

5. Dez. 2012

von benkamis

in Cyber Security,  
Popkultur,  
Sicherheitskultur,  
Versicherheitlichung

Kommentare ( 20 )

## How to catch a Battletroll: States and the yarns they tell about the Internet, from the minnows to the whoppers

von Ben Kamis

**Battletroll** ('bætəl'troul) n.

1. an **Internet troll** whose comments are not only inflammatory but militaristic
2. an obscure **1990s toy** figurine

Last summer my esteemed and illustrious colleague **Thorsten Thiel** and I were talking about possible future projects. Thorsten is an expert on democratic theory and the politics of the internet, and I know a thing or two about international law and international security. In the course of the conversation, I asked the good doctor what I thought was an obvious question:

“ *Even the post-modern wars, like the Global War on Terror and the War on Drugs are fought with the typical means of violence as a deterrent, right? I mean, states go around chasing terrorists and drug lords with implements of pain and destruction, hoping that, if their targets are not killed in the process, they will at least be scared enough to seek another line of business. So what's with all this talk about 'cyberwar'? The Internet is just a network of ways to send weak electromagnetic pulses in certain patterns. Violence over the Internet is impossible in principle, so what does 'cyberwar' really mean, and why do people keep using such a peculiar word?*

Thorsten didn't have a good answer, and neither did I. Kids, listen: if even the experts don't have a good answer to your question, then it's what the professionals call a **research question**. Since this question required *research*, and research on tough questions is how all the fellows and chairs and doctors and professors at universities justify their burden to society, we set to work.

### SOCIAL MEDIA



### SUCHE

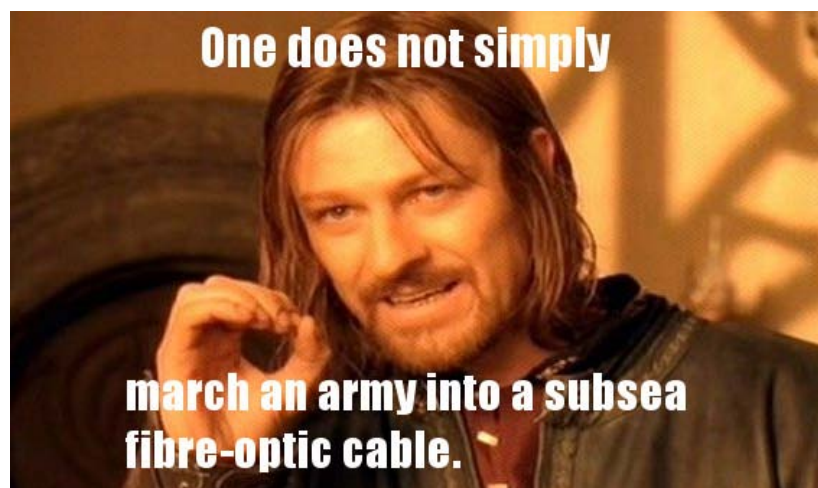
### TWITTER FEED

Ben Kamis: The concept of #cyberpeace is linguistic trolling. Cyberpeace: post-war is war, only more so <http://t.co/fkaHhcgekK> #cyberwar  
ungefähr 3 Stunden her von &s

Wer wissen will was #cyberpeace ist, sollte wissen was dieser sog. #cyberkrieg ist: Matthias Schulze dazu bei uns <http://t.co/LyvFdE29dN>  
8. Dezember 2014, 11:08 von &s

Neue #Jobs für Politikwissenschaftler\_innen!  
<http://t.co/f3vSzfJpMG>  
5. Dezember 2014, 9:03 von &s

### TAGS



Before I say anything about where we looked and what we found, let me disclaim grandiose statements based on this **preliminary** research. Before applying for lots of tax money and resources to answer the question, we wanted to conduct a ‘plausibility probe’, which is a kind of mini-study to find out whether the researchers’ initial intuitions are worth pursuing and if they can even get their hands on the right data. So what I’m reporting here are plausible, but not solid, peer-reviewed, ‘scientific’ results. So far, we’ve only presented our results at the **1st Annual HIIG Colloquium** (Kareful – ze Link ist in Dscherman), where they were well-received. Use them at your own risk.

So in what sense are states Battletrolls? Well, high-priced scientists like us cannot simply answer any question as posed. No, we need a theory to put our results in the context of other things we think we know about the world. This makes different bits of knowledge fit together better, and it lets us use fancy words, like ‘contingent generalization’. So the first step was to compose a theory that would explain why states would act like Battletrolls in the first place and give us an excuse to look.

