Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

18.xxx

Botschaft zum Verpflichtungskredit für das nationale sichere Datenverbundsystem

vom ...

Sehr geehrter Herr Nationalratspräsident
Sehr geehrte Frau Ständeratspräsidentin
Sehr geehrte Damen und Herren

Mit dieser Botschaft unterbreiten wir Ihnen, mit dem Antrag auf Zustimmung, den Entwurf eines Bundesbeschlusses über den Verpflichtungskredit für das nationale sichere Datenverbundsystem.

Wir versichern Sie, sehr geehrter Herr Nationalratspräsident, sehr geehrte Frau Ständeratspräsidentin, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

…

Im Namen des Schweizerischen Bundesrates

Der Bundespräsident: Alain Berset
Der Bundeskanzler: Walter Thurnherr

Übersicht

Die Führungsorgane von Bund, Kantonen, Gemeinden, die für Sicherheit und Rettung zuständigen Behörden und Einsatzorganisationen sowie die Betreiberinnen von kritischen Infrastrukturen sind bei ihrer täglichen Arbeit, vor allem aber bei Katastrophen und Notlagen, auf einen schnellen, gesicherten Austausch von Informationen angewiesen. Im Rahmen der Sicherheitsverbundsübung 2014 wurde festgestellt, dass die heute verfügbaren zivilen Telekommunikationssysteme im Fall einer Strommangellage ausfallen würden oder deutlich eingeschränkt wären. Im Weiteren wurde betont, die fehlende Gesamtdarstellung mit Lagebildern, der Lageverbund, sei ein zu behebender Schwachpunkt der nationalen Ereignisbewältigung. Die strategische Führungsübung 2017 bestätigte diesen Sachverhalt. Zur Schliessung dieser Sicherheitslücke beantragt der Bundesrat mit vorliegender Botschaft einen Verpflichtungskredit von 150 Millionen Franken für die Entwicklung und Beschaffung des nationalen sicheren Datenverbundsystems.

Ausgangslage

Die Veränderung der Risikolandschaft und Bedrohungslage stellen den Bevölkerungsschutz vor neue Herausforderungen. Die Abhängigkeit von einer funktionierenden Stromversorgung wächst stetig. Die Telekommunikationssysteme stehen bei einem Stromausfall nicht mehr zur Verfügung. Neue Risiken wie gezielte Cyberangriffe auf die Behörden oder die Betreiberinnen kritischer Infrastrukturen nehmen global zu. Die Terrorbedrohung hat sich verschärft.

Die heute verfügbaren Telekommunikationssysteme weisen Sicherheitsdefizite auf. Im Rahmen der Sicherheitsverbundsübung 2014 (SVU 14) wurde festgestellt, dass die Telekommunikationssysteme im Fall einer Strommangellage ausfallen würden oder deutlich eingeschränkt wären. Dies ist insbesondere darauf zurückzuführen, dass die benutzten kommerziellen Netze eine geringe oder keine Krisenresistenz aufweisen. Systeme, deren Funktionalität eingeschränkt ist, ermöglichen keinen stabilen, zeitgerechten und verlässlichen Daten- und Informationsfluss. Zusätzlich fehlt ein gesichertes System, das bei einem Erdbeben, einem Kernkraftwerksunfall oder einem Terroranschlag die Gesamtsicht über eine komplexe Lage oder ein gemeinsames Lagebild gewährleisten kann. Diese Erkenntnis wurde im Rahmen der strategischen Führungsübung 2017 (SFU 17) bestätigt.

Gerade bei Katastrophen und Notlagen sind die Führungsorgane, die weiteren involvierten Behörden und Organisationen sowie die Betreiberinnen von kritischen Infrastrukturen auf funktionierende Kommunikationssysteme und ein konsolidiertes Lagebild angewiesen, um die Bevölkerung zu alarmieren, kritische Dienstleistungen aufrechtzuerhalten und rechtzeitig Sicherheitsmassnahmen zum Schutz der Bevölkerung anzuordnen. Sie benötigen Lageinformationen in allen Lagen und Führungssysteme, um schnell und umfassend über die wichtigsten Grundlagen zu verfügen und um die Umsetzung von Schutzmassnahmen sicherstellen zu können.

Um die erkannten Sicherheitsdefizite zu schliessen, bedarf es neuer Telekommunikationssysteme für die Führungsorgane von Bund, Kantonen, Gemeinden, für die für

Sicherheit und Rettung zuständigen Behörden und Einsatzorganisationen sowie für die Betreiberinnen von kritischen Infrastrukturen. Der Bundesrat hat das Eidgenössische Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) am 18. Dezember 2015 beauftragt, eine Auslegeordnung über die Telekommunikationsvorhaben zu erstellen, die für den Schutz der Schweizer Bevölkerung wichtig sind. Im Bericht wird insbesondere aufgezeigt, welche Systeme für den angemessenen Schutz der Schweizer Bevölkerung unentbehrlich sind und damit kurzfristig realisiert oder weiterentwickelt werden sollen. Das VBS hat die Auslegeordnung von September bis Dezember 2016 bei den Kantonen, Bundesstellen, Betreiberinnen von kritischen Infrastrukturen und weiteren Organisationen in Konsultation gegeben und 72 Stellungnahmen dazu erhalten. Die Konsultation hat gezeigt, dass ein gegen Stromausfall und Cyberattacken gehärtetes und gesichertes, leitergebundenes Datenverbundsystem bei den Bundesstellen, den Kantonen und den Betreiberinnen von kritischen Infrastrukturen höchste Priorität hat.

Um die Ausfallsicherheit der Telekommunikationssysteme und des breitbandigen Informations- und Datenaustauschs der Führungsorgane, Sicherheitsbehörden, Einsatzorganisationen und Betreiberinnen von kritischen Infrastrukturen sowie den Schutz vor Cyberangriffen zu erhöhen, soll ein nationales sicheres Datenverbundsystem aufgebaut werden. Dabei handelt es sich um ein Verbundsystem, an dem sich Bund, Kantone und Dritte gemeinsam beteiligen.

Die Regelung der Zuständigkeiten und der Finanzierung des Systems zwischen Bund, Kantonen und Dritten ist in der Botschaft zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes (BZG) enthalten. Die Totalrevision des BZG wird dem Eidgenössischen Parlament in einer separaten Botschaft unterbreitet. Der Bundesrat beabsichtigt, das revidierte BZG, vorbehältlich des Beschlusses des Parlaments, auf den 1. Januar 2020 in Kraft zu setzen. Die vorgeschlagene Lösung entspricht einem breiten Konsens zwischen Bund und Kantonen.

Die vorgeschlagene Entwicklung und Beschaffung des nationalen sicheren Datenverbundsystems hilft massgeblich mit, eine erkannte Sicherheitslücke zu schliessen und damit den Schutz der Bevölkerung zu verbessern.

Inhalt der Vorlage

Mit dem Bundesbeschluss soll das Parlament einen Verpflichtungskredit in der Höhe von 150 Millionen Franken bewilligen. Die Freigabe erfolgt in drei Schritten. Für die erste Etappe sollen Mittel im Umfang von 14,7 Millionen Franken mit dem Bundesbeschluss freigegeben werden. Über die Freigabe der Mittel für die zweite Etappe im Umfang von 83,6 Millionen Franken und für die dritte Etappe im Umfang von 51,7 Millionen Franken kann der Bundesrat aufgrund des Projektfortschritts entscheiden.

Die Investitionen werden bis 2027 getätigt. Das Bundesamt für Bevölkerungsschutz (BABS) ist verantwortlich für die Projektführung, das Projektmanagement und in Delegation ausserdem für die Beschaffungen. Der Verpflichtungskredit umfasst das Projektmanagement, Entwicklungsarbeiten, Hard- und Softwarebeschaffung, Lizenzen, Netzinfrastrukturen sowie Leistungen im Netzmanagement und in der Instandhaltung.

Durch den Betrieb und den Unterhalt des Datenverbundsystems erhöht sich der Funktionsaufwand des BABS im Jahr 2020 um 100 000 Franken, im Jahr 2021 um 600 000 Franken, im Jahr 2022 um 1,5 Millionen Franken, im Jahr 2023 um 7 Millionen Franken, im Jahr 2024 um 10 Millionen Franken, im Jahr 2025 um 12 Millionen Franken, im Jahr 2026 um 13,9 Millionen Franken und ab 2027 um jährlich 15 Millionen Franken. Darin ist der zusätzlich erforderliche Personalaufwand nicht eingerechnet. Der Betrieb und der Unterhalt umfassen Leistungen für die Instandhaltung und den Betrieb des Basisnetzes sowie der 120 geplanten Nutzerstandorte inkl. eines rund um die Uhr aktiven Notbetriebsmanagements. Durch die Ausserbetriebnahme des Meldesystems Vulpus fallen ab 2026 Betriebsaufwände von jährlich 1,5 Millionen Franken weg.

Damit das Projekt innerhalb der zeitlichen, finanziellen und qualitativen Vorgaben umgesetzt und ein sicherer Betrieb des Systems gewährleistet werden kann, sind beim VBS bis zu 30 Vollzeitstellen erforderlich, wovon während der Projektphase. 15 zusätzliche Vollzeitstellen erforderlich sind. Von diesen 15 zusätzlichen Stellen sind bei Projektabschluss 10 Stellen für den technischen Betrieb und Unterhalt, den jährlichen Werterhalt sowie das Management der Leistungsbezüger erforderlich. Diese 10 Stellen werden dauerhaft benötigt.

