Social perception of Risk and Threat of "Cyber Warefare" in the German speaking blogosphere

Henrike Francesca Höpker

Henrike Francesca Höpker, 26, from Augsburg (Germany), is currently finishing her M.A. degree in "Social and Political Conflict Studies" at the University of Augsburg. She holds a B.A. from the Friedrich-Schiller-University Jena in Sociology and Economic Science. Her master thesis is about the construction of the phenomenon "cyberwarfare" in the German speaking blogosphere. Her research interests are in sociology of risk, security studies, good governance and cyber conflicts.

Abstract

This paper presents some selected findings from a previous study. It aimed at establishing an overview of the discourse on "cyberwar" within the German speaking blogosphere. A profound basis could be established collecting data, to be analyzed with the Sociology of Knowledge Approach to Discourse. Therefore the study combined quantitative comparability with qualitative exploration.

The here presented items were chosen with regard to their relevance for the social perceptions of risk. The latter first introduced by Ulrich Beck were used to analyze the construction of cyberwar in the German blogosphere. Discussed aspects include the perception of threat, the associated state actors as well as the types of debated scenarios. Based on these indicators some well-founded assumptions are made regarding the high diversity of scenarios as well as the commonalities within the blogosphere. Even though the study analyzed 148 blog posts this amount is not sufficient to generalize the results.

Keywords

Beck, Blogosphere, Cyberwar, Risk, Social Perception, Threat Scenario

Introduction

> *"The global anticipation of catastrophe for the most part resists the methods of scientific calculation. The less calculable risk becomes, however, the more weight cultural shifting perceptions of risk acquire, with the result that the distinction between risk and cultural perception of risk becomes blurred." (Beck 2009: 12)*

There are many areas in which we may anticipate catastrophe today. Between cancer risks through chemical by-products and the consequences of climate change, danger originating in the digital world – the world wide web – is just one of many risks. But as (digital) interconnectedness is growing and no longer only links people, but also objects, from the digital scale that posts your weight-loss directly on Facebook to the air condition of your office, the area has been of increasing importance: With the advent of the "internet of things" the first infection of for example a freezer with malicious software was only a matter of time.[9] In a world where freezers are part of botnets the all-encompassing dangers emerging from the brave new digital world are up to debate – and nowhere more so than in cyberspace itself. The digital arena has since been dubbed as the "fifth domain of warfare" (War in the fifth domain' 2010).

This paper focuses on the social construction of "cyberwarfare" within the German speaking blogosphere. Academics have yet to agree on the question what exactly a "cyberwar" would look like or if the term is applicable at all. But while this academic debate is going on, the term has reached the public discourse. While widely used, there is nevertheless no common definition of the term. As varied as the academic opinions on "cyberwar" are, as diverse is its use in public discourse.

The analysis will not be focused on the discourse in newspapers, but on the seemingly anarchic blogosphere, populated by potentially anyone with access to a computer. While there is an array of studies on the English speaking blogosphere, which is considerably larger than any other, there are only few studies on the much smaller German speaking blogosphere.

[9]In 2014 a botnet was discovered which consisted to approximately 25 percent of "things", including a freezer (Pluta 2014).

Therefore this paper is going to cast a glance at the way "risk" is constructed and perceived in this elusive arena of discourse in connection to "cyberwarfare".

As in the initial quote an objective quantification of risks is not necessarily possible, as it may blur with its cultural perception and hence become something more fluid and changing. Ulrich Beck stresses, that "the dynamic of society rests less on the assumption that now and in the future we must live in a world of unprecedented dangers; rather we live in a world that has to make decisions concerning its future under the conditions of manufactured, self-inflicted insecurity." (Beck 2009: 8)

Consequently, in order to understand the social *consequences* to risks, you must not only try to gauge the objective "amount" of risk, but its cultural perception as well.

And while the blogosphere might still be a niche discursive field, especially in German speaking regions, it is steadily growing. It cannot be assumed that the well-established theories of communication valid for the "traditional media" are automatically applying to bloggers, too. The lack of adequate theories not only attracted my interest in this area but also gives relevance to the research. The analysis however, only scratches the surface of the matter and can merely be viewed as a starting point for further research into the subject. Focusing on one linguistic area can be legitimated with Beck's design of a world risk society which assumes that cultures may differ in their perception of risk. Hence, it does not seem sufficient to just assume that findings for the English speaking blogosphere can be applied one-to-one to the German speaking arena.

The question this paper will provide an insight into: What kind of perceptions of risk regarding "cyberwarfare" exists in the German blogosphere?

Literature Review

Cyberwar

As already pointed out, there is quite a bit of academic literature on "cyberwar". Amongst the most popular is Thomas Rid's explanation as to why "cyberwar will not take place" (2012). In this paper Rid draws on the definition of war, as it was put forward by Clausewitz (Kapitel 1; Definition). According to this a war is marked by being

a) violent
b) goal-oriented and
c) political in nature

Arguably, no actions in the past, that are limited to the digital sphere, do satisfy all of these requirements, ergo cannot to be classified as "war". Regardless, Rid does not deny threats in general coming from cyberspace – he merely takes exception to the use of the term "war". He amends even: „Yet such mediated destruction [like an attack on critical infrastructure such as a power grid] caused by a cyber offense could, without doubt, be an act of war, even if the means were not violent, only the consequences." (Rid 2012: 9)

Some scholars disagree with Rid's point of view: "Cyberwar is not only a new dimension of war or a new type of weapon. It is a new type of war."[10] (Gaycken 2012: 69)

This however is not just a matter of semantics.

> *„The absence of clear cyber terminology contributes to conceptual vagueness and inaccuracy. [...] Different classifications have different meanings and consequences. [...] [Defining those is] crucially important, since differences in threat assessment can make national and international cooperation efforts difficult." (Hegenbert 2014: 6)*

The full scope of implications on the spectrum of social perception regarding the difference between cyberwar or cyber threats will not be gauged in the context of this study, as this work

[10] "Cyberwar ist nicht nur eine neue Dimension des Krieges oder eine neue Waffengattung. Es ist eine ganz neue Art von Krieg." (Translation correspondingly by HH)

aims to merely explore the conception of cyberwar. Future research however might focus on determining reasons for and differences in the social construction of the former and the latter.

This work aims at the social reality – not the academic conception – of "cyberwar". Therefore the work is done exploratively, meaning the justification of using the term "cyberwar" will not be examined. If a blogger chooses to describe a phenomenon as "cyberwar" it is treated as such, even though it might not fit with certain constructions of the concept.

Blogosphere

When it comes to the blogosphere, matters are quite different: For all the differences in terminology, the issue of "cyberwar" is though possibly not defined in HD clarity, at least sketched out in pencil. The same cannot be said about the blogosphere at all. Appropriately Lovink explains the dilemma of the subject:

> *"Blogs are the proxy of our time. It is a techno-affect that cannot be reduced to the character of the individual blogger. There are possibly as many blogs as there are voices and topics. [...] How can you do research when your object is in a state of hyper-growth and permanent transformation?" (Lovink 2008: xxiii)*

This is precisely the issue to face when researching "the" blogosphere: we have no way of actually knowing, how many blogs are out there or how many people are blogging, much less in which intervals. There is no comprehensive register of the Internet to look up those things. Consequently research into this area necessarily has to deal with assumptions, guesses and incomplete data.

This starts out with the very definition of what a weblog actually is. Generally it is understood to be an online publication, that is marked by having reverse chronologically structured postings as well as being oriented towards a dialog and being especially expressive and authentic in form (Zerfass 2005: 20).[11] The name is a composition of "Web" short for the

11 "Online-Publikationen, die sich durch kurze umgekehrt chronologisch angeordnete Einträge sowie eine starke Dialogorientierung auszeichnen und besonders expressive, authentische Ausdrucksformen ermöglichen." Translation accordingly by HH.