Our theory starts by looking at the Internet. In the olden days, when Yahoo! was a dynamic start-up, Nirvana was a little band in Seattle waiting for a break, and home supercomputers with 10 MB hard drives were something for celebrities and tycoons, the Internet existed, but it was something for basement-dwelling aficionados. Many people had heard of the network the Pentagon had built that connected their hospital to the local university, for example, but only geeks and technicians had anything to do with it. These geeks came up with ideas about how this technology would change society, though, and the main idea was that the Internet would connect everybody to everybody else, allowing everyone to participate directly and equally in collective decision making. You wouldn’t have to vote for people anymore, because you would be able to discuss and vote on topics of public concern with everybody directly. These geeks realized that this would be a threat to traditional governments, and they even composed ‘**A Declaration of the Independence of Cyberspace**’, basically telling governments “Shove off, old timer!”.

Even though states had built the physical infrastructure of the Internet, they

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science!  
Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier  
Raum sein

Deutschlands Irak-Politik –  
Verantwortung nach außen,  
Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle  
Gewalt als politisches Mittel

## KATEGORIEN

Außenpolitik (59)

Bürgerkriege (16)

Cyber Security (42)

Demokratisierung (9)

Drohnen (15)

Humanitäre Interventionen (15)

Innere Sicherheit (24)

Interviews (10)

Katastrophen (4)

Konferenz (20)

Militär (28)

Pandemien (2)

Podcast (7)

Popkultur (21)

Sanktionen (8)

were starting to look like horseshoes on a sports car. For centuries, about 5 to be exact, states had been the main political units on the planet. They were organized hierarchically around some kind of central authority, they extracted resources from their populations (i.e. they forced people to pay taxes), and they justified all this by arguing that people needed them for protection and coordination. Nobody else is going to make sure that everyone has clean water or safe roads, and if the neighbours ever invade, you'll need an army to push them back.

So the idea is that states are just doing what they know. They claim to exist to protect you against violence (and to threaten others with violence on your behalf, if need be), and since the violence doesn't really apply to the Internet, states have to put it there. But since they can't export violence onto the Interwebz directly, it being a series of cables, satellites and microwave transmitters, why not do it with metaphor? Cyberwar isn't war, but if you can make it seem enough like war for the comparison to seem sensible, you can continue extracting resources and 'coordinating' people. The first step is to convince people that there's a real threat on the Internet that is so dire, they will be overwhelmed alone and need the state's help. 'Cyberwar' might just be that kind of threat (and **the latest James Bond** testifies to this theory – without James Bond & Star Wars, there would be no social science).

## Put the military in



Sounds like a workable theory, so now comes the time to go out and observe things. To make sure that we weren't just full of paranoid delusions and any further research would have a decent chance of producing interesting results, we picked 'hard cases', reasoning that if our theory worked where you would least expect it, it should work everywhere. To find cases where our Battletroll theory would be least likely to work, we took the top 5 countries from Freedom House's '**Freedom of the Net**' index: 1. Estonia; 2. USA; 3. Germany; 4. Australia; 5. Hungary. And to make sure these weren't Internet-friendly countries with obscenely-sized militaries, we also checked how much

Security Culture (14)
Sicherheits-Kommunikation (14)
Sicherheitskultur (205)
Sozialwissenschaft Online (57)
Stellenangebote (42)
Strategie (10)
Terrorismus (14)
Theorie (2)
Umwelt (1)
Versicherheitslichung (22)
Visualisierung (5)
Whistleblowing (8)
WikiLeaks (17)
WMD (10)
Zivilgesellschaft (48)

## BLOGROLL

Arbeitskreis soziale Bewegungen
Augen geradaus
Dan Drezner
Dart-Throwing Chimp
David Campbell
de.hypotheses.org
Demokratieforschung Göttingen
Duck Of Minerva
Future and Politics
Hylaeen Flow
Internet und Politik
IR Blog
Just Security Blog
justsecurity.org
Killer Apps
Kings Of War


they spend on defence per person. Although the USA is near the top of the list, Estonia and Australia were roughly in the middle, and Germany and Hungary are pussycats in terms of military expenditure. From a population of around 200 countries, we had found a sample of 5 hard cases, and it was time to collect data.

