Bundesministerium
der Verteidigung

Rede der
Bundesministerin der Verteidigung
Dr. Ursula von der Leyen

bei der Aufstellung des neuen militärischen Organisationsbereichs und des Kommandos Cyber- und Informationsraum (CIR)

am 5. April 2017

im BMVg, Bonn

Es gilt das gesprochene Wort!

Sperrfrist für die Veröffentlichung der Rede ist 15:00 Uhr!

Agenturen können vorab berichten, mit Hinweis auf die Sperrfrist 15:00 Uhr für die Veröffentlichung.

Heute ist ein historischer Tag für die Bundeswehr.
Ich stelle heute den neuen militärischen Organisationsbereich Cyber- und Informationsraum in Dienst – mit dem neuen Kommando CIR an der Spitze. Ein Meilenstein deutscher Sicherheits- und Verteidigungspolitik.
Für eine moderne Großorganisation wie die Bundeswehr ist Cyber – Digitalisierung und der Informationsraum das Megathema. Und das Thema wächst rasant.

Im Weißbuch 2006 tauchte das Wort „Cyber“ genau ein einziges Mal auf. In unserem neuen Weißbuch 2016 kommt es 72 Mal vor, also rein rechnerisch auf jeder 2. Seite. Das ist nur ein winziges Detail – aber es zeigt bildlich, wie stark das Thema Cyber und Digitalisierung die nächste Dekade beherrschen wird. Und es gibt kaum einen Bereich in der Bundeswehr, der davon nicht betroffen ist. Ob das die Logistik, die Mobilität, unsere Kommunikation in Deutschland wie im Einsatz oder fast alle unsere Waffensysteme sind.
Denken wir an den MedEvac-Hubschrauber in Mali, der nicht abhebt, ohne dass er an ein SAP-Programm angeschlossen wurde. Oder nehmen wir unsere neuen Fregatten der Reihe F125. Durch die Einführung einer weitgehenden Automation können wir bei diesen Schiffen die Besatzungsstärke auf fast die Hälfte reduzieren. Leistungsfähigere Schiffe, dank moderner Technik, trotz kleinerer Crew.
Oder der Eurofighter, der allein 80 Computer an Bord hat und 100 km Kabel.
Aber durch diese Vernetzung und Technisierung sind wir auch verwundbarer gegen Cyber-Angriffe geworden. Die Angriffe auf unsere Systeme und Netze kommen täglich, unabhängig von Begriffen wie Frieden, Krise, Konflikt oder Krieg. Und sie kommen von unterschiedlichen Akteuren, Staatlichen wie Privaten. Sie sind automatisiert oder hoch differenziert und maßgeschneidert.
Allein in den ersten 2 Monaten des Jahres wurden über 280.000 Ereignisse gezählt, die als Cyber-Attacken gegen die Bundeswehr gewertet werden können.
Es geht von der einfachen Spionage, Datenklau über Zerstören bis Manipulieren und Beeinflussen.
Und um eins klarzustellen: Wenn die Netze der Bundeswehr angegriffen werden, dann dürfen wir uns auch wehren.

Sobald ein Angriff die Funktions- und Einsatzfähigkeit der Streitkräfte gefährdet, dürfen wir uns auch offensiv verteidigen.
Bei Attacken auf andere staatliche Institutionen können wir immer im Rahmen der Amtshilfe tätig werden. In den Auslandseinsätzen ist die Lage klar. Hier bestimmen die Bundestagsmandate die Möglichkeiten - und Grenzen - das gilt selbstverständlich auch für den Cyberraum.
Und soweit es darüber hinaus noch rechtlichen Klärungsbedarf gibt, stehen wir ohnehin in engem Austausch mit den zuständigen Ressorts.
Dabei ist Cyber nur einer der wesentlichen Anteile im größeren Informationsraum.
Die Vielfalt stellt uns tagtäglich vor neue Herausforderungen. Mit der hybriden Kriegführung in der Ostukraine haben wir einen Vorgeschmack bekommen.
Und die Drohung eines virtuellen Kalifats ist keine leere mehr. Wir erinnern uns an den Bundestagshack ebenso wie an die Fake-News-Kampagne gegen die Bundewehr in Litauen.

Der Cyber- und Informationsraum ist eine eigene sicherheitspolitische Domäne geworden neben Land, Luft, See und Weltraum und er ist ein neuer Operationsraum für die Bundeswehr.
Deswegen bündeln und stärken wir unsere Expertise in der Truppe. Das geht vom Betrieb der eigenen IT-Systeme im In- und Ausland über die vorausschauende Analyse potenzieller Gefahren bis hin zu den Fähigkeiten von Aufklärung und Wirkung im Cyber- und Informationsraum.
Cyber-Angriffe auf Staaten und besonders deren kritische Infrastrukturen sind schon lange keine Fiktion mehr. Sie sind bittere Realität.
Und die Bundeswehr trägt ihren Teil der gesamtstaatlichen Sicherheitsvorsorge.

