Bundesministerium
der Verteidigung

Volker Wieker
Generalinspekteur der Bundeswehr

HAUSANSCHRIFT Stauffenbergstraße 18, 10785 Berlin
POSTANSCHRIFT 11055 Berlin

TEL +49 (0)30 2004[redacted]
FAX +49 (0)30 2004[redacted]
E-MAIL [redacted]@BMVg.Bund.de

Ich erlasse das

Konzept für die personelle Unterstützung

der „Cyber-Community" der Bundeswehr („*Cyber-Reserve*")

Der Gesamtvertrauenspersonenausschuss beim BMVg wurde beteiligt, der Hauptpersonalrat, die Gleichstellungsbeauftragte und die Gesamtschwerbehindertenvertretung beim BMVg wurden gehört.

[redacted]

Berlin, 2.3.2017

Inhalt

1. Vorbemerkung

Staat, Wirtschaft und Gesellschaft sind in einer digitalisierten Welt zunehmend auf Daten und Informationen aus einem vernetzten Umfeld angewiesen. Daten und Informationen wirken als Motor des technologischen Fortschritts und eröffnen Chancen und Potenziale für die weitere digitale Entwicklung. Die Verfügbarkeit, der Schutz und die Unverfälschtheit von gespeicherten, übertragenen und verarbeiteten Informationen sind folglich von strategischem Interesse.

Einhergehend mit dieser Entwicklung erhöhen sich jedoch auch die Missbrauchspotenziale durch nicht gewollte Eingriffe und Attacken Dritter. Nicht-staatliche und staatliche Akteure suchen offene Zugänge und andere Schwachstellen von kritischen Infrastrukturen, Industrieanlagen, IT-Netzwerken oder Datenbanken, um sie zu manipulieren oder unter ihre Kontrolle zu bringen. Auch geschützte Zugänge werden inzwischen vermehrt überwunden. Dieser gesamtstaatlichen Bedrohung wird durch eine Ressort-übergreifende, gesamtstaatliche Sicherheitsvorsorge besonders auch in Zusammenarbeit mit dem BMI begegnet werden.

Die Bundeswehr wird deshalb zur Erfüllung ihres Auftrages bei der gesamtstaatlichen Sicherheitsvorsorge in der Dimension Cyber- und Informationsraum (CIR) einen neuen Organisationsbereich einrichten, der die diesbezüglichen Fähigkeiten unter einem Kommando Cyber- und Informationsraum zusammenfasst. Zur personellen Ergänzung und Verstärkung wird die Bundeswehr gezielt eine hoch qualifizierte und schlagkräftige *„Cyber-Reserve"* zur bedarfsorientierten Unterstützung des aktiven Cyber-Personals der Bundeswehr aufbauen. Mit der Übernahme bereits existierender Dienststellen wie beispielsweise Zentrum für Informationstechnik der Bundeswehr, Kommando Strategische Aufklärung der Bundeswehr, Führungsunterstützungskommando der Bundeswehr, Zentrum Operative Kommunikation der Bundeswehr und Zentrum für Geoinformationswesen der Bundeswehr werden dem Organisationsbereich CIR bereits existente Reservestrukturen und beorderte sowie interessierte Reservistinnen und Reservisten zur Verfügung gestellt, die es beim Aufbau der *„Cyber-Reserve"* aktiv zu nutzen gilt.

Das vorliegende Konzept wird von einem erweiterten Verständnis getragen, nicht nur auf das Potenzial früherer Soldatinnen und Soldaten, sondern auch auf ungediente Freiwillige und Seiteneinsteigerinnen bzw. Seiteneinsteiger zurückzugreifen, um beim Aufbau von Fähigkeiten im Cyber- und Informationsraum in der Bundeswehr zu unterstützen und damit wirkungsvolle Beiträge bei der gesamtstaatlichen Sicherheitsvorsorge zu leisten. Die Möglichkeit, auch außerhalb des Status Reservistin bzw. Reservist in der *„Cyber-Reserve"* aktiv zu werden, ist neu, herausfordernd in der Umsetzung und kennzeichnend für das erweiterte Verständnis. Eine *„Cyber-Reserve"* ist inhaltlich demnach weitaus umfassender zu sehen und geht über eine aus Reservistinnen und Reservisten bestehende Reserve deutlich hinaus.