"World Wide Web" and "Log" as a form of record or diary, the shorthand "blog" has widely replaced the actual term and is synonymous. "Blogging" is the act of writing in a blog, the author is referred to as a "blogger".[12] What differentiates blogs from other websites is partially that they are created by the use of a Content Management System (CMS), which also factors in the popularity of blogs, as those are mostly easy to use for the layman and require very little skills. Additionally, many allow commenting and embedding into other blogs in real time (Zerfass 2005: 20). In this paper the blogosphere will be understood as a tight knit linkage of content, comments and automatic references that create a global network in its totality (Zerfass 2005: 20).[13]

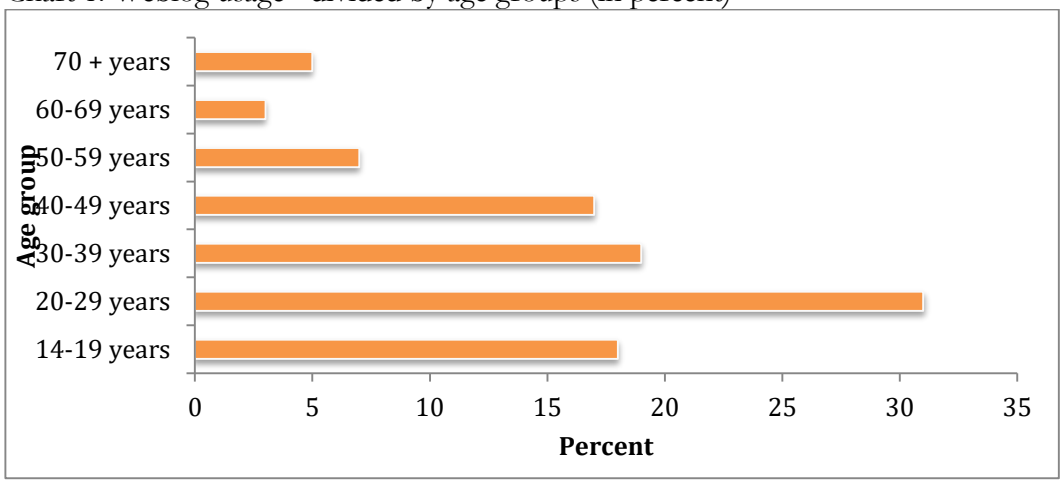
The concept dates back to 1997 when the US-American Jon Barger named his online diary a weblog. This was followed by the development of software and online tools such as CMSes. The concept gained traction when the Harvard University held the first "Bloggercon"-conference in 2003 and the medium was of central importance in the US-presidential elections of 2004 (Schmutte 2013).

As fragmented as the research on the subject is, some statements can still be concluded from it. The annual study on usage of the Internet in Germany conducted by ARD and ZDF found that usage of weblogs was distributed in the following way across the age groups:

12 As the analysis focuses on the German language area it should be noted that the term "blog" was imported as well as "blogger", "blogging" however is inflicted in German as "bloggen", forming a "denglisch" term that integrates more naturally into speech. The term was officially adopted by being incorporated in 2006 into the "Duden" the German reference guide (Duden 2014). This may be viewed as further proof of the novelty of blogs on the on hand, but also of the growing importance of the medium on the other hand.

13 "Als "Blogosphäre" bezeichnet man das durch "die enge und dichte Verknüpfung von Inhalten, Kommentaren und automatischen Referenzen [gebildete] globale Netzwerk in seiner Gesamtheit."
Translatation accordingly by HH.

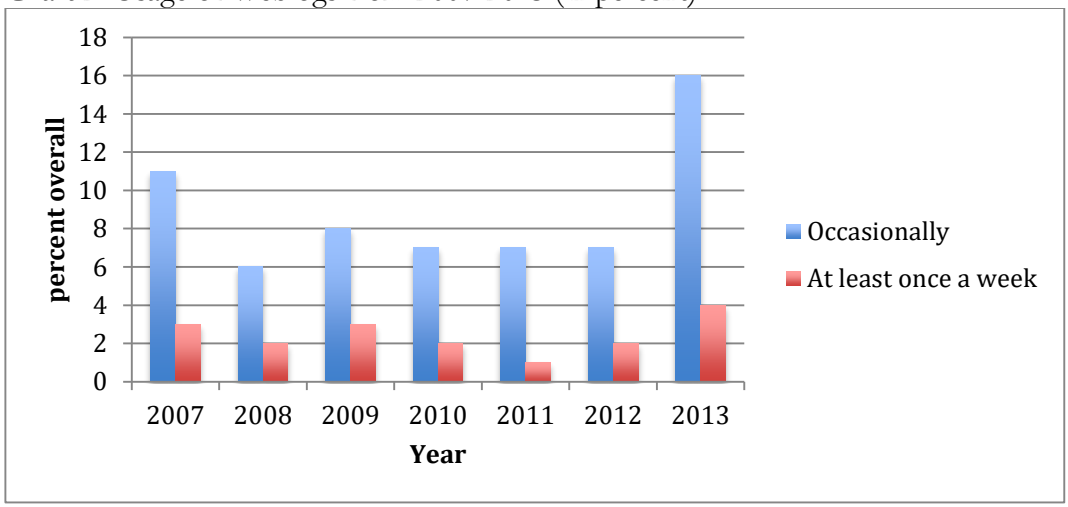
Chart 1. Weblog usage[14] divided by age groups (in percent)



Source: ARD/ZDF Online Studie 2012, displayed by author

Unsurprisingly the usage is focused on the younger population. More interesting is, that blogging is not actually a teenage phenomenon, but is used almost twice as much by "twenty-somethings". Still, in this context it should not be withheld, that blogs are still a rather niche medium, though gaining importance. Over the last years the following usage tendencies could be observed:

Chart 2. Usage of Weblogs from 2007-2013 (in percent)



Source: ARD/ZDF Online Studie 2012, Display by Author

[14] Usage (ger. "Nutzung") can imply active blogging or just reading as well.

The most commonly used CMS is without a doubt "wordpress", with according to their own testimony have a market share of 66% with over 66 million downloads (Schmutte 2013). This of course, does not imply that there are 100 million bloggers in the world as some people may have several blogs and many who downloaded the software may have never used the tool after all. Beyond that not all webpages that use "wordpress" can be technically considered as blogs, seeing as it is one of the simplest tools to create a website. "Wordpress" itself estimates that 15 % of all Webpages are based on "wordpress" (Schmutte 2013).

The online platform wordpress.org[15] noted 42 million new blog posts in May 2014 alone. This can give at least an idea of the scope of the blogosphere. The analysis tries not to superimpose too many assumptions on the material in order to ensure the explorative character of the study.

Theoretical framework

This paper draws on my research, which was designed to accumulate a comprehensive overview of the scenarios associated with "cyberwarfare" in the German speaking blogosphere. The overview was put together in order to provide data from which a theoretical sample for an in-depth discourse analysis could be selected.[16] The subsequent analysis took a theoretical frame into account while at the same time this frame was only to be used as a supportive tool – a tool which does not interfere with the explorative nature of the study. Due to the purpose of the research design the items, which showed a high variety of features, were sampled quantitatively. In the context of this paper only a few selected aspects can be discussed. The items discussed were those most relevant to (gaining a deeper understanding of) the social perception of risk, as introduced by Beck.

The first question to be addressed would deal with the relevance of understanding the construction of risk. Beck explains that, "in dealing with catastrophic risks, the present of the future planetary state of exception, which can no longer be contained and managed at the national level, is being negotiated." (Beck 2009: 76) To understand that this is not merely, or

[15] Which relies on "wordpress" but is distinct from the software.

[16] The discourse analysis is based on the Sociology of Knowledge Approach as defined by Reiner Keller (2011). At the point of writing the paper I am conducting this analysis as my master thesis.

even mainly, a matter of defining whether or not there *is* a threat coming from or through cyberspace and if it should be dubbed a "war" or not, the concept of "securitization" shall be mentioned:

> *"When states or nations securitize an issue – "correctly" or not – it is a political fact that has consequences, because this securitization will cause the actor to operate in a different mode than he or she would have otherwise." (Buzan et al 1998: 30)*

Hence, the social perception of risk or as Beck put it "the anticipation of the catastrophe" is a reality, be it scientifically "right" or "wrong". And as such a reality will always have real consequences, which is why this paper focuses on those "social realities".

