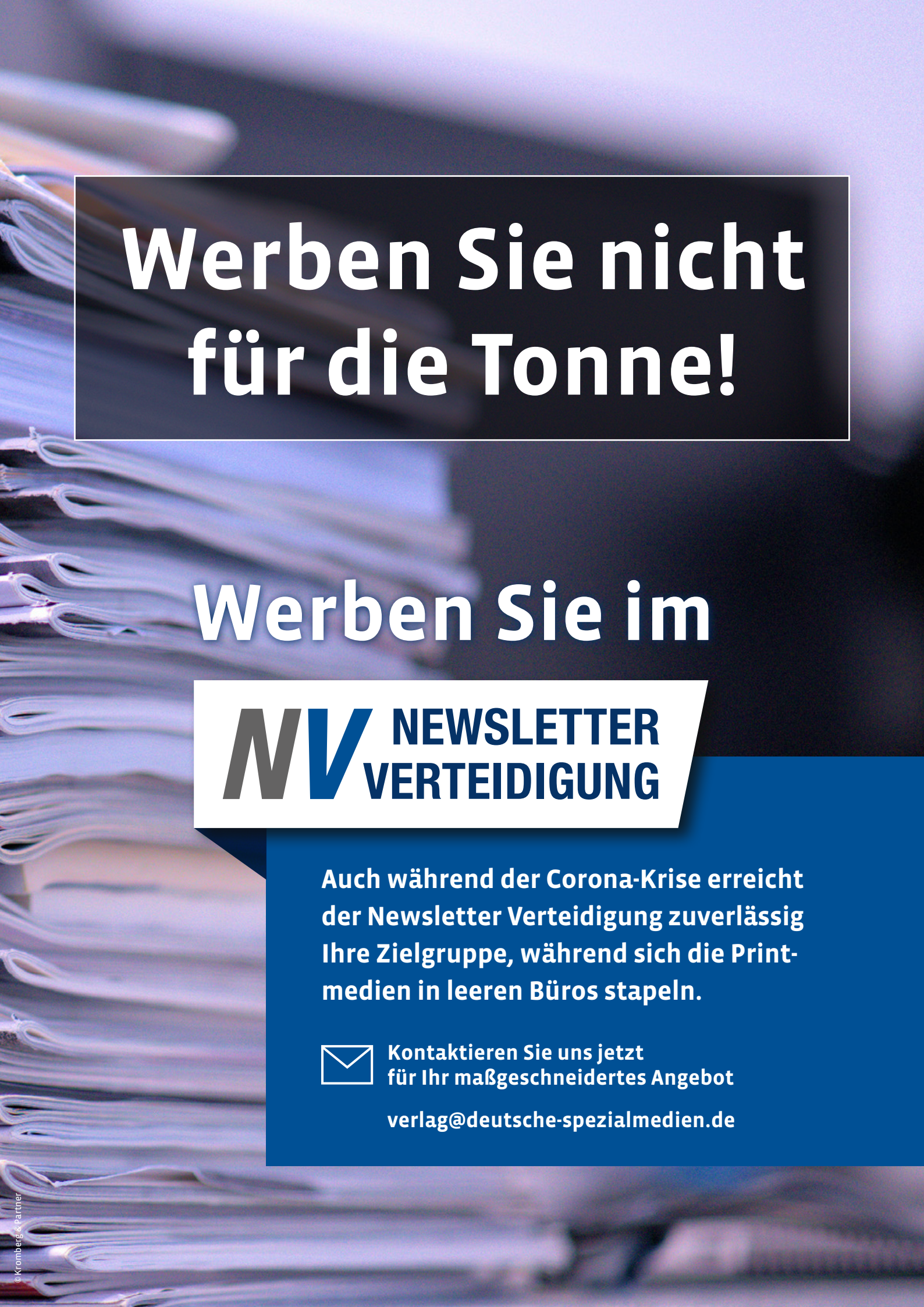
NEWSLETTER VERTEIDIGUNG

07. APRIL 2020 I ISSN 2194-0088 I 12. JAHRGANG

AUSGABE 14

Zugreifen bitte! –

FML plädiert für Reaktivierung von Bunker MARTIN


Werben Sie nicht
für die Tonne!
Werben Sie im
NV NEWSLETTER VERTEIDIGUNG
Auch während der Corona-Krise erreicht der Newsletter Verteidigung zuverlässig Ihre Zielgruppe, während sich die Print-medien in leeren Büros stapeln.
Kontaktieren Sie uns jetzt
für Ihr maßgeschneidertes Angebot
verlag@deutsche-spezialmedien.de
© Kromberg & Partner

Business Continuity

Kommentar von Andreas Hubert, Präsident Forum der Militärischen Luftfahrt e.V. (FML)


© FML

Andreas Hubert setzt sich für die Reaktivierung des verbunkerten Gefechtsstands MARTIN durch die Bundeswehr ein.

„Gerade bei den Streitkräften, einem Kern staatlicher Daseinsfürsorge, geht es um Betriebskontinuität in allen Lagen. Was für Unternehmen gilt, sollte ohne Wenn und Aber auch für die Bundeswehr zutreffen: Vor dem Hintergrund möglicher Risiken mit hohem Schadensausmaß, das heißt disruptiver Ereignisse, gilt es, die Sicherstellung des Auftrages zu gewährleisten, Prozesse zu schützen und alternative Abläufe zu ermöglichen.

Mit alternativen Abläufen sind in den Streitkräften sicher nicht nur Verfahrensoptimierungen gemeint, sondern eben auch alternative, robuste Stationierungsobjekte. Die derzeitige COVID-19-Epidemie führt uns schmerzlich vor Augen, was wir im Rahmen der Einlösung der sogenannten „Friedensdividende“ alles aus der Hand gegeben haben: (Zu) viele Reservekapazitäten im Bereich des Zivil- und Katastrophenschutzes.

Wer (spätestens) jetzt an den strategischen Gefechtsstand auf der Schwäbischen Alb denkt, liegt nicht falsch. Lesenswert hierzu: „FML on Tour – Sicherheit durch Luftverteidigung hat ihren Preis“ in JetNews 1/2019 (www.fml-online.org). Wir erinnern uns: Das vierstöckige Premiumobjekt MARTIN, seit den 1960er-Jahren ein tragender und beständig modernisierter Pfeiler der Landes- und Bündnisverteidigung, ging erst 2014 vom Netz, wurde zur vollumfänglichen Schließung und somit zur Abgabe an die BImA vorbereitet – bis dann im Mai 2018 der Haltebefehl kam. Im Rahmen der Trendwende sollte ein neuer Bedarf für den verbunkerten Gefechtsstand bis Ende 2019 geprüft werden. Mittlerweile wurde diese Prüffrist aufgrund andauernder Untersuchungen noch einmal bis Ende 2020 verlängert.

