling for the mobilization of all governmental resources from parliament and intelligence agencies to schools.

The second great metonymy in the discourse where 'cyber war' is invoked depicts the state as a coherent, unified, acting subject. Such usage can include greater or lesser degrees of personification. For example, the phrase '22 countries had signed [the Council of Europe Convention on Cybercrime]' (Estonia, 2008, p. 17) is a fairly common, yet clearly metonymic, diction that one might encounter in any given piece of journalism, academic writing or everyday speech. By contrast, 'Estonia was a founding player' (Estonia, 2008, p. 22) clearly depicts the state, a complex composition of institutions, material resources, ideas and laws, as a person with a single mind and will. 'Society' as a source domain is also depicted this way in some documents, but less frequently.[13]

Again, two interpretations for the use of this metonymy suggest themselves. First, it could simply be a rhetorical embellishment to make the content more vibrant and to avoid torturing the prose to disaggregate the state into its active components. This type of construction is common in literature. In the case of states, it can be benign or pernicious. As with all metaphors, depicting states thus both hides and reveals. To the extent that it presents an unwarranted image of coherence, consent and unanimity, it is to be condemned, but in many instances it might simply lend the text greater syntactical economy. Second, this form of metonymy is more semantically coherent in the context of the statist narrative and the other metaphors that frequently appear in this type of discourse. The Hobbesian narrative of many social actors leaving the state of nature by joining together in a larger, corporate body is an obvious parallel to this metonymy. Just as the Hobbesian metaphor can be used at the level of the state's internal structure as well as the structure states collectively form, we encounter metaphors stating that 'Hungary needs to stay vigilant to potential threats of foreign origin' (Hungary, 2012, p. 12). Further, as we will discuss below, violence, infection, and biological evolution routinely appear as source domains, and these metaphors would be awkward or simply unintelligible unless a given state were depicted as a subject capable of fighting, an organism subject to infection, in need of improving its evolutionary fitness or at risk of extinction.

Discourse is a battlefield

Before considering the metaphorical productivity of 'cyber war', we should first assess in what sense that term is itself a metaphor. As noted above, 'cyber' as a prefix conveys little literal meaning in itself, functioning nearly as an empty signifier except for the indefinite relation to computers. War, however, does admit literal definition. The Oxford English Dictionary defines it as 'Hostile contention by means of armed forces, carried on between nations, states, or rulers, or between

12 Although state agents seem particularly prone to fetishizing all things 'cyber', academics are not necessarily immune. Indeed, the metonymy is reproduced in academic texts far more often than it is problematized.

13 We will frequently describe our findings in terms of frequency without providing systematized comparisons of quantity. This is not an oversight but merely a function of the texts that served as data, which are hardly comparable with each other in quantitative terms, with some spanning a few pages and others several dozen and treating slightly different, but related topics. However, when we invoke frequency, there is in every case some quantitative, if informal, logic behind it.

parties in the same nation or state; the employment of armed forces against a foreign power, or against an opposing party in the state' (OED Online, 2013b). Much activity on the Internet, whether by state-run botnets or just in the comments section of any given popular website, could be considered hostile, but describing activity between computers as 'armed force' is indubitably hyperbolic. As for international law, terms such as 'use of force' and 'intervention' have supplanted 'war' since the mid-20th century, and the law of war is now generally referred to euphemistically as 'international humanitarian law' (Brownlie, 2003). The academic literature typically uses the basic concept of armed conflict, with any armed conflict that exceeds 1000 battle deaths per year counting as war (Themnér & Wallensteen, 2013), which is certainly not the case with any event or activity referred to as 'cyber war' (Rid, 2013).

By contrast, Susan Sontag (1988) argues that capitalist societies abuse military metaphors as a matter of course, but they depict 'war' as an effort for which no expense is too great and that should not necessarily be considered 'realistically'. But such a depiction might not make cyber war less metaphorical; rather, it would seem to make conventional war, at least conducted by the modern democracies considered here, *more* metaphorical and *less* real. This would make cyber war analogous to Baudrillard's reading of the first Gulf War and 9/11, according to which they involved very little effort or sacrifice for most members of the modern, democratic societies involved, who were instead focused primarily on their representational aspects (Baudrillard, 1991, 2005). And like the other great representational war, the 'global war on terror' (Spencer, 2012), cyber war can continue indefinitely.