While the concept of securitization is defined much clearer than the question of the social perception of risk, the idea stems from the same root: The fact that risks or dangers are coloured painted in one way or another, will lead to the manner in which they are treated and the real physical consequences they generate.

Methodology

The applied methodology was inspired by the methodology utilized by Beverly Silver (2003: 182-204) to establish a database of labour unrest. It has however been adapted and modified generously to fit the purpose of the research.

Given the limited amount of research regarding the German speaking blogosphere and the varied outlook on cyberwarfare in general several issues had to be taken into account in the analysis: on the one hand the analysis is quantitatively oriented and thus standardized, to get a broad overview on the subject, but on the other hand it needed to be explorative, as to not preliminary exclude insights based on insufficient information. So the research was conducted in two phases.

The design was created to first exploratively establish a list of factors in the construction of scenarios in the German speaking blogosphere, which were then implemented into a standardized form and compiled in IBM SPSS. As pointed out, this study was conducted to

explore the field and set up an overview. One big advantage at this stage was the possibility to analyse a much larger number of blog posts, as would have been possible in purely qualitative study. Due to the novelty and in accordance with keeping the research as open as possible to new data there were a number of non-standardized categories from which some were also converted to standardized categories after the analysis.

Data

As mentioned the study was conducted in two phases:

Phase 1 was the pre-test and the exploration and phase 2 a more standardized quantitative survey. The Pre-Test contained a sample of 56 blogposts on cyberwarfare. Compiled aspects included:

1) the title of the post
2) the date of the post
3) the URL
4) the topic – this was coded openly and later condensed to a set used in the survey of the second phase. Focus was being laid on the main elements and subjects in context to cyberwarfare so a quantitative comparison was possible.
5) the name of the blog
6) the amount of comments to the post
7) the type of blog using adapting the ideal types introduced by Eikmann (2006)
8) the amount of pictures used in the post
9) the Sense of threat – as well as the topic; this was incorporated in an open form and later condensed to categorizes.

Most of the cases included in the pre-test were transformed and taken into the standardized survey.

In the second phase the main survey used a word-scan for keywords. The first part of the survey utilized the so-called "German Blogcharts" ("Deutsche Blogcharts"). For the first 30 blogs on the list of May 2014 the search function of the blogs themselves was used to search

for the words "cyberwar" and "Cyberkrieg" (German: cyberwar)[17]. The aim of this first step was to gather especially relevant blogs, which means in this case especially popularly received ones.

To introduce a larger variety of blog (post) types into the sample in a next step the blog search engine "Meltwarter Icerocket" was applied, which allowed for a reliable language filter. This engine was applied to find less optimized and professional blogs. It only scans the rather recent past. In contrast to this the "Google Blog Search" was searched only for "cyberkrieg" as it predefines the language very effectively. Google is the most relevant search engine and could not be ignored for the analysis, even though the algorithms, which it uses, are rather mysterious. As a third step relevant posts, which were linked in sampled posts, were also incorporated. The aim of this sophisticated approach was to obtain a sample as diverse as possible. The reason for the application of search methods was to limit the distortion by the algorithm of a single search engine.[18]

The sample used for analysis contained 148 cases.

Limitations of the analysis

> *„How can you do research when your object is in a state of hyper-growth and permanent transformation?" (Lovink 2008: xxiii)*

The results of this analysis are necessarily very limited. That is not least due to the temporal and financial constraints of a student. The size of the parent population is unknown, thus we cannot make probable assumptions about the representativeness of the sample. We can however speculate, that due to the diversity of the analysed materials representativeness cannot

[17] The use of "Internetkrieg" (german: Internet-War) was dropped after the first part of the survey, because it wasn't rendering results. While possible as a term for any such construct it is not popularly used in the online community.

[18] Not surprisingly, not all results found by the described methods were actually relevant to the answer of the research question. For that reason a rather detailed criteria catalogue was designed, intending to sample only relevant cases, without compromising the openness.

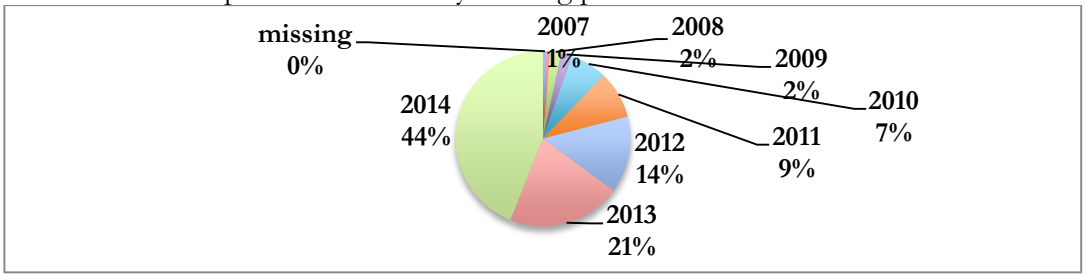
be assumed. To alter the relevance and generalizability of the survey multiple means of selection were applied. Yet the current analysis has to be viewed as giving a foundation to educated guesses, more than concluding facts.

The reliability of the purely quantitative factors in the sample is solid, but as this is a mixed-methods approach, those parts that are of a more qualitative nature rely on interpretation and can be seen as more vulnerable. Most prominently this would be true for the "threat perception" category, which ultimately is based on a decision by the researcher, who has to classify the kind of threat perception that is expressed in a post. While done with a lot of care and aimed to be as objective as possible, the reliability for qualitative research is always limited.

Another problem is the "Logic of Google": What has been clicked, linked and shared a lot is listed on top of the results list and thus again is most often clicked. This makes the process effectively self-enforcing (Keller 2012: 41). Therefore we can expect a high impact of Google even on the not "googled" results. At the same time a complete blindness to the social reality of a numeric-statistic perception of knowledge would not have been desirable. As the objective of the analysis is to depict the discourse, one thing has to be kept in mind: everybody may be able to speak on the Internet, but in no way is everybody actually heard.

For the here-portrayed findings it is very relevant to note that there is a certain temporal bias in the sampled data. As can be seen in the chart, the closer to the present, the more data was found[19].

Chart 3. Years of publication of analysed blog posts[20]



Source: Author.

[19] Do note that the data collection took place between March and August of 2014.
[20] Table with numbers can be found in Appendix Table 1.

There are four feasible reasons for this: Firstly, quite possibly the algorithms of the utilized search engines gave higher relevance to newer posts. Secondly, blogging per se is very new, and has only recently started to become a mass phenomenon, as was shown. Therefore it does seem likely to be representative that there is a prevalence of recent posts. Thirdly, in contrast to the often-stated platitude "the web never forgets" the web does forget quite a lot. Users as well as service providers often delete inactive blogs. The longer it has not been used, the more likely it is to be "axed" for one reason or another. The fourth reason is rooted in the topic itself: Cyberwar as a concept is not new in itself, but constantly gained attention in the German public sphere over the last few years.

Intentionally, nothing was done to correct this tendency to prefer newer posts, as it is not possible to discern whether it is due to a bias in methodology or actually to the research question and founded naturally in the data.

The used form had a rather large number of items on it and there is only space to review some of those here. Particularly those items that considered especially the nature of the blogosphere in context of the discussion of "cyberwarfare" will not be discussed here. Instead this paper shows a review of the threat scenarios, the state actors and the types and topics of "cyberwarfare".

