Rede von Thomas Gruber, *Informationsstelle Militarisierung,*

beim Mainz-Wiesbadener Ostermarsch 2018 in Wiesbaden

Karsamstag, 31. März 2018

Es gilt das gesprochene Wort

Das fünfte Schlachtfeld: Der Cyber- und Informationsraum

Der Virenangriff auf das iranische Atomprogramm 2010, die Spionageattacken auf das südkoreanische Militär 2017 und das Eindringen ins afghanische Mobilfunknetz durch Bundeswehr-Hacker_innen 2015 -- Cyberattacken sind als Spionage- oder Sabotagewerkzeug längst vollkommen normal.

Im April 2017 setzte das Bundesverteidigungsministerium aber noch einen drauf: Es stellte das "Kommando Cyber- und Informationsraum" auf und erklärte damit den virtuellen Raum neben Land, Wasser, Luft und All zum fünften militärischen Operationsgebiet.

Größtenteils werden bereits bestehende Truppenteile in das neue Kommando eingegliedert: Die klassische Spionage (strategische Aufklärung), Propaganda (operative Kommunikation) und auch die elektronische und Cyber-Kampfführung

Die Ziele für das neue Kommando sind dabei klar formuliert: Einerseits sollen deutsche Kriegseinsätze im Cyberraum unterstützt werden -- also etwa durch Absicherung des IT-Systems der Bundeswehr und Angriffe auf feindliche Computernetzwerke. Andererseits soll die Bundeswehr immer mehr auch im zivilen Cyber- und Informationsraum positioniert werden -- z. B. bei der Abwehr von feindlicher Propaganda im In- und Ausland oder durch quasi-polizeiliche "Beiträge zur gesamtstaatlichen Sicherheitslage".

Das brauchen wir beides nicht! Weder eine noch effektivere deutsche Armee, noch die Vereinnahmung eines so wichtigen zivilen Raumes!

Immerhin sind große Teile unserer Energie- und Gesundheitsversorgung sowie unserer privaten Kommunikation mit diesem Raum verbunden.

Die Folgen dieser militärischen Vereinnahmung des virtuellen Raumes sind absehbar und spürbar:

1. Weltweites Wettrüsten im Cyberraum. Keine Großmacht will bei diesen Entwicklungen hintenan stehen.

2. Zunehmende Unsicherheit von Verschlüsselung und privater Kommunikation. Sicherheitslücken werden von Geheimdiensten und militärischen Gruppen absichtlich verbreitet und offen gehalten, damit sie selbst über diese Schwachstellen in Computernetze eindringen können.

3. Niedrigschwelliger, kostengünstiger Einsatz. Cyberattacken können weitgehend ungeächtet und oft unbemerkt durchgeführt werden. Sie sind außerdem relativ günstig.

Und als 4. Punkt etwas ausführlicher: Eskalation und Kriegstreiberei.
Neuerdings werden herkömmliche geheimdienstliche Spionage und Eigentumsdelikte im Cyberraum immer häufiger zu kriegerischen Aktionen hochstilisiert.

Dazu kommt, dass der geografische und politische Ursprung von Hacking-Attacken häufig überhaupt nicht feststellbar ist. Trotzdem werden sehr oft nach größeren Angriffen Vermutungen geäußert (die sich dann auch hartnäckig halten), dass Hacker_innen aus Russland, China oder Nordkorea hinter den Cyberattacken stecken.

Und um darauf dann auch eine militärische Antwort parat zu haben, sollen in solchen Fällen zukünftig auch der NATO-Bündnisfall oder die EU-Beistandsklausel herhalten.

Also eine konventionelle militärische Antwort auf einen Hacking-Angriff?
So ein gefährlicher Blödsinn!
Es muss endlich Schluss gemacht werden mit dieser ständigen Eskalationspolitik!

Die Bundeswehr und andere militärische Akteur_innen stellen sich auch im virtuellen Raum oft als selbstlose Beschützer der Allgemeinheit hin. In Wirklichkeit aber leidet die Zivilgesellschaft (wie immer bei militärischen Aktionen) am meisten unter der militärischen Vereinnahmung des Cyber- und Informationsraumes.

Denn es ist unsere zivile Infrastruktur und unsere private Kommunikation, die dabei ins Kreuzfeuer geraten. Und im Schlimmstfall kann auf der Basis einer Cyberattacke auch noch ein konventioneller Krieg ausbrechen -- die westlichen Militärbündnisse ebnen gerade den Weg dafür.

Diese Art von "Schutz" brauchen wir wirklich nicht!

So eine Heuchelei können sich die Bundeswehr und andere Armeen schenken!