So weit, so gut. Noch einmal Zeit gewonnen. Nichts brennt an. Die vielen Kubikmeter Stahlbeton ruhen in sich selbst, die gute Eignung zur Aufnahme „größerer Gebinde“ (Headquarter) wurde national frisch befunden und es ist Vorsorge getroffen, dass dies absehbar auch so bleibt. Aber inhaltlich? Tut sich auch wirklich etwas in und um MARTIN?


© Schwarzwälder-Bote/Alfred Reck

Eingang zum geschützten Gefechtsstand

Mit Interesse beobachte und zähle ich die mittlerweile deutlich zweistelligen Revisionen der Standortentscheidungen von 2011. Im Übrigen ohne, dass in allen Fällen schon bis ins letzte ausgefeilt Nutzungskonzepte vorlägen. Weit überwiegend geht es bei diesen Reaktivierungen um Einzelaspekte des Betriebes in den Streitkräften, wie z. B. die Bevorratung von Munition oder „einfach“ die Stationierung der wieder wachsenden Truppe. Wo aber ist eine gewisse Priorisierung einer elementar wichtigen resilienten Führungsfähigkeit in allen Lagen?

Wäre es nicht an der Zeit, sich (mangels Alternativen!) ein Herz zu fassen, einen entsprechenden Bedarf an MARTIN in JEDEM Fall festzuschreiben und JETZT zur Einleitung der Reaktivierung zu schreiten? Was hindert? Die (im Übrigen überschaubaren) Kosten? Der Zeitbedarf? Eher wäre es doch so, dass gerade der (leider nicht unerhebliche) Zeitbedarf ein Präjudiz dafür wäre, zeitnah den Startschuss zu geben. Alles andere folgt.

Damals auf der Höhe der Zeit, müsste die komplette technische Ausstattung für die Reaktivierung erneuert werden.

Im Übrigen deutet sich an, dass Deutschland nicht allein die finanziellen Lasten von Reaktivierung und Betrieb stemmen müsste. Wenn etwas richtig und zielführend für die nationalen Streitkräfte ist, dann ist es dies auch für die Streitkräfte der Allianz. Nicht umsonst hat (mindestens) das alliierte Kommando in Ramstein, basierend auf einem Angebot unserer militärischen Führung, längst ein Auge auf MARTIN geworfen. Auch die unmittelbare Nähe der Hochalb zum neuen Ulmer Kommando (JSEC) sollte beim Nachdenken über einen robusten Ausweichgefechtstand auf den bewährten Bunker führen.

Wie gesagt, man müsste nur dann absehbar auch auf die Zielgerade einbiegen. Im Bereich der Allianz würde meines Erachtens dazu gehören, auf höherer militärischer und politischer Ebene für MARTIN zu werben, seine Vorteile herauszustellen, dabei konkrete Kostenteilungsangebote zu unterbreiten und insgesamt den richtigen, positiven Spin im Sinne eines „Win-win“ auf das Dossier zu bringen.

Geschäftiges Treiben herrschte noch vor wenigen Jahren im Bunker auf der Hochalb.

Bisweilen entsteht demgegenüber der Eindruck, unsere Nation warte für ein konkretes Angebot auf die Allianz und umgekehrt. Ob das angesichts der nicht schlafenden Konkurrenz in anderen Nationen reicht? Wie zu hören ist, gibt die Disruption durch COVID-19 nun etwas mehr Zeit, den Entscheidungsfindungsprozess der NATO hinsichtlich einer Alternative für das Kommando in Ramstein substanziell(er) zu begleiten.

Aber auch national sollte eigentlich jedem Kundigen mittlerweile klar sein, dass wir viel zu wenig Objekte haben, bei denen wir im Bedarfsfall die Türen schließen, Schutzluft fahren und gut abgeschirmt unserer Arbeit nachgehen können.

Der Bunker MARTIN liegt auf dem Silbertablett. Zugreifen bitte!“

Zum Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie

Gemeinsame Stellungnahme von Bitkom und BDSV

Achim Berg, Präsident des 1999 gegründeten Bitkom e.V.

Der Bitkom und der BDSV begrüßen, dass sich die Bundesregierung in ihrem Strategiepapier zur Stärkung der Sicherheits- und Verteidigungsindustrie zu dem Erfordernis einer innovativen, leistungs- und wettbewerbsorientierten Sicherheits- und Verteidigungsindustrie bekennt. In Anbetracht wachsender sicherheitspolitischer Herausforderungen ist eine Stärkung heimischer sicherheitsrelevanter Technologien von größter strategischer Bedeutung. Das Strategiepapier erkennt richtig die Bedeutung der Digitalisierung als technologische Herausforderung für unsere Sicherheit und Verteidigung sowie die Gewährleistung der Cybersicherheit als Grundvoraussetzung für die fortschreitende Digitalisierung von Staat, Wirtschaft und Gesellschaft und als Element der Souveränität Deutschlands und Europas. Vor diesem Hintergrund ist auch der angekündigte strukturierte Dialog mit der zivilen Sicherheitsindustrie zur Stärkung der digitalen Souveränität im Hinblick auf den Bedarf der Kritischen Infrastrukturen unter Leitung des BMI begrüßenswert. Ein Strategiepapier kann jedoch nur so gut wie seine Umsetzung sein.

Aus Sicht des Bitkom und des BDSV werden die folgenden Maßnahmen für eine Operationalisierung empfohlen:

1. Partnerschaft zwischen Staat und Wirtschaft

In Bezug auf das jeweilige sicherheitspolitische Umfeld gehen wir als Wirtschaft davon aus, von Seiten der Bundesregierung bei der Analyse der aktuellen digitalen Bedrohungen angemessen über anstehende Herausforderungen informiert zu werden. Nur wenn für die Wirtschaft Planbarkeit und Transparenz bestehen, kann von ihr erwartet werden, dass sie auch langfristig als Partner der Sicherheitsorgane in Deutschland erhalten bleibt. Eben dies gilt auch für alle Maßnahmen, die im Bereich der Förderung von digitalen Schlüsseltechnologien geplant und umgesetzt werden. Wir unterstützen nachdrücklich alle Maßnahmen, die auf eine digitale Souveränität in den im Strategiepapier umrissenen Bereichen abzielen und arbeiten hieran gerne auch aktiv mit. Dies betrifft nicht zuletzt auch den sog. »Ausverkauf« von Assets, die für die nationale Sicherheit von Bedeutung sind. Allerdings erwarten wir, dass in gleichem Maße auch solche industriellen Assets identifiziert werden, die diese Sicherheitsrelevanz nicht haben. Solche Assets müssen gem. AWG/AVO entsprechend fungibel ausgestaltet werden, um eine wirtschaftliche Werthaltigkeit zu gewährleisten.