Given that there is hardly a sense in which the term 'cyber war' can be taken literally, it must have a metaphorical character. It is also current. Each country we examined invoked it with varying degrees of inflammatory rhetoric, ranging from warning against military attacks in cyberspace (Germany, 2006) to calling it 'the unnoticed Third World War' (Aaviksoo, 2007), so even if the phenomenon is not literally real, the metaphor most definitely is. And the question is what further metaphors this one inspires, what representational baggage it carries, what kind of reality it presumes. Though the overall image is very extensive, we have selected a few metaphorical correlates that the war metaphor implies and that appeared frequently for further examination: the location or spatiality of cyber war, the activity and implements involved, the momentousness attributed to it, and the participants it involved.

With regards to the spatiality of cyber war, the most commonly invoked metaphorical construction is the ubiquitous metonymy of 'cyberspace' and related variants, like 'cyber domain'. As with other uses of the 'cyber' prefix, there is generally little consideration as to what 'cyberspace' actually is. Its most frequently mentioned quality, when it is qualified, is its 'virtual' character, which clarifies little. Another commonly invoked characteristic is the inapplicability of borders and territorial jurisdiction, which can range from anodyne personifications of cyberspace 'reaching' across state borders (Estonia, 2008) to the vivid imagery of the Estonian Minister of Defence, Jaak Aaviksoo, explaining the amorphousness of a 2007 distributed denial of service (DDOS) event: 'there were no electronic men marching over an electronic border' (Aaviksoo, 2008). The emphasis on the borderlessness of cyberspace, however, is more common in the Estonian and Hungarian texts, perhaps because emphasizing this characteristic makes international legislation and policing more appealing as a solution, which would allow these smaller states with weaker capacities to profit from larger states' resources. And cyberspace as a generic space is also readily combined with other metaphors, as Viktor Orban, Hungarian Prime Minister, exemplifies by calling cyberspace a '*virtual* space consisting of computers and cables' and in the same speech that 'cyberspace is *in reality* a world without walls' (Orban, 2012, emphasis added), which is reminiscent of the linguistic tic of using 'literally' as a figurative particle for emphasis, but not *literally*.

However, cyberspace is not always presented so generically in texts treating cyber security and cyber war. It is often depicted in far more militaristic terms. For example, in two different speeches by two different individuals, Estonian state agents described cyberspace not only as a 'battlefield', but as a 'perfect battlefield of the 21st century' (Aaviksoo, 2007; Paet, 2007b). Not to be outdone,

the National Cyber Security Strategy of Hungary waxes hysterically about how Hungarian 'vital electronic information systems […] are threatened by a new form of warfare, information warfare, making cyberspace one of the most important theatres in modern warfare' (Hungary, 2013, p. §4). This conforms to the feature of the Hobbesian statist narrative that fear both of a hypothetical violent past as well as a dire, threatening future motivates the existence and persistence of states. Indeed, Hungary also seems to present a direct contrast to the Hobbesian state of nature by depicting the desired state of cyberspace to be a 'reliable and secure environment for individuals and communities to ensure […] communication based on liberty, freedom from fear' (Hungary, 2013, p. §8). Indeed, the perils of cyberspace as a potential battlefield in the statist narrative parallel the legendary dangers of the Hobbesian *homo homini lupus.*[14]

Reading these two characteristics together, the indivisibility of cyberspace and its status as a quintessential battlefield, raises very troubling implications. Just as cyber war has no foreseeable end, it equally resists containment, permeating any physical means of digital storage and transmission as well as any data there. It's the interminable global war that fits in your pocket. Even if international law is fairly ambiguous about the ontological status of war, it is a form of normativity for and by states, and it predictably adapts the normativity of war to what states, as self-perpetuating institutions, require (Hsiung, 1997).