Die *„Cyber-Reserve"* ist bewusst konzeptionell weit gefasst, sie öffnet sich neuen Zielgruppen und steht einem umfangreicheren Personenkreis offen, als dies in der herkömmlichen Reserve der Fall ist (Anlage 1). Auf Grund der damit verbundenen neuen Dimensionen ist gesetzgeberischer Handlungsbedarf erforderlich und den identifizierten Maßnahmen gegebenenfalls vorzuschalten.

2. Zweck, Fähigkeiten und personeller Bedarf einer *„Cyber-Reserve"*

Mit dem Aufbau der *„Cyber-Reserve"* möchte die Bundeswehr das Potenzial hochqualifizierter Cyber-Spezialistinnen und Cyber-Spezialisten für die Aufgabenwahrnehmung bei der gesamtstaatlichen Sicherheitsvorsorge besser ausschöpfen.

Neben der notwendigen Duplizierung vorhandener Expertise und Kräfte (auf Basis der Personalergänzung und Personalverstärkung der Organisationsstrukturen im Bereich CIR auf Dienstposten / Beorderungsmöglichkeiten der Verstärkungs- und Personalreserve) sollen zusätzlich auch die derzeit nicht oder nicht ausreichend vorhandenen, aber unverzichtbar benötigten Fähigkeiten und Kompetenzen besser abrufbar sein. Außerhalb der Bundeswehrstrukturen[1] vorhandene Personen mit Schlüssel-Know-How können bei Bedarf zur Unterstützung staatlicher Strukturen und zum Schutz kritischer Infrastrukturen genutzt werden. Dies schließt die Gewährleistung der Verfügbarkeit bundeswehreigener informationstechnischer Systeme und die Möglichkeit zur Begegnung übergreifender Cyber-Angriffe und -Attacken gegen Staat, Wirtschaft und Gesellschaft ein.

Diesen Grundanliegen Rechnung tragend werden mit dem Aufbau der *„Cyber-Reserve"* mittels qualifizierter Spezialistinnen und Spezialisten speziell für den Fähigkeitsbereich Cyber primär drei Ziele verfolgt:

1. Bildung eines zusätzlichen Kräfteelements im Inland, um für die Abwehr von schwerwiegenden Cyber-Angriffen und eine Betätigung im Bereich CIR weitere Kräfte (auch kurzfristig) zur Verfügung zu stellen.
2. Bündelung von Spezialistinnen und Spezialisten, um durch gemeinsames Üben eine wirkungsvolle und state-of-the-art Cyber-Wirkkomponente, gegebenenfalls auch mit internationalen Verbündeten aufzubauen.
3. Die Förderung des Erfahrungsaustausches von eigenem Cyber-Personal mit entsprechenden Spezialistinnen und Spezialisten außerhalb der Bundeswehr durch Community-Bildung wird ebenfalls angestrebt.

Die genauen und darauf bezogenen spezifischen Anforderungen an die *„Cyber-Reserve"* sind im Zuge der Aufstellung und des weiteren Aufwuchses des militärischen Organisationsbereiches CIR zu formulieren. Im jetzigen Verständnis stehen insbesondere vier Zielgruppen für die *„Cyber-Reserve"* im Fokus:

1. **Exzellenzen, TOP-Führungskräfte**, die beispielsweise für ausgewählte Projektarbeiten, spezifische Beratungsleistungen, Vorträge und Aus-/Weiterbildung gewonnen werden:

Dazu können unter anderem Geschäftsführende oder Vorstände aus mittleren oder größeren Unternehmen mit einschlägigen Aufgabenbereichen gehören, aber auch CIOs oder CISOs. Weiter kommen hier auch wissenschaftliche Honoratioren (z.B. Professorinnen und Professoren, Doktoren vergleichbar), Wissenschaftler in Betracht oder Führungskräfte (Spitzenbeamtinnen und Spitzenbeamte) aus anderen Behörden oder Einrichtungen mit vergleichbarem Hintergrund (beispielsweise IT-Governance, IT-Betrieb, Informationssicherheit, IT-Revision, Kommunikationstechnik).