Lieber Herr General Leinhos,
gleich werde ich Ihnen das Kommando über den inzwischen 6. militärischen Organisationsbereich CIR übertragen.
Damit etablieren wir einen Inspekteur Cyber und Informationsraum, der wie die Inspekteure Heer, Luftwaffe, Marine, Streitkräftebasis und Sanität, „seine“ Domäne verantwortlich führt, gestaltet und national und international vertritt.
Als 6. Inspekteur der Bundeswehr werden Sie, General Leinhos, die Aufgaben

- Cyber,
- IT,
- Militärisches Nachrichtenwesen, Geoinformationswesen,
- und Operative Kommunikation,

aus einer Hand fachlich führen.
Zudem wird Ihr Kommando zentrale Ansprechstelle sein für andere Ressorts des Bundes, die Wirtschaft und unsere internationalen Verbündeten.
Ihr Pendant im Ministerium ist die Abteilung CIT, die ich im Oktober aufgestellt habe.
Bereits im Juli werden Ihrem Kommando rund 13.500 Soldatinnen und Soldaten und zivile Mitarbeiterinnen und Mitarbeiter unterstellt sein. Sie kommen aus den unterschiedlichsten Ecken unserer Streitkräfte.
Für all diese Menschen gilt es, eine neue Heimat zu schaffen, eingebettet in unsere Bundeswehr.
Eine gemeinsame Identität. Denn nur als Team können Sie die Herausforderungen bestehen. Und dass Sie ab heute ein Team sind, können wir daran sehen, dass Sie alle das dunkelblaue Barett tragen, mit eigenem Abzeichen. Die kleine Weltkugel darauf steht für globale Aufklärung und Vernetzung.

Mit der nationalen Vernetzung fangen wir hier in Bonn schon an. Denn die Zentrale des Kommandos CIR liegt in direkter Nachbarschaft zu einem unserer wichtigsten Partner, dem Bundesamt für Sicherheit in der Informationstechnik. Das BSI wird an den Bonner Rheinauen in den nächsten Jahren einen neuen Standort aufbauen.

Meine Damen und Herren,
Soldatinnen und Soldaten,

Bei der Ausplanung der neuen Strukturen haben alle Verantwortlichen eine Menge Herzblut investiert und ordentlich aufs Tempo gedrückt.
Dafür danke ich Ihnen ausdrücklich.

Sie haben etwas geschaffen, das seinesgleichen sucht. Sie werden in Ihrer Dienststelle neue digitale Plattformen und Arbeitsmechanismen nutzen.
Wir erhöhen gemeinsam die Attraktivität des Arbeitgebers Bundeswehr durch flexiblere Laufbahnen und Werdegänge.
Man kann jetzt auch als Cybersoldat bei der Bundeswehr Karriere machen!
Und wir bilden auch selber aus. Ein internationaler Master-Studiengang für Cyber-Sicherheit wird an der Universität der Bundeswehr in München geschaffen. Als Starttermin für zunächst 70 Studenten ist der Januar 2018 geplant.
13 neue Professuren wurden dazu eingerichtet. Insgesamt sind im aktuellen Haushalt rund 1,6 Mrd. € für alle IT-bezogene Aufwendungen vorgesehen. Das reicht von neuen Funkgeräten über Hardware bis hin zu Verträgen mit Providern. Für 2018 planen wir mit einem weiteren deutlichen Anstieg. Oben drauf kommen jeweils jährlich Personalkosten von knapp 1 Mrd. €.

Diese Zahlen machen noch einmal deutlich, dass wir bereit und gefordert sind, die Investitionen auch in diesem Bereich deutlich zu verstärken,

- um aufzuholen, was bisher versäumt wurde,
- um Schritt zu halten mit technischen Innovationen,
- aber auch mit unseren Partnern und Verbündeten auf höchstem Niveau zusammen zu arbeiten.

Genau das müssen wir immer mitdenken, wenn wir jetzt aktuell die notwendige Finanzausstattung der Bundeswehr diskutieren.
Stillstand wäre Rückschritt und den haben wir schon zu lange gehabt. Ja, wir müssen richtig Gas geben, um die klügsten Köpfe zu bekommen und zu halten. Und die ersten Früchte unserer Arbeitgeber-Kampagne können sich auch schon sehen lassen. Im letzten Jahr ist es uns gelungen, 60% mehr Informatikerinnen und Informatiker einzustellen als im Jahr davor. Ein Ergebnis, das Mut macht!

Meine Damen und Herren,
die heutige Geburtsstunde des Kommandos CIR ist für die Bundeswehr mehr als ein Meilenstein. Damit stellen wir uns international im Spitzenfeld auf.
Die Liste der anderen Nationen, die Ihre Kräfte vergleichbar gebündelt haben, ist klein und renommiert: wie z.B. die USA und Israel.
Und ich freue mich sehr, dass heute auch eine kleine Delegation unseres Cyber-Innovations-Hubs angetreten ist. Diese Plattform hat in Berlin gerade die Arbeit aufgenommen. Es ist unsere Schnittstelle zu den treibenden Kräften der IT-Community. Sie sollen den regelmäßigen Dialog mit den Treibern aus der Forschung, Wissenschaft, Wirtschaft und Industrie aktiv suchen. Vor allem interessiert uns aber auch das Start-Up Ökosystem. Wir warten nicht, bis sich ein start-up bei uns meldet…. Wir suchen disruptive Technologien. Wir bewerten sie hinsichtlich eines Mehrwerts für die Bundeswehr und wenn wir fündig werden, wollen wir diese Technologien schnell einführen und als IT-Service anbieten zu können.

Soldatinnen und Soldaten,
Meine Damen und Herrn,

Auf Ihnen ruhen hohe Erwartungen.
Mit unserer neuen digitalen Aufstellung gehören wir zu den Vorreitern in unseren Bündnissen – nutzen Sie diese Pole-Position!
Gehen Sie mit Neugierde und Schwung ans Werk.
Lassen Sie den neuen Organisationsbereich CIR zu dem werden, was er sein soll: ein Zentrum für Innovation, Kreativität und hohe Expertise im Cyber- und Informationsraum.
Und Sie leisten von heute an einen existenziellen Beitrag für die Sicherheit der Bundeswehr und der Bürgerinnen und Bürger dieses Landes.
Wir vertrauen Ihnen
Und wir trauen Ihnen viel zu!