The most frequent depiction of unwanted use or access to electronic resources or paraphernalia is as 'attacks'. This may seem like a literal use of the term, but the OED defines an attack principally as 'The act of falling upon with force or arms, of commencing battle; an offensive operation; an onset, an assault. The common military term; opposed to *defence*' (OED Online, 2013a). Further, the military connotation was often accentuated with qualifiers, such as 'combat cyber attack' (Estonia, 2008), 'military attacks' (Germany, 2006) and 'targeted attacks' (Germany, 2011a), and closely related variants, such as 'advanced assault methods' (Estonia, 2008), 'offensive cyber campaign' (Aaviksoo, 2008) and 'malicious cyber activity, threat, attack or emergency' (Hungary, 2013). There also seems to be a close discursive connection between 'cyber attack' and 'cyber terrorism', which both Estonia and Hungary invoked, although it is difficult to assess their conceptual proximity.

The metaphor of 'cyber attacks' also suggests, as does the definition of the word, the complementary metaphor of 'cyber defence', which was invoked repeatedly in documents of each state. This metaphor is striking because of its implicit suggestion of an institutional solution to unwanted use and access, and one that already exists, namely state ministries of 'defence'. This becomes apparent when one considers a home or corporate network, for which the verb 'defend' or the term 'cyber defence' would seem fairly hyperbolic. It is wise to encrypt one's home router connection for reasons of privacy, but not as a means of 'cyber defence'. It is also instructive to contrast this term with 'cyber security', which seems like an idiomatically legitimate corollary of cyber crime, which is metonymic if not metaphorical. A large corporation might indeed have a cyber security policy or department, but 'cyber defence' again seems like a distinctly statist means of depicting effort and measures to prevent undesired use and access to electronic resources and equipment.

Metaphors invoking weapons as a source domain were present but not terribly widespread. In fact, there was only one instance in which the market for the use of botnets to be used in DDOS events was depicted as a 'black arms market' and as the natural progression of technological development, just as 'With cars and planes came tanks and bombers, and with nuclear energy came atomic

14 Cyberspace is less often presented in these terms with direct reference to the international context, at least in these documents originating in national governments. However, the international level among states is frequently presented as a realm of fear requiring legal authority and a monopolization of violence in NATO documents, of which the *National Cyber Security Framework Manual* (2012) is a particularly good example. Although we did not analyze such texts systematically because of our logic of case selection, all three states we examined are NATO members, so the extrapolation here is not groundless.

weapons. This is not any different for computers' (Aaviksoo, 2008). Similarly, a home computer was depicted as 'a simple machine to lounge [sic] an attack' (Orban, 2012).

Although it would seem that invoking war would sufficiently indicate the importance state agents attach to such activities, two other metaphors are common, but they carry opposite inflections. The first depicts the participants of 'cyber war' as organisms involved in an evolutionary struggle of life and death, proliferation and extinction. The coincidence of the biological domains of evolution and, especially, infection and military and geostrategic topics is well-established (Shimko, 1994; Sontag, 1979, 1988). However, the metaphor seems even more common in discourse about cyber war, which Dunn-Cavelty (2008b) suggests is a result of the affinity of many involved in the discourse for science fiction literature. But the relationship might not be so incidental. It could be the case that the similarities between the two domains allow for systematic mapping. Computer viruses can self-replicate and hijack host processes much like biological viruses, they can be programmed with 'genetic' algorithms to improve their fitness from one generation to the next, they are communicable, and so on.

Empirically, we certainly encountered metaphors of infection, like a 'virus in code' (Germany, 2011a) and 'constant risk of infection' (Estonia, 2008), but these were not as common as the depiction of the state and society as living organisms engaged in an evolutionary struggle. The most common indicator of the former was the ubiquitous use of 'vital' as an adjective, as in 'vital services' (Estonia, 2008), 'vitally important infrastructure' (Paet, 2007a), and 'vital electronic information systems' (Hungary, 2013), which depicts computer equipment and resources as the states' organs and blood that, if harmed, would compromise 'the country's wellbeing' (Estonia, 2010). The evolutionary pressures on this life are frequently portrayed with reference to the need to 'adapt' strategies and organizations to 'the evolution of new security risks' (Hungary, 2013). This reflects both of the essential criteria of the Hobbesian narrative: a vital, in the sense of living, collective actor motivated by the fear of death in anarchy.