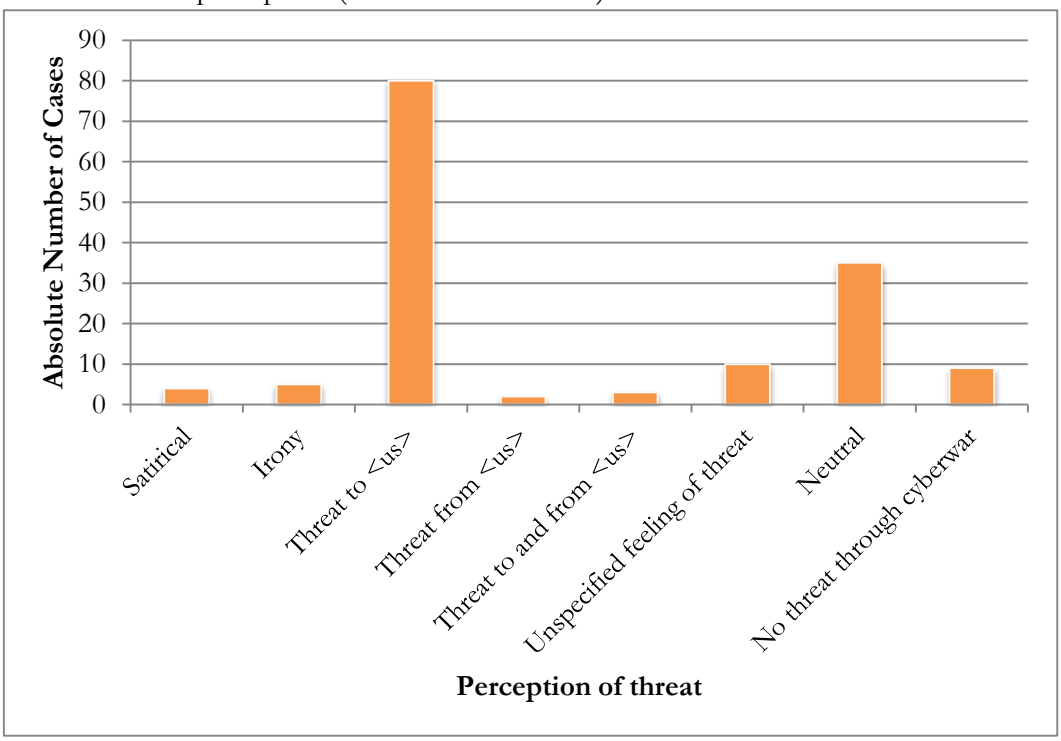
Analysis and findings

Not really surprising are the findings regarding threat perception. This category is not a real quantitative category, but has to be viewed rather as a mixed category. In the latter the perception of threat expressed by the blogger was analysed. The distilled categories are "threat to <us>", "threat from <us>", "threat to and from <us>" with <us> being an unspecified group to which the blogger is counting her or himself to, explicitly or implicitly.[21] Further, a "neutral" and a "no threat through cyberwar" item are designed as well as another item

[21] An example for this would be a blogger talking about a danger to (or) from „Germany“ and express worry over it. While never expressly identifying as a German therefore being threatened as a German is implied. In a lot of cases there is a more vague reference to a danger to „us“, not elaborating who „us“ actually is, which is where the name of the category stems from.

compiling those cases that express an "unspecified threat". Those describe a scenario in which cyberwar is a threat, yet does not tell who is threatened or what this threat refers to.[22] Separate from those labels, the categories "irony" and "satire" were established. This was done because, while these rhetorical devices may be downplaying threats, as they are humorous, they at the same time are often used to address very real concerns and cannot be interpreted as purely dismissive. This analysis shows the following result:

Chart 4. Threat perception (in absolute numbers)[23]



Source: Author.

We can see that an overwhelming majority of the analysed blog posts express a feeling of being threatened by cyberwarfare. The second largest group shows a neutral stand[24]. Only a very small group does not see cyberwar as threatening to anyone and dismisses the issue as not serious.

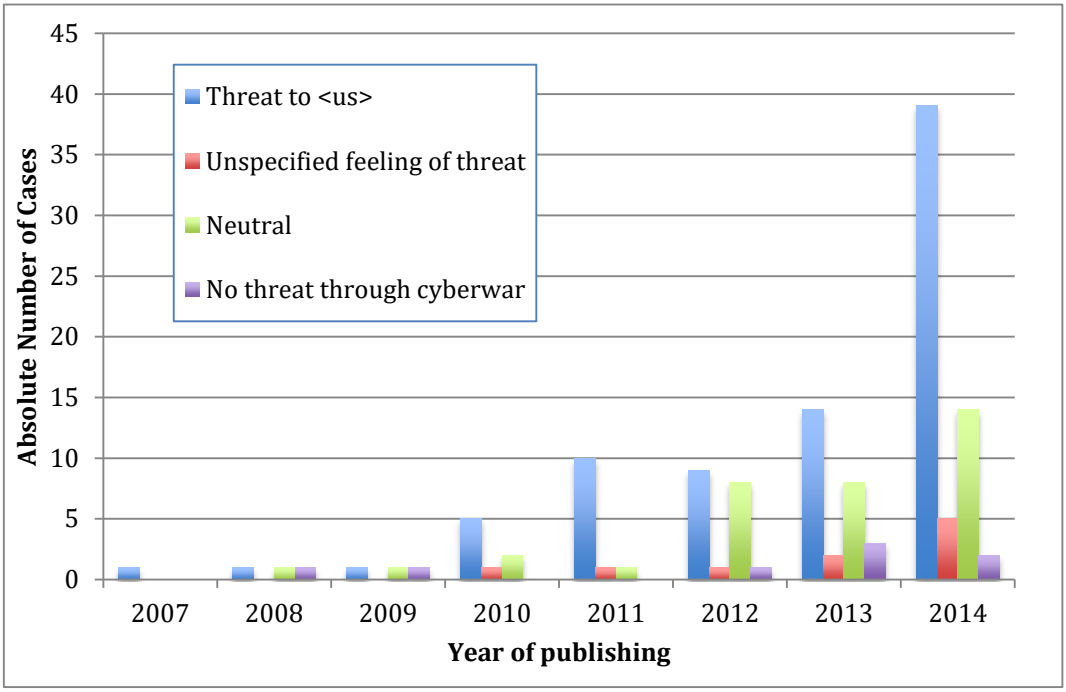
[22] Note that, since bloggers are not professional journalists and often do not strive to be, sometimes very personal or unspecific messages are sent. Therefore a clear identification of the blogger's viewpoint is at the least difficult/hardly possible.

[23] Table with numbers can be found in Appendix Table 2.

[24] Or does not express an opinion.

Here we can see a development:

Chart 5. Development of selected threat perception over time[25]



Source: Author.

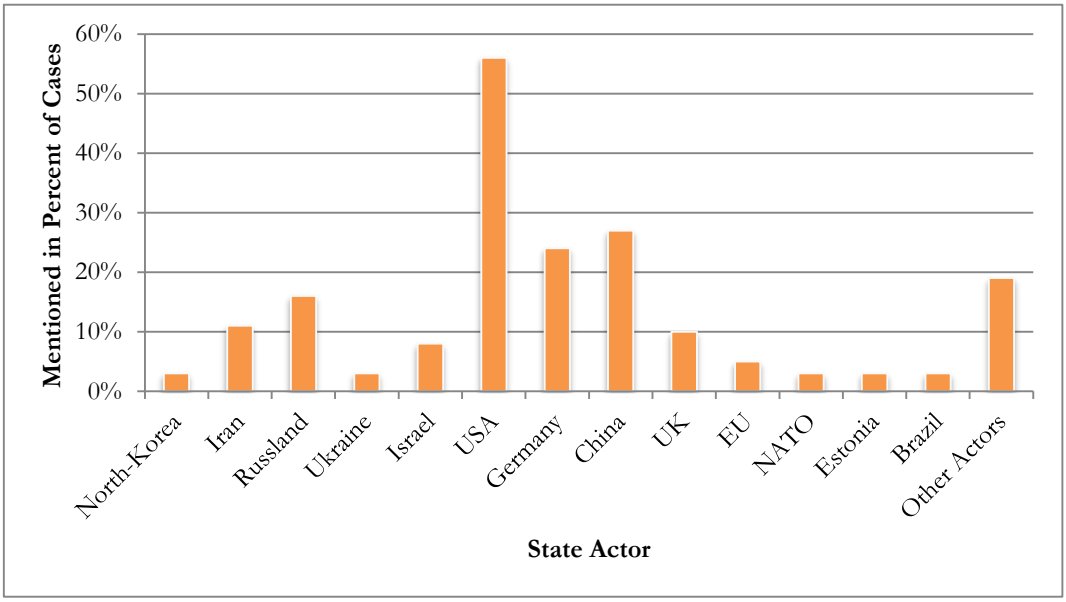
As chart 5 shows, the perception of threat towards <us> has been increasing enormously after 2010, especially in comparison to the other categories. That might not be surprising as the whole topic gained higher public relevance when in 2010 the malware Stuxnet was discovered and publically discussed.[26]

[25] Table with numbers can be found in Appendix Table 3.