The data we collected was in the form of official cyber security policies and statements, which is a logical place to look if you think that relatively peaceful and net-friendly countries will use violent metaphors for the Internet. Given that we had chosen hard cases, the results were fairly surprising, except for Estonia. Even though Estonia hosts NATO's cyber security headquarters and was subject to massive DDOS attacks from a large neighbouring country who shall remain nameless (but we all know it was Ru55!a) Estonia was the most benign of the Trolls. Its official documents depicted cybercrime as a civil matter for the police, and 'cyberattacks' were only mentioned twice. For a sample of the documents we analysed in Estonia's case, see [here](#) and [here](#).

Second in order of non-trollery was Australia. Even Australia's cyber security intelligence bureau provided tips on how to secure home and business systems without militarist rhetoric or metaphors. See [here](#) for an example. An important white paper that was supposed to provide more details about Australia's cyber security policies has been delayed for 18 months, and the final verdict depends on its content, but Australia is prima facie a net-friendly Untroll.


In the middle of the pack was Hungary. Hungary doesn't publish much about official policy, at least not in a language Thorsten or I can understand. Instead, they publish more speeches and sound bites by officials. When they do refer to an existing policy, it usually consists of simply linking to a NATO policy paper, and they seem to outsource most of their thinking about cyber security to NATO. The **2012 National Security Strategy** did, however, casually relate cyber security to terrorism, crime, national defense and disaster prevention without clarifying this bewildering and diverse set of issues. Although Hungary's Internet policies are relatively free, according to Freedom House, they do present the Internet as quite the threat. Hollow rhetoric to inflame and aggravate the discussion is the essence of trolling.

Second place in the preliminary Battletroll ranking goes to the United States. Taking a look at the **Cyberspace Policy Review** and the **"International" Strategy for Cyberspace**, we find some heavy trolling. The most troubling example of which is from the latter document, stating "the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. ... We reserve the right to use all necessary means – diplomatic, informational, military, and economic – as appropriate and consistent with applicable international law, in order to defend our Nation, our allies, our partners, and our interests." Think about this for a second. First, the escalation is built in. You mess with their immaterial data, and they're threatening to visit you with invasion, cruise missiles, drones, or whatever

 [netzpolitik.org](http://netzpolitik.org)

[perception](#)

 [shabka.org](http://shabka.org)

 [Terrorismus in Deutschland](#)

 [theorieblog.de](http://theorieblog.de)

 [Verfassungsblog](#)

 [Vom Bohren harter Bretter](#)

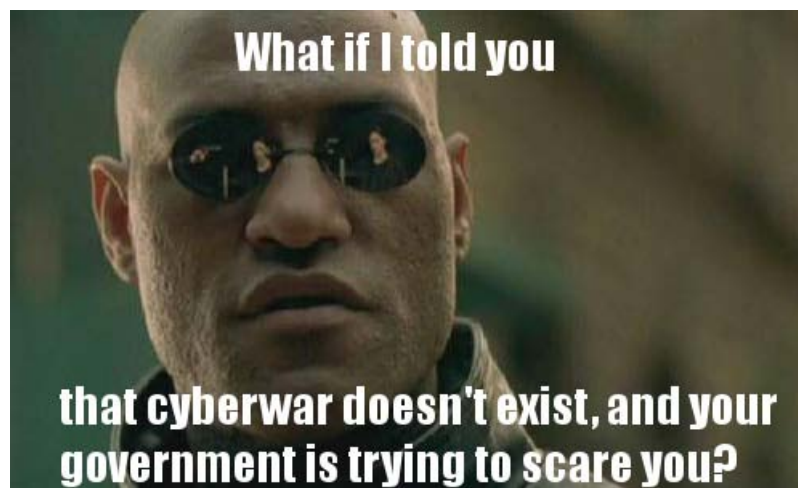
 [whistleblower-net.de](http://whistleblower-net.de)

## ARCHIV

Wähle den Monat



other military means they happen to fancy. Scary. Second, they dare to invoke international law. Don't get me wrong. I have **plenty to criticize** when it comes to the utility and coherence of international law, but if anything, international law here is a constraint. International law sets a pretty high bar on legitimate uses of force, but the American policy seems to think that whatever their policy happens to be is sanctioned by international law because they put 'international' in the policy's title. International law is a mess, but it's not that silly.