2. Optimierung der Beschaffungsorganisation

Wie im Strategiepapier identifiziert besteht der dringende Bedarf einer Optimierung der Beschaffungsvorgänge innerhalb der Einkaufsorganisationen. Die Berücksichtigung der strategischen Vorgaben muss formal in die Beschaffungsrichtlinien Eingang finden und sich spürbar auf allen Ebenen des Beschaffungswesens auswirken. Darüber hinaus müssen als Grundlage für die Beschaffungsabwicklung Veränderungen der Budget- und Beschaffungsplanung sowie die zeitnahe Adaption von Innovationen durch Verwender erfolgen. Speziell in dem Bereich Cyber/IT unterliegen Innovationen

sehr kurzen Zyklen und können bereits bei einem vergleichsweise niedrigen Mittelaufwand einen erheblichen Nutzen bringen. Neben der Reform der Vorgänge in den Verwender- und Beschaffungsorganisationen wird eine Einbindung des Finanzministeriums bezüglich der Mittelbereitstellung, sowie des Justizministeriums zur möglichen Anpassung von Beschaffungsrichtlinien als potenziell notwendig erachtet.

3. Präzisierung der Schlüsseltechnologien

Die im Strategiepapier vorgenommene Darstellung der Technologiefelder ist weder ebenengerecht noch vollständig. Zudem sind sie aus systemischer Sicht auf unterschiedlichen Systemebenen verankert. Unsere Unternehmen gehen davon aus, auch hinsichtlich der Präzisierung der der digitalen Schlüsseltechnologien und -fähigkeiten an der Diskussion beteiligt und jeweils zeitnah in die Erarbeitung entsprechender Ergebnisse einbezogen zu werden. Aufgrund der bestehenden Unklarheiten sollten Unternehmen eine Ansprechstelle haben, die ihnen dabei hilft festzustellen, ob sie »nationale Schlüsseltechnologie« führen und ggf. entsprechende Vor- und Nachteile berücksichtigen müssten.

4. Klarheit zur Exportkontrolle schaffen

Insbesondere in innovativen Nischen im Dual-Use-Güterbereich entstehen innerhalb der Digitalwirtschaft Schlüsseltechnologien. Die derzeitigen Vorschriften der Exportkontrolle und der im Vergleich zum (europäischen) Ausland für den Bereich der sicherheitskritischen Technologien sehr langwierige Genehmigungsprozess mit unklarer Auskunftslage gegenüber Kunden ist insbesondere für kleine und mittelständische Unternehmen (KMU) problematisch. Es besteht eine signifikante Gefahr, dass innovative KMU und auch größere Konzerne ihren Entwicklungs- und Produktionsstandort ins Ausland verlagern müssen, um nicht Insolvenz zu riskieren, wenn internationale Kunden wegen einer fehlenden zeitnahen Zu-/Absage Bestellungen stornieren.

5. Ressortübergreifenden Ansatz ausbauen

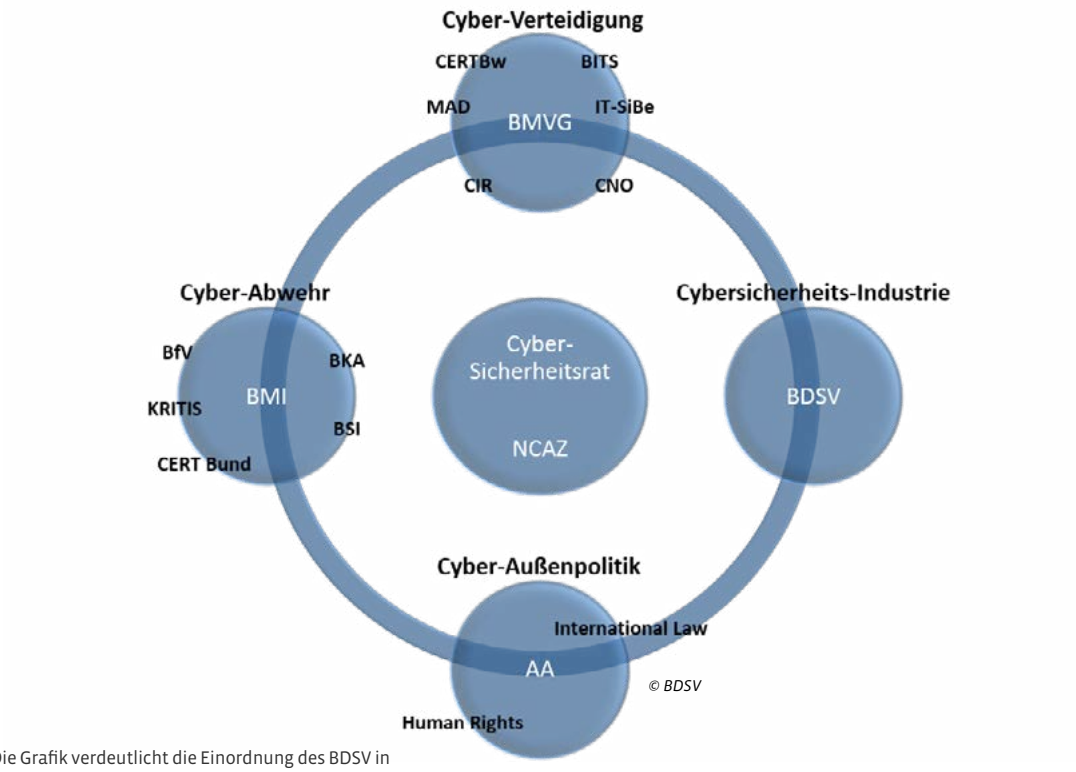
Der Erfolg des Strategiepapieres hängt mit Blick auf Start-ups und den Mittelstand davon ab, dass die Maßnahmen von allen Ressorts getragen und umgesetzt werden. Es wäre sinnvoll, auch das Bundesministerium für Bildung und Forschung eng in den Austausch mit Verwendern von Sicherheitstechnologie und den entwickelnden Unternehmen einzubinden. Damit das Strategiepapier auch einen praktischen positiven Effekt hat, ist die Umsetzung in allen betroffenen Bereichen und auf allen Hierarchiestufen eng zu begleiten. Periodisch sollte der Fortschritt der getroffenen Maßnahmen erfasst und evaluiert werden. Dies wäre als Zielvorgabe für eine hiermit speziell betraute Stelle oder einen Ausschuss wünschenswert.