[26] Stuxnet is a malware that uses a zero day exploit to target nuclear power plants. The United States and Israel later admitted that the creation of Stuxnet was a product of their collaboration. It was meant to disable the Iranian nuclear program. Edward Snowden confirmed that confession in 2013 ('Snowden confirms NSA created Stuxnet with Israeli aid' 2013).

Taking a look at the state actors that are mentioned in context of cyberwar the following results can be seen:

Chart 6. State Actors in Cyberwar (in percent of cases that mention state actors)[27]



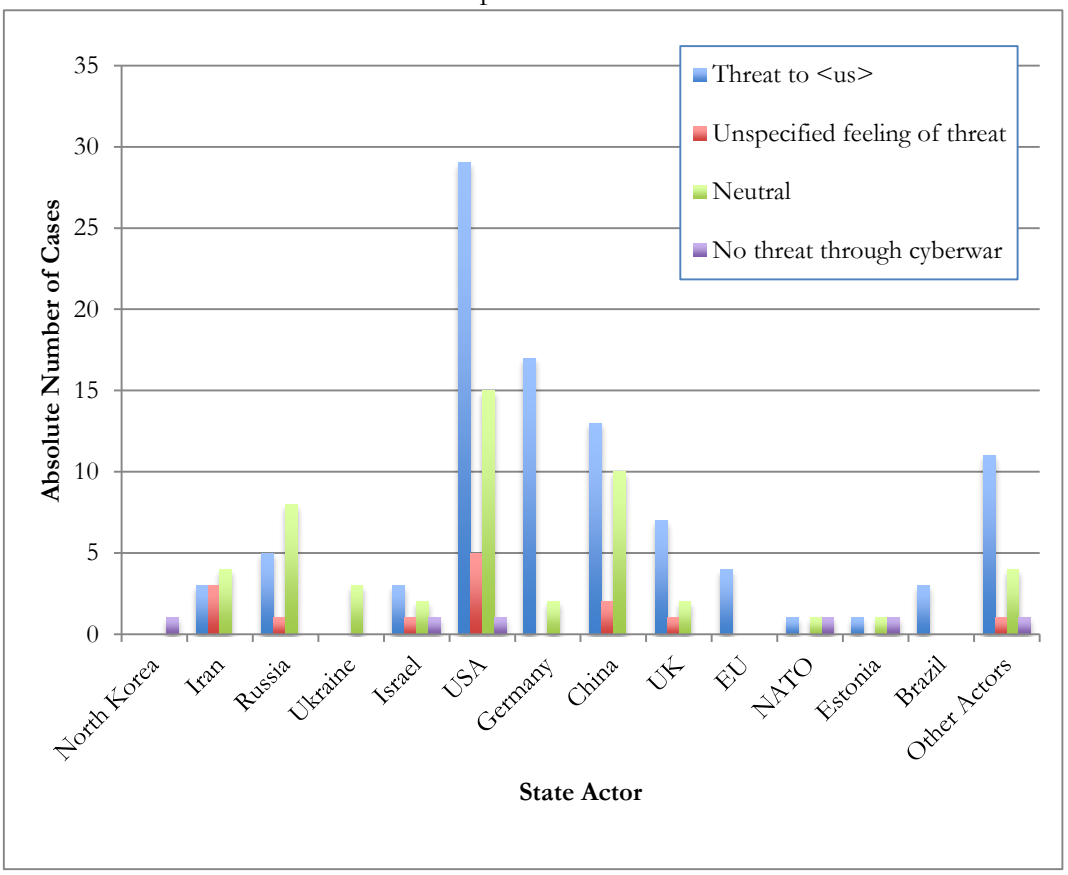
Source: Author.

The chart only displays posts that mention state actors, which is only true for about two thirds of all sampled cases.[28] Again half of them mention the USA and only about a quarter talked about Germany. This is surprising, as most compiled posts are written by and large from a German perspective. Apart from the US and Germany the number of references made to China and Russia is noticeable. It is important to keep in mind, that the items compile state actors that were: firstly, named as actors in a (potential) cyberwar, and secondly, only if they were described as a political entity. That is to say "hackers in China" or "Chinese hackers" does not make the state an actor and thus was not noted as Chinese, in contrast to "hackers on behalf of China", which implies an active involvement of the state rather than stating a nationality. Additionally, the data is not compiled in a directed form, meaning that the named actors can be aggressors or victims or innocent bystanders trying to mediate.

[27] Note that this is a multiple answer set - many blogposts mention more than one actor.
[28] 67,7%, which makes exactly 100 blog posts. Table with numbers can be found in Appendix Table 4.

When cross-referencing the perception of threat and the state actor we can make an educated guess:

Chart 7. State Actors and Threat-Perception[29]



Source: Author.

Russia is mentioned more often in posts taking a neutral viewpoint in regard to a potential threat compared to those bloggers that view a threat for <us> coming from cyberwar. This obviously looks different for blog posts about the USA. The highest disparities can be observed however when talking about Germany, which would be the most logic group to relate to as <us>. Therefore the assumption that especially the US is perceived as an aggressive force in cyberspace is not much of a stretch. [30]

[29] Perception of threat cleaned by all with 5 or less mentioning for better visibility. Table with numbers can be found in Appendix Table 5.

[30] As this focused on the German language area for completion: Switzerland was mentioned four times, and was recorded as "Other Actor". Austria was not mentioned as actor, but there was one mentioning of the GDR (ger.

The next aspect that should be mentioned here is about the "*topic* of cyberwar" found in the analysed data: As discussed, in the literature review section, there are a lot of different opinions on the nature of a cyberwar and which – if any – types of threat or aggression are to be understood as a cyberwar. Common ground is essentially "something that has to do with computers and is potentially dangerous". Outside of an academic discussion, the variety of interpretation is even broader amongst bloggers.

This study focused on extracting in the first phase "topics": definitions of what a cyberwar actually is about. Those were standardized and expanded in the second phase. It is important to note, that the compilation of topics was done exploratively from the material. The aim is to understand the view of the bloggers as precise and comprehensive as possible and not to apply previously established constructs and force them on the data. For this reason scholars would traditionally evaluate some of the topics differently. Also, it should be noted that this was a multiple answer set, so none of the categories excludes any of the others.

The following list, was compiled as discussed topics of cyberwar:

- **Interception**

  Intercepting citizens with technical methods through the own or an allied state. Espionage being the interception between countries was coded as Competition Dispute. This is founded in the purely empirical findings, in which espionage between countries is viewed as a danger of an economical nature in the end.

- **Islamic Terror**

  Cyberwar as a method of fundamentalist Islamism.

- **Other Terror**

  Cyberwar as a method of other extremist groups to broaden their agenda.

- **"Hot War"**

  Understanding cyberwar as an antecedent or part of a "real" physical war.

- **"Cold War"**

DDR = Deutsche Demokratische Republik/ East Germany) as well as the fictional state of the Republik Freies Deutschland (RFD). While German is also an official language in other countries the majority of findings was authored by German bloggers.

Cyberwar understood as a surrogate for the physical enactment of a war. This does not imply there are no victims, but attacks are conducted purely on a digital level.

- **Software Attacks**

Attacks on and through software are conducted. Those are mainly DDoS-Attacks and Botnets.

- **Hardware Attacks**

Physical Infrastructure is attacked through cyberspace or digital weaponry. Focuses mostly on critical infrastructure and SCADA systems.

- **Info War**

Information is used as a "weapon" in cyberwar. This includes misinformation and propaganda as well as withholding information.

- **Robotics**

Drones, Robots or other physical technical systems are characteristic parts of a cyberwar.

- **Guerilla Cyberwar**

Cyberwar as a medium for small political groups to push their agenda. This is sometimes viewed as legit sometimes not, but is clearly differentiated from terror in the view of the blogger.