Inhaltsverzeichnis

Botschaft

1 Ausgangslage und Rahmenbedingungen

1.1 Ausgangslage

Eine sichere Kommunikation und ein gesicherter Austausch von Informationen und Lagebildern zwischen den Führungsorganen, den für die Sicherheit und Rettung zuständigen Behörden, den Einsatzorganisationen sowie den Betreiberinnen von kritischen Infrastrukturen sind von entscheidender Bedeutung, um Ereignisse wirkungsvoll zu bewältigen und die Sicherheit und den Schutz der Bevölkerung in jeder Lage angemessen zu gewährleisten.

Der Austausch von grossen Datenmengen und die Nutzung von Anwendungen erfolgen zurzeit bei Bund und Kantonen über das KomBV-KTV, die kantonalen Polizeinetze und über Netze kommerzieller Anbieter.

Die heute eingesetzten zivilen Informations- und Kommunikationssysteme weisen Sicherheitsdefizite auf. Im Rahmen der SVU 14 wurde festgestellt, dass diese Systeme im Fall einer Strommangellage deutlich eingeschränkt wären und einer Lage mit komplexen Auswirkungen nicht mehr gerecht würden. Die verwendeten Netze bieten keine Sicherheit für einen regelmässigen, zeitgerechten und verlässlichen Daten- und Informationsfluss. Sie können im Ereignisfall wegen Überlastung, Strompannen oder Cyberattacken ausfallen. Zusätzlich fehlt ein gesichertes System für eine Gesamtsicht über eine komplexe Lage, die beispielsweise durch ein Erdbeben, einen Kernkraftwerksunfall oder Terroranschläge verursacht werden kann. Die SFU 17 hat diese sicherheitsrelevanten Mängel bestätigt. Wie aus dem Auswertungsbericht zur SFU 17 vom 9. Mai 2018[1] hervorgeht, ist das fehlende gemeinsame Lagebild ein fundamentaler Schwachpunkt der nationalen Krisenbewältigung. Neben Massnahmen zur Entwicklung eines gemeinsamen Lageverständnisses ist die Weiterentwicklung der technologischen Instrumente zwingend. Daraus resultiert die Empfehlung, dass die laufenden Bestrebungen, die ELD und den Lageverbund zu einer Gesamtlagedarstellung mit Lagebildern für die Lagebeurteilung weiterzuentwickeln, prioritär verfolgt werden müssen.

1.2 Problemlage und Anlass des Finanzbegehrens

Der Bundesrat hat am 1. Dezember 2017 eine Auslegeordnung über die Telekommunikationsvorhaben, die für den Schutz der Schweizer Bevölkerung wichtig sind, zur Kenntnis genommen. Im Bericht vom 29. September 2017[2] wird insbesondere

1 Der Bericht ist im Internet abrufbar unter: www.bk.admin.ch > Dokumentation > Führungsunterstützung > Strategische Führungsübung (SFU).

2 Der Bericht ist im Internet abrufbar unter: www.admin.ch > Dokumentation > Medienmitteilungen > Eingabe: Organisationen: VBS, Datum: 1.12.2017 > Alarmierung und Kommunikation für den Bevölkerungsschutz zukunftsorientiert gestalten > Dokumente > «Bericht zur Zukunft der Alarmierungs- und Telekommunikationssysteme für den Bevölkerungsschutz».

aufgezeigt, welche Systeme für den angemessenen Schutz der Schweizer Bevölkerung unentbehrlich sind und damit kurzfristig realisiert oder weiterentwickelt werden sollen. Die Auswertung von 72 Stellungnahmen zum Bericht hat gezeigt, dass ein gegen Stromausfall und Cyberattacken gehärtetes und gesichertes, leitergebundenes Datenverbundsystem sowie die Ablösung des veralteten Meldesystems Vulpus bei den Bundesstellen (z. B. fedpol, NDB, EZV, MeteoSchweiz, BAFU, BFE, BSTB oder NAZ), bei den Kantonen und bei den Betreiberinnen von kritischen Infrastrukturen (z. B. Swissgrid AG, SBB AG, Schweizerische Nationalbank) höchste Priorität hat und diese möglichst rasch Zugang zum neuen System wünschen.

Mit der Digitalisierung der Kommunikation zwischen den Behörden und der Bevölkerung entstehen nämlich neue Verletzlichkeiten. Die Abhängigkeit von einer funktionierenden Stromversorgung wächst stetig. Die Telekommunikationssysteme stehen bei Stromausfall, verursacht durch technische Fehler oder Naturereignisse, nicht mehr zur Verfügung. Neue Risiken wie Cyberangriffe auf Behörden oder Betreiberinnen von kritischen Infrastrukturen nehmen global zu. Die Terrorbedrohung hat sich verschärft. Gleichzeitig werden analoge Technologien nicht mehr weiter unterhalten, was beispielsweise zur Folge hat, dass das Meldesystem Vulpus von verschiedenen zivilen Sicherheitsbehörden in der Schweiz nicht mehr weiter betrieben werden kann und durch ein neues System ersetzt werden muss.

Der Bundesrat hat an seiner Sitzung vom 1. Dezember 2017 festgehalten, dass die Verfügbarkeit und damit die Ausfallsicherheit der Telekommunikationssysteme und des breitbandigen Datenaustauschs der Führungsorgane, Sicherheitsbehörden und Betreiberinnen von kritischen Infrastrukturen sowie der Schutz vor Cyberangriffen verbessert werden sollen. Dazu soll ein nationales sicheres Datenverbundsystem erstellt werden.

Das nationale sichere Datenverbundsystem soll die Vernetzung zwischen den Bundesstellen, den Kantonen und den Betreiberinnen von kritischen Infrastrukturen breitbandig auch im Fall einer länger andauernden Strommangellage, bei einem Stromausfall oder bei einem Ausfall der kommerziellen Kommunikationsnetze während mindestens zwei Wochen sicherstellen sowie die Integrität und den Schutz gegenüber Cyberattacken wesentlich verbessern. Das Datenverbundsystem besteht aus dem sicheren Datenverbundnetz, dem Datenzugangssystem und dem Lageverbundsystem, das den Austausch von Informationen, inkl. Lagebildern, für die Gesamtlagedarstellung sicherstellt. Letzteres soll das veraltete Meldesystems Vulpus ablösen.

Das nationale sichere Datenverbundsystem basiert im Wesentlichen auf der gehärteten Grundinfrastruktur (Standorte, Glasfaserinfrastruktur) des Führungsnetzes Schweiz. Es verbindet breitbandig rund 120 Nutzerstandorte und verwendet dazu eine andere, schon bestehende Glasfaserinfrastruktur, die sich direkt oder im erweiterten Sinn im Besitz der öffentlichen Hand befindet.

Das Meldesystem Vulpus wird heute von der Armee betrieben. Es kann nach der Betriebsaufnahme des Datenverbundsystems und des Lageverbundsystems abgestellt werden. Durch den Ersatz des veralteten Meldesystems Vulpus durch ein nationales Lageverbundsystem wird den Führungsorganen, Sicherheitsbehörden, Einsatzorganisationen und Betreiberinnen von kritischen Infrastrukturen eine Ge-

samtlagedarstellung mit Lagebildern zur Verfügung gestellt. Dies ist eine entscheidende Führungsgrundlage, damit Ereignisse mit komplexen, interkantonalen, gesamtschweizerischen oder internationalen Auswirkungen schnell und effizient bewältigt werden können.

Das nationale sichere Datenverbundsystem soll zukünftig für grosse Datenmengen die Grundlage für alle sicherheitspolitisch relevanten Telekommunikationssysteme bilden. Damit wird es zum zentralen Transportnetz für Daten und Informationen im Bevölkerungsschutz und im nationalen Krisenmanagement in allen Lagen (z. B. auch bei Terroranschlägen). So ist u. a. vorgesehen, auch die Sicherheitssysteme Polycom, Polyalert und das Notfallradio IBBK auf das sichere Datenverbundsystem zu migrieren. Es steht damit den Behörden auch für den Austausch von sicherheitsrelevanten Informationen im täglichen Gebrauch zur Verfügung. Auch das KomBV–KTV kann als separates Kommunikationsnetz die Sicherheitsinfrastruktur des nationalen sicheren Datenverbundnetzes nutzen und erhält damit im gemeinsam genutzten Bereich eine verbesserte Stromsicherheit.

Vorgesehen sind gemäss aktueller Planung die Erschliessung von 120 Nutzerstandorten bei Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen. In Zukunft können bei Bedarf und Erfüllung der Anschlussvoraussetzungen weitere Standorte erschlossen werden.

1.3 Bedeutung des zu finanzierenden Vorhabens

Die Verletzlichkeit des breitbandigen Informations- und Datenaustauschs der Führungsorgane, Sicherheitsbehörden, Einsatzorganisationen und Betreiberinnen von kritischen Infrastrukturen stellt ein grosses Sicherheitsrisiko dar.