6. Industrie- und Forschungsförderung gleichberechtigt ausgestalten

Dr. Hans Christoph Atzpodien, Hauptgeschäftsführer des Bundesverbands der Deutschen Sicherheits- und Verteidigungsindustrie.

Im Strategiepapier wird dargelegt, dass die Sicherheits- und Verteidigungsindustrie durch Investitionen in Forschungsmaßnahmen gefördert werden soll. Als mögliche Maßnahmen sehen wir die gleichberechtigte Förderung von Forschungseinrichtungen und Wirtschaft.

Zwei Aspekte stehen hier im Vordergrund: Zum einen die Offenlegung von Forschungsergebnissen im Sinne einer »Open-Source« Politik und die Sicherung der Nutzung von Forschungsergebnissen durch die hier im Fokus stehenden Unternehmen. Zum anderen die konsequente Weiterführung von »Open Data«, indem die Daten maschinenlesbar per API bereitgestellt werden. Über die Veröffentlichung als Studien hinaus sind die Rohdaten und maschinenlesbaren Ergebnisse ebenfalls zur Verfügung zu stellen.



Die Grafik verdeutlicht die Einordnung des BDSV in die Cyber-Sicherheitsarchitektur der Bundesrepublik.

7. Abhängigkeiten vermeiden – Souveränität sicherstellen

Die Nutzung von Kernfähigkeiten der SVI durch öffentliche Auftraggeber kann unter Umständen mit signifikanten Abhängigkeiten verbunden sein. Zur Sicherung der Handlungsfähigkeit des öffentlichen Auftraggebers sollte sichergestellt werden, dass Kernfähigkeiten nicht nur durch einzelne Anbieter, sondern im europäischen und transatlantischen Wettbewerb erbracht werden können. Dieser Wettbewerb sichert zusätzlich die Weiterentwicklung und Innovation in den Kernfähigkeitsclustern und schafft damit Wettbewerbsfähigkeit im internationalen Wettbewerb.

Fakten

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 1.800 Direktmitglieder. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein.

Der BDSV vertritt die gebündelten Interessen der deutschen Sicherheits- und Verteidigungsindustrie. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen und bietet Informationen über die relevanten Themen der deutschen Sicherheits- und Verteidigungsindustrie. Der BDSV fungiert als Point of Contact der deutschen Sicherheits- und Verteidigungsindustrie und als Scharnier zwischen Unternehmen, Politik, Gesellschaft, Institutionen und Medien.

Text: BDSV/Bitkom

Bundeskriminalamt stärkt die Cybercrimebekämpfung

Neue Abteilung „CC“ nimmt die Arbeit auf

Das Bundeskriminalamt (BKA) hat zum 01.04.2020 die Abteilung „Cybercrime“ (CC) eingerichtet und vollzieht damit einen weiteren wichtigen Schritt, um Kompetenzen zur Bekämpfung dieses Phänomens zu bündeln und die erforderliche Spezialisierung seiner Mitarbeiterinnen und Mitarbeiter in diesem Bereich voranzutreiben. Denn die Digitalisierung ist aus vielen Bereichen unseres Lebens nicht mehr wegzudenken. Eine Entwicklung, die sich leider auch Kriminelle zu Nutzen machen, um ihre Straftaten zu begehen – schnell und weltweit per Mausklick. Nicht selten werden sie dabei durch unterschiedliche rechtliche Regelungen in den Staaten, aber auch fehlende informationstechnische Sicherungsmaßnahmen und digitale Kompetenzen begünstigt.

Das BKA blickt bei der Bekämpfung von Cyberkriminalität bereits auf eine langjährige Erfahrung zurück. Ihren Anfang nahm diese unter der Bezeichnung „Informations- und Kommunikationskriminalität“ in einem kleinen Arbeitsbereich des Referates für Wirtschaftskriminalität der damaligen Abteilung Organisierte und Allgemeine Kriminalität (OA) Mitte der 1990er Jahre.

Nach einem stetigen Zuwachs an Aufgaben und Personal entstand im Jahr 2013 die Gruppe „Cybercrime“, die mit über 100 Mitarbeiterinnen und Mitarbeitern in der Abteilung Schwere und Organisierte Kriminalität (SO) aufgebaut wurde. Diese Gruppe bildet nunmehr den personellen wie fachlichen Grundstein der neuen Abteilung, die in den nächsten Jahren schrittweise auf rund 280 Mitarbeiterinnen und Mitarbeiter anwachsen soll.

Kriminalbeamte, Analysten und IT-Experten mit verschiedensten Spezialisierungen arbeiten hier Hand in Hand. Geleitet wird die Abteilung durch Carsten Meywirth, der nach seiner Verwendung als Stabsleiter der Abteilung Informationstechnik (IT) die Gruppe „Cybercrime“ vom November 2013 bis Mai 2016 leitete, bevor er für die Abteilung Zentrale Verwaltung für Baumaßnahmen, Liegenschaftsverwaltung und zentrale Services verantwortlich zeichnete.

Die neue Abteilung wird neben den klassischen Zentralstellenaufgaben wie der Koordinierung des internationalen Informationsaustausches zu diesem Phänomenbereich die Analysekompetenz des BKA, etwa bei neuen Cybercrime Phänomenen und digitalen Angriffsmustern, erweitern. Aber auch Ermittlungen gegen kriminelle Akteure, Netzwerke und Strukturen sollen hier verstärkt geführt werden. Die Vernetzung auf nationaler wie internationaler polizeilicher Ebene wird dabei eine ebenso wichtige Rolle spielen wie die Kooperation mit unterschiedlichen Akteuren aus anderen Behörden und der Wirtschaft.

Holger Münch ist seit 2014 Präsident des Bundeskriminalamtes.