2. **Ausscheidende Berufs- und Zeitsoldatinnen bzw. Berufs- und Zeitsoldaten** (mit und ohne Studium, jedoch mit einschlägigen, für die *„Cyber-Reserve"* nutzbaren Verwendungen und Kenntnissen; dazu zählen auch Freiwillig Wehrdienstleistende):

Im Fokus stehen über alle Dienstgradgruppen hinweg Personen, die über Spezialisten-Ausbildungen oder herausragende Fähigkeiten, Fertigkeiten und Kompetenzen in einschlägigen Bereichen oder Funktionen verfügen.[2] Es ist entscheidend, diese bestmöglich

[1] Dies beinhaltet die Wirtschaft, den öffentlichen Dienst / Sektor und die Verwaltung.
[2] Fachkräfte und Expertinnen bzw. Experten mit einschlägigem MINT-Studium sind explizit zu betrachten. MINT steht für die Fächergruppen Mathematik, Informatik, Naturwissenschaft und Technik.

zu informieren, zu gewinnen und zu binden, bevor sie aus dem aktiven Bundeswehrdienst ausscheiden.

3. Seiteneinsteigerinnen und Seiteneinsteiger

Hier kommen in der Bundeswehr ungediente beziehungsweise gediente Personengruppen mit einschlägigem fachlichem Hintergrund in Betracht, die über etablierte Fach-Foren, formelle oder informelle Netzwerke, Fach-Veranstaltungen oder vergleichbare Plattformen als potenzielle Cyber-Reservisten identifiziert werden und aktiv geworben werden können.

4. Freiwillige, die sich außerhalb der Reserve engagieren wollen

Dazu zählen Fachkräfte, Experten oder Führungskräfte beispielsweise aus dem „CERT" (computer emergency response team) -Umfeld, IT- und Informationssicherheitsverantwortliche, aber auch auch Freiwillige, wie beispielsweise Studierende, Angehörige von Nicht-Regierungsorganisationen, Vereinen oder Verbänden, sonstige Talente und Freiberufler, die für vielfältigste Aufgaben im Cyber-/IT-Bereich herangezogen werden können (Beispiel: „Ethical" Hacker, die in gemeinsamen Übungen Cyberangriffe simulieren) und die im Rahmen eines ehrenamtlichen oder bürgerschaftlichen Engagements in der Bundeswehr - ohne Soldatenstatus - tätig werden.

Der Aufbau der *„Cyber-Reserve"* nutzt die bestehenden Reservestrukturen der in den Organisationsbereich CIR zu überführenden Dienststellen. In einer ersten Phase werden zusätzlich zu Reservestrukturen einzelne herausragende Expertinnen und Experten benötigt, die während der Aufstellung und Feinausplanung Beratungs- und Projektaufgaben übernehmen, zum Beispiel beim Aufbau von Know-How für das Zentrum Cyber-Sicherheit der Bundeswehr, der Festlegung der notwendigen Cyber-Ausbildung (nicht-wissenschaftliche Anteile) oder im Bereich des aufzubauenden Forschungs- und Innovationsmanagement. Der dazu erforderliche organisatorische Koordinierungsbedarf ist durch den Organisationsbereich CIR zu leisten. Dieser Bedarf kann innerhalb der Struktur einer *„Cyber-Reserve"* oder außerhalb (Individuallösung) gedeckt werden.

Bis Mitte 2018 (das heißt ca. ein Jahr nach Aufstellung) werden begleitend zum personellen Aufwuchs von Fähigkeiten im Organisationsbereich CIR in der *„Cyber-Reserve"* Reservistinnen und Reservisten sowie andere Expertinnen und Experten benötigt, die qualifiziertes Wissen aus dem Bereich Cyber mitbringen und damit helfen, das bundeswehreigene Fachwissen vor allem im Bereich der Cyber-Verteidigung zu vertiefen und zu verbreitern.

Bis Ende 2019 soll Personal in Strukturen der *„Cyber-Reserve"* so gebunden werden, dass die personellen Fähigkeiten des Kommandobereichs CIR wirksam ergänzt und verstärkt werden können.

