neues deutschland
SOZIALISTISCHE TAGESZEITUNG

06.06.2013 / Ausland / Seite 7

Vom Hindukusch zum Cyberwar

Die NATO baut ihre elektronische Kriegführung massiv aus

Von Olaf Standke

Bevor die Verteidigungsminister der 28 NATO-Staaten am Mittwoch ein militärisches Einsatzkonzept für Afghanistan nach dem Jahr 2014 beschlossen, haben sie über die Kriege der Zukunft nachgedacht: Cyberwar heißt das neue Schlagwort.

Der Krieg am Hindukusch war ein Desaster, und die NATO sucht nun eine gesichtswahrende Variante für das Ende des »Kampfeinsatzes« der von ihr geführten internationalen Schutztruppe ISAF. Gestern beschlossen die Verteidigungsminister der 28 Mitgliedstaaten ein Einsatzkonzept für die Militärpräsenz nach dem Jahr 2014. Allerdings stehen weder die Zahl der künftigen Ausbilder und Berater noch die für ihren Schutz weiterhin notwendigen Kampftruppen fest. Nur »bedeutend kleiner« als die bisherigen ISAF-Einheiten - derzeit sind noch immer fast 100 000 Soldaten in Afghanistan stationiert - sollen die künftigen Verbände sein.

Zuvor dachte man im größten Militärbündnis der Welt über die Kriegführung der Zukunft nach. Längst sieht der Nordatlantik-Pakt elektronische Angriffe aus dem Internet als ernsthafte Bedrohung, der USA-Regierung sollen die »lautlosen, schleichenden und hinterhältigen« Cyberattacken inzwischen größere Sorgen machen als der Terrorismus. Allein im Vorjahr registrierte man rund 2500 Versuche, in das Internetsystem der Allianz einzudringen. Vor allem China wird dabei immer wieder beschuldigt. Kein Wunder also, dass dieses Schlachtfeld ohne herkömmliche Waffen jetzt in Brüssel erstmals auf der Agenda eines Treffens der Verteidigungsminister stand. Im militärischen Hauptquartier der Allianz in Mons versucht eine spezielle Abteilung, die eigenen Systeme vor Datenschädlingen zu schützen. Schon 2008 hat man in Estland - ein Jahr zuvor Ziel massiver elektronischer Attacken - ein Forschungszentrum für die Abwehr solcher Angriffe installiert. Die Mitarbeiterzahl des vor drei Jahren gegründeten Cyber Command des Pentagons mit Sitz in Fort Meade

wird in den nächsten Jahren von 900 auf 4900 wachsen.

Nun soll der sogenannte Cyberwar ständiger Tagesordnungspunkt und Teil der Verteidigungsplanung im Bündnis werden. Bis Oktober dieses Jahres sei eine »schnelle Einsatzgruppe« startklar. Wobei zivile Netze und damit weite Bereiche der Infrastruktur noch weitaus gefährdeter erscheinen als militärische Strukturen. Allerdings konnten sich die Verteidigungsminister nicht darauf verständigen, ob und wie das Bündnis vorgeht, sollten Mitgliedstaaten um Hilfe gegen Cyberangriffe auf ihre nationale Einrichtungen bitten. Wie Deutschland sehen auch andere NATO-Staaten etwa den Schutz der eigenen Kommunikationsnetze als Sache der jeweiligen Regierung an.

Über die eigenen elektronischen Angriffsfähigkeiten sprach NATO-Generalsekretär Anders Fogh Rasmussen jetzt nicht. Vor drei Jahren etwa sollen auf Befehl von USA-Präsident Barack Obama Higtech-Krieger den verheerenden Angriffscode »Stuxnet« in iranische Atomanlagen geschmuggelt haben. Längst hat man in der NATO über präventive digitale Erstschlagszenarien nachgedacht - und über militärische Antworten auf Cyberangriffe, auch wenn die auf ökonomische Schäden zielen. Gerade ist man dabei, sich dafür eine völkerrechtliche Legitimation basteln zu lassen.

Die Bundeswehr wird spätestens in drei Jahren vollständig zu Angriffen über das Internet in der Lage sein. Eine »Anfangsbefähigung« sei zwar jetzt schon erreicht, es fehle aber noch an geschützten Fahrzeugen für mobile Cybertrupps, so Brigadegeneral Jürgen Setzer, Chef des in Rheinbach bei Bonn stationierten und weitgehend geheim agierenden Kommandos Strategische Aufklärung (KSA).

URL: http://www.neues-deutschland.de/artikel/823582.vom-hindukusch-zum-cyberwar.html