The virological and evolutionary source domains are significant for three reasons. First, the connotations of septic and unsanitary conditions are an affront to the hypermodern image of a tuned mechanical society, which was frequently presented as a contrasting image. Second, it obscures the identity of any antagonistic agents. State agents often lamented the anonymity of their antagonists, which might be an advantage to the extent that their identities, reasons and motives are of no concern if they have no identity. Third, the evolutionary metaphor reinforces the interminable nature of the problem. Infection – or extinction – is a constant risk, and the nature of the struggle precludes victory even in principle, so it is a matter of constantly adding and improving countermeasures, never rescinding them.

The other common metaphor to describe the process and its participants seems directly opposed to infection and evolution in terms of importance, namely that cyber war is a game. Again, the game source domain is common to the geostrategic target domain in general and the academic discussion of it in particular (Chilton & Lakoff, 1989). Oddly, however, a game is a structured and orderly form of conflict that would diverge from the narrative that equates anarchy with war and a state-based order with peace. Thus, it diverges from our theoretical expectations. Dunn-Cavelty (2013) attributes this to affinity for video games in hacker culture. Indeed, as she notes, already in 1983 there was a film about a boy-hacker who almost caused a nuclear war called *War Games*. However, given the cultural milieu of the state agents, this attribution is doubtful. For example, when bemoaning 'the anonymity of the players' (Aaviksoo, 2007), the Estonian defence minister is doubtfully making reference to his favourite MMORPG.

A plausible alternative source of this metaphor would be the academic discourse. That is, state agents may well have appropriated the representation of war, including cyber war, as a game from the social scientific community. This interpretation is reinforced by the invocation of the common metaphor of the Cold War era, 'the domino effect' (Estonia, 2008; Shimko, 1994). Although a systematic test of this explanation would require further study, this initial indication is enough to

give scholars pause in considering how they construe the Internet, its users and the activities it enables so as not to become complicit in a militarized image or a narrative of violent conflict.

The results, therefore, do indeed reflect our theoretical expectations. When they are clear, the metaphors state agents use in talking about the Internet are metaphorically productive in a way that is conducive to the Hobbesian narrative characterised by chaos and violence. Where they are less precise, as in the instance of the 'cyber' prefix, the metaphors are expansive to allow states greater freedom of policy and action than more restrictive terms and images would permit.

6. Conclusion

The Internet is a revolutionary force in terms of its ability to affect social life. Because of this significance, there is considerable dissent about how to represent it in the social imaginary, how to determine what it does and will mean. The most prominent factions in this struggle consist of those who see in the Internet a means of organizing social life on a horizontal basis of deliberation and communication and that of states, according to which the threat of violence is a pertinent to the Internet as it is to seafaring or any other traditionally territorial and political activity.

Focusing on the statist side of the discourse, we examined the metaphorical productivity of 'cyber war' to learn more about how this discourse unfolds and what semantic companions it enlists. Looking at states we suspected would be relatively pacific and Internet-friendly, we found nearly ubiquitous use of 'cyberspace' as a metonymy and personification of the state. Further, the 'cyber war' metaphor seemed especially prone to inspire other metaphors of space, of weapons, of infection and evolutionary competition and games. In all cases, these metaphors serve to naturalize the Internet as subject to warlike events and states as the protagonists in the activity of prosecuting and defending against 'cyber war'.

Just as 'cyber war' can inspire a great number of other metaphorical constructions, the discourse itself is open. What cyberspace is, what it will mean and how it will fit in the social imaginary is far from determined. While we remain ambivalent about the ostensibly progressive effects of the Internet as well as the need for and ability of states to engage in warlike activity there, we are concerned with the consequences of the discourse on social reality. Just as the only ones to profit from a conventional war are the crows, the only ones to profit from 'cyber war' are likely to be the trolls.