- **Internet Rights**

This entails all that includes internet governance or rights, as well as laws in cyberspace.

- **Fiction**

This is a Meta-Category which encompasses games, movies and books, as well as simulations of cyberwar. As those are fictional matters this has to be noted since they may be viewed as plausible, but are not real in the actual sense. The category also takes a closer look at the influence of fiction on the construction of cyber threats and risks in general.

- **Cyber Crime**

Applies when criminal acts are re-interpreted as acts of (cyber-)war.

- **Competition Dispute**

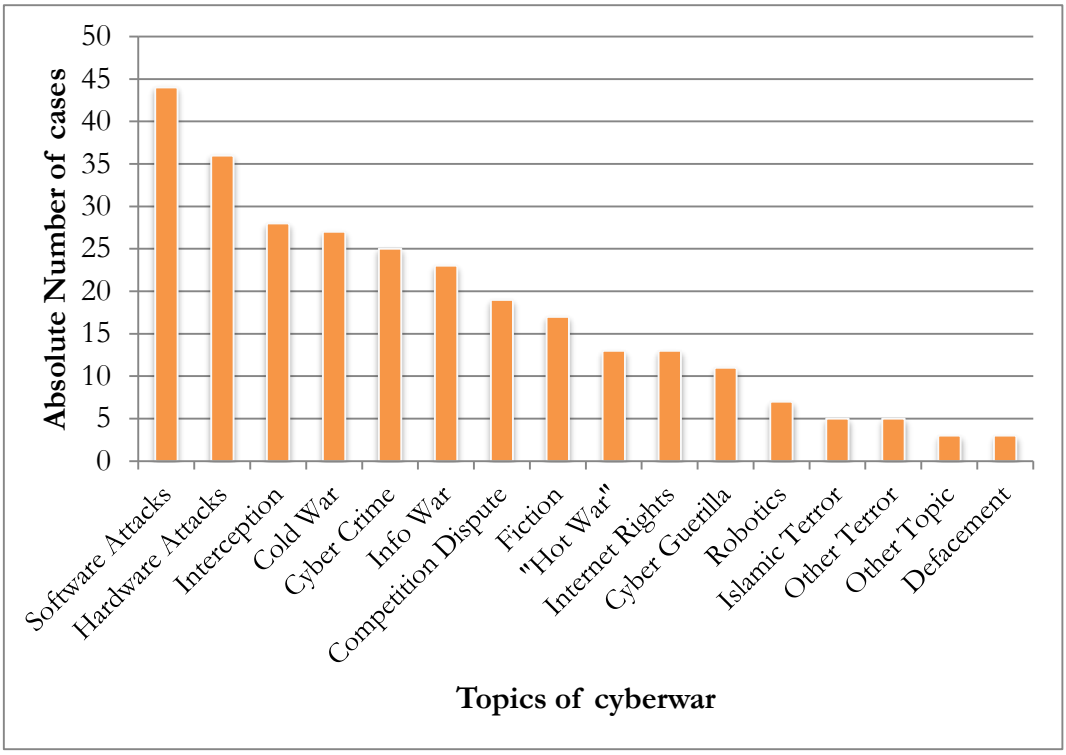
Cyberwar can be viewed as a capitalistic Dispute between competitors. That means (businesses) enterprises act also as (potential) aggressor and not only as victims of a cyberwar. It also applies to cyber espionage as explained above.

- **Defacement**

  Defacement of Websites as acts of cyberwar.

As there is no good way to draw a comparison, at this point, it is unclear, which parts of this are actually specific for the German language area. In an overview the findings are as follows:

Chart 8. Topics of cyberwar in all cases (in absolute numbers)[31]



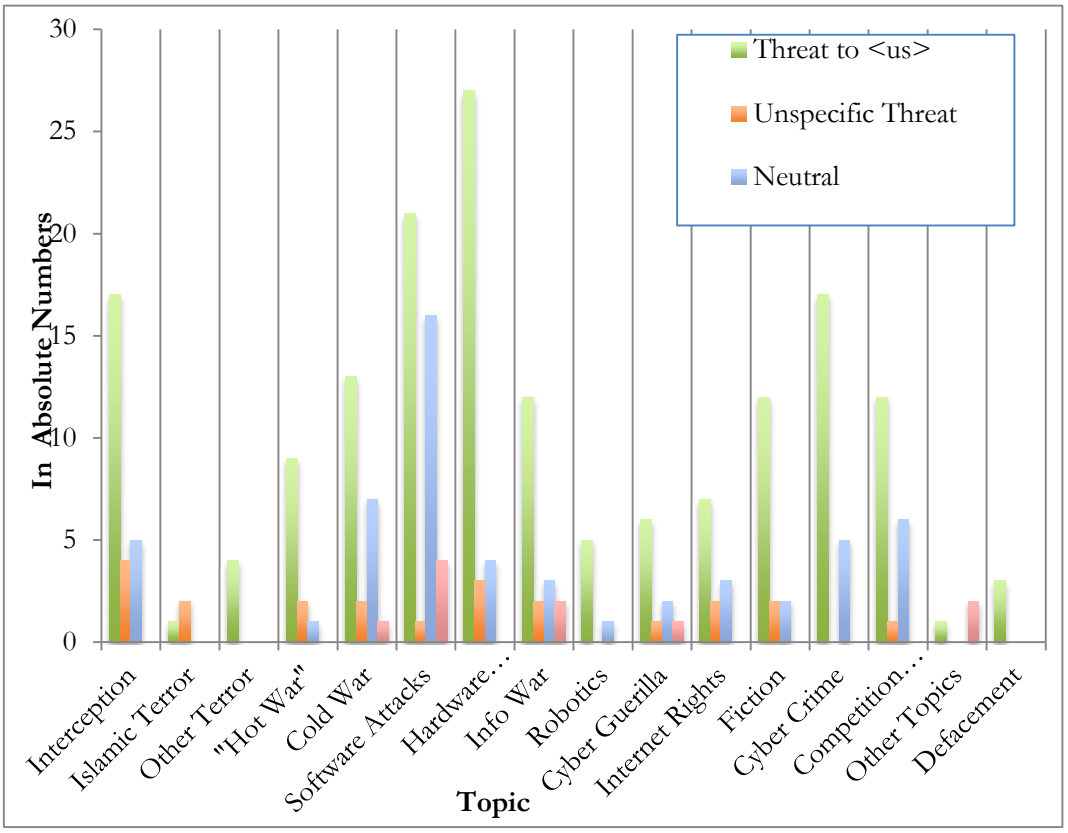
Source: Author.

While it might not surprise that software and hardware attacks were mentioned a lot more frequently as forms of cyberwar, the fact that interception is often viewed as a form of cyberwar is something that would not have been part of traditional views of cyberwar. This suggests that for a real understanding of the social perception of cyberwar, indeed a opener approach is needed.

[31] Table with numbers can be found in Appendix Table 6.

Taking a look at some selected factors of threat perception of those topics shows this:

Chart 9. Threat perception of topics of cyberwar (in absolute numbers)[32]



Source: Author.

Chart 9 proves that interception is not at all something that should be shrugged off as a perceived risk. Terror however does not rate very high in comparison. Hardware Attacks show up as a definite peak in threat perceived by the bloggers. While Software Attacks are also perceived as potential risks they are amongst those that are most described neutral or not threatening at all. In contrast to that, there is a very high correlation between cyber crime and perception of personal danger. This is much more likely to have a personal effect on the blogger, which is interesting, yet not that surprising.