Um Ereignisse wirkungsvoll zu bewältigen, spielen die Kommunikation und eine schnelle und sichere Darstellung der Gesamtlage, inkl. Lagebildern, eine zentrale Rolle. Bereits bei grösseren Ereignissen, wie sie in der Schweiz in den letzten Jahren vorkamen (Vivian 1990 oder Lothar 1999, Hitzewellen 2003 und 2015, Hochwasser 2005 und 2007, Ausfall der SBB 2005, Schweinegrippe 2009, Waldbrand Visp 2011, Bergsturz Bondo 2017), nimmt die Bedeutung der Zusammenarbeit verschiedener Behörden, Einsatzkräfte und Betreiberinnen von kritischen Infrastrukturen zu. Dies erfordert eine gute Vernetzung und Lageinformation aller Beteiligten. Die SVU 14 und die SFU 17 haben dieses Erfordernis bestätigt.

Erfahrungen aus dem Ausland haben gezeigt, dass Ereignisse mit komplexen Auswirkungen (z. B. Erdbeben, Terroranschläge) nur effizient und schnell bewältigt und weitere Verletzte, Todesopfer und Sachschäden nur verhindert werden können, wenn rasch eine umfassende Lageübersicht für alle involvierten Akteure zur Verfügung steht. Dazu dient ein Lageverbund, der die bestehenden Lagesysteme von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen vernetzt und die Informationen aus den verschiedenen Systemen zu einer Gesamtlagedarstellung mit Lagebildern automatisiert zusammenführt. Dieses System kann gleichzeitig das im Einsatz stehende, veraltete Meldesystem Vulpus ersetzen.

Mit dem Aufbau des nationalen sicheren Datenverbundsystems wird das heute bestehende Sicherheitsdefizit beim Austausch von Informationen und Lagebildern zwischen den involvierten Stellen behoben, das Ausfallrisiko der Systeme wesentlich reduziert und die Sicherheit für die Bevölkerung erhöht. Das sichere Datenverbundsystem bringt aber auch einen erheblichen Sicherheitsgewinn im Alltag. Beispielsweise können die für den Betrieb der Flughäfen erforderlichen Informationen von MeteoSchweiz mit einer wesentlich höheren Sicherheit bzw. Verfügbarkeit ausgetauscht werden.

1.4 Interesse des Bundes am Vorhaben

Im Rahmen ihrer Zuständigkeiten arbeiten im Bevölkerungsschutz der Bund und die Kantone sowie weitere Stellen zusammen, namentlich im Bereich der Alarmierungs- und der Kommunikationssysteme. Die Interoperabilität dieser Systeme und sichere Verbindungen zwischen diesen Stellen sind im Interesse aller. Mit der Bereitstellung der zentralen Komponenten für das nationale sichere Datenverbundsystem sichert der Bund die Interoperabilität der Systeme, bietet er den Bundesstellen, Kantonen und Betreiberinnen von kritischen Infrastrukturen die Möglichkeit, ihre eigenen Systeme an ein Gesamtsystem anzuschliessen und legt er die Grundlage für eine gesicherte, breitbandige Vernetzung. So hat beispielsweise die Schweizerische Nationalbank in ihrer Stellungnahme zur Auslegeordnung der bevölkerungsschutzrelevanten Telekommunikationssysteme festgehalten, dass die Realisierung des nationalen sicheren Datenverbundsystems einen wesentlichen Beitrag zur operativen Resilienz des Finanzplatzes Schweiz beitragen würde. Nicht zuletzt kann nach Realisierung des sicheren Datenverbundsystems zusammen mit dem Lageverbundsystem das veraltete Meldesystem Vulpus abgelöst werden.

Bei nationalen Katastrophen und Notlagen hat auch der Bund eine bestimmte Führungsverantwortung. Diese kann er wesentlich zielführender ausüben, wenn er mit den kantonalen Führungsorganen und den Betreiberinnen von kritischen Infrastrukturen gesichert verbunden ist und über ein Bild der konsolidierten Gesamtlage verfügt.

1.5 Zukunftsperspektiven

Der Aufbau des nationalen sicheren Datenverbundsystems wird den Einsatz digitaler Hilfsmittel bei der Ereignisbewältigung fördern. Durch die Härtung des Systems gegen Stromausfall und den Schutz vor Cyberrisiken lassen sich die Vorteile der digitalen Entwicklungen im Bereich der Kommunikation und des Informationsaustauschs aufgrund seiner Resilienz im Bereich der Sicherheit besser nutzen. Dadurch werden die Einsatzeffizienz und der Schutz der Bevölkerung verbessert.

Es ist denkbar, dass das Kommunikationssystem Polycom dereinst durch ein mobiles breitbandiges Sicherheitskommunikationssystem abgelöst wird, sofern die Standardisierung von Sprachfunkanwendungen für die digitale Breitbandkommunikation erfolgt ist. Damit das Bedürfnis für eine sichere und resiliente Datenkommunikation bis zum mobilen Endgerät für die Einsatzorganisationen landesweit harmonisiert

abgedeckt werden kann, könnte bedarfsorientiert eine mobile Verlängerung des sicheren Datenverbundsystems mit eingeschränkter Kapazität in Betracht gezogen werden. Da das nationale sichere Datenverbundsystem resilient gegenüber Stromausfällen und Cyberattacken sein wird, hätten die Nutzer damit ein durchgängig sicheres und hochverfügbares Transportnetz mit mobilem Anteil, das in allen Lagen zur Verfügung stünde.

Das sichere Datenverbundnetz stellt für andere Nutzer, die einen hohen Anspruch an die Verfügbarkeit im Fall von Strom- und IKT-Ausfällen stellen, einen Mehrwert dar. Es kann verschiedenen anderen Systemen als Übertragungsplattform dienen und die Ausfallsicherheit dieser Systeme signifikant verbessern.

Zudem können mit einem bestehenden sicheren Datenverbundnetz weitere Redundanzen mit anderen Netzen geprüft und allenfalls abgebaut werden. In Bereichen wie der Energieversorgung und dem Finanzplatz Schweiz könnte das System als redundantes Datentransportnetz verwendet und so die Resilienz dieser kritischen Sektoren gesteigert werden. Daneben bestehen etliche weitere sicherheitsrelevant Nutzungsmöglichkeiten des nationalen sicheren Datenverbundsystems.

Nicht Bestandteil der vorliegenden Botschaft ist das Erfordernis, auf einem Teil der getätigten Investitionen periodisch Werterhaltungsmassnahmen mit Investitionscharakter vorzunehmen. Diese gingen gemäss der in der Botschaft vom …[3] zur Totalrevision des Bevölkerungs- und Zivilschutzgesetzes (BZG-Botschaft) vorgeschlagenen Finanzierungsregelung zulasten des Bundes. Dazu wird zu gegebener Zeit wiederum ein Verpflichtungskredit beantragt.

1.6 Einbezug der interessierten Kreise

Nach Artikel 2 Absatz 1 des Vernehmlassungsgesetzes vom 18. März 2005[4] (VlG) wird mit der Durchführung einer Vernehmlassung bezweckt, dass die Kantone, die politischen Parteien und interessierte Kreise an der Meinungsbildung und Entscheidfindung des Bundes mitwirken können. Obschon es sich um ein Vorhaben von grosser finanzieller Tragweite handelt, wurde auf die Durchführung eines Vernehmlassungsverfahrens verzichtet. Im Vorfeld dieser Botschaft wurden bereits umfangreiche Konsultationen zu den Systemen durchgeführt. Es werden deshalb keine neuen Erkenntnisse in einer zusätzlichen Konsultation erwartet.

Im Rahmen der Erstellung und der Konsultation des Berichts zur Zukunft der Telekommunikationssysteme im Bevölkerungsschutz wurden die relevanten Stellen von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen sowie Verbände und Organisationen der Zivilgesellschaft zur Priorisierung der Systeme konsultiert. Insgesamt sind 72 Stellungnahmen eingegangen. Die Konsultation hat gezeigt, dass das sichere Datenverbundsystem, die Ablösung des veralteten Meldesystems Vulpus sowie die Erstellung eines Lageverbundsystems von höchster Priorität sind. Es wurde gefordert, dass bei all diesen Vorhaben die Kosten möglichst zu konkretisie-

3 BBl …
4 SR **172.061**

ren sind, sobald der politische Grundsatzentscheid über die Realisierung der Vorhaben getroffen ist.

Im Rahmen der Spezifikation des Lageverbundsystems wurden in der Initialisierungsphase unter Einbezug von mitinteressierten Stellen des Bundes und der Kantone verschiedenste Arbeiten und Abklärungen gemacht. Dazu gehörte eine schriftliche Umfrage bei 18 Stellen des Bundes und 59 Stellen der Kantone. In fünf Plenarworkshops mit jeweils mehr als 100 Adressaten wurden die Erwartungen und Grobanforderungen an das System besprochen und vertieft. Die Resultate wurden anschliessend in einer Studie niedergeschrieben. Nebst der Studie wurden auch eine technische Beschreibung der Systemarchitektur sowie eine Zweckbestimmung des Systems verfasst. Ein Umsetzungskonzept beschreibt das Vorhaben für die strategische Stufe. Als letzter Schritt hat das BABS bei der Industrie eine Umfrage zur Schaffung eines elektronischen Lageverbunds durchgeführt. Die Resultate zeigen, dass die Industrie das Vorhaben als technisch, betrieblich und organisatorisch nutzbringend und gut umsetzbar einschätzt.