3. Personalgewinnung und -bindung

Die Personalinformation und Personalgewinnung muss sowohl die "neue" Zielgruppe ansprechen als auch die Personalbindung derjenigen ausscheidenden Soldatinnen und Soldaten und zivilen Mitarbeiterinnen und Mitarbeiter gleichwertig beachten, die über Spezialkenntnisse verfügen und deshalb an die "*Cyber-Reserve*" gebunden werden müssen. Freiwillige, die sich außerhalb dieser Reservestrukturen engagieren wollen, finden über ein

ziviles Beschäftigungsverhältnis[3] ein attraktives Angebot zu einem Engagement in der *„Cyber-Reserve"* der Bundeswehr beziehungsweise für die Bundeswehr. Dies betrifft auch Personen, die nicht als Reservistin beziehungsweise als Reservist verwendet werden können (zum Beispiel wegen der gesundheitlichen Anforderungen), möchten (zum Beispiel wegen der persönlichen Verfügbarkeit) oder dürfen (zum Beispiel kein Deutscher im Sinne des Grundgesetzes). Ergänzend sind die bereits vorhandenen flexiblen Möglichkeiten zur Personalgewinnung/-bindung voll auszuschöpfen, um die notwendige Expertise für die Bundeswehr zu sichern (besonders der Seiteneinstieg in die Laufbahnen der Reserve mit höherem Dienstgrad). Zur Gewinnung qualifizierten Personals bedarf es in diesem Fall innovativer und vermehrt auch unkonventioneller Methoden und Verfahren[4]. Die speziellen Fähigkeiten und Fertigkeiten müssen dabei im Vordergrund stehen. Inwieweit dann hierbei militärische Ausbildung und soldatische Grundfertigkeiten vermittelt werden müssen, ist im Einzelfall flexibel und pragmatisch festzulegen.
Zur Bindung ausscheidender Soldatinnen und Soldaten ist die konsequente Umsetzung der seit 8. Juli 2015 veröffentlichten Zentralanweisung B1-1330/0-5003 „Reservistenberatung" erforderlich. Ein klares Bekenntnis aller Vorgesetzten zur Reserve - auch über den eigenen fachlichen Zuständigkeitsbereich hinaus - ist der maßgebliche Faktor, um das Personal mit seiner in der Bundeswehr erworbenen Cyber-Expertise an die Bundeswehr zu binden. Es bedarf eines gezielten und konsequenten Ansprechens durch alle an der Personalgewinnung oder -bindung beteiligten Stellen, um qualifizierte Soldatinnen und Soldaten sowie zivile Mitarbeiterinnen und Mitarbeiter vor dem Verlassen der Bundeswehr beziehungsweise dem Übergang in das zivile Erwerbsleben für ein weiteres Engagement in der *„Cyber-Reserve"* der Bundeswehr zu gewinnen.

Mit der Aufnahme eines verpflichtenden Hinweises des beziehungsweise der beurteilenden Vorgesetzten zu „Verwendungsvorschlägen Reserve" in der letzten Beurteilung vor Dienstzeitende, einschließlich der Möglichkeit zur Stellungnahme des beziehungsweise der Beurteilten, kann dieser Prozess gezielt unterstützt werden.

Für den zielgerichteten Aufbau der *„Cyber-Reserve"* kommt es darauf an, jetzt unverzüglich konkrete Verwendungsmöglichkeiten für interessierte qualifizierte Bewerberinnen und Bewerber zu schaffen, um dieses Potenzial nicht zu verlieren. Maßgeblich hierfür ist der durch den Bedarfsträger zu strukturierende und zu spezifizierende Bedarf. Parallel könnten attraktive monetäre und nicht-monetäre Maßnahmen – unter Beachtung der steuerrechtlichen Gegebenheiten – entwickelt werden, um ein zusätzliches Anreizpaket zu schaffen.

4. Informationskampagne und Begleitkommunikation

Eine personalwerbliche Kommunikation zur *„Cyber-Reserve"* wird anlassbezogen im Rahmen des „Projekts Digitale Kräfte" erfolgen. Zunächst sind weiterhin vorrangig IT-Fachkräfte zu bewerben.