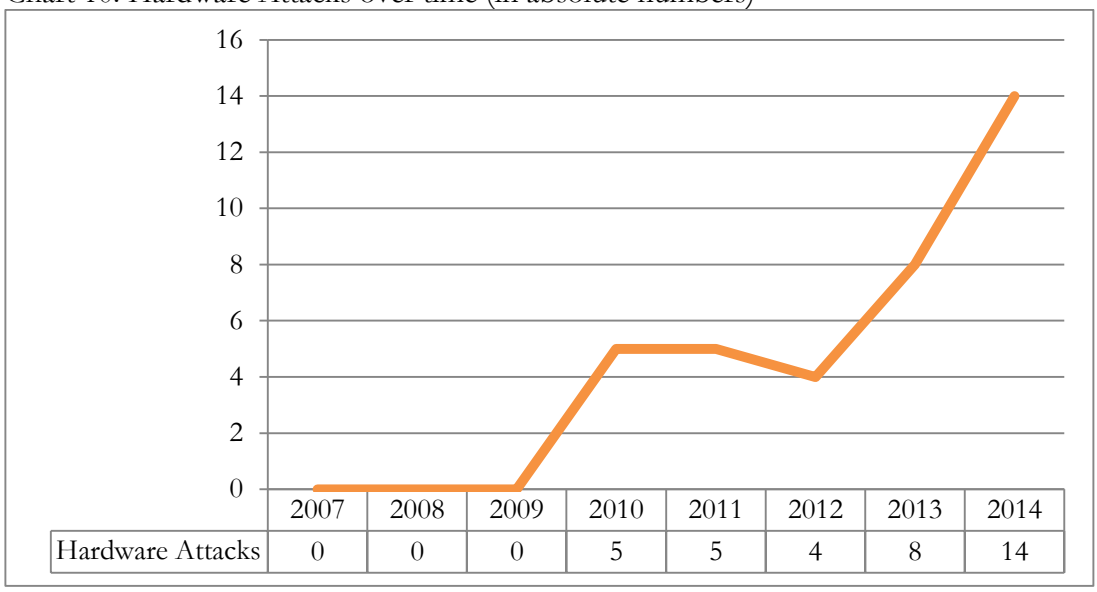
[32] Table with numbers can be found in Appendix Table 7.

Overall, the most fearsome risk seems to be that of "Hardware Attacks" – attacks on (critical) infrastructure by the use of digital weaponry. As this is arguably the most likely way to cause victims in a cyberwar, that result could have been expected. Also, Stuxnet has been in various ways described as

> *"the Hiroshima of cyber-war. That is its true significance, and all the speculation about its target and its source should not blind us to that larger reality. We have crossed a threshold, and there is no turning back." (Vanity Fair 2011)*

It seems only logical to take this into account when connecting this result with Beck's construction of „potential catastrophes". The fact that this particular event had such a large impact is supported by the appearance of the topic over time:

Chart 10. Hardware Attacks over time (in absolute numbers)[33]



	2007	2008	2009	2010	2011	2012	2013	2014
Hardware Attacks	0	0	0	5	5	4	8	14

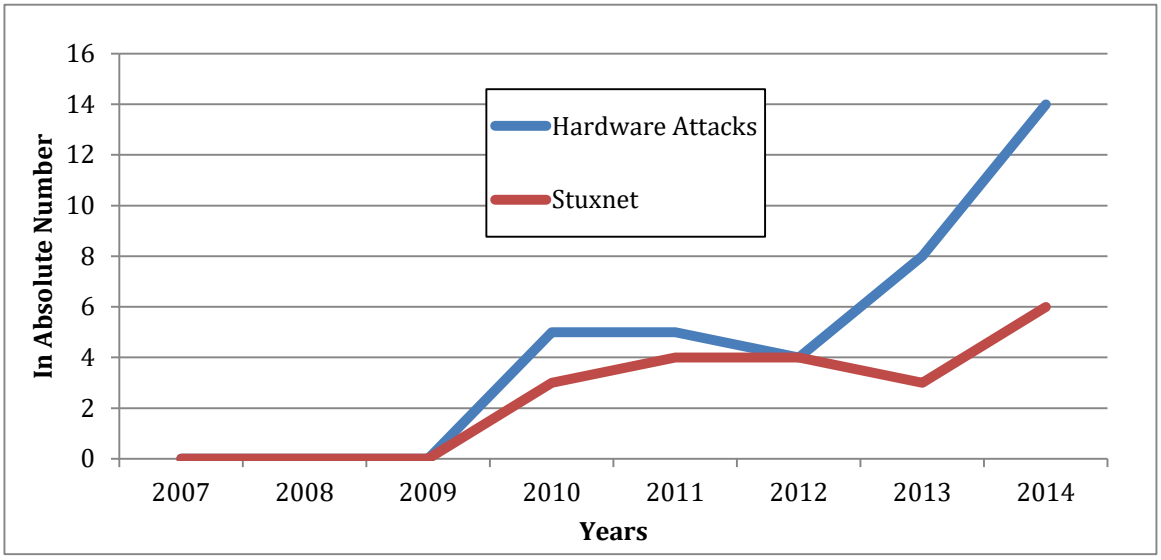
Source: Author.

With the discovery of Stuxnet in 2010, the topic is first observed at all. However, with some surprise I found that in spite of the public attention Stuxnet got, it was only mentioned in 20 of the analysed cases. That makes 13 percent of all cases, but only accounts for almost half of the cases mentioning "Hardware Attacks". Even more surprisingly, those references are

[33] Table with numbers can be found in Appendix Table 8.

spaced out pretty evenly over the observed time – so the topic has not lost its appeal. When you however compare those two data points a new aspect draws attention:

Chart 11. Hardware Attacks and mentions of Stuxnet in comparison over time



Source: Author.

While until 2012 most of the posts on "Hardware Attacks" mentioned Stuxnet, since then the discussion has expanded. Conclusively, Stuxnet indeed is very prominent and relevant but reducing the discourse on cyberwar to the discovery of Stuxnet would be rather faulty.

Conclusions

As this brief insight into the study shows, the perceived risk of "cyberwar" could be different than you might expect on the first glance. Most surprising is maybe that the "big boogieman" of the twenty first century, the fundamentalist terror, does not play a large role in the reviewed discourse. This does not necessarily mean, that the bloggers perceive no risk in this respect, but it does indicate that particularly interception and cyber crime are viewed as more immediate threats than those acts of violence in the context of cyberwar. Of course this study is by no means conclusive and further studies might completely disprove this as fluke.

Calculating the risk that comes with being intercepted by secret agencies is very nearly imponderable. As the popular saying goes "if you have nothing to hide, you have nothing to fear". Yet we have seen that the popular perception of this is very different. It should be taken into consideration, that in this context at least it was labelled as a "war" which adds weight to the obviously perceived seriousness of the issue.

What can be noted with a certain amount of caution is the overall perception of risks coming from cyberspace. There may be some confusion about the terminology and cyberwar is at least in some instances likely to be used synonymously with cyber threat. Yet the fact that the fourth most compiled topic is "Cold War" – and therefore expressing a digital variety of a war in lieu of the "traditional" war on battlefields – stresses, that there is some actual fear of war.

The "expected catastrophe" has many faces and is very divers once you take a closer look, as can be seen in the discussion of the significance of Stuxnet. The perception of the possibility of "Hardware Attacks" has since exuded the singular occurrence and reached the public mind as a general risk.

As pointed out initially, the presented study can only be the basis for a discourse analysis of the topic. That qualitative approach will be able to shed more light on many aspects that could not be addressed in this context. A special place in that study will be given to the comments, as they are an integral part of the blogosphere, yet could not be taken into account for the presented work.

Still, many questions remain. Future research should collect a much bigger sample of blog posts as a way to see if the presented findings are actually representative or if they are too strongly biased. Further it would be of great value to discern in how far there is a difference between the perception of "cyberwar" and "cyber threats" as well as differentiating between the perception of danger, risk and threats more accurately. The social impact of those perceptions is difficult to calculate, yet it stands to reason that the more complete the picture of it is compiled, the more insightful those impacts can be noted. In the long run, the effects of those perceptions of risks and threats are likely to affect policy setting as well as the social

differentiation of society in general. As the interconnectedness of things and people is steadily rising and cyberspace is a vital part of social interactions, dangers, be they real or only perceived, have to be handled and addressed. Conflicts in and around cyberspace are therefore likely to only grow in importance in the coming years.

Being a field that is so very new and at the same time changes so very fast, pinpointing anything in cyberspace is a challenge and the presented work can only scratch the surface and act as a starting point for future explorations.

References

ARD/ZDF (2013): 'Onlinestudie', Accessible at WWW: http://www.ard-zdf-onlinestudie.de/ (10 August 2014).