Holger Münch, Präsident des Bundeskriminalamts, unterstrich anlässlich der Arbeitsaufnahme der Abteilung CC:

„Die Abhängigkeit unserer Gesellschaft von einer funktionsfähigen technischen Infrastruktur nimmt stetig zu. Zugleich haben Straftäter es noch immer vergleichsweise einfach, sich im Netz kriminelle Kompetenz einzukaufen, um ohne umfängliche technische Kenntnisse etwa die Webpräsenzen ganzer Unternehmen zu blockieren oder die Informationstechnik in Krankenhäusern und Verwaltungen anzugreifen. Hier gilt es für uns, mit diesen Entwicklungen Schritt

zu halten und unsere Kompetenzen stetig fortzuentwickeln, um Straftaten im digitalen Raum schnell analysieren, wirkungsvoll bekämpfen und die Täter ihrer realen Verantwortung zuführen zu können. Mit dem Aufbau der Abteilung CC schaffen wir hierfür eine wichtige Grundlage, die nun mit Leben gefüllt werden muss."

Text und Bild: BKA

Nationales Cyber-Abwehrzentrum

Plattform zum schnellen Informationsaustausch

Das nationale Cyber-Abwehrzentrum ist Bestandteil der Cyber-Sicherheitsstrategie für Deutschland, die von der Bundesregierung im Februar 2011 beschlossen und im November 2016 erneuert wurde. Die offizielle Eröffnung erfolgte im Juni 2011. Ziel ist es, die Zusammenarbeit zwischen Nachrichtendiensten, Polizeidienststellen des Bundes und der Länder sowie Ministerien beim Kampf gegen Cyberangriffe zu verbessern.

Neben dem Bundesministerium der Verteidigung sind am nationalen Cyber-Abwehrzentrum unter anderem folgende Behörden beteiligt: Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Verfassungsschutz, Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, Bundeskriminalamt, Bundesnachrichtendienst, Bundespolizei, Zollkriminalamt und die Bundesanstalt für Finanzdienstleistungsaufsicht.

Die zentrale Aufgabe des Cyber-Abwehrzentrums hierbei ist es, IT-Sicherheitsvorfälle früh zu erkennen, schnell und umfassend zu bewerten und abgestimmte Handlungsempfehlungen zu erarbeiten. Dies geschieht auf Basis eines ganzheitlichen Ansatzes, der die verschiedenen Gefährdungen im Cyberraum zusammenführt. Hierzu zählen Cyber-Spionage, Cyber-Ausspähung, Cyber-Terrorismus und Cyber-Crime. Das Ziel ist eine wirksame Abwehr. Eine enge Zusammenarbeit der Sicherheitsbehörden ist hierbei zwingend. Ein frühzeitiger Informationsaustausch zwischen den Akteuren ist grundlegende Voraussetzung für ein konsequentes und wirksames Vorgehen im Schadensfall.

Text: BMVg

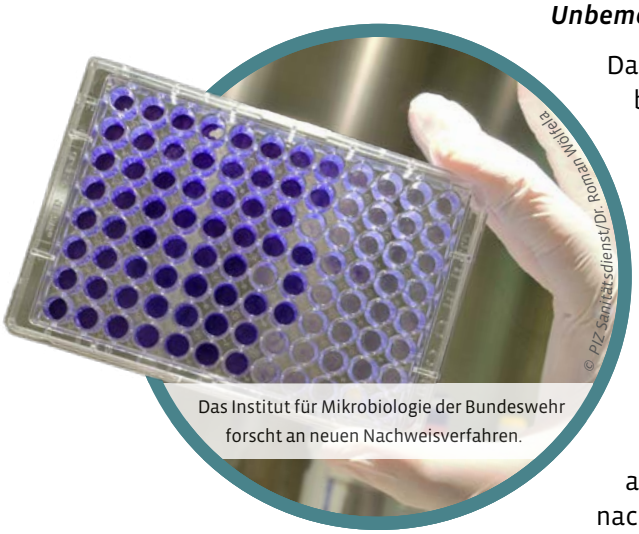
© Bundeswehr/Tom Twardy

Das nationale Cyber-Abwehrzentrum schützt kritische IT, z.B. der Bundeswehr, vor Cyber-Attacken. Dafür nutzt es seit Kurzem auch Informationen der Abteilung Cybercrime des BKA.

Institut für Mikrobiologie der Bundeswehr im COVID-19-Modus

Auf der Suche nach einer Antwort auf die Frage, ab wann COVID-19-Patienten bei begrenzten Bettenkapazitäten frühestens aus dem Krankenhaus entlassen werden könnten, sind derzeit Wissenschaftler des Instituts für Mikrobiologie der Bundeswehr (IMB), der Berliner Charité und der München Klinik Schwabing. In einer gemeinsamen Pressemitteilung veröffentlichten sie nun erste Ergebnisse. In einer Studie mit neun Patientinnen und Patienten der sogenannten Münchner Fallgruppe konnte die Forschungsgruppe viele wichtige Details über das neue Virus sammeln. Dazu wurden bei der Patientengruppe über den gesamten Verlauf der Infektion täglich Abstriche aus dem Nasen-Rachen-Raum und Proben des Husten-Auswurfs entnommen. Zusätzlich sammelten die Forschenden, wann immer möglich und sinnvoll, Stuhl-, Blut- und Urin-Proben. Alle Proben wurden anschließend unabhängig voneinander in zwei Labors auf das neuartige Coronavirus analysiert: im Institut für Virologie am Campus Charité Mitte in Berlin und im Institut für Mikrobiologie der Bundeswehr in München.

Die Forschungsgruppe konnte beobachten, dass die Virusausscheidung im Rachen der COVID-19-Erkrankten in der ersten Woche nach Beginn der Symptome sehr hoch war. Auch im Husten-Auswurf konnten große Mengen Virus-Erbgut nachgewiesen werden. Sowohl aus den Rachen-Abstrichen als auch aus dem Husten-Auswurf ließen sich infektiöse Virus-Partikel isolieren. Für Oberstarzt Privatdozent Dr. Roman Wölfel, Leiter des Instituts für Mikrobiologie der Bundeswehr, und einer der Erstautoren der Studie, ist die starke Vermehrung von Viren im Rachen ein wesentlicher Grund warum sich das Coronavirus so schnell verteilt.



Das Institut für Mikrobiologie der Bundeswehr forscht an neuen Nachweisverfahren.