Der Zugang zu geeignetem Personal für die *„Cyber-Reserve"* wird maßgeblich durch die zu entwickelnde Begleitkommunikation gesteuert.

Die Zielstruktur des Organisationsbereichs CIR wird voraussichtlich im Jahr 2021 eingenommen. Die Erstbefähigung des Kommando CIR ist für Mitte 2017 geplant. Nach Abschluss der darauf aufbauenden schrittweisen Aufstellung sowie der damit verbundenen personellen Feinausplanung liegen dann diejenigen Erkenntnisse vor, die über Umfang,

[3] Der Abschluss ziviler Beschäftigungsverhältnisse (wie z.B. Dienst-, Honorar- oder Werkverträge) liegt in der Zuständigkeit des Organisationsbereichs CIR. Hiermit ist nicht die Anstellung von Zivilpersonal mittels eines Arbeitsvertrages durch den Organisationsbereich Personal gemeint.
[4] einschließlich des Angebotes von modernen und flexiblen Modellen hinsichtlich Arbeitszeit und Arbeitsort.

Anforderungen und Fähigkeiten einer *„Cyber-Reserve"* Auskunft geben. Die folgende externe Kommunikationsstrategie ist maßgeblich hieran anzulehnen, um zielgerichtete Angebote unterbreiten zu können. Maßnahmen vor diesem Zeitpunkt können sich nur auf Einzelpersonal beziehen und werden nicht im Rahmen einer Kampagne kommuniziert.

Eine Begleitkommunikation wird ab der Aufbauphase angewendet. Eine entsprechende inhaltliche Zuarbeit durch den Organisationsbereich CIR ist hierfür die Voraussetzung.

5. Bundeswehr und Arbeitgeber

Sicherheit im digitalen Zeitalter kann nur im Rahmen eines gesamtgesellschaftlichen Ansatzes realisiert werden, weil sich Arbeitgeber der Wirtschaft, des Öffentlichen Dienstes/Sektors und der Verwaltung der Cyber-Bedrohung in gleicher Weise ausgesetzt sehen wie die Bundeswehr als Institution. Aus diesem Grund ist eine erweiterte Kooperation im Hinblick auf eine gemeinsame Nutzung dieses insgesamt limitiert vorhandenen Personals zur Begegnung und Bekämpfung dieser Bedrohung im mehrheitlichen Interesse und für alle Seiten bedeutsam. Von den hierdurch möglichen Synergieeffekten profitieren beide Seiten (im Sinne der Cyber-Sicherheitsstrategie der Bundesregierung).

Ein Aufruf des BMVg an die Zielgruppen und einschlägigen Institutionen des Öffentlichen Dienstes/Sektors, der Verwaltung sowie der Wirtschaft-mit ihren IT-Unternehmen, Hard- und Softwarefirmen etc. zur Beteiligung an der *„Cyber-Reserve"* der Bundeswehr wird neue Potenziale erschließen helfen und die Bereitschaft, gesamtstaatliche und ressortübergreifende Verantwortung zu übernehmen, zu fördern und zu unterstützen.

Kurzfristig werden die potenziellen einschlägigen Arbeitgeber, die sich den CIR-relevanten Thematiken angenommen haben, hinsichtlich der gemeinsamen Interessen und Möglichkeiten zur Kooperation mit der Bundeswehr informiert. Ziel ist es, die vielfältigen Möglichkeiten darzustellen und mit potenziellen Partnern weiterzuentwickeln. Dies schließt Ausbildungs-/Weiterbildungs- und Qualifizierungsangebote der Bundeswehr ein (zum Beispiel aktuell erzielbare Qualifikationen im Aufgabengebiet Cyber, Modul Cyberspace national bzw. CyberSecurity international für Führungskräfte, etc.).