Beck, Ulrich (2009): World at risk. Cambridge, UK; Malden, MA: Polity.

Buzan, Barry; Waever, Ole; Jaap de Wilde (1998): Security: a new framework for analysis.

Boulder, Colo: Lynne Rienner Pub.

Clausewitz, Carl von. (2008): Vom Kriege. Hamburg: Nikol.

Duden: Blog. Accessible at WWW: http://www.duden.de/rechtschreibung/Blog (11 March 2015)

Eikmann, Julia (2006): 'Die Blogosphäre: Teenager auf Selbstfindungskurs neben One-Man-Journalismus', Forschungsjournal Neue Soziale Bewegungen 19 (2): 91–103.

Gaycken, Sandro (2012): Cyberwar: Das Wettrüsten hat längst begonnen; vom digitalen Angriff zum realen Ausnahmezustand. München: Goldmann.

Gross, Michael Joseph (2011): 'A Declaration of Cyber-War', Vanity Fair. Accessible at WWW: http://www.vanityfair.com/news/2011/04/stuxnet-201104 (27 March 2015).

Hegenbert, Christine (2012): 'Semantics Matter – NATO Cyberspace and Future Threats', Research Paper No. 103. Rome: NATO Defense College.

Keller, Reiner (2011): Wissenssoziologische Diskursanalyse: Grundlegung eines Forschungsprogramms. Wiesbaden: VS Verl. für Sozialwissenschaften.
Keller, Reiner (2012): 'Die Unordnung der Diskurse. In Grenzen des Wissens.' In Ulrich Wengenroth (eds.) Grenzen des Wissens. Weilerswist: Verbrück Wissenschaft. 23-55.

Lovink, Geert (2008): Zero comments: blogging and critical Internet culture. New York: Routledge.

Pluta, Werner, (2014, January 17): 'Thingbot: Botnetz infiziert Kühlschrank' Golem.de. Online-Magazin, Accesible at WWW: http://on.rt.com/qeyfk5 (8 October 2014).

Rid, Thomas (2012): 'Cyber War Will Not Take Place', Journal of Strategic Studies 35 (1): 5-35.

Schmutte, Manuel (2013, May 27): '10 Jahre WordPress! Wir feiern – du kannst gewinnen! (inkl. Infografik)', MarketPress Deutschland. MarketPress.de, Accessible at WWW:

http://marketpress.de/2013/10-jahre-wordpress-wir-feiern-du-kannst-gewinnen-inkl-infografik/ (27 March 2015).

Silver, Beverly J. (2003): Forces of Labor: Workers' Movements and Globalization Since 1870. New York: Cambridge University Press.

'Snowden confirms NSA created Stuxnet with Israeli aid' [Online-Article], (2013, September 7). RT, Accesible at WWW: http://rt.com/news/snowden-nsa-interview-surveillance-831/ (18 March 2015)

'War in the fifth domain' [Article] (2010, July). The Economist, Accessible at WWW: http://www.economist.com/node/16478792 (27 March 15).

Zerfass, Ansgar; Boelter, Dietrich (2005): Die neuen Meinungsmacher. Weblogs als Herausforderung für Kampangnen, Marketing, PR und Medien. Graz: Nausner und Nausner.

Appendix

Table 1. Years of publication of analysed blog posts (absolute numbers)

	Frequency
missing	1
2007	1
2008	3
2009	3
2010	10
2011	13
2012	21
2013	31
2014	65
Total	148

Table 2. Threat perception (displayed in gray)

	Frequency	Percent	Valid Percent	Cumulative Percent
Satirical	4	2,7	2,7	2,7
Irony	5	3,4	3,4	6,1
Threat to <us>	80	54,1	54,1	60,1
Threat from <us>	2	1,4	1,4	61,5
Threat to and from <us>	3	2	2	63,5
Unspecified feeling of threat	10	6,8	6,8	70,3
Neutral	35	23,6	23,6	93,9
No threat through cyberwar	9	6,1	6,1	100
Gesamtsumme	148	100	100	

Table 3. Development of selected threat perception over time

		Year								
		2007	2008	2009	2010	2011	2012	2013	2014	
Threat Perception	Threat to <us>	1	1	1	5	10	9	14	39	80
	Unspecified feeling of threat	0	0	0	1	1	1	2	5	10
	Neutral	0	1	1	2	1	8	8	14	35
	No threat through cyberwar	0	1	1	0	0	1	3	2	9
		1	3	3	10	13	21	31	65	148

Table 4. State Actors in Cyberwar (displayed in gray)

		Answers		
		Frequency	Percent	Percent of cases
State Actors ALL	North-Korea	3	1,60%	3,00%
	Iran	11	5,80%	11,00%
	Russland	16	8,40%	16,00%
	Ukraine	3	1,60%	3,00%
	Israel	8	4,20%	8,00%
	USA	56	29,30%	56,00%
	Germany	24	12,60%	24,00%
	China	27	14,10%	27,00%
	UK	10	5,20%	10,00%
	EU	5	2,60%	5,00%
	NATO	3	1,60%	3,00%
	Estonia	3	1,60%	3,00%
	Brazil	3	1,60%	3,00%
	Other Actors	19	10,00%	19,00%
Total		191	100,00%	191,00%

Table 5. State Actors and Threat-Perception

		Threat to <us>	Unspecified feeling of threat	Neutral	No threat through cyberwar	Total
State Actors All	North Korea	0	0	0	1	3
	Iran	3	3	4	0	11
	Russia	5	1	8	0	16
	Ukraine	0	0	3	0	3
	Israel	3	1	2	1	8
	USA	29	5	15	1	56
	Germany	17	0	2	0	24
	China	13	2	10	0	27
	UK	7	1	2	0	10
	EU	4	0	0	0	5
	NATO	1	0	1	1	3
	Estonia	1	0	1	1	3
	Brazil	3	0	0	0	3
	Other Actors	11	1	4	1	16
Total		52	7	24	4	100

Table 6. Topics of cyberwar in all cases (displayed in gray)

		Answers		
		Frequency	Percent	Percent of cases
Topic All	Software Attacks	44	15,80%	30,60%
	Hardware Attacks	36	12,90%	25,00%
	Interception	28	10,00%	19,40%
	Cold War	27	9,70%	18,80%
	Cyber Crime	25	9,00%	17,40%
	Info War	23	8,20%	16,00%
	Competition Dispute	19	6,80%	13,20%
	Fiction	17	6,10%	11,80%
	"Hot War"	13	4,70%	9,00%
	Internet Rights	13	4,70%	9,00%
	Cyber Guerilla	11	3,90%	7,60%
	Robotics	7	2,50%	4,90%
	Islamic Terror	5	1,80%	3,50%
	Other Terror	5	1,80%	3,50%
	Other Topic	3	1,10%	2,10%
	Defacement	3	1,10%	2,10%
Total		279	100,00%	193,80%

Table 7. Threat perception of topics of cyberwar (selected items; in absolute numbers)

Year \ Topic	Satire	Irony	Threat to <us>	Unspecific Threat	Neutral	No threat through cyberwar	Total
Inter-ception	0	1	17	4	5	0	28
Islamic Terror	1	0	1	2	0	0	5
Other Terror	0	1	4	0	0	0	5
"Hot War"	0	0	9	2	1	0	13
Cold War	2	1	13	2	7	1	27
Software Attacks	1	1	21	1	16	4	44
Hardware Attacks	1	0	27	3	4	0	36
Info War	1	2	12	2	3	2	23
Robotics	0	0	5	0	1	0	7
Cyber Guerilla	1	0	6	1	2	1	11
Internet Rights	0	0	7	2	3	0	13
Fiction	0	1	12	2	2	0	17
Cyber Crime	1	0	17	0	5	0	25
Competition Dispute	0	0	12	1	6	0	19
Other Topics	0	0	1	0	0	2	3
Defacement	0	0	3	0	0	0	3
Total	4	5	78	10	34	8	144

Table 8. Hardware Attacks over time (in absolute numbers)

Topic\Year	2007	2008	2009	2010	2011	2012	2013	2014	Total
Hardware Attacks	0	0	0	5	5	4	8	14	36