Unbemerkt infektiös

Dabei merkten einige Infizierten anfänglich nicht, dass sie bereits infektiös waren. Zu dem Zeitpunkt waren sie oft noch symptomfrei. Wie infektiös ein COVID-19-Patient ist, hängt laut der Studie von der Viruslast im Rachen, beziehungsweise der Lunge ab. Für Wölfel ist dies ein wichtiger Faktor für die Entscheidung, wann ein Patient bei knappen Bettenkapazitäten und entsprechendem Zeitdruck frühestens aus dem Krankenhaus entlassen werden kann. Laut den Autoren und Autorinnen der Studie könnten COVID-19-Patienten in die häusliche Quarantäne entlassen werden, wenn sich nach dem zehnten Tag der Erkrankung weniger als 100.000 Kopien des Viren-Erbguts im Husten-Auswurf nachweisen lassen.

Ab dem achten Tag dreht sich das Blatt

Das neuartige Coronavirus lässt sich anhand seines Erbguts mit sehr empfindlichen Nachweisverfahren, beispielsweise aus einem Rachen-Abstrich eines Patienten, bestimmen. „Wenn die von uns untersuchten COVID-19-Patienten länger als acht Tage krank waren, konnten wir aus den Proben kein Coronavirus mehr in Zellkulturen anzüchten“, so Wölfel. Diese Beobachtung hängt, so die Forschenden, auch mit der Immunantwort des Körpers zusammen, durch die ab dem achten Tag Antikörper gegen das Virus gebildet werden.

Zusammenarbeit als Schlüssel zum Erfolg

Als Ende Januar im Landkreis Starnberg bei München erstmals COVID-19-Verdachtsfälle in Deutschland auftraten, lieferte das Institut für Mikrobiologie der Bundeswehr die ersten Labornachweise für das neuartige Coronavirus. Mehrere bei diesen Untersuchungen erkannte Patienten wurden daraufhin im Krankenhaus München-Schwabing isoliert. Die dann folgenden Laboruntersuchungen waren, wie immer beim Auftreten neuer und zuvor unbekannter Krankheitserreger, sehr umfangreich. Für Wölfel war es daher nur logisch und sehr sinnvoll, arbeitsteilig mit den Kollegen des Instituts für Virologie der Charité vorzugehen. Die Forschungsteams aus Berlin und München haben sich mehrfach täglich abgestimmt und Ergebnisse ausgetauscht. „Nur durch diese Zusammenarbeit konnten wir beispielsweise das Erbgut des Virus in lediglich zwei Tagen entschlüsseln“, betont Wölfel. Dabei ist der Wissenschaftler stolz darauf, dass die erste Virusanzucht des neuen Erregers in Europa zuerst am IMB gelang. Aber auch mit dem Krankenhaus München Schwabing arbeitet das IMB schon seit vielen Jahren eng zusammen. Die dort für München bereitgehaltene Sonderisolierstation nutzt immer wieder die schnellen Diagnostikfähigkeiten des Instituts für seltene und gefährliche Infektionskrankheiten. So konnte das IMB in den letzten Jahren immer wieder zur raschen Klärung von Verdachtsfällen, wie beispielsweise Ebola- oder Lassafieber, bei Reiserückkehrern beitragen.

Das IMB Im Kampf gegen das Virus

Das COVID-19-Virus bestimmt derzeit ganz wesentlich den Arbeitsalltag des IMB: Der Zentralbereich Diagnostik des Instituts wurde erheblich verstärkt und arbeitet seit Februar mit 24 Personen in drei Dienstgruppen jeden Tag von 7 bis 22 Uhr. Mehr als 40 weitere Mitarbeiterinnen und Mitarbeiter sind mit der Entwicklung neuer Coronavirus-Diagnostikverfahren, der Suche nach Medikamenten zur Behandlung von COVID-19, mit der Aufklärung von Infektionsketten oder mit anderen Unterstützungsleistungen beschäftigt. Die bisherige Struktur der Forschungsgruppen wurde dafür vorübergehend komplett neu strukturiert.

Oberstarzt Dr. Roman Wölfel leitet seit Oktober 2019 das Institut für Mikrobiologie der Bundeswehr in München.

In insgesamt neun Teams arbeiten Biologen, Biochemikerinnen, Biotechnologen, Tierärztinnen und Humanmediziner zusammen an verschiedenen Fragestellungen. Dabei bringen alle ganz spezielle Fachkenntnisse für die Erkennung und Behandlung der SARS-CoV-2 Infektionen mit ein. In den vergangenen Wochen ist es dem IMB so gelungen, mehrere zusätzliche Nachweisverfahren für SARS-CoV-2 aufzubauen, um auch bei Lieferengpässen bei Reagenzien und Verbrauchsmitteln immer Diagnostik anbieten zu können. Erste Erfolge zeigen sich auch bei der Suche nach Medikamenten, die das Viruswachstum bremsen. Außerdem wurden mehrere Tests zum Nachweis von schützenden Antikörpern gegen das Virus entwickelt.

Quelle: Pressemitteilung der Berliner Charité, des Instituts für Mikrobiologie der Bundeswehr und der München Klinik Schwabing.

Kommodore wechselt im Marinefliegergeschwader 3 „Graf Zeppelin“

Am 03. April 2020 wechselte die Spitze des Marinefliegergeschwaders 3 „Graf Zeppelin“. Der Kommodore, Fregattenkapitän Jörg Matthée, übergab das Kommando an seinen Nachfolger, Fregattenkapitän Oliver Ottmüller. Aufgrund der derzeitigen Corona-Krise verzichtet man auf das sonstige militärische Zeremoniell. Die Übergabe fand im „engsten Kreis“ statt.

Ursprünglich sollte der Kommodorewechsel mit zahlreichen Gästen aus Politik und Wirtschaft, Partnern und Musikkorps vollzogen werden, doch die „Corona-Krise“ schränkt nicht nur das öffentliche Leben erheblich ein. Auch der Dienstbetrieb im Marinefliegerstützpunkt Nordholz steht Kopf. Der Kommandeur des Marinefliegerkommandos, Kapitän zur See Thorsten Bobzin, steht vor der Herausforderung, Einsätze und andere Verpflichtungen wie den Such- und Rettungsdienst aufrecht zu erhalten, Kräfte für Hilfeleistungen vorzuhalten und gleichzeitig Maßnahmen zum Schutz der eigenen Soldaten und Mitarbeiter zu treffen. „Routineaufgaben haben wir weitgehend eingestellt, um Einsatzbereitschaft, Fürsorge und Hilfestellung für die Region gleichermaßen bieten zu können“, betont der Kommandeur.

