Eingangsstatement

Generalmajor Jürgen Setzer,

Stellvertreter Inspekteur Cyber- und Informationsraum,

für das Panel

„Verteidigungspolitische, militärstrategische und innenpolitische Herausforderungen im Zeitalter digitaler Verwundbarkeiten und hybrider Bedrohungen: Brauchen wir einen neuen Ansatz für die Gesamtverteidigung?“

bei der 53. Sicherheitspolitischen Informationstagung der Clausewitz-Gesellschaft e.V.

am 5. September 2019 in Hamburg

1. Dilemma – Digitalisierung – freiheitlich demokratischer Staaten

Wir leben in einer Welt fortschreitender Digitalisierung. Digitalisierung bietet in unseren demokratischen, freiheitlichen Gesellschaften ungeheure Chancen für unsere Gesellschaft insgesamt, für unsere Wirtschaft und jeden einzelnen von uns. Sie bietet aber zugleich auch neue Möglichkeiten für potentielle Gegner – seien es Kriminelle, Terroristen oder staatliche Akteure bzw. ein Mix aus diesen Gruppen - und damit Risiken für unsere Gesellschaft. Digitalisierung eröffnet eine neue Art der Konfliktaustragung: Das wahrscheinlichste zukünftige Konfliktbild zwischen Staaten wird durch Hybridität geprägt sein.

2. Hybride Strategien beinhalten besondere Herausforderungen

Sie nutzen Freiräume im Recht, die durch technologischen Fortschritt entstanden sind. Sie nutzen Übergänge in Zuständigkeiten/ Verantwortlichkeiten – Stichwort Abgrenzung innere und äußere Sicherheit. Sie können schleichend beginnen und bleiben in der Regel unterhalb der Schwelle des „klassischen“ Krieges. Das heißt aber nicht, dass sie gewaltfrei verlaufen. Die Gefahren- und Bedrohungslage hat sich durch die Digitalisierung deutlich verkompliziert. Ich nenne zusätzlich nur die Attributionsproblematik bei Cyber-Angriffen.

3. Wir stehen einer gesamtstaatlichen Herausforderung gegenüber, die nur in einem vernetzten Ansatz gemeistert werden kann

Bezogen auf die Dimension Cyber legt die von der Bundesregierung 2016 aktualisierte Cyber-Sicherheitsstrategie für Deutschland Zuständigkeiten fest für Cyber-Abwehr und Cyber-Verteidigung (auch Cyber-Außenpolitik). In Umsetzung dieser und als Reaktion auf die Auswirkungen der zunehmenden Digitalisierung wurde im Geschäftsbereich des BMVg der militärische Organisationsbereich Cyber- und Informationsraum – CIR – im April 2017 aufgestellt: Bisherige Expertise wurde gebündelt und neue, weitere Fähigkeiten wurden aufgebaut. Wir haben z. B. ein Lagezetrum für die Dimension CIR aufgebaut und können so für die Bundeswehr eine 24/7-Reaktionsfähigkeit sicherstellen.

Gesamtstaatlich verfügt die Bundesrepublik Deutschland seit 2011 über ein Nationales Cyber-Abwehrzentrum (BMI (BuPol, BKA, BVerf, BBK, BSI), BKAmt (BND) u. BMVg (MAD, CIR)) als erstes Forum für die Zusammenarbeit staatlicher Stellen im Cyberraum. Zunächst war dies im Wesentlichen eine Informationsplattform mit festgelegten Strukturen für die Fallbearbeitung. Die meisten Vertreter waren nur temporär vor Ort. Ab September dieses Jahres sind die oben genannten Kernbehörden mit Vertretern vor Ort präsent. Der kontinuierliche Informationsaustausch zur Cyber-Sicherheitslage erfolgt nun nach dem „Need-to-share-Prinzip“. Ein eingeteilter Koordinator leitet die Geschäftsstelle des Cyber-AZ, nimmt in den Besprechungen eine moderierende Rolle zwischen den Vertretern der beteiligten Einrichtungen ein und kann notwendige Entscheidungen durch die beteiligten Einrichtungen initiieren. Mit der Koordinator-Funktion ist jetzt eine erste Handlungsfähigkeit gegeben. Es gilt weitere entscheidende Akteure im Bereich

Cyber einzubeziehen, d. h. z. B. auch die Bundesländer, Betreiber kritischer Infrastrukturen und Internet Service Provider. Das Kommando Cyber- und Informationsraum pflegt unabhängig vom NCAZ bereits Kooperationen u.a. zu Telekom Security, dem Fraunhofer INT und dem Cyber Security Cluster Bonn e.V.

4. Vernetzter Ansatz – über alle Dimensionen

Die Gefahren im Cyber- und Informationsraum erfordern einen vernetzten Ansatz über alle Dimensionen hinweg, denn Effekte im Cyberraum betreffen alle Bereiche unserer Gesellschaft – etwa exemplarisch bei KRITIS.
In der Bundeswehr ist ein entsprechendes Jointness-Verständnis vorhanden. Effekte in der Dimension CIR betreffen alle Dimensionen, also Land, Luft, See, Weltraum und CIR. Folglich können diese nicht isoliert betrachtet werden. Der daraus resultierende Handlungsbedarf wurde erkannt. Das Lagebild der Dimension CIR wird in das zukünftige Gesamtlagebild des noch aufzustellenden Joint Intelligence Centers einfließen. Damit werden die Grundlagen für Resilienz und Reaktionsfähigkeit in der Dimension CIR, welche für die nationale Führungsfähigkeit entscheidend ist, geschaffen.
Für eine Reaktionsfähigkeit im Kontext hybrider Bedrohungen ist die Betrachtung aller PEMSII-Faktoren (political, military, economic, social, infrastructural and informational) im Rahmen des gesamtstaatlichen Lagebildes sowie die Vernetzung innerhalb dieser Ebenen von wesentlicher Bedeutung.

5. Vernetzter Ansatz auch international notwendig

Der Cyber- und Informationsraum macht nicht an Staatsgrenzen halt, Effekte sind länderübergreifend spürbar, und nicht nur die Attributionsproblematik erfordert zwingend internationale Zusammenarbeit. Im militärischen Bereich findet bereits eine sehr enge bilaterale Zusammenarbeit auf EU- und NATO-Ebene statt.

6. Fazit: Erste wichtige Schritte sind eingeleitet, müssen aber konsequent weiterverfolgt und umgesetzt werden!

Die Digitalisierung und die damit verbundenen Chancen und Risiken verlangen eine neue Qualität der gesamtstaatlichen, nationalen und multinationalen Vernetzung zur Situational Awareness und Responsiveness in der Dimension CIR, aber auch ebenso dimensionsübergreifend unter dem Aspekt PMESII.