uz

Sozialistische Wochenzeitung Zeitung der DKP

www.unsere-zeit.de

Heinrich Fink im Interview

„Ich warne davor, die AfD zu unterschätzen. Sie verbindet rechtskonservative Kreise mit Personen, die sich offen rassistisch gerieren.“

Seite 9

30 Jahre nach Tschernobyl

Am 26. April 1986 geriet in Tschernobyl der Reaktor Nummer 4 während einer Simulation außer Kontrolle.

Seite 12

unsere Zeit

UZ-Pressefest ★ Volksfest der DKP ★ 1.–3. Juli 2016 Dortmund Revierpark Wischlingen

6. Mai 2016 · Nr. 18 · 48. Jahrgang

PVSt K 4956 D · Entgelt bezahlt · **2,80 €**

Landser im Cyberraum

Auch das Internet ist „militärischer Operationsraum“

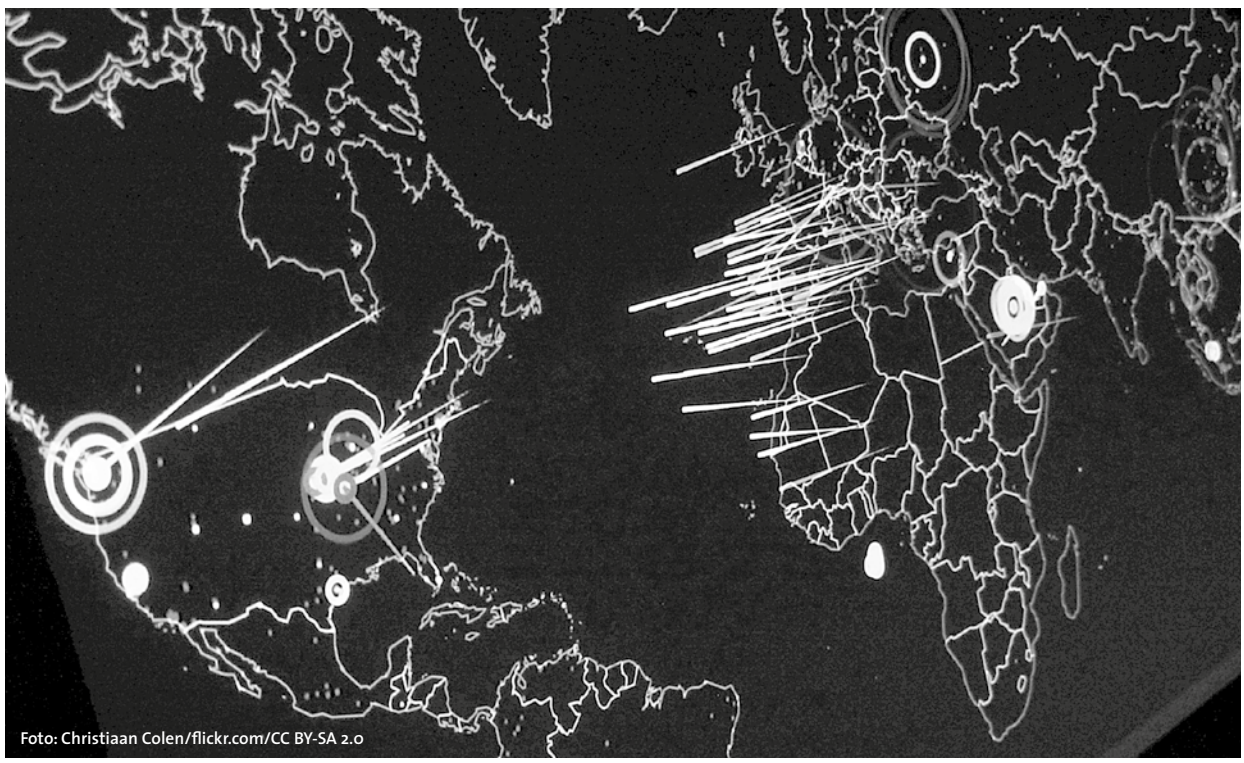

Foto: Christiaan Colen/flickr.com/CC BY-SA 2.0

Echtzeitsimulation von Angriffshandlungen. Der Krieg im Cyberraum bietet schon vorher die Möglichkeit in die Steuerung der Waffensysteme, des Nachschubs usw. sowie der Wirtschaft von Staaten in aller Welt einzugreifen

Noch bis Mai sollen die Plakate an Straßenrändern, Haltestellen hängen. Anzeigen werden in Zeitungen geschaltet, Werbevideos laufen im Internet und Fernsehen. Mit ihrer scheinheiligen Kampagne „Mach, was wirklich zählt“ wirbt die Bundeswehr dieses Mal im Rahmen des „Projektes Digitale Kräfte“ aber um ganz spezielle zivile und militärische „Mitarbeiter“: „Deutschlands Freiheit“ soll nämlich auch im Cyberraum „verteidigt“ werden.

Mit dieser Aussage oder Slogans wie „Gegen virtuellen Terror hilft kein Dislike-Button“ hofft man IT-Fachkräfte für die Bundeswehr zu gewinnen. Gebraucht werden sie für den „Kampf im Cyberraum“, der zum Operationsgebiet der Bundeswehr wird. Angeblich eine rein defensive Maßnahme zur Verteidigung von Angriffen auf Militär, Staat, Industrie und Infrastruktur – auch Krankenhäuser und Energieversorgung – aus dem Internet. Eine wachsende Gefahr in einer zunehmend vernetzten Welt. Schon jetzt gebe es viele Hackerangriffe und Angriffe mit Schadsoftware.