Mittelfristig soll unter anderem die gemeinsame Aus-, Fort- und Weiterbildung von Cyber-Spezialisten und Cyber-Spezialistinnen zudem im Rahmen eines auch für andere Ressorts und ausgewählte zivile Teilnehmende offenen Studienganges „Cyber-Sicherheit" an der Universität der Bundeswehr in München sowie anderer attraktiver Fortbildungssangebote realisiert werden. Gemeinsame Forschungsprojekte auf dem Gebiet Cyber-Sicherheit sind eine weitere Möglichkeit zur Festigung der Kooperationen und zur Erzielung von Synergieeffekten.

Den außerhalb der Bundeswehr stehenden Verantwortlichen ist hierbei zu vermitteln, dass eine Kooperation mit der Bundeswehr ein Gewinn in Bezug auf die eigene Sicherheit und/oder die Qualifikation der eigenen Belegschaft darstellt.

Langfristig ist diese Kooperation weiterzuentwickeln. Maßnahmen sind vor allem beim beabsichtigten Bildungspass, der Anerkennung der bei der Bundeswehr erworbenen Kompetenzen durch externe Arbeitgeber / Institutionen sowie der gegenseitigen Anerkennung von Inhalten und Abschlüssen (wie beispielsweise Grade, Zertifikate, Zeugnisse) erforderlich.

Der erfolgreiche Aufbau einer *„Cyber-Reserve"* hängt insgesamt wesentlich davon ab, dass sich die Bundeswehr attraktiver und stärker auf die Bedürfnisse und Ideen der externen Arbeitgeber und Institutionen beziehungsweise der Zielgruppen zubewegt.

6. Informations- und Kommunikationsangebote („Cybernetz“[5])

Dem in der *„Cyber-Reserve“* tätigen Personenkreis stehen bereits heute differenzierte, auf die einzelnen Zielgruppen, Bereiche und Bedürfnisse ausgerichtete Informations- und Kommunikationsangebote zur Verfügung.

Die folgenden Dienststellen sind primär im Rahmen der Zuständigkeit für die Informationsbereitstellung und individuelle Beratung zuständig:

1. Kommando CIR,
2. Beorderungsdienststellen der beorderten Reservistinnen und Reservisten,
3. Bundesamt für das Personalmanagement der Bundeswehr sowie
4. Kompetenzzentrum für Reservistenangelegenheiten der Bundeswehr.

Kurzfristig ist für Interessierte eine Ansprechstelle in Verantwortung des Kommandos CIR aufzubauen, um den Informationsbedarf potenzieller Bewerberinnen und Bewerber durch eine fachlich versierte Wahrnehmung zu decken. Weitere Maßnahmen sind durch die Ansprechstelle in Zusammenarbeit mit den maßgeblichen CIR-Dienststellen sowie dem Bundesamt für das Personalmanagement der Bundeswehr zu veranlassen.

Für den fachlichen Dialog zum Themenbereich „Cyber- und Informationsraum“ betreibt Kommando CIR mittelfristig ein Expertenportal (Arbeitsbegriff „Cybernetz“). Es bietet eine gesicherte, geschützte und verlässliche Kommunikationsmöglichkeit der Cyber-Community der Bundeswehr innerhalb und außerhalb des Kommando CIR, um aktuelle Fragen und Herausforderungen zu diskutieren und im Dialog weiterzuentwickeln. Es gewährleistet den sicheren fachlichen Dialog sowie die Nutzung und Verwendung geschützter Inhalte. Dieses Cybernetz ist in das Dachkonzept Online-Medien einzubinden.

Damit wird der Individualisierung der heterogenen Zielgruppen Rechnung getragen und ein vertiefendes Engagement in diesem Bereich gefördert.

7. Interessenkollision, Geheim- und Sabotageschutz

Eine Interessenkollision bei Reservistendienst leistenden Firmenangehörigen und Angehörigen sonstiger Organisationen und Interessenverbände ist gem. Abschnitt 2.1.4.4 (Nummer 2045 bis 2050) der Zentralrichtlinie A2-1300/0-0-2 "Die Reserve der Bundeswehr" auszuschließen. Die Prüfung der Interessenkollision erfolgt in jedem Einzelfall durch die anfordernde Stelle (mit Ausnahme der Reservistendienstleistungen im BMVg und im Kommando CIR - vgl. Nummer 2050). Interessierte/Bewerberinnen bzw. Bewerber außerhalb der herkömmlichen Reserve, welche z.B. durch Dienst-, Honorar- oder Werkverträge gebunden werden sollen, sind ebenfalls hinsichtlich einer Interessenkollision zu überprüfen. Das Ergebnis der jeweiligen Überprüfung ist aktenkundig zu machen.