But who is the acting King of the Battletrolls? Astonishingly, it's Germany. I say 'astonishingly' because Germans really agonize about their military. There is some kind of documentary about the Nazis running on some cable TV channel almost 24 hours a day, and whenever a fairly benign foreign policy action requires any military contingent, like patrolling the seas of East Africa for pirates or off the coast of Lebanon for weapons shipments, there is still a protracted public discourse of soul searching and existential angst. And whenever you see kids playing cops and robbers with toy guns, or even imaginary finger guns, all the parents sneer and harrumph away. What did Germany do to earn the crown? Well, it was the only country to invoke the term 'cyberwar' explicitly in any official document, and it used 'attack' more frequently than anybody else. Startlingly, Germany even used the term 'Cyber Warfare' in **German language documents**. Imagine you saw a term like 'Blitzkrieg' in the American or Australian defence policy papers. Even if you knew they were using it rhetorically, what a choice of words!?! And from the gun-shy Germans, of all people?! There's an old saw in communications studies that electronic communication reduces inhibitions, lowering barriers of formality and making rudeness socially easier and less punishable. You would almost suspect something similar is going on in the German government with regard to cyber security. Normally übercautious, the Internet seems to bring out the Germans' inner Battletroll.

👉 Tags: **Cyberwar, Militarisierung, Sprechakte, Troll, Versicherunglichung**

« **Podcast #3: Gespräch mit Wolfgang Kraushaar**  
**Der Fall Palästina und die Bedeutung internationaler Anerkennung** »

## 20 Kommentare zu “How to catch a Battletroll: States and the yarns they tell about the Internet, from the minnows to the whoppers”

Felix | 5. Dez. 2012 um 10:23 |

#1

Great article! Looking very much forward to the more detailed study. (and please, please keep the jpegs, at least in the manuscript. And then post the reviewer’s reactions on this blog... and who knows, maybe you’ll be the first to introduce the Boromir meme to a major Poli-Sci Journal. I’d buy you a beer.).

A quick question on your case selection, though: aren’t your cases actually “easy” cases? Let me follow your assumption that states do what they know best (protecting us from war, **building infrastructure** etc.). A state with a high score on FH’s Freedom on the Net index is likely to have a sophisticated internet infrastructure, a lot of internet user, and a large part of their economy will be based on the internet. Aren’t these states highly likely to securitize their internet safety policy with a war metaphor to ensure support for the protection of this infrastructure? I mean, any attack on this kind of infrastructure would be much more devastating to these states than on others, so we are very likely to see them using “war metaphors” related to cybersecurity to ensure public and parliamentary support for this policy.

ANTWORTEN



benkamis | 5. Dez. 2012 um 11:01 |

#2

Wow. I wasn’t exactly expecting a methodological question that could inform future work, but I’m thankful for it.

As for whether our cases are hard or easy, I’d still say they’re hard because the securitizing acts are used as a reason for the states to regulate and penetrate the internet more, which is conceptually opposed to internet freedom a la Declaration of Independence for Cyberspace. Whether free internet policies lead to heavier internet use and economic reliance on the ‘net in a given jurisdiction is an interesting empirical question because it seems like the causal arrow could plausibly point in both directions. However, the two might not even be correlated. China, for example, has a vibrant e-commerce sector, but China also has notoriously unfree internet policies. There’s also value in keeping the theoretical story simple and keeping the causal story closely tied to it. The theoretical story we have now, which fits pretty well with the empirics, is that the existing state narrative & institutions affect the metaphors and discursive moves states make about the Internet, which is prima facie a state-free zone. The one you’re proposing would require the theoretical addition of political economic history and motives in there somewhere, which makes the causal narrative and theoretical explanation more nuanced, maybe, but also a lot messier, so it would be harder to tell what’s changing what.

ANTWORTEN

Felix | 5. Dez. 2012 um 14:15 |

#3

Thanks for the quick reply. Don't get me wrong, I do buy your argument. I think it's very fitting for the cases you analyze. And keeping it simple definitely has value and I think you did actually a pretty good job in delivering the story in "plain English." No seriously, writing a concise post about securitization without actually mentioning that monster of a word (The German "Versicherheitlichung" is even worse) is quite an achievement! Kudos.  
Back to the methods. 😊

*As for whether our cases are hard or easy, I'd still say they're hard because the securitizing acts are used as a reason for the states to regulate and penetrate the internet more, which is conceptually opposed to internet freedom a la Declaration of Independence for Cyberspace*

The point is well taken and I think you should make it stronger, because the logic wasn't immediately obvious to me from reading the post. But that's probably because I wasn't reading carefully enough. 😊

I'm still somewhat struggling, because following your hard case-easy case logic, your causal story should be even more prominent in much easier cases. Now, I don't know about the cyber strategy of countries like Georgia, Nigeria, Brazil, etc. but they haven't come across as very much cyberwar-hawks in the news lately (granted, that's not a scientifically valid baseline for judgement).