Vom Cuxland in die Hansestadt

Der scheidende Kommodore hatte die Verantwortung über das Traditionsgeschwader „Graf Zeppelin“ im November 2015 übernommen. Während seiner Amtszeit hatte Fregattenkapitän Jörg Matthée viele Herausforderungen zu meistern. Neben zahlreichen infrastrukturellen Hürden im Zusammenhang mit der Einführung des neuen Hubschraubers vom Typ „Sea Lion“ beschäftigte Matthée vor allem die Umrüstung der eigenen P-3C-Orion-Flotte, die in den zurückliegenden Jahren leider massiven Einfluss auf die technische Bereitschaftslage mit sich führte. Die Regeneration von fachlich hoch qualifiziertem Personal stellte eine weitere Hürde dar, so dass die Sicherstellung der laufenden Einsatzverpflichtungen einem steten Drahtseilakt glich.

Kapitän zur See Bobzin hob daher abschließend auch die aus seiner Sicht beeindruckende Gesamtleistung des Geschwaders unter Matthées Führung bei schwierigen Rahmenbedingungen hervor. Als besonderes Highlight verzeichnete Matthée hingegen die Besuche der Orion-Staffeln in Brasilien und Pakistan im Rahmen der internationalen Kooperationsprogramme. Fregattenkapitän Matthée wechselt nach knapp viereinhalb Jahren als Dienststellenleiter an die Elbmetropole, wo er in der Fakultät Management an der Führungsakademie der Bundeswehr im Bereich der Lehre eingesetzt wird.

(v.l.) Jörg Matthée, Thorsten Bobzin, Oliver Ottmüller

Auch der neue Geschwader-Kommodore wird sich mit der mangelhaften Bereitschaftslage der Seefernaufklärer P-3C Orion auseinandersetzen müssen.

Das Zepter übernommen

Staffelkapitän der 2. fliegenden Staffel, Kommandeur der Fliegenden Gruppe im Marinefliegergeschwader 3 „Graf Zeppelin“ und zuletzt als Chef des Stabes im Marinefliegerkommando. Fregattenkapitän Oliver Ottmüller hat im Rahmen seiner militärischen Laufbahn bereits diverse wichtige Führungspositionen im Marinefliegerstützpunkt besetzt und kennt die militärischen Strukturen am Standort wie seine Westentasche. Er selbst bezeichnet den Marinefliegerstützpunkt als seine militärische Heimat. Mit der kommenden Verwendung als Kommodore des Marinefliegergeschwader 3 „Graf Zeppelin“ geht ein Traum in Erfüllung.

„Die Verwendung als Kommodore eines fliegenden Verbandes ist und bleibt DIE fliegende Verwendung. Ich freue mich riesig auf die neue Verwendung, die die Krönung meiner fliegerischen Laufbahn darstellt! Mit der Verwendung sind viele Herausforderungen verbunden, die ich mit allen Geschwaderangehörigen gemeinsam meistern möchte. In der aktuell schwierigen Situation der Corona-Krise gilt es, auch weiterhin die Einsatzbereitschaft sowohl der P-3C Orion als auch der DO-228 und auch des Marinefliegerstützpunktes aufrecht zu erhalten und den Einsatzverpflichtungen nachzukommen, stets mit dem Blick für die angespannte personelle und materielle Situation“, hob der neue Kommodore Ottmüller hervor.

Text und Bild: PIZ Marine

Niederlandische Luftwaffe übernimmt ersten modernisierten „Chinook“

US-Luftfahrtkonzern Boeing hat vor Kurzem den ersten CH-47F Chinook mit modernisiertem Cockpit an die Königlich Niederländische Luftwaffe (Koninklijke Luchtmacht, KLu) übergeben und damit seine Erfolgsbilanz pünktlicher Lieferungen nochmals bestätigt.

Mit der CH-47F verfügt die KLu über die modernste Konfiguration dieses Hubschraubertyps.

Die KLu betreibt künftig eine Flotte von 20 CH-47F Chinook der neuesten Konfiguration, die derzeit global im Einsatz ist. „Die KLu hat uns deutlich gesagt, dass sie die fortschrittlichen und bewährten Fähigkeiten des CH-47F schon heute benötigt“, erläuterte Andy Builta, Vice President Cargo & Utility Helicopters und H-47-Programm-Manager: „Ich möchte mich bei unserem großartigen Team bedanken, dass während einer schwierigen Situation hart gearbeitet hat, um die Hubschrauber sicher auszuliefern. Dies zeigt einmal mehr, wie wichtig der Chinook für unsere Kunden ist“.

Die Flotte aus 20 CH-47F Chinook-Hubschraubern wird mit der gleichen hochmodernen Technologie wie die US-Armee ausgestattet sein, einschließlich digitaler, automatischer Flugsteuerung, einem voll-integrierten Common Avionics Architecture System (CAAS) Glascockpit und fortschrittlicher Frachtabfertigungsfähigkeiten. Die einheitliche Konfiguration führt außerdem zu niedrigeren Gesamtlebenszykluskosten. Die KLu fliegt derzeit eine Mischung aus Chinooks der F-Modellreihe mit dem Advanced Cockpit Management System (ACMS) sowie des Typs CH-47D.

„Es war uns eine Freude, eng mit den Teams der US-Armee und Boeing zusammenzuarbeiten, um diesen Meilenstein zu erreichen“, sagte Col. Koen van Gogh vom niederländischen Beschaffungsamt Defensie Materieel Organisatie (DMO). „Der Chinook-Hubschrauber ist für unsere Missionen von entscheidender Bedeutung. Die pünktliche Lieferung unterstützt zudem unsere Einsatzplanung. Ich begrüße die anhaltenden Bemühungen der Mitarbeiter von Boeing, die dies in diesen beunruhigenden Zeiten ermöglicht haben, sowie der Vertreter der US-Armee, die dazu beigetragen haben, uns auf Kurs zu halten“.

Die Lieferungen an die KLu werden voraussichtlich bis ins Jahr 2021 hinein erfolgen. Chinooks sind derzeit weltweit bei 20 Streitkräften im Dienst oder unter Vertrag. Dazu gehören die US-Army und Special Operations Forces, sowie acht NATO-Mitgliedsstaaten.

Text und Bilder: Boeing

Die niederländischen Chinooks kommen auch regelmäßig bei gemeinsamen Übungen mit der Bundeswehr zum Einsatz.

Die Schweiz verfügt über insgesamt 20 Einsatzmuster vom Typ EC 635.