Die Abklärungen haben gezeigt, dass bei der Ablösung des Meldesystems Vulpus und der Schaffung eines Lageverbundsystems ein grosses Synergiepotenzial besteht. Mit einer modernen Systemlösung für die Ablösung von Vulpus können die für das Lageverbundsystem erforderlichen Funktionalitäten ebenfalls weitgehend erfüllt werden.

Für die Klärung der Zuständigkeiten und Finanzierungsfragen haben der Departementsvorsteher des VBS sowie die Präsidenten der KKJPD und RK MZF am 10. Januar 2017 eine aus Vertretern von Bund und Kantonen zusammengesetzte Arbeitsgruppe einberufen. Dabei konnten eine Konsenslösung gefunden und die grundsätzliche Finanzierung bei den Kantonen vereinbart werden.

2 Inhalt des Kreditbeschlusses

2.1 Antrag des Bundesrates

Das nationale sichere Datenverbundsystem ist ein Schlüsselprojekt im Bereich der Informations- und Kommunikationstechnologie des Bundes. Der Bundesrat beantragt dafür einen Verpflichtungskredit von 150 Millionen Franken. Der Bund übernimmt dabei die Investitionen für die Entwicklung und Beschaffung der zentralen Komponenten des Systems, d. h. derjenigen Komponenten, die von allen Nutzern (Bundesstellen, Kantonen, Betreiberinnen von kritischen Infrastrukturen) gemeinsam beansprucht werden.

Der Verpflichtungskredit soll in drei Etappen freigegeben werden. Mit der Genehmigung des Verpflichtungskredits soll das Parlament 14,7 Millionen Franken für die erste Etappe freigeben. Über die Freigabe der Mittel der zweiten Etappe über 83,6 Millionen Franken und der Mittel der dritten Etappe über 51,7 Millionen Franken soll der Bundesrat gestützt auf den Projektfortschritt entscheiden.

2.2 Beschreibung des Inhalts der Vorlage im Einzelnen

Das nationale sichere Datenverbundsystem beinhaltet:

a. das sichere Datenverbundnetz;

b. das Datenzugangssystem; sowie

c. das Lageverbundsystem, das das veraltete Meldesystem Vulpus funktionell ablösen soll.

2.2.1 Das sichere Datenverbundnetz

Das sichere Datenverbundnetz soll als Transportnetz (Layer 1 und 2) für die breitbandige Datenkommunikation die Grundlage für alle sicherheitspolitisch relevanten Telekommunikationssysteme des Bevölkerungsschutzes bilden. Das System soll die Vernetzung zwischen den Bundesstellen, Kantonen und Betreiberinnen von kritischen Infrastrukturen breitbandig auch im Fall einer länger andauernden Strommangellage, bei Stromausfall oder beim Ausfall der kommerziellen Kommunikationsnetze während mindestens zwei Wochen autonom sicherstellen. Mit dem Verpflichtungskredit werden 120 Nutzerstandorte an dieses gesicherte Netz angeschlossen. Jeder Nutzerstandort wird von mindestens zwei gehärteten Netzknoten aus erschlossen. Für Bundesstellen wie fedpol, NDB, EZV, GWK, BAFU, BFE, MeteoSchweiz, BSTB oder NAZ sind 40 Anschlüsse eingeplant, für die Betreiberinnen von kritischen Infrastrukturen wie Flughäfen, SBB AG, Swissgrid AG, Schweizerische Nationalbank, Radio- und Rundfunkstationen, Migros Genossenschaften, Coop AG usw. und Dritte, beispielsweise das Fürstentum Liechtenstein, sind 44 Anschlüsse vorgesehen. 36 Anschlüsse sind für die Kantone (mindestens ein Anschluss pro Kanton) geplant. Die kantonalen Anschlüsse werden in der Regel in den kantonalen Alarm- und Einsatzzentralen der Polizei installiert, die bereits gegen Stromausfall gehärtet sind.

Sofern die Sicherheitsanforderungen eingehalten werden, können die Nutzer gemäss ihren Bedürfnissen ihre eigenen, z. B. kantonalen Netze an ihren Anschluss anschliessen und so verschiedene kantonale Stellen miteinander vernetzen. Damit kann auch mehreren Fachstellen innerhalb des Nutzerkreises, z. B. innerhalb eines Kantons, eines Betriebs oder einer Verwaltungseinheit, Zugang zum System ermöglicht werden. Für die Konzipierung dieser dezentralen Komponenten und die Stromausfallsicherheit der einbezogenen Fachstellen sind die Nutzer selber verantwortlich.

Gemäss dem Bundesratsentscheid vom 20. Mai 2015 soll die Realisierung des sicheren Datenverbundnetzes soweit möglich auf den physischen Infrastrukturen des Führungsnetzes Schweiz basieren, d. h. Glasfaserinfrastrukturen sowie gehärteten Standorten. Es wird so realisiert, dass der Datenverkehr der Armee auf dem Führungsnetz Schweiz physisch vollständig vom Datenverkehr der Nutzer des nationalen sicheren Datenverbundsystems getrennt ist. Damit wird den Sicherheitsbedürfnissen der Armee und den Nutzern des Systems Rechnung getragen. Für die Erschliessung der Nutzerstandorte werden zusätzlich Glasfaserinfrastrukturen von Bund (z. B. Nationalstrassen), Kantonen oder Betreiberinnen kritischer Infrastruktu-

ren genutzt. Wo die Erschliessung der Nutzerstandorte nicht mit bestehenden Glasfaserinfrastrukturen realisiert werden kann, werden neue Glasfaserstrecken gebaut. Bei der Planung werden insbesondere diejenigen Netzinfrastrukturen in die Konzeption miteinbezogen, die bereits den Anforderungen an die Stromausfallsicherheit genügen, d. h. über eine entsprechende Notstromversorgung verfügen. Ansonsten wird die Stromausfallsicherheit der miteinbezogenen Drittnetze überprüft und unter Umständen verbessert. Eine Realisierung auf einem kommerziellen Netz wäre mit sehr hohen Kosten verbunden, weil sämtliche einbezogenen Knoten im Netz und ein Anteil Glasfaserstrecken gehärtet sowie umfangreiche Spleissarbeiten ausgeführt werden müssten. Durch die Nutzung der physischen Infrastrukturen des Führungsnetzes Schweiz, die bereits heute eine hohe Robustheit und Energieautonomie aufweisen, sowie dessen Verbund mit weiteren bestehenden Glasfaserinfrastrukturen im Eigentum der öffentlichen Hand können weitgehende Synergien genutzt und in der Folge ein verhältnismässig kostengünstiges Netz aufgebaut werden, das den Vorgaben an die Stromausfallsicherheit gerecht wird.

2.2.2 Das Datenzugangssystem

Das Datenzugangssystem ist ein geschlossenes Anwendernetz (Layer 3). Unter geschlossenen Anwendernetzen werden isolierte logische Netze verstanden, die keine Übergänge ins Internet oder andere Netze haben. Mit dem Datenzugangssystem wird den Nutzern in Zukunft der sichere und in allen Lagen garantierte Zugang zu den bevölkerungsschutzrelevanten Alarmierungs- und Telekommunikationssystemen gewährleistet. Für die Nutzung der Anwendungen werden dedizierte Endgeräte eingesetzt. Da es sich um ein geschlossenes Netzwerk handelt, ist keine Koordination mit anderen Netzen notwendig. Auf dem sicheren Datenverbundnetz können in Kombination mit dem Datenzugangssystem alle bevölkerungsschutzrelevanten Anwendungen (bestehende und zukünftige) in allen Lagen sicher betrieben werden. Anwendungen in diesem Netz sind beispielsweise das Polycom für den Sprachfunk und das Polyalert für die Alarmierung sowie weitere sicherheitsrelevante Systeme und Applikationen. Durch die Isolation von allen anderen Netzen, beispielsweise dem Internet, wird die Resilienz gegenüber Cyber-Angriffen signifikant erhöht.

2.2.3 Die Ablösung des Meldesystems Vulpus und das Lageverbundsystem

Beim sicheren Datenverbundnetz handelt es sich, vereinfacht gesagt, um die Hardware, beim Datenzugangssystem um das Betriebssystem. Für die eigentliche Datenkommunikation braucht es noch eine Anwendung. Es ist vorgesehen, diese Anwendung als Ablösung für das veraltete Meldesystem Vulpus zu realisieren. Dabei handelt es sich um ein geschütztes, ziviles Meldesystem von Bund, Kantonen und Dritten, das von ca. 70 Stellen genutzt wird. Es dient seit rund 30 Jahren dem Informationsaustausch (v. a. Textmeldungen) der Bundesanwaltschaft, der kantonalen Polizeikorps, der Stadtpolizei Zürich, des Grenzwachtkorps, der militärischen Sicherheit, der NAZ, des NDB, verschiedener Sonderstäbe des Bundesrates, des

BABS und verschiedener Alarmformationen. Es wird heute bei der Alarmierung, der Alarmfahndung und beim Vermitteln der Naturgefahrenwarnungen der Fachstellen des Bundes unter Einbezug der Medien (Radiostationen) eingesetzt. Das System wird im Tagesgeschäft der genannten Organisationen und Behörden verwendet. Es wird heute von der Armee und der RUAG betrieben und auch im Wert erhalten. Das System ist nicht gegen Stromausfall gesichert. Es basiert auf dem Telefonienetz der Swisscom. Der Weiterbetrieb der Anschlüsse kann mit verschiedenen Massnahmen längstens bis 2025 sichergestellt werden. Die Armee und der NDB haben keinen Bedarf mehr am Meldesystem Vulpus.