Im vergangenen Jahr erließ Bundesverteidigungsministerin Ursula von der Leyen eine geheime Leitlinie zur „Cyber-Verteidigung“. Diese, von der Ministerin schon am 16. April 2015 unterzeichnet, wurde erst im Sommer 2015 bekannt, nachdem Medien über deren Existenz berichtet hatten und sie im Internet veröffentlicht wurde. Vorgeschlagen wird in diesem Papier nicht nur, die Bundeswehr könne Netze für andere Behörden betreiben. Vor allem wird darin der „Cyber-Raum“ zum Kriegsgebiet erklärt. Die Bundeswehr rüstet sich zum digitalen Angriff mit „offensiven Cyber-Fähigkeiten“ im In- und Ausland. Damit erlangt sie die Fähigkeit, in die Steuerung der Waffensysteme, des Nachschubs usw. sowie der Wirtschaft der Staaten in aller Welt eingreifen zu können.

Auch in einem Ende April 2016 an die Öffentlichkeit gelangten Konzeptpapier der Bundeswehr wird der Cyberspace als „militärischer Operationsraum“ bezeichnet.

Bereits in der Leitlinie vom April 2015 wurde eine deutliche Aufstockung und Zentralisierung der IT-Ressourcen der Bundeswehr gefordert. Das soll jetzt geschehen: Am Dienstag wurde offiziell, dass die Bundeswehr bis Oktober eine neue Einheit mit bis zu 14 000 zivilen und militärischen Mitarbeitern aufbaut, die Anfang 2017 aktiv werden soll.

Ob sie ihre Vorgänger völlig ersetzen wird, ist unklar: Bereits 1992 entstand eine Einheit, die sich mit der Abwehr von Angriffen auf die Bundeswehr im Internet beschäftigte. 2007 wurde laut netzpolitik.org bei der Bundeswehr die Truppe „Computer Netzwerk Operationen“ (CNO) etabliert. Ihr gehören ca. 40 Mann an. Sie gehört zum „Kommando Strategische Aufklärung“ (KSA) und ist bei Bonn stationiert. Zu ihren Aufgaben gehört das „Wirken gegen und in gegnerischen Netzen in bewaffneten Konflikten“, kurzum: Der Cyberkrieg. Die Bundeswehr nennt das den „Kampf in der fünften Dimension“ – diese 5. Dimension ist das Internet. Angeblich wurde die Truppe noch nirgends eingesetzt. Sie trainiert aber fleißig – auch mit anderen NATO-Partnern.

Abgeordnete der Partei „Die Linke“ hatten im Zusammenhang mit der Leitlinie aus dem Bundesverteidigungsministerium bereits im Oktober 2015 eine kritische Anfrage an die Bundesregierung gestellt. Die Antwort darauf blieb vage. Behauptet wurde, der „Cyberwar“ sei kein Rezept für die Bundeswehr. Auf die Frage „Unter welchen Voraussetzungen soll die Bundeswehr nach Vorstellung der Bundesregierung offensive Cyber-Fähigkeiten einsetzen dürfen?“ kam die Antwort, dies geschehe auf der Grundlage des Grundgesetzes und des Völkerrechts. Umgangen wurde eine Antwort auf die Frage, welche Auswirkungen auf weitere, für die Zivilbevölkerung relevante Bereiche, Angriffe der Bundeswehr im „Cyberraum“ haben könnten. (Bundestag, Drucksache 18/6989, 10.12.2015)

„Die Einrichtung der neuen Cyber-Abteilung ist Teil einer IT-Aufrüstungsspirale“, kritisierte in der vergangenen Woche Christine Buchholz, Verteidigungspolitische Sprecherin der Fraktion der Partei „Die Linke“, die Vorstellung des neuen Cyberkonzepts durch Verteidigungsministerin von der Leyen. Buchholz weiter: „Die Verteidigungsministerin will uns weismachen, dass es sich bei der Einrichtung einer ganzen Teilstreitmacht für den Cyber-Krieg um eine defensive Maßnahme handelt. Das ist Unsinn. Im Internet gibt es keine klare Abgrenzung zwischen defensiven und offensiven Aktivitäten. Zum Schutz von internen Netzen der Bundeswehr braucht man keine 13 500 IT-Soldaten. Es geht um die Befähigung zum virtuellen Angriff.“ Sie machte auch darauf aufmerksam, dass das Verteidigungsministerium in einem internen Papier die gesammelten internationalen Datennetze als einen „militärischen Operationsraum“ definiert. Damit wird die Bundeswehr befähigt, „auch zivile Einrichtungen digital ins Visier zu nehmen – nicht nur im Ausland, auch im Inland“. Und, dass „ausgerechnet ein Industriemanager die neue Abteilung im Verteidigungsministerium leiten soll“, zeige „wie eng im Cyberbereich militärische Fähigkeiten und wirtschaftliche Interessen verquickt werden“.

Mit der neuen Abteilung gehen Bundesregierung und Bundeswehr einen weiteren Schritt bei Ausbau und Aufrüstung der Bundeswehr zur Interventionsarmee, die weltweit agieren kann.

Nina Hager