Helikopter für den Transport von Corona-Patienten umgerüstet

RUAG MRO Schweiz hat kürzlich das Helikoptermodell EC 635 für den Transport von COVID-19-Patienten umgerüstet. Bei diesem zeitkritischen Projekt haben RUAG MRO Schweiz, die armasuisse und die Luftwaffe gemeinsam an geeigneten Lösungen gearbeitet, um Piloten wie auch Patienten bestmöglich zu schützen. Zwei Helikopter sind bereits umgerüstet und stehen einsatzbereit bei der Luftwaffe.

Das Helikoptermodell EC 635 dient der Schweizer Armee in der Regel zu Schulungs- und Trainingszwecken. Durch seine grossen Platzverhältnisse eignet es aber auch ideal als Einsatzflugzeug und ist weltweit der am häufigsten verwendete Helikopter für Rettungsdienste. Auch bei der Schweizer Armee kommt er für spezifische Operationen wie Personen- und Patiententransport zum Einsatz und besitzt zu diesem Zweck eine Grundausstattung an medizinischer Versorgung.

Aufgrund der aktuellen Lage hinsichtlich des Coronavirus hat die Schweizer Luftwaffe RUAG MRO Schweiz damit beauftragt, die Infrastruktur dieses Helikoptertypen spezifisch für den Transport von COVID-19-Patienten umzurüsten. Einerseits ist eine räumliche Abtrennung des Cockpits von der Kabine notwendig, um Piloten bestmöglich vor der Krankheit zu schützen und ihre Einsatzfähigkeit für weitere Flüge zu gewährleisten. Andererseits bedarf es einer geeigneten Methode zur Desinfizierung des gesamten Helikopters. Nicht zuletzt gilt es, unterschiedliche medizinische Geräte von COVID-19-Patienten auf etwaige Störsignale zu prüfen und diese zu berücksichtigen.

Bereits zwei Helikopter wurden innerhalb weniger Tage umgerüstet und stehen der Luftwaffe einsatzbereit zur Verfügung. RUAG MRO Schweiz hat desweiteren die notwendige Fabrikation für den kurzfristigen Umbau weiterer Helikopter des Typs EC 635 sichergestellt.

Durch eine enge Zusammenarbeit zwischen RUAG MRO Schweiz und dessen Partnern armasuisse und Luftwaffe war es möglich, binnen kürzester Zeit umsetzbare Lösungen zur Verfügung zu stellen. «Wir rücken nicht nur mit der fortschreitenden Entflechtung näher zusammen. Insbesondere diese aussergewöhnlichen Situationen zeugen von gegenseitigem Vertrauen und hervorragender Zusammenarbeit. So ist es uns möglich, gemeinsam gute Lösungen zu erarbeiten, um diejenigen zu unterstützen, die auf unsere Hilfe angewiesen sind», sagte Andreas Baumann, General Manager Helicopters, RUAG MRO Schweiz.

Text und Bild: RUAG

Saab liefert Mobile Camouflage System

Saab hat einen Auftrag für das Mobile Camouflage System (MCS) erhalten, dessen Auslieferung an die Bundeswehr noch im Jahr 2020 erfolgt. Die Bundeswehr nutzt bereits seit 2008 das Mobile Camouflage System unter der Bezeichnung Multispektraler Mobiler Tarnsatz (MMT) für die Fahrzeugmuster Marder, PzH 2000, Leopard, Boxer und Büffel.

Der Auftrag umfasst MCS für die von der Bundeswehr genutzten Fennek Fahrzeuge in Wald-, Schnee- und Wüstentarnung. „Wir freuen uns sehr, erneut den Auftrag zur Lieferung des Mobile Camouflage Systems an die Bundeswehr zu erhalten. Dieser Auftrag umfasst die Ausstattung der Bundeswehr mit modernstem multispektralen Schutz für mobile Operationen“, erläuterte Görgen Johansson, Leiter der Business Area Saab Dynamics.

Saabs weltweit führende multispektrale Tarnsysteme decken sämtliche Vegetationsbereiche ab – Wüste, Wald, Arktis und Dschungel. Sie werden für jedes Fahrzeugmuster maßgeschneidert, um die perfekte Passform zu gewährleisten. Darüber hinaus bietet das MCS nicht nur einen vollumfänglichen multispektralen Schutz, sondern enthält auch Saab’s CoolCam Funktionen, welche die in heißen Klimazonen auftretenden thermischen Aufladungen im Inneren der Fahrzeuge zuverlässig reduzieren.

Text und Bild: Saab

IMPRESSUM

Newsletter Verteidigung veröffentlicht in deutscher Sprache aktuelle Aufsätze, Berichte und Analysen sowie im Nachrichtenteil Kurzbeiträge zu den Themen Rüstungstechnologie, Ausrüstungsbedarf und Ausrüstungsplanung, Rüstungsinvestitionen, Materialerhaltung, Forschung, Entwicklung und Erprobung sowie Aus- und Weiterbildung. Newsletter Verteidigung hat eine europäische, aber dennoch vorrangig nationale Dimension. Aus der Analysearbeit von Newsletter Verteidigung werden regelmäßig hoch priorisierte Themenfelder aufgegriffen, welche interdisziplinär einen Bogen spannen von der auftragsgerechten Ausstattung der Bundeswehr mit Wehrmaterial, der Realisierungsproblematik von militärischen Beschaffungsvorhaben, der Weiterentwicklung der Streitkräfte, den technologischen Trends und Entwicklungstendenzen bei Wehrmaterial, der Weiterentwicklung der heimischen wehrtechnischen Industriebasis und der Rüstungs- und Sicherheitspolitik bis hin zur Rüstungszusammenarbeit mit Partnerländern und gemeinsamen Beschaffung von Wehrmaterial.

Newsletter Verteidigung erscheint auf elektronischem Wege (PDF-Format) mit 50 Ausgaben im Jahr. Eine Weiterverbreitung von Inhalten des Newsletter Verteidigung darf nur im Wege einer Gruppenlizenz erfolgen. Das Abonnement verlängert sich automatisch um ein weiteres Jahr, wenn es nicht drei Monate vor Ablauf mit Einschreiben gekündigt wird.

Verlagsanschrift:
VDS Verlag Deutsche
Spezialmedien GmbH

Ketzerbach 25-28
35037 Marburg, Germany

Tel. +49 6421 1832-899
Fax +49 6421 18329-05

E-Mail:
verlag@deutsche-spezialmedien.de

Gerichtsstand:
AG Marburg an der Lahn

Verantwortlicher im Sinne des Presserechts:
Daniel Kromberg (DK),
Chefredakteur

E-Mail:
redaktion@newsletter-verteidigung.de