Die Funktionen des Meldesystems Vulpus sind von zentraler Bedeutung für die Kommunikation der Behörden und müssen auch in Zukunft im Tagesgeschäft sowie in Katastrophen und Notlagen zur Verfügung stehen. Das System ist veraltet und soll darum durch ein neues Datenkommunikationssystem abgelöst werden. Dieses muss auch komplexe Lageinformationen, Daten oder Lagebilder austauschen können, um eine Gesamtlage darzustellen.

Mit dem nationalen Lageverbund wird deshalb ein System entwickelt, das die bisherigen Funktionen des Meldesystems Vulpus nicht nur ersetzt, sondern als weitere Funktion auch den Austausch von komplexen Informationen, beispielsweise die Funktion einer Gesamtlagedarstellung mit Lagebildern, enthält.

Die verschiedenen Organisationen, die in die Bewältigung von Katastrophen und Notlagen involviert sind, nutzen bereits elektronische Lagesysteme (Fach- und Führungssysteme). Dazu gehört beispielsweise auch die ELD, die von der NAZ im BABS betrieben wird und schwerpunktmässig auch vom NDB, fedpol und von kantonalen Stellen genutzt wird. Diese Systeme sind zwar auf die spezifischen Aufgaben und Bedürfnisse der jeweiligen Organisationen zugeschnitten, untereinander aber gar nicht oder ungenügend vernetzt. Daneben gibt es zahlreiche Organisationen, die derzeit über kein eigenes ELD-System verfügen. Dieses Lageverbundsystem wird auf dem sicheren Datenverbundnetz und dem Datenzugangssystem realisiert. Die Ausfallsicherheit und der Schutz des Systems vor Cyberangriffen sind somit sichergestellt und gegenüber dem Meldesystem Vulpus signifikant erhöht. Die Armee wird über Schnittstellen an das Lageverbundsystem angeschlossen, was ihr insbesondere Informationen über die zivile Lage ermöglicht und die Zusammenarbeit der zivilen und militärischen Stellen, z. B. bei einem Terroranschlag oder einem Katastrophenereignis, wesentlich verbessert.

2.2.4 Investitionen

Für den Aufbau des nationalen sicheren Datenverbundsystems ist eine enge Zusammenarbeit mit einer Vielzahl von verschiedenen Stakeholdern (Bundesstellen, Kantonen, Betreiberinnen von kritischen Infrastrukturen), verschiedenen Lieferanten und Eignern von Glasfaserkabel sowie Eigentümerinnen und Eigentümern von Immobilien notwendig. Im Verpflichtungskredit sind auch die Investitionsausgaben für bauliche Massnahmen enthalten (vorwiegend im Bereich der Netzinfrastruktur und der Nutzerstandorte des Bundes). Die Umsetzung erfolgt in Zusammenarbeit mit dem Bau- und Liegenschaftsorgan des Bundes.

Das VBS benötigt daher für das Projektmanagement bis zum Projektabschluss externe Unterstützung durch verschiedene Fachexpertinnen und -experten. Sie unterstützen das projektverantwortliche BABS während der Aufbauphase, bei der Koordination des Projekts, bei der Planung sowie bei der Erarbeitung von Lieferobjekten (z. B. Anforderungen, Stakeholdermanagementkonzepten, Rechtsgutachten, Verträgen und Service Level Agreements, Projekthandbüchern, Sicherheitskonzepten, Standortanalysen, Ausschreibungsunterlagen, Aufbau der Governance-Strukturen für die Führung in der Nutzungsphase, Durchführung von Tests, Abnahme von Systemen, Controllingaufgaben). Die veranschlagten Projektmanagementkosten sind im Vergleich zu anderen Projekten verhältnismässig hoch. Dies ist einerseits damit zu begründen, dass das Projekt zusammen mit einer Vielzahl von Stakeholdern aus der Bundesverwaltung, den Kantonen und Dritten umgesetzt werden muss. Gleichzeitig werden im Vorhaben massgebliche Synergien mit dem Führungsnetz Schweiz genutzt (Backbone, Glasverbindungen, gehärtete Standorte, NCC, PRZ, SOC), was die Kosten für die Netzinfrastruktur senkt, die Managementkosten aber erhöht.

Der Hauptanteil an den Entwicklungsarbeiten umfasst die Entwicklung der Software für das Lageverbundsystem sowie die Programmierung der Schnittstellen zwischen den zentralen Komponenten des Systems und den dezentralen Lagedarstellungssystemen, die bereits in den Kantonen und bei den Betreiberinnen von kritischen Infrastrukturen in Betrieb sind. Für das Netz wird ein Knoten- und Netzwerkdesign erstellt, und für das Datenzugangssystem muss ein IP-Netzwerk aufgebaut werden. Neben den technischen Entwicklungsarbeiten sind im Rahmen der Konzeptphase für jedes der vier Vorhaben verschiedene Analysen durchzuführen (Systemanalysen, technische Analysen, rechtliche Abklärungen usw.), um das System zu konzipieren. Diese Analysen dienen als Grundlage für die Erstellung der Lieferprodukte in der Konzeptphase nach der Projektmanagementmethode Hermes sowie die Entwicklung von normativen Vorgaben und Standards.

Für den Aufbau des Systems muss Hardware für das NCC, das SOC und das PRZ beschafft werden. Es wird eine konfigurierte Software (Betriebssystem) für das Datenzugangssystem sowie die erforderlichen Lizenzen von Software (z. B. Virenprogramm) für den Betrieb des Datenzugangssystems und des Lageverbundsystems beschafft. Die Kosten sind im Vergleich zu den Entwicklungskosten tief, weil Synergien im Bereich der Hardware und Software mit dem Führungsnetz Schweiz genutzt und existierende Produkte auf dem Markt beschafft werden können.

Die Netzinfrastruktur des Führungsnetzes Schweiz (Backbone) wird für das Datenverbundnetz und das Zugangssystem mit zusätzlicher Netzinfrastruktur ausgerüstet werden (Aktivkomponenten wie Multiplexer, Router, Switches).

Für die redundante Anbindung der Nutzerstandorte an das Führungsnetz Schweiz (Backbone) werden – quasi für die «letzte Meile» – z. T. Glasfaserstrecken neu gebaut, weil auf diesen Abschnitten keine bestehenden Glasfaserleitungen genutzt werden können.

An den 120 Nutzerstandorten werden Netzwerkkomponenten (Switches, Router) für alle Vorhaben installiert, um den Übergang zwischen der zentralen Komponente und den dezentralen Komponenten (Anschluss) zu gewährleisten.

Aufgrund der Anforderungen an die Infrastruktur hinsichtlich Verfügbarkeit und Vertraulichkeit sind Investitionen für die Härtung der Nutzerstandorte des Bundes erforderlich. Insbesondere muss die Stromversorgung über zwei unabhängige, voneinander separat geführte Stromeinführungen sichergestellt werden, und bei Ausfall der externen Stromversorgung muss eine Eigenstromanlage die notwendige Autonomie gewährleisten. Da die Sicherstellung der Energieversorgung der Nutzerstandorte Aufgabe der jeweils angeschlossenen Nutzer ist, werden diese Investitionen vom Bund bei seinen eigenen Standorten selber getätigt.

Das Netzmanagement beinhaltet das Leistungsmanagement, das Konfigurationsmanagement sowie das Fehlermanagement. Als zentrale Instanz zur dauerhaften Überwachung und Kontrolle sowie Steuerung der Prozesse und Funktionen werden zwei technisch, betrieblich und geografisch redundante NCC benötigt. Im Rahmen der Projektphase wird konzeptionell abgeklärt, auf welche bereits bestehenden NCC dabei aufgebaut werden kann. Die Erkennung und Bewertung von potenziellen Angriffen aus dem Cyber-Raum wird im SOC sichergestellt. Ein RPZ ist notwendig, um Änderungen vor der Einbringung in die Wirkungsumgebung zu testen und Fehlerbilder zur Mängelbehebung simulieren zu können.

Die Entwicklung und der Aufbau des nationalen sicheren Datenverbundsystems erfolgen aus der Perspektive der Informationstechnologien über einen verhältnismässig langen Zeitraum mit vielen unterschiedlichen Nutzern. Die Realisierung ist mit Unsicherheiten verbunden. Das Vorhaben befindet sich gemäss Hermes in der Initialisierungsphase. Dem BABS stehen keine Planungskredite zur Verfügung, um diese Unsicherheiten zu reduzieren. Erst nach dem politischen Entscheid zur Umsetzung des Vorhabens stehen die notwendigen Mittel für die Projektphase, in der weitere konzeptionelle Klärungen erfolgen, bereit. Da sich das Vorhaben aber noch nicht in der Projektphase befindet, wird zum jetzigen Zeitpunkt der entsprechende Risikozuschlag mit 15 Prozent veranschlagt.

