Fremde Federn: Rainer Arnold und Lars Klingbeil

Ein digitales Update für das Völkerrecht

Die Bundeswehr muss sich, wie alle Streitkräfte, mit den wachsenden Problemen der Digitalisierung auseinandersetzen. Jeden Tag gehen 1,1 Millionen E-Mails durch ihre internen Netze und werden über 6500 Attacken auf diese Netze verübt. Alle neuen Waffensysteme der Streitkräfte arbeiten computergestützt; sie sind vernetzt und damit verwundbar für Schadsoftware. 2015 gab es 71 Millionen unberechtigte beziehungsweise schädigende Zugriffsversuche auf Netze der Bundeswehr.

Niemand stellt in Frage, dass die Bundeswehr in der Lage sein muss, die eigene IT-Infrastruktur zu sichern und zu verteidigen. Die deutschen Streitkräfte sind ein beliebtes Ziel für Attacken, und sie müssen die Möglichkeit haben, zum Schutz der verletzlichen digitalen Infrastruktur des Heimatgebiets wie auf dem digitalen Gefechtsfeld vorzugehen. Nur: Wo schlägt Verteidigung in völkerrechtlich problematische Angriffe um, wo endet der Schutz und beginnt die aktive Verteidigung, wenn die Grenzen der Kriegführung durch die digitalen Möglichkeiten zunehmend verschwimmen?

Bislang zieht sich das Verteidigungsministerium beim Thema Cyberkriegführung auf das klassische Rollenbild für die Streitkräfte zurück: Verteidigung, Abschreckung, Vorbereitung. Diese Unterscheidung ist überholt. Die Fähigkeit, offensive Attacken zu führen, wird seit 2006 im Kommando Strategische Aufgaben in Rheinbach bei Bonn aufgebaut. Derzeit üben rund 60 Mitarbeiter „Computer-Netzwerk-Operationen" (CNO), also Attacken im Cyber- und Informationsraum. Selbstverständlich müssen unsere Streitkräfte nicht nur das Know-how für den Schutz besitzen, sondern auch für den Angriff; die Instrumente dafür sind gleich.

Eine Voraussetzung für diese Arbeit ist die Zusammenarbeit mit den Geheimdiensten. Ohne sie wird es schwierig, den Angreifer zu identifizieren und zu entscheiden, wer tatsächlicher Angreifer und wer nur ausführende Kraft ist. Die zunehmende Verzahnung von Innen- und Verteidigungsministerium im Bereich IT-Sicherheit lässt die klassische Trennung der Zuständigkeiten verschwimmen. Die Kontrolle über die Zusammenarbeit von Diensten und Operationen der Bundeswehr im Cyberraum muss zwingend durch das Parlamentarische Kontrollgremium gewährleistet werden. Auch der Verteidigungsausschuss muss einbezogen werden.

Wir werden dafür sorgen, dass der Parlamentsvorbehalt sichergestellt wird. Wie sollen künftig komplexe, zeitaufwendige Cyberoperationen, die in der Regel im Verborgenen vorbereitet und durchgeführt werden, zeitlich angemessen vom Parlament beraten werden? Was muss ein Cybermandat umfassen, und wie müssen die laufenden Mandate für die laufenden Einsätze weiterentwickelt werden? Auch Ministerin Ursula von der Leyen wird sich diesen Fragen stellen müssen. Wir werden als Parlament klare Ansprüche an die zukünftige Mandatierung formulieren, um mehr Rechtssicherheit herzustellen.

Deutschland ist gut beraten, auch auf internationaler Ebene eine Debatte über ein digitales Update des Völkerrechts anzustoßen. Das Kriegsvölkerrecht und das humanitäre Völkerrecht müssen weiterentwickelt werden, es muss Antworten auf die Herausforderungen der digitalen Kriegführung geben. Dies betrifft ein besseres Verständnis, welche Art des Einsatzes von Cybermitteln völkerrechtlich zulässig ist und wo die Schwelle zum bewaffneten Angriff überschritten sein kann. Auch die Frage des Umgangs mit der Kennzeichnung *(false flag)* und die Frage der Zurechenbarkeit sind ungelöste Probleme. Es muss neue, internationale Vereinbarungen geben, um die Möglichkeiten der digitalen Kriegführung zu begrenzen. So haben die Vereinigten Staaten mit Russland und China sowie Russland und China untereinander Verabredungen zum Umgang mit Bedrohungen aus dem Cyberraum im Sinne eines Rüstungskontrollvertrages zum Cyberwar getroffen. Deutschland sollte mit Schlüsselpartnern ähnliche Absprachen anstreben und sich auf europäischer Ebene dafür einsetzen, dass derartige Rüstungskontrollverträge auch in der EU vereinbart werden.

Die digitale Reform darf nicht bei Strukturveränderungen stehen bleiben. Die Debatte über die rechtlichen und ethischen Grenzen von digitalen Fähigkeiten der Bundeswehr hat noch gar nicht richtig begonnen. Sie gehört in den Mittelpunkt der Diskussion.

Die Autoren sind Mitglieder des Bundestages und verteidigungspolitischer sowie netzpolitische Sprecher der SPD-Fraktion.