Die Bestimmungen der Zentralvorschrift A-1130/3 (MilSichh-Personeller Geheim- und Sabotageschutz) sind zu berücksichtigen. Für eine Verwendung im Geschäftsbereich des BMVg in einer sicherheitsempfindlichen Tätigkeit (wovon beim Thema Cyber grundsätzlich auszugehen ist), ist die Person vorher einer Sicherheitsüberprüfung zu unterziehen (Nr. 2405).

[5] Arbeitsbegriff.

8. Weitere Maßnahmen

Die weitere Ausgestaltung erforderlicher Maßnahmen erfolgt in Verantwortung der fachlich zuständigen Stellen anhand der Bedarfsformulierungen des Kommando CIR. Die Umsetzung des Konzeptes, die Chancen und mögliche auftretende Schwierigkeiten, sind im Rahmen einer regelmäßigen Erfolgskontrolle und eines „best practise" Prozesses in enger Abstimmung zwischen dem BMVg und dem Kommando CIR zu begleiten.
Die Zuständigkeit und die fachliche Verantwortung für die Weiterentwicklung dieses Konzepts sind unter Berücksichtigung der fortschreitenden Aufstellung des militärischen Organisationsbereichs CIR ggf. neu festzulegen. Daher beläuft sich die Gültigkeit dieses Konzeptes auf zunächst drei Jahre nach Schlusszeichnung und wird danach einer Revision unterzogen.

9. Anlagen

Personal-Pool *„Cyber-Reserve"*

Verteiler (Verteilung erfolgt ausschließlich per E-Mail)

Büro Parlamentarischer Staatssekretär Dr. Brauksiepe
Büro Parlamentarischer Staatssekretär Grübel
Büro Staatssekretärin Dr. Suder
Büro Staatssekretär Hoofe

Abteilung Politik
Abteilung Ausrüstung
Abteilung Cyber/ Infromationstechnik
Abteilung Planung
Abteilung Führung Streitkräfte
Abteilung Strategie und Einsatz
Abteilung Haushalt und Controlling
Abteilung Recht
Abteilung Personal
Abteilung Infrastruktur, Umweltschutz und Dienstleistungen
Leitungsstab
Presse- und Informationsstab
Stab Organisation und Revision
Steuerungsboard Attraktivität
Gesamtvertrauenspersonenausschuss beim BMVg
Hauptpersonalrat beim BMVg
Militärische Gleichstellungsbeauftragte des BMVg
Gesamtschwerbehindertenvertretung beim BMVg

Kommando Heer	Strausberg
Kommando Luftwaffe	Gatow
Marinekommando	Rostock
Kommado Streikräftebasis	Bonn
Kommando Sanitätsdienst der Bundeswehr	Koblenz
Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr	Koblenz
Bundesamt für Infrastruktur, Umweltschutz und Dienstleistungen der Bundeswehr	Bonn

Bundesamt für das Personalmanagement der Bundeswehr	Köln
Aufstellungsstab Cyber- und Informationsraum (als Vorläufer Kommando CIR)	Bonn
Einsatzführungskommando der Bundeswehr	Schwielowsee
Führungsakademie der Bundeswehr	Hamburg
Planungsamt der Bundeswehr	Berlin
Luftfahrtamt der Bundeswehr	Köln-Wahn
Kompetenzzentrum für Reservistenangelegenheiten der Bw	Bonn

Extern

Der Wehrbeauftragte des Deutschen Bundestages	Berlin
Verband der Reservisten der Bundeswehr	Berlin
Beirat Reservistenarbeit beim VdRBw	Berlin
Deutscher Bundeswehrverband	Berlin

„Cyber-Reserve“ Personal-Pool

Anlage
zum Konzept für die personelle Unterstützung
der „Cyber-Community“ der Bundeswehr
(„Cyber-Reserve“)