16. Dez. 2014

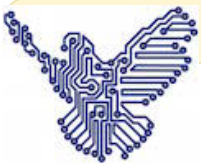
von gast

in Cyber Security, Security Culture, Sicherheitskultur

Kommentare (1)

How to Abolish Cyberwar

by Myriam Dunn Cavelty



Part III of our series on cyberpeace

Cyberwar is like a discursive plague. After years and years of writing texts about it and against it, the concept is still scary, still spreading, still harmful. Its power is such that it is not simply being used in discourse – but is in fact forcing its specific discursive structures and rules on us. In short, we may keep questioning this concept, but we will never get rid of it.

Is there a way out of this? Yes, there is.

First, we scholars need to realize that discussions about whether cyberwar exists or not are missing the point. It is not important what people say about cyberspace – it is important what they do in it and with it. However, most texts that engage critically with cyber-security are interested in how different actors in politics have tried to argue the link between the cyber-dimension and national security and therefore focus on politically salient speech acts by 'visible' political figures that can be approved (or disproved) by general public. Such a focus reveals the constitutive effects the discursive practices of actors with power have in world politics, but it is blind towards how they are facilitated or thwarted by preceding linguistic and non-linguistic practices of actors that are not as easily visible, also outside of governments. In addition, existing scholarship has only ever grasped a limited expression of cyber-in-security (usually cyber-war) that is topmost on these people's minds. The very real effects of this are that our attention on cyberwar has directed intellectual resources away from clandestine cyber-operations that nobody spoke about (at least before Snowden).

Second, cyber-security is as a type of security that enfolds in and through cyberspace, so that the making and practice of cyber-security is at all times constrained and enabled by this environment and its technical logic. Cyber-(in)-security is therefore inseparable from the technical-material (referent) object that it deals with: computers and computer networks. The effects of neglecting the technical underpinnings of cyberspace and "banal" everyday practices by programmers, hackers, computer security specialists and IT support staff in the server rooms of this world in our studies are a disconnect from the material reality of insecurity and possibilities of countermeasures.

To find a way out of the cyberwar trap, two moves are necessary. First, we must stop chasing after discursive formations. Cyberwar is too powerful and is simply reinforced by our continued involvement with it. Rather, we must focus our attention on the practices of professionals of cyber-(in-)security. We must understand the workings of vulnerabilities and exploits, of backdoors, of code, of modes of attack and modes of "defense". And that is why, second, we need to force the discourse back into the technical domain, where it ultimately belongs.

It's well-known that cyberspace is an entirely man-made domain. So is the mantra that cyber-security is not the same as IT-Security: The latter is

mainly a technical discourse that only has a limited bearing in politics. Cyber-security on the other hand is first and foremost a political concept that invades the technical discourse and creates the illusion of new factual and practical constraints. However, the solutions are not to be found in political concepts that dodge definitions and come with their own skewed logics. The (only) solution is to abolish the technical base and possibilities of cyberwar, which is humanly and technically possible.

What does that mean? It means investing in IT Security research and education, into the exposure of computer vulnerabilities by technologically apt people ("hackers"). It means providing economic incentives structures so that security will no longer be constantly "underproduced" in a market dominated by the so-called network effect (which means that the benefits of a product increase when the number of users does). It means changing the skewed balance between offense and defense in the favor of defense. Ultimately, the solution must be a secure and resilient cyberspace that is no longer strategically exploitable. If we get there, we have abolished cyberwar, which has simply become impossible.

Dr. Myriam Dunn Cavelty is Head of the New Risk Research Unit at the Center for Security Studies, ETH Zurich, Switzerland and was Fellow at the "stiftung neue verantwortung" in Berlin, Germany. She publishes regularly in international journals and has authored and edited several books on information age security issues

Tags: cyber peace, Cyber Security, Cyber War, cyberpeace, cyberspace, Cyberwar, discursive practices, resilience

« "2014": Putin's Lies and Russia's New "Doublethink"
We wouldn't recognize cyberpeace if we saw it »

Ein Kommentar zu "How to Abolish Cyberwar"

benkamis | 17. Dez. 2014 um 17:45 | **#1**

This makes a lot of sense, but I have a reservation: it's a very elitist way of approaching the problem. Deconstructing the bogeymen of cyberspace/-security with technological competence sounds like a good means of defanging the inflammatory political discourse, but it's not a mode of discourse that's open to many. You even say that it's a discourse for hackers more than for the average user. This approach of leaving it up to the literate is a fine thing for technical security questions that don't affect most people, like COIN tactics or the best form of submarine propulsion, but cyberspace is different because the Internet is so heavily used by the technically illiterate. The mothers who call us about how to log into Facebook on a strange computer or how to make a screenshot get sucked into the cyberwar debate whether they belong there or not. They are assets and targets in addition to being an audience. Because the Internet is a mass phenomenon, it might be too important and too broad to be left to experts. (There's an analogy to the old counterforce vs. counter-population debates in the strategy of nuclear war here, I'm sure, but I'm too knackered to develop it.)

It's not Cyberwar, stupid!
Das Internet darf ein cyberfreier Raum sein
Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.
Wir haben Geburtstag!

KATEGORIEN

ANTWORTEN

Einen Kommentar hinterlassen

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

Benachrichtige mich über nachfolgende Kommentare per E-Mail.

BLOGROLL

- Arbeitskreis soziale Bewegungen
- Augen geradaus
- Dan Drezner
- Dart-Throwing Chimp
- David Campbell
- de.hypotheses.org
- Demokratieforschung Göttingen
- Duck Of Minerva
- Future and Politics
- Hylaean Flow
- Internet und Politik
- IR Blog
- Just Security Blog
- justsecurity.org
- Killer Apps
- Kings Of War
- netzpolitik.org
- percepticon
- shabka.org
- Terrorismus in Deutschland
- theorieblog.de
- Verfassungsblog
- Vom Bohren harter Bretter
- whistleblower-net.de

ARCHIV

Wähle den Monat