Für die Investitionen in die Entwicklung und die Beschaffung beantragt der Bundesrat für den Zeitraum 2020–2027 einen Verpflichtungskredit von 150 Millionen Franken. Der Verpflichtungskredit setzt sich wie folgt zusammen:

Tabelle 1

Investitionsausgaben für die Entwicklung und die Beschaffung

	Mio. Fr.
Projektmanagement	29,5
Entwicklungsarbeiten	17,7
Hardware, Software, Lizenzen	14,8
Netzinfrastruktur Backbone	6,4
Netzinfrastruktur Nutzerstandorte	35,7
Netzmanagement	8,3
Nutzerstandorte Bund	18,0
Risikozuschlag (15 %)	19,6
Investitionen für Entwicklung und Beschaffung	**150,0**

2.2.5 Staffelung und Freigabe

Der Verpflichtungskredit wird in drei Etappen freigegeben. Die Etappierung entspricht der Empfehlung an den Bundesrat, die die EFK im Rahmen ihres Berichts «Prüfung des IKT-Schlüsselprojektes Verbrauchssteuerplattform» vom 16. Oktober 2015[5] abgegeben hat, sowie einer entsprechenden Forderung der FinDel vom März 2014 und dem Bundesratsbeschluss vom 21. Mai 2014 zum zugehörigen Antwortschreiben.

Durch die Aufteilung in drei Etappen wird nur der Teil zur Umsetzung freigegeben, für den zum Zeitpunkt der Freigabe die Voraussetzungen erfüllt sind. Damit verfügt der Bundesrat über eine wirksame finanzielle Steuerung und kann in zeitlich abgegrenzten Etappen die Projektumsetzung freigeben.

Ziel der ersten Etappe von 2020 bis 2021 ist die Konkretisierung der vier Teilvorhaben. In dieser Phase werden die Lieferprodukte der Konzeptphase nach Hermes erarbeitet. Insbesondere werden die Realisierbarkeit bestätigt, die Kosten für das System bzw. die Teilsysteme sowie der Personalbedarf geschärft und die Risiken reduziert. Dazu wird ein Proof of Concept durchgeführt. Zudem werden die Sicherheitsbedingungen für die Anschlüsse festgelegt. Da das Meldesystem Vulpus aus technischen Gründen Ende 2025 abgestellt werden muss, wird bereits in der ersten Etappe die für die Ersatzbeschaffung notwendige WTO-Ausschreibung so weit vorbereitet, dass nach der Freigabe der zweiten Etappe der Zuschlag erteilt werden kann.

5 Der Bericht ist im Internet abrufbar unter: www.efk.admin.ch > Publikationen > Informatikprojekte > Archiv Informatikprojekte.

Über die Freigabe der finanziellen Mittel für die erste Etappe befinden die eidgenössischen Räte mit dem vorliegenden Bundesbeschluss. Die Kosten für die erste Etappe belaufen sich auf 14,7 Millionen Franken.

Ziel der zweiten Etappe von 2022 bis 2024 sind der Aufbau eines Testbetriebs und die anschliessende Inbetriebnahme des Netzes. Dafür ist es notwendig, das Datenzugangssystem zu entwickeln und in Betrieb zu nehmen. Die Hauptnutzer des Meldesystems Vulpus werden 2024/2025 an das Netz angeschlossen, damit die Ablösung des Systems Anfang 2026 eingeführt werden kann. Es ist vorgesehen, nach Abschluss der Einführungsphase und des aus Sicherheitsüberlegungen einjährigen Parallelbetriebs des alten und des neuen Systems Ende 2025 den Betrieb des Meldesystems Vulpus einzustellen. Dies ist auch insofern eine Randbedingung, weil das System dann am Ende seiner Lebenszeit angelangt ist. Eine weitere Betriebsverlängerung wäre mit unverhältnismässigen Mehrkosten verbunden. 2023 und 2024 werden die ehemaligen Vulpus-Nutzerinnen und -Nutzer auf den neuen Systemen ausgebildet.

Der Antrag für die Freigabe der Mittel für die zweite Etappe im Umfang von 83,6 Millionen Franken wird der Generalsekretärenkonferenz zur Beurteilung und anschliessend dem Bundesrat zum Entscheid unterbreitet. Die Kriterien für die Freigabe sind:

- Die Konzeptphase nach Hermes ist abgeschlossen.
- Die Realisierbarkeit ist bestätigt, die Kosten für das System bzw. die Teilsysteme und der Personalbedarf sind konkretisiert und die Einführungsrisiken sind beurteilt.
- Der PoC für das Netz und das Zugangssystem ist abgeschlossen.
- Die Anschlussbedingungen für Bund, Kantone und Betreiberinnen von kritischen Infrastrukturen sind festgelegt.
- Die WTO-Ausschreibung für die Ablösung des Meldesystems Vulpus und die Vorbereitung für den Zuschlag sind erfolgt.

In der dritten Etappe von 2025 bis 2027 werden die in der zweiten Etappe noch nicht angeschlossenen Nutzerinnen und Nutzer an das Netz angeschlossen und das Datenzugangssystem weiterentwickelt. Für die Integration der verschiedenen ELD-Systeme werden Schnittstellen entwickelt und dann sukzessive an das Lageverbundsystem angeschlossen. Gleichzeitig wird das Set von Funktionalitäten für den Lageverbund erweitert, z. B. die Funktion zur Darstellung von geografischen Informationen. Nach Projektende im Jahr 2027 werden 2028 noch notwendige Abschluss- und Garantiearbeiten ausgeführt.

Die Freigabe der Mittel für die dritte Etappe im Umfang von 51,7 Millionen Franken wird erneut der Generalsekretärenkonferenz zur Beurteilung und anschliessend dem Bundesrat zum Entscheid unterbreitet. Die Kriterien für die Freigabe sind:

- Das Datenverbundnetz ist operativ und die Betriebsprozesse sind konsolidiert.
- Die Infrastruktur der ursprünglichen Hauptnutzerstandorte sind gehärtet und an das Netz angeschlossen.

– Die Ablösung des Meldesystems Vulpus ist eingeführt.
– Ein erstes Funktionalitätenset für das Lageverbundverbundsystem ist umgesetzt und im Probebetrieb.

Tabelle 2

Aufteilung des Verpflichtungskredites auf die drei Etappen (in Millionen Franken)

	Etappe 1	Etappe 2	Etappe 3
Total	14,7	83,6	51,7

2.2.6 Betrieb und Unterhalt

Damit die Verfügbarkeit und die Sicherheit während der ganzen Lebensdauer sichergestellt werden können, muss das System laufend den aktuellen Standards angepasst und instand gehalten werden. Dies beinhaltet die Reparatur und den Ersatz von Hardware (z. B. nach Elementarschäden oder technischen Defekten) sowie Sicherheitsupdates und Installationen von neuen Software-Releases. Die dazu notwendigen Dienstleistungen wie Inspektionen, Wartung, Reparaturen, Entwicklungen und Updates werden durch externe Fachdienstleister bzw. Fieldforceorganisationen schweizweit und permanent sichergestellt. Die Spezialisten arbeiten gemäss den Standards der Informatikbranche und den speziellen Anforderungen des Systems.

Für Reparaturen, Wartung, den Ersatz von Komponenten sowie Software-Releases und Updates, Mietkosten usw. während eines Lebenszyklus der Systeme sind 15 Prozent der jährlich anfallenden Betriebs- und Unterhaltsaufwände eingeplant. Für die Betriebs- und Unterhaltskosten der unterschiedlichen Netzelemente an den Nutzerstandorten wird mit fünf Prozent der installierten Basis gerechnet. Dafür steht eine Fieldforce mit verschieden Rollen an 365 Tagen 24 Stunden im Einsatz. Mit den Leistungserbringern und Lieferanten sind entsprechend umfassende Wartungs- und Serviceverträge abzuschliessen. Bei den Glasfaserstrecken von Kantonen und Dritten handelt es sich um Beistellungen, die ebenfalls umfassende Netzmanagement-, Wartungs- und Serviceverträge mit den Leistungserbringern und Lieferanten erfordern und einen hohen Koordinationsaufwand zur Folge haben.

Gemäss Zuständigkeits- und Finanzierungsregelung muss jeder Nutzer selber für den Betrieb der dezentralen Komponenten aufkommen. Für die Instandhaltung der spezifischen Nutzerstandorte des Bundes werden von 2023 bis 2027 insgesamt 13,5 Millionen Franken veranschlagt. Mit den vorgesehenen Mitteln werden die anschlussspezifischen Wartungs- und Betriebskosten, z. B. der Unterhalt der Schnittstelle von den dezentralen Komponenten zur zentralen Komponente abgedeckt. Gerechnet wird zurzeit mit 40 Bundesanschlüssen. Für die spezifischen Standortkosten der 36 Kantonsanschlüsse, die 43 Anschlüsse von kritischen Infra-

strukturen sowie für den Anschluss des Fürstentums Liechtenstein kommen die Nutzer selber auf.

Durch den Betrieb und Unterhalt des sicheren Datenverbundsystems erhöht sich der Funktionsaufwand des BABS im Jahr 2020 um 100 000 Franken, im Jahr 2021 um 600 000 Franken, im Jahr 2022 um 1,5 Millionen Franken, im Jahr 2023 um 7 Millionen Franken, im Jahr 2024 um 10 Millionen Franken, im Jahr 2025 um 12 Millionen Franken, im Jahr 2026 um 13,9 Millionen Franken und ab 2027 um jährlich 15 Millionen Franken (vgl. Tabelle 4). Darin ist der zusätzlich erforderliche Personalaufwand nicht eingerechnet. Die Arbeitsplatzkosten belaufen sich von 2020 bis 2028 auf insgesamt 1,7 Millionen Franken (vgl. Tabelle 4).