References

Aaviksoo, Jaak. (2007). *Cyber Defence – The Unnoticed Third World War*. Talinn: Ministry of Defence Retrieved from www.kaitseministeerium.ee/en/1468 (21.8.2013).

Aaviksoo, Jaak. (2008). *Estonian Approach to Cyber Security: Estonian National Strategy on Cyber Security and Cooperative Cyber Defence Centre of Excellence*. Talinn: Ministry of Defence.

Abell, Peter. (2001). Causality and Low-Frequency Complex Events: The Role of Comparative Narratives. *Sociological Methods & Research, 30*(1), 57-80.

Abell, Peter. (2009). A Case for Cases: Comparative Narratives in Sociological Explanation. *Sociological Methods & Research, 38*(1), 38-70.

Barthes, Roland. (1977). Introduction to the Structural Analysis of Narratives (S. Heath, Trans.). In S. Heath (Ed.), *Image Music Text*. London: Fontana Press.

Baudrillard, Jean. (1991). *The Gulf War Did Not Take Place*. Bloomington, IN: Indiana University Press.

Baudrillard, Jean. (2005). War Porn. *International Journal of Baudrillard Studies, 2*(1).

Benkler, Yochai. (2006). *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. New Haven, CT: Yale University Press.

Benkler, Yochai. (2013). Practical Anarchism: Peer Mutualism, Market Power, and the Fallible State. *Politics & Society, 41*(2), 213-251.

Bennett, Lance, & Segerberg, Alexandra. (2013). *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics*. Cambridge: Cambridge University Press.

Bevir, Mark, & Rhodes, R.A.W. (2006). Defending Interpretation. *European Political Science, 5*, 69-82.

Brownlie, Ian. (2003). *Principles of Public International Law* (6th ed.). Oxford: Oxford University Press.

Bruner, Jerome. (1991). The Narrative Construction of Reality. *Critical Inquiry, 18*, 1-21.

Castells, Manuel. (2010). *The Rise of the Network Society* (Vol. 2). Cambridge, MA.: Blackwell.

Chilton, Paul, & Lakoff, George. (1989). Foreign Policy by Metaphor. *Center for Research in Language Newsletter, 3*(5), 4-19.

Cover, Robert. (1983-1984). Foreword: *Nomos* and Narrative. *Harvard Law Review, 97*(4), 4-68.

Dahlberg, Lincoln. (2010). Cyber-Libertarianism 2.0. A Discourse Theory/Critical Political Economy Examination. *Cultural Politics, 6*(3), 331-356.

Deibert, Roland J., & Crete-Nishihata, Masashi. (2012). Global Governance and the Spread of Cyberspace Controls. *Global Governance, 18*, 339-361.

Deibert, Roland J., Palfrey, John, Rohozinski, Rafal, & Zittrain, Jonathan. (2012). Access Contested. Toward the Fourth Phase of Cyberspace Controls. In R. J. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds.), *Access Contested. Security, Identity and Resistance in Asian Cyberspace* (3-20). Cambridge, MA: MIT Press.

Der Derian, James. (1993). The Value of Security: Hobbes, Marx, Nietzsche and Baudrillard. In D. Campbell & M. Dillon (Eds.), *The Political Subject of Violence* (94-113). Manchester: Manchester University Press.

Drezner, Daniel. (2004). The Global Governance of the Internet: Bringing the State Back In. *Political Science Quarterly, 119*(3), 477-498.

Dunn Cavelty, Myriam. (2008a). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London: Routledge.

Dunn Cavelty, Myriam. (2008b). Cyber-Terror – Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology & Politics, 4*(1), 19-36.

Dunn Cavelty, Myriam. (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105-122.

Estonia. (2008). *Cyber Security Strategy*. Talinn: Ministry of Defence.

Estonia. (2010). *National Security Concept of Estonia*. Talinn: Riigikogu.

Fierke, Karen. (2002). Links Across the Abyss: Language and Logic in International Relations. *International Studies Quarterly, 46*, 331-354.