Maybe I'm struggling because I'm reading your post as trying to explain *where* different levels of cyber-securitization occur, which I don't think you're actually trying to do (correct me if I'm wrong). If you do (e.g. why do the countries differ their degree of cyber-securitization), then you'd probably need to be more careful in your case selection strategy. But for illustrating the mechanisms you propose your strategy is quite apt and delivers very interesting results (I mean, why Germany?).

(Although you could still argue that the higher the economic and social use of the internet, the more likely countries are to employ cyber-securitization strategies. Which would fit the China story. But then again, this is getting in the why-question territory, which we're not in.).

Anyway, this is not a peer review, I am not the most appropriate person to judge this (I know next to nothing about securitization and my knowledge on cyber-security ends with clearing the cache of my Firefox), and **maybe I just want to be right, although I'm not.** 😊

But I know James Bond and Star Wars (very extensive knowledge here) so that makes me at least somewhat qualified. 😊

ANTWORTEN



benkamis | 5. Dez. 2012 um 15:38 |

#4

Thanks for the engagement. For the record, anyone who spends the time and effort to invest time and effort in understanding and thinking about an argument is an appropriate person to judge it, and don't let anyone else tell you different.

But I think you've pretty much answered your own question. The idea is more

why the utterly peculiar metaphor of ‘cyberwar’ has so much traction in general and in state-based discourse in particular. Therefore, a state needs to have a fairly well-developed political discourse about the internet in order to be an interesting case in the first place. Ergo, the fact that you don’t hear much from Nigeria, Malawi, or Papua New Guinea is telling in itself. A hard case is a state that should not be choosing this metaphor; not a state that has yet to face the choice.

The most probable direction for future research would be to make these initial impressions more intensive than extensive. This would entail looking at \*how\* states deploy the cyberwar and related metaphors, in what contexts, and to what precise purposes, not necessarily to account for variation in which states use it at all (although our intensive results might provide some indication of that as well).

ANTWORTEN

Martin Pleiß | 5. Dez. 2012 um 11:20 |

#5

Nicely done. By the way, se dscherman link also is aweilable in änglisch:

<http://www.hiig.de/en/1st-berlin-colloquium-data-privacy-and-battle-trolls/>



ANTWORTEN

Andreas Schmidt | 13. Dez. 2012 um 1:31 |

#6

Kleiner Dribbdebach-research-proposal-peer-reviewer-arsch-Trollversuch.

Die Schreibe ist lässig. Die Definition von Research question groß. Die Hypothese ist gut.

Die Methode: Worthäufigkeitsanalysen kann man prinzipiell machen. Ob im internationalen Vergleich, da bin ich mir unsicher. Ob hochoffizielle Politikdokumente den öffentlichkeitswirksamen Diskurs bestimmen, bezweifle ich. Die Auswahl der bisherigen Dokumente ist schlecht. Die vermeintliche Erkenntnis, das Deutschland mit seiner offiziellen Politik relativ zu den anderen der Battletroll #1 ist, läßt sich aus der Analyse nicht ableiten. (Und dass obwohl, sagen wir, Indizien dafür sprechen, dass die deutsche Politik auf Trollen im Cybersec steht.)

Barlow’s Declaration of Independence of Cyberspace

Die beste Zusammenfassung, was mit den Cyberilliteraten zu tun sei, stammt immer noch von ihm selbst: “Well, fuck them.”

[http://w2.eff.org/Censorship/Internet\\_censorship\\_bills/barlow\\_0296.declaration](http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration)

(Meine bisher größte halbwissenschaftliche Leistung war es, meine Magisterarbeit mit diesen drei Worten einzuleiten. Ich befürchte, es war der Zenit meines Könnens.)

Official cyber security policies and statements

Im Text heißt es dazu: “a logical place to look if you think that relatively peaceful and net-friendly countries will use violent metaphors for the Internet”. Ich glaube, das Gegenteil ist der Fall. Offizielle Policydokumente sind immer abgeschliffen, geben nie die Schärfe und Spitzen des politischen Diskurses wider.