2.2.7 Regelung der Zuständigkeiten und Finanzierung

Beim nationalen sicheren Datenverbundsystem handelt es sich um ein Verbundsystem, an dem sich Bund, Kantone, Betreiberinnen von kritischen Infrastrukturen und Dritte gemeinsam beteiligen. Bei Verbundsystemen wird zwischen zentralen und dezentralen Komponenten unterschieden. Die zentralen Komponenten vernetzen die Nutzer miteinander und werden von allen Nutzern gemeinsam beansprucht. Bei den dezentralen Komponenten handelt es sich um Komponenten, die proprietär von Bundesstellen, beispielsweise von der EZV, den Kantonen und Dritten genutzt werden und diesen die Nutzung der zentralen Komponenten ermöglichen.

Der Departementsvorsteher des VBS sowie die Präsidenten der KKJPD und der RK MZF haben für die Klärung der Zuständigkeiten und Finanzierungsfragen am 10. Januar 2017 eine aus Vertretern von Bund und Kantonen zusammengesetzte Arbeitsgruppe einberufen. Dabei konnte eine Konsenslösung gefunden und die grundsätzliche Finanzierung mit den Kantonen vereinbart werden. Die Kantone bestellen beim Bund 36 Anschlüsse. Die Verteilung der 36 Anschlüsse auf die 26 Kantone und den interkantonalen Verteilschlüssel für die jährlichen Betriebs- und Unterhaltskosten regeln sie untereinander. Folgende Regelungen wurden festgehalten:

Bei Verbundsystemen ist der Bund für die zentralen Komponenten zuständig. Für die dezentralen Komponenten sind Bund (Bundesstellen), Kantone, Betreiberinnen von kritischen Infrastrukturen sowie Dritte selber zuständig.

Unter dem Begriff «Investition» werden alle Aufwände verstanden, die für den Aufbau und die Einführung eines neuen Systems notwendig sind. Beim nationalen sicheren Datenverbundsystem sind darunter Investitionen für Gebäude, Kabel, Hardware, Software, Notstromaggregate, Klimaanlagen usw. zu verstehen (vgl. Tab. 4). Die zentralen Komponenten werden durch den Bund finanziert. Diese Investitionen fallen einmalig an. In Bezug auf das Datenverbundsystem beinhaltet dies die Investitionen für das Grundnetz (Backbone) bis zum Übergangspunkt an einem Nutzerstandort (Anschluss), die Investitionen für das Datenzugangssystem und die Investitionen für die Ablösung des Meldesystems Vulpus bzw. für das Lageverbundsystem. Die Investitionen der dezentralen Komponenten finanzieren die Kantone, die Betreiberinnen von kritischen Infrastrukturen und die Dritten selbst. Dazu gehört auch die Stromsicherheit des angeschlossenen Nutzerstandorts. Soweit es sich um

Anschlüsse der dezentralen Komponenten von Bundesstellen handelt, werden diese vom Bund selbst finanziert. Die damit verbundenen Ausgaben sind im vorliegenden Antrag enthalten.

Nach Ablauf des Lebenszyklus eines Systems fallen erfahrungsgemäss Werterhaltungsmassnahmen an. Diese haben Investitionscharakter. Unter Werterhalt werden dementsprechend grössere Reinvestitionen verstanden, die innerhalb von sechs bis acht Jahren nach der Erstinvestition anfallen können. Die Kosten dafür entsprechen etwa 60 Prozent der relevanten Erstinvestitionskosten und werden für die zentralen Komponenten vom Bund finanziert. Die Kantone und Dritten tragen ihrerseits die Werterhaltungskosten für die dezentralen Komponenten. Dies gilt auch für Bundesstellen, soweit diese über dezentrale Komponenten verfügen.

Als jährliche Betriebs- und Unterhaltskosten werden die Aufwendungen für Leistungen zur Sicherstellung des unterbruchsfreien und gesicherten Betriebs der Systeme bezeichnet. Dazu zählen beispielsweise die Wartung der Systeme, deren Überwachung, das Service- und Notfallmanagement sowie Software-Updates und Security-Patches. Der Abschreibungsaufwand zählt nicht dazu. Es wird davon ausgegangen, dass während des Lebenszyklus der Systeme rund 15 Prozent der jährlich anfallenden Betriebs- und Unterhaltskosten für werterhaltende Massnahmen eingesetzt werden. Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten des sicheren Datenverbundsystems werden durch alle angeschlossenen Nutzer anteilmässig finanziert. Der Betrieb und der Unterhalt der dezentralen Komponenten werden durch die Kantone, die Betreiberinnen von kritischen Infrastrukturen und die Dritten selbst sowie bei angeschlossenen Bundesstellen durch den Bund finanziert.

Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten des sicheren Datenverbundnetzes, des Datenzugangssystems und der Ablösung des Meldesystems Vulpus bzw. des Lageverbundsystems werden zu 30 Prozent von den Kantonen, zu rund 40 Prozent vom Bund und zu rund 30 Prozent von den Betreiberinnen kritischer Infrastrukturen getragen. Die Kantone werden damit berechtigt, maximal 36 Anschlüsse an dieses System zu realisieren. Der Bund, die Betreiberinnen von kritischen Infrastrukturen und Dritte können ihrerseits rund 80 bis 90 Anschlüsse realisieren. Die Finanzierung erfolgt anteilsmässig. Falls zusätzliche Anschlüsse über die geplanten 120 Anschlüsse hinausgehend realisiert werden, wird der Kostenschlüssel nach dem gleichen Prinzip angepasst.

Tabelle 3

Investition, Werterhalt sowie Betrieb und Unterhalt

	Investition	Werterhalt (Reinvestition)	Betrieb und Unterhalt
Gegenstand	Gebäude, Klimaanlage, Notstromaggregat, Hardware, Software, Lizenzgebühren usw.	Grundsätzlicher Wechsel, Hardware (z. B. Router), Software usw.	Wartung, Software-Release/Update, Ersatzteile, Mietkosten usw.
Häufigkeit	einmalig[6]	ca. alle 6–8 Jahre	jährlich
Finanzierung	Zentrale Komponenten: Bund Dezentrale Komponenten: Bundesstellen, Kantone und Dritte	Zentrale Komponenten: Bund Dezentrale Komponenten: Bundesstellen, Kantone und Dritte	Zentrale Komponenten: Nutzer (Bund mit Dritten[7]/ Kantone: 70/30) Dezentrale Komponenten: Bundesstellen, Kantone und Dritte

3 Auswirkungen

3.1 Auswirkungen auf den Bund

3.1.1 Finanzielle Auswirkungen

Die Investitionsausgaben für die Entwicklung und die Beschaffung betragen für den Bund 150 Millionen Franken. Vorbehalten bleiben die Beschlüsse des Bundesrates im Rahmen der Bereinigung der kommenden Voranschläge mit integriertem Aufgaben- und Finanzplan.

Dem Verpflichtungskredit liegt der Stand des Landesindexes der Konsumentenpreise vom Dezember 2017 (100,8 Punkte; Dez. 2015 = 100 Punkte) zugrunde. Es wird von einer Teuerungsannahme von 1 Prozent ab 2020 ausgegangen.

Der Verpflichtungskredit wird in drei Etappen freigegeben. Die erste Etappe soll mit dem Bundesbeschluss zur vorliegenden Botschaft freigeben werden. Über die Freigabe der Mittel für die beiden weiteren Etappen soll der Bundesrat aufgrund des Projektfortschritts entscheiden.

Für den Betrieb und den Unterhalt wird in den Jahren 2020 und 2021 mit einem zusätzlichen Aufwand von 100 000 bzw. 600 000 Franken gerechnet, da bereits in der Planungsphase Betriebsaufwände im Rahmen des Proof of Concept bzw. für die Vorbereitung des Testbetriebs in den Folgejahren notwendig sind. Die Betriebsaufwände steigen 2022 bis 2027 kontinuierlich an und betragen für den Regelbetrieb ab

6 Respektive sehr lange Zyklen von Jahrzehnten, z. B. Gebäudeerneuerung.
7 Bund mit Betreiberinnen von kritischen Infrastrukturen und Dritten.

2028 15 Millionen Franken pro Jahr (ohne Eigenleistung). Die Betriebsaufwände sind in Tabelle 4 dargestellt.

Die Eigenleistungen der Bundesverwaltung in Form von Personalkosten betragen ab 2020 durchschnittlich 4,3 Millionen Franken pro Jahr und im Regelbetrieb ab 2028 4,1 Millionen Franken jährlich.

Die Gesamtausgaben für den Bund belaufen sich von 2020 bis zum Projektende im Jahr 2027 auf 241,5 Millionen Franken brutto. Sowohl die Investitionen wie auch der Betrieb können nicht vollständig mit den bestehenden Mitteln des VBS (BABS) finanziert werden.