Fierke, Karin. (1997). Changing Worlds of Security. In K. Krause & M. Williams (Eds.), *Critical Security Studies: Concepts and Cases* (223-252). Minneapolis, MN: University of Minnesota Press.

Flanik, William. (2011). 'Bringing FPA Back Home:' Cognition, Constructivism, and Conceptual Metaphor. *Foreign Policy Analysis, 7*, 423-446.

Freedom House. (2012). Freedom on the Net 2012: A Global Assessment of Internet and Digital Media. In S. Kelly, S. Cook & M. Truong (Eds.).

Germany. (2006). *White Paper 2006 on German Security Policy and the Future of the Bundeswehr*. Berlin.

Germany. (2011a). *Cyber Security Strategy for Germany*. Berlin: Federal Ministry of the Interior.

Germany. (2011b). *Defence Policy Guidelines: Safeguarding National Interests – Assuming International Responsibility – Shaping Security Together*. Berlin: Ministry of Defence.

Glucksberg, Sam. (2008). How Metaphors Create Categories – Quickly. In R. Gibbs (Ed.), *The Cambridge Handbook of Metaphor and Thought* (67-83). Cambridge: Cambridge University Press.

Goldsmith, Jack, & Wu, Tim. (2006). *Who Controls the Internet? Illusions of a Borderless World*. Oxford: Oxford University Press.

Hansen, Lene, & Nissenbaum, Helen. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*, 1155-1175.

Hart, Catherine, Jin, Dal Yong, & Feenberg, Andrew. (2014). The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States. *International Journal of Communication, 8*, 2860-2878.

Holland, John. (1995). *Hidden Order: How Adaptation Builds Complexity*. Reading: Helix Books.

Hsiung, James. (1997). *Anarchy and Order: the Interplay of Politics and Law in International Relations*. Boulder: Lynne Riennner.

Hungary. (2012). *Hungary's National Security Strategy*. Budapest.

Hungary. (2013). *Goverment Decision No. 1139/2013 (21 March) on the National Cyber Security Strategy of Hungary*. Budapest.

Kelty, Christopher. (2005). Geeks, Social Imaginaries, and Recursive Publics. *Cultural Anthropology, 20*(2), 185-214.

Klimburg (ed.), Alexander. (2012). *National Cyber Security Framework Manual*. Tallinn: NATO Cooperative Cyber Defense Center of Excellence.

Krasner, Stephen D. (2001). Abiding Sovereignty. *International Political Science Review, 22*(3), 229-251.

Lakoff, George. (1992). Metaphor and War: The Metaphor System Used to Justify the War in the Gulf. In H. Kreisler (Ed.), *Confrontation in the Gulf: University of California Professors Talk about the War*. Berkeley: Institute of International Studies.

Lakoff, George. (1993). The Contemporary Theory of Metaphor. In A. Ortony (Ed.), *Metaphor and Thought,* 2, 203-251. Cambridge: Cambridge University Press.

McGlone, Matthew. (2007). What is the Explanatory Value of a Conceptual Metaphor? *Language & Communication, 27*, 109-126.

Milliken, Jennifer. (1999). The Study of Discourse in International Relations: A Critique of Research and Methods. *European Journal of International Relations, 5*(2), 225-254.

Morozov, Eugeny. (2011). *The Net Delusion*. London: Allen Lane.

Mueller, Milton, Schmidt, Andreas, & Kuerbis, Brenden. (2013). Internet Security and Networked Governance in International Relations. *International Studies Review, 15*(1), 86-104.

Mutimer, David. (1997). Reimagining Security: The Metaphors of Proliferation. In K. Krause & M. Williams (Eds.), *Critical Security Studies: Concepts and Cases* (187-221). Minneapolis, MN: University of Minnesota Press.

Nissenbaum, Helen. (2004). Hackers and the Contested Ontology of Cyberspace. *New Media & Society, 6*(2), 195-217.

Nissenbaum, Helen. (2005). Where Computer Security Meets National Security. *Ethics and Information Technology, 7*(2), 61-73.

OED Online. (Ed.) (2013a) Oxford English Dictionary Online. Oxford: Oxford University Press.

