Opinions on Security

Meinungspapier der DAG – Ausgabe 05 – 13.12.2021

Hybride Bedrohungen – Ist Deutschland gewappnet?

Theresa Caroline Winter
Referentin für vernetzte Sicherheit und Verteidigungspolitik;
erweitertes Vorstandsmitglied WIIS.de (Women in International Security)

Nein, Deutschland ist nicht gewappnet und kann es auch nicht sein: einerseits ist die Begrifflichkeit zu umfassend, andererseits ist die Bekämpfung hybrider Bedrohungen (mittels des vernetzten Ansatzes) nicht ausreichend institutionalisiert.

Spätestens seit der Ukraine-Krise sind die Begriffe „hybride Bedrohungen" und „hybride Kriegsführung" modern. 2016 fanden sie sich das erste Mal als zentrale sicherheitspolitische Herausforderung im Weißbuch der Bundesregierung wieder, zusammen mit der dazugehörigen Antwort des vernetzten Ansatzes. Hybride Bedrohungen – ein Bedrohungspotential, das unsere liberalen Demokratien auf unterschiedlichsten Wegen destabilisieren kann. Die erforderliche Reaktion (besser: Prävention) muss *qua natura* interdisziplinär und ressortübergreifend sein und bedarf zivil-militärischer Zusammenarbeit, institutionalisierter Regeln und Prozesse und Resilienz in der Bevölkerung.

Das Spektrum hybrider Bedrohungen ist enorm breit. Innerhalb des Cyberraums geht es um Hackerangriffe, Online-Propaganda und Radikalisierung und die Verbreitung von Desinformation. Die Akteure sind schwer nachzuverfolgen, Einfluss und Umfang der Aktion sind oft erst spät einschätzbar. Die Themen und angesprochenen Bevölkerungsgruppen sind so divers, dass die Unterscheidung zwischen autonomer gesellschaftlicher Entwicklung und gezielter, akteursgesteuerter Taktik oft unklar ist und fließend ineinander übergehen kann. Wesentlich offensiver ist die Instrumentalisierung von Flüchtlingen (jüngstes Beispiel an der belarusisch-polnischen Grenze), bei der Akteure, Taktik und Ziel schnell identifizierbar sind, die Handhabung allerdings politisch sensibel und komplex. Ebenso gravierend: Investitionen und die Kontrolle fremder Staaten in bzw. über kritische Infrastruktur wie beispielsweise Energieversorgung, (Flug-)häfen und Mobilfunknetze. Dabei spielt Wirtschaftspolitik eine ebenso große Rolle wie Außen- und Sicherheitspolitik.

Diese Dynamik bedarf eines vernetzten Ansatzes in der Bekämpfung, das heißt die Beteiligung unterschiedlicher Akteure aus Militär, Politik, Zivilgesellschaft und Wissenschaft. Diese zu mobilisieren und ressortübergreifend zu koordinieren ist vielschichtig, vor allem wenn es darum geht, Prozesse, Strukturen und Verantwortlichkeiten festzulegen und zu bestimmen, was genau in diesen vernetzten Ansatz einfließt. Prävention, Reaktion und Resilienzförderung erfordern die wissenschaftliche Analyse gesellschaftlicher und sicherheitspolitischer Entwicklungen, eine ressortübergreifende Risikobewertung, nationale und multilaterale Absprachen und Informationsaustausch, die Sicherung von Infrastruktur, die Reglementierung von Sanktionsmaßnahmen, politische Bildung sowie die Förderung von Zivilcourage.

Seit Aufnahme in das Weißbuch der Bundesregierung wechselte die ministeriale Federführung für hybride Bedrohungen mehrfach und liegt jetzt beim Bundesministerium des Innern (zuvor lag sie im Bundeskanzleramt und zwischenzeitlich im Bundesministerium der Verteidigung). Der vernetzte Ansatz ist verteidigungspolitisch im Bundesministerium der Verteidigung verankert. Es fehlt an Prozessen, die die ministeriale und

ressortübergreifende Zusammenarbeit transparent machen und Redundanz verhindern: Analyse und Bewertung finden teilweise parallel und unabgestimmt statt, Handlungsempfehlungen werden oft erst mit großer Verzögerung umgesetzt.

Für eine effizientere und effektivere Bekämpfung hybrider Bedrohungen müssen sowohl die Begrifflichkeit als auch der Lösungsansatz interdisziplinär und ressortübergreifend operationalisiert werden. Akteure, Mittel und Wirkung sollten klassifiziert und darauf aufbauend modulare Handlungsoptionen entwickelt werden. Außerdem gibt es kulturelle und strukturelle Defizite im Austausch auf Augenhöhe zwischen Militär und Zivilgesellschaft, die dringend angegangen werden müssen. Ein Beispiel ist der Austausch von Informationen, der traditionell militärseitig auf dem Prinzip des *Need to Know* basiert und streng hierarchisch strukturiert ist. Zivilgesellschaftlich werden Prozesse und Entscheidungen wesentlich öfter hinterfragt, da gilt eher „je mehr Informationen, desto besser". Das Umdenken von *Need to Know* zu *Dare to Share* muss vielen Köpfen erst noch angewöhnt werden. Nicht zuletzt muss die Zivilbevölkerung viel stärker eingebunden werden – vor allem wenn es darum geht, hybride Bedrohungen als solche zu erkennen.