Estland

Die Dokumente, zu denen verlinkt wird, sind keine Cybersse-Strategien, sondern beschreiben die allgemeine Sicherheitsstrategie Estlands in der Internationalen Politik wider. Diese Dokumentenauswahl ist völlig daneben. In Estland wird das Internet mit Ökonomie und Innovation verbunden — der frog leap in den 1990ern von der Sowietkolonie zum hochvernetzten Land, Skype und was sonst noch an kleineren Sachen.



Aber eben gerade auch mit cyberwar. Wie wär's mit solchen Dokumenten: "Cyber Warfare: Unity in Defence," interview of Estonian President by JINSA's James Colbert in Silicon Republic, June 20, 2011" <http://www.jinsa.org/jinsa-media/cyber-warfare-unity-defence-interview-estonian-president-jinsas-james-colbert-silicon-re>. Oder der hier, cyberarmy, "EU to study Estonia's world-leading cyber defense mechanisms", <http://www.alaskadispatch.com/article/eu-study-estonias-world-leading-cyber-defense-mechanisms>. Oder der hier: "West risks losing the cyberwar, Estonia's president warns", <http://www.network54.com/Forum/680705/thread/1335005186/last-1335062675/>.

Australien

"Even Australia's cyber security intelligence bureau provided tips on how to secure home and business systems without militarist rhetoric or metaphors." Wie das BSI bei uns. 😊

Über die USA.

Vergeltung. "You mess with their immaterial data, and they're threatening you with invasion..."

Wahrscheinlich falsch. In Diskussionen von Leuten aus Sicherheitskreisen heißt meist, dass die Cyberangriffe in ihrer Wirkungen herkömmlichen kinetischen entsprechen müssen. Also: "You hack SCADA system of big dam, dam breaks, floods my country, I'll invade you." Klingt fast vernünftig, sogar stabilisieren, nicht eskalierend.

Internationales Recht. "They dare to invoke international law." Ja, tun sie und können sie bald auch, jetzt vielleicht noch nicht, aber die Entwicklungen, Umdeutungen gehen in die Richtung. Besagtes CCDCOE hat gerade ein Sammelband mit Artikeln von allerlei Rechtswissenschaftlern herausgebracht. Wem das zu lang ist, kann mal beim Atlantic Council vorbeischaun, acus.org, und lesen, was z.B. Jason Healey dazu schreibt. Das kann gefallen oder nicht, aber in diese Richtung geht's.

Deutschland.

Ihr verlinkt zu einem Dokument aus dem Jahre 2009 ("German language documents"). In Deutschland war Internetsicherheitspolitik lange Brachland; es gab nicht viele, die Internationale Politik, Sicherheitspolitik und Internetsicherheit in jener Zeit zusammen dachten. Deshalb haben sie den Diskurs aus den USA übernommen (woher auch sonst). In 2009 wurde Estland 2007 in den USA auch noch als Cyberwar angesehen; mittlerweile rückt man zumindest in den außerpolitischen Kreisen ab vom weiten Cyberwar-Begriff, verengt ihn, beschränkt ihn auf Angriffe-auf-ICT-Systeme-die-so-schaden-wie-Bomben-und-Granaten. (Vgl. etwa Nye)

ANTWORTEN

## Trackbacks/Pingbacks

1. **IB Online (2/12): Eine kleine Netzschau « Bretterblog** - 10. Dez. 2012

[...] dem Sicherheitspolitik-Blog schreibt Ben Kamis (sehr lesenswert) über Cyberwar und welche Staaten diesen Begriff am häufigsten "versicherunglichen". Erstaunlicherweise ist Deutschland in der Gruppe der ausgewählten Staaten auf Platz [...]

2. **Inhaltsanalyse offizieller Dokumente: Nur in Deutschland ist die Sprache über das Internet so militärisch** - 12. Dez. 2012

[...] Ben Kamis und Dr. Thorsten Thiel untersuchen an der Goethe Universität Frankfurt am Main den Sprachgebrauch von Staaten über das Internet. Eine erste Präsentation hielten sie Ende Oktober in Berlin, jetzt haben sie vorläufige Ergebnisse auf dem Sicherheitspolitik-Blog veröffentlicht. [...]