OED Online. (Ed.) (2013b) Oxford English Dictionary Online. Oxford: Oxford University Press.

Orban, Viktor. (2012). *Speech at the 'Budapest Conference on Cyber Space'*. Paper presented at the 'Budapest Conference on Cyber Space', Budapest.

Paet, Urmas. (2007a). *Address by Minister of Foreign Affairs of Estonia, Urmas Paet*. Strasbourg: Council of Europe.

Paet, Urmas. (2007b). *Celebrating 85 Years of Friendship: Ideals in Practice*. Ministry of Foreign Affairs.

Rheingold, Howard. (1993). *The Virtual Community. Homesteading on the Electronic Frontier*. Cambridge, MA: MIT Press.

Rheingold, Howard. (2002). *Smart Mobs. The Next Social Revolution*. Cambridge, MA: Basic Books.

Rid, Thomas. (2013). *Cyber War Will Not Take Place*. Oxford: Oxford University Press.

Schmidt, Eric, & Cohen, Jared. (2013). *The New Digital Age: Reshaping the Future of People, Nations and Business*. New York, NY: Borzoi.

Searle, John. (1979). *Expression and Meaning: Studies in the Theory of Speech Acts*. Cambridge: Cambridge University Press.

Semino, Elena. (2008). *Metaphor in Discourse*. Cambridge: Cambridge University Press.

Shimko, Keith. (1994). Metaphors and Foreign Policy Decision Making. *Political Psychology, 15*(4), 655-671.

Shirky, Clay. (2008). *Here Comes Everybody*. London: Penguin Books.

Singh, J.P. (2013). Information Technologies, Meta-power, and Transformations in Global Politics. *International Studies Review, 15*(1), 5-29.

SIPRI. (2012). SIPRI Military Expenditure Database 2012. Stockholm: Stockholm International Peace Research Institute.

Sontag, Susan. (1979). *Illness as Metaphor*. New York, NY: Farrar, Straus and Giroux.

Sontag, Susan. (1988). *AIDS and Its Metaphors*. New York, NY: Farrar, Straus and Giroux.

Spencer, Alexander. (2012). The Social Construction of Terrorism: Media, Metaphor and Policy Implications. *Journal of International Relations and Development, 15*(3), 393-419.

Themnér, Lotta, & Wallensteen, Peter. (2013). Armed Conflict, 1946-2012. *Journal of Peace Research, 50*(4), 565-575.

Turner, Fred. (2006). *From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: Chicago University Press.

Westerwelle, Guido. (2010). *Außenminister Westerwelle im Interview mit der Financial Times über das Strategische Konzept der NATO, Afghanistan und die Lage der Euro-Zone (Engl.)*. Berlin: Foreign Ministry Retrieved from www.auswaertiges-amt.de/DE/Infoservice/Presse/Interviews/2010/101117-BM-Interview-FT-NATO.html (13.08.2013).

Winter, Steven. (2008). What Is the 'Color' of Law? In R. Gibbs (Ed.), *The Cambridge Handbook of Metaphor and Thought* (363-379). Cambridge: Cambridge University Press.

Wu, Tim. (2010). *The Master Switch. The Rise and Fall of Information Empires*. New York, NY: Knopf.

Zinken, Jörg. (2003). Ideological Imagination: Intertextual and Correlational Metaphors in Political Discourse. *Discourse Society, 14,* (507-523).

Zittrain, Jonathan. (2009). *The Future of the Internet. And How to Stop It*. London: Penguin.Wiener, Antje/Puetter, Uwe 2009: The Quality of Norms is what Actors Make of It: Critical Constructivist Research on Norms, in: Journal of International Law and International Relations 5(1), 1-16.

Contact

Ben Kamis
ben.kamis@normativeorders.net

Tel: +49 69 798 31451

Dr. Thorsten Thiel
thiel@hsfk.de

Tel: +49 69 959 104-59

Imprint/Disclaimer

Peace Research Institute Frankfurt
Baseler Straße 27-31
60329 Frankfurt am Main, Germany

The authors of this working paper are solely responsible for its content.