3. **Mythos Battletroll oder wenn Akademiker konstruieren – Sajonara.de –**

**Internetmagazin** - 12. Dez. 2012

[...] darstellt. Also muss man sich etwas einfallen lassen. Die Hypothese ist, dass Staaten den "Battletroll" im Internet mimen. Sie hausieren mit der Idee vom Cyberwar, vor dem natürlich alle [...]

4. **Another Awards Update » Duck of Minerva** - 14. Dez. 2012

[...] Kaims, "How to Catch a Battletroll: States and the Yarns they Tell about the Internet, from the Minnows to t..."  
[...]

5. **Awards Update » Duck of Minerva** - 22. Dez. 2012

[...] Kamis, "How to Catch a Battletroll: States and the Yarns they Tell about the Internet, from the Minnows to t..."  
[...]

6. **Penultimate Call for Award Nominations » Duck of Minerva** - 27. Dez. 2012

[...] Kamis, "How to Catch a Battletroll: States and the Yarns they Tell about the Internet, from the Minnows to t..."  
[...]

7. **2012 International Studies Blogging Awards: Final Call » Duck of Minerva** - 31. Dez. 2012

[...] Kamis, "How to Catch a Battletroll: States and the Yarns they Tell about the Internet, from the Minnows to t..."  
[...]

8. **"Final List" of Award Nominees and Additional ISA Reception Details » Duck of Minerva** - 2. Jan. 2013

[...] Kamis, "How to Catch a Battletroll: States and the Yarns they Tell about the Internet, from the Minnows to t..."  
[...]

9. **Das Internet. Unendliche Weiten... umkämpfte Grenzen » theorieblog.de** - 29. Jan. 2013

[...] und Gesellschaft (Bericht) wurde mittlerweile in einen Blogbeitrag auf dem Sipo-Blog umgewandelt (How to Catch a Battle Troll) und auch auf Netzpolitik diskutiert. Mehr wird folgen, hier aber nun erst einmal die [...]

10. **Security Culture: Lost (and found) in Translation | sicherheitspolitik-blog.de** - 20. Feb. 2013

[...] perhaps because of what the state needs to perpetuate itself as an institution – something like this.) But why is 'security' becoming so much more popular than 'defence'? The paranoid view, [...]

11. **Final Call | Alexander von Humboldt Institut für Internet und Gesellschaft** - 21. Jun. 2013

[...] Nationen vorstellten. Um Interessierten einen Einblick zu geben sei an dieser Stelle auf die Veröffentlichung ihres Papers bei sicherheitspolitik-blog sowie auf die Nachbesprechung des Kolloquiums durch die Doktoranden des Instituts Blog [...]

12. **Final Call | Alexander von Humboldt Institut für Internet und Gesellschaft** - 21. Jun. 2013

[...] in metaphors of violence and war. To gain an insight, we recommend their paper published on sicherheitspolitik-blog, as well as the review of the colloquium from the perspective of the institute's doctoral [...]

13. **Trust me, I'm an expert | sicherheitspolitik-blog.de** - 28. Jan. 2014

[...] such phenomena as the dramatic leaks of the last decade, the vibrant and inflammatory discourse about 'cyberwar' and the conflation of the Anti-Counterfeiting Trade Agreement with the [...]

14. **Cyberpeace: post-war is war, only more so | sicherheitspolitik-blog.de** - 9. Dez. 2014

[...] argues that 'cyberwar' is not war in any way that we usually understand war. I'm sympathetic. But in deconstructing the term 'cyberwar' Matthias also hopes to eliminate the term [...]

## Einen Kommentar hinterlassen

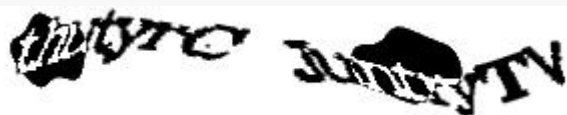
Name

Email

Webseite

Kommentar

Geben Sie den Text ein.



[Datenschutz](#) - [Nutzungsbedingungen](#)

Benachrichtige mich über nachfolgende Kommentare per E-Mail.



Impressum | 

Dieses Werk bzw. Inhalt steht unter einer Creative Commons Namensnennung-NichtKommerziell-KeineBearbeitung 3.0 Unported Lizenz.  
Über diese Lizenz hinausgehende Erlaubnisse können Sie unter [redaktion@sicherheitspolitik-blog.de](mailto:redaktion@sicherheitspolitik-blog.de) erhalten