Durch die Ausserbetriebnahme des Meldesystems Vulpus fallen ab 2026 Betriebsaufwände von jährlich 1,5 Millionen Franken weg. In der Zeit des Systemwechsels (2025) wird ein Parallelbetrieb sichergestellt.

Ab vollständiger Inbetriebnahme des Grundnetzes im Jahr 2026 beteiligen sich die Kantone mit einem jährlichen Beitrag von 4,5 Millionen Franken an den Betriebs- und Unterhaltskosten des nationalen sicheren Datenverbundsystems (36 Anschlüsse). Dies entspricht durchschnittlichen jährlichen Kosten von rund 125 000 Franken pro Nutzerstandortanschluss. Bestandteil dieser Kosten sind die Kosten für die Eigenleistung des Bundes sowie die Aufwände für Betrieb und Unterhalt. Nicht eingerechnet in diesem Betrag sind die anschlussspezifischen Kosten, die letztlich von den Nutzern selber zu tragen sind. Die Beiträge der Betreiberinnen von kritischen Infrastrukturen und Dritten, die das System nutzen wollen, kommen ebenfalls dem Bund zugute. Bei einer Annahme von insgesamt 120 Anschlüssen (36 für die Kantone, einer für das Fürstentum Liechtenstein, 40 für die Bundesstellen, 43 für die Betreiberinnen von kritischen Infrastrukturen) resultieren daraus ohne Risikozuschlag jährliche Beiträge an den Bund von zehn Millionen Franken.

Tabelle 4

Gesamtausgaben für das nationale sichere Datenverbundsystem 2020–2027 in Millionen Franken

in Mio. CHF	2020	2021	2022	2023	2024	2025	2026	2027	Total
Gesamtausgaben	9,2	11,7	28,9	38,0	48,1	41,9	33,6	30,1	241,5
Investitionen	6,8	7,9	23,8	26,9	32,9	24,7	15,8	11,2	150,0
Projektmanagement	3,1	3,4	4,8	4,8	4,5	3,7	3,4	1,8	29,5
Entwicklungsarbeiten	1,5	1,0	4,4	3,0	4,0	2,8	0,5	0,5	17,7
Hardware, Software, Lizenzen	0,8	1,0	1,0	2,0	2,5	2,5	2,5	2,5	14,8
Netzinfrastruktur Backbone	0,0	0,0	1,5	2,8	1,6	0,5	0,0	0,0	6,4
Netzinfrastruktur Nutzerstandorte	0,0	0,0	4,0	6,8	8,0	8,0	5,5	3,4	35,7
Netzmanagement	0,0	1,0	2,0	1,0	1,0	2,0	0,8	0,5	8,3
Nutzerstandorte Bund	0,5	0,5	3,0	3,0	7,0	2,0	1,0	1,0	18,0
Risikozuschlag (15%)	0,9	1,0	3,1	3,5	4,3	3,2	2,1	1,5	19,6
Aufwand Betrieb und Unterhalt	0,1	0,6	1,5	7,0	10,0	12,0	13,9	15,0	60,1
Betrieb und Instandhaltung	0,0	0,4	1,0	5,8	8,3	9,3	9,6	10,7	45,1
Arbeitsplatzkosten	0,1	0,2	0,2	0,2	0,2	0,2	0,2	0,2	1,7
Nutzerstandorte Bund	0,0	0,0	0,3	1,0	1,5	2,5	4,1	4,1	13,5
Eigenleistungen	2,3	3,2	3,6	4,1	5,2	5,2	5,4	5,4	34,4
Personal (15 FTE bestehend)	0,9	0,9	0,9	1,4	2,5	2,5	2,7	2,7	14,5
Personal (15 FTE zusätzlich)	1,4	2,3	2,7	2,7	2,7	2,7	2,7	2,7	19,9
Ausserbetriebnahme Vulpus	0,0	0,0	0,0	0,0	0,0	0,0	-1,5	-1,5	-3,0

3.1.2 Personelle Auswirkungen

Damit das Projekt innerhalb der zeitlichen, finanziellen und qualitativen Vorgaben realisiert und der landesweite Betrieb des nationalen sicheren Datenverbundsystems zusammen mit den Leistungserbringern (FUB und externen Lieferanten) rund um die Uhr gewährleistet werden kann, sind im Endausbau (ab 2028) voraussichtlich 25 Stellen erforderlich. Verschiedene dieser Stellen sind notwendig, weil der Betrieb des Systems auch in besonderen und ausserordentlichen Lagen sichergestellt bleiben

muss. Die Umsetzung und der Betrieb des sicheren Datenverbundsystems verursacht beim VBS (BABS, FUB) im Zeitraum 2024–2027, in dem sich die Umsetzung und der Betrieb stark überlagern, einen personellen Aufwand von 30 Vollzeitstellen. Davon werden dauerhaft 15 VBS-intern kompensiert. Die übrigen 15 Vollzeitstellen werden während der Projektphase aufgestockt, wovon ab dem Regelbetrieb 2028 zehn dauerhaft bestehen bleiben. Das BABS und die FUB können den Zusatzaufwand für das System ohne diese Personalaufstockung nicht bewältigen.

Weil es sich um ein nationales und ausgesprochen komplexes Projekt im Bereich der Sicherheit handelt, besteht ein ausgeprägtes Interesse, eine maximale Unabhängigkeit zu erreichen und den Knowhow-Erhalt und die Technologieevolution bei den Schlüsselkompetenzen intern sicherzustellen. Es ist zwar vorgesehen, dass spezifische, befristete und nicht zum Kerngeschäft zählende Aufgaben und Expertisen von externen Dienstleistern erfüllt werden. Gemäss den Empfehlungen des Berichts vom 24. Juni 2015[8] der Finanz- und der Geschäftsprüfungskommissionen der eidgenössischen Räte zur Stellungnahme des Bundesrates vom 25. Februar 2015 und der Stellungnahme der EFK vom 24. Februar 2015 zum Informatikprojekt INSIEME sollen aber die Schlüsselrollen und das dazugehörige Knowhow bundesintern sichergestellt werden. Dieser Empfehlung will der Bundesrat, soweit es die Ressourcensituation erlaubt, nachkommen. Durch die Aufstockung des Personals können die interne Applikationsverantwortung übernommen, das Stakeholder-Management sichergestellt und die Kompetenzen aufgebaut werden, die für Betrieb, Werterhalt und Entwicklung notwendig sind.

Für den Aufbau und die Entwicklung sowie den zukünftigen Werterhalt des Datenverbundnetzes, des Datenzugangssystems, des Lageverbundsystems sowie das Management der Leistungsbezüger (Bundesstellen, Kantone, Betreiberinnen kritischer Infrastrukturen) sowie für Leistungen in der Betriebsphase benötigt das BABS zusätzlich insgesamt 10 Vollzeitstellen, die ab 2028 für den Regelbetrieb eingesetzt werden. In der Betriebsphase setzt das BABS für das sichere Datenverbundnetz und das Zugangssystem sechs Stellen und für das Lageverbundsystem vier Stellen ein. Diese werden aus dem Personalpool der Projektphase in die Betriebsphase transferiert. Die FUB ihrerseits benötigt für den Betrieb in allen Lagen und den 7x24-Stunden Notfallservice für das sichere Datenverbundsystem fünf zusätzliche Vollzeitstellen, die im Regelbetrieb ab 2028 VBS-intern kompensiert werden.

Im BABS ergibt sich kein zusätzlicher Flächenbedarf. Der Flächenbedarf für die zusätzlich beantragten Stellen im Rahmen des sicheren Datenverbundsystems kann im Rahmen von Projektarbeitsplätzen und Synergien mit der Reorganisation des BABS sowie dem Umzug der NAZ von Zürich nach Bern kompensiert werden. Die FUB ihrerseits hat ebenfalls keinen zusätzlichen Flächenbedarf.

Die Gesamtkoordination und die Projektverantwortung für das sichere Datenverbundsystem werden vom BABS wahrgenommen.

Das VBS wird zusätzlich komplexe Aufgaben und Verantwortung in verschiedenen Bereichen übernehmen müssen: Der Aufbau des Systems und dessen Betrieb müssen mit den Leistungserbringern, beispielsweise mit den Eigentümerinnen und

8 BBl **2016** 4253

Eigentümern von Glasfaserkabeln und Infrastrukturen, und mit den Leistungsbezügern koordiniert werden. Es müssen Verhandlungen geführt und Verträge ausgearbeitet werden. Lieferobjekte müssen abgenommen und getestet werden. Das Betriebsmanagement und die Instandhaltung sowie das Sicherheits- und Qualitätsmanagement müssen sichergestellt werden.

Für die Gesamtleitung des Projekts und die Koordination der Teilprojekte wird eine Projektleiterin oder ein Projektleiter eingesetzt.

Für das Management der vier Teilvorhaben wird je eine Teilprojektleiterin oder ein Teilprojektleiter eingesetzt. Die Teilprojektleiterinnen und -leiter betreuen die Nutzer von Bund und Kantonen sowie die Betreiberinnen von kritischen Infrastrukturen bei der Projektplanung, bei der Umsetzung vor Ort und beim Betrieb. Sie sind verantwortlich für das Schnittstellenmanagement des sicheren Datenverbundsystems zu den Netzen der Nutzerorganisationen.

Die Verantwortlichen für das Auftragsmanagement sind Ansprechperson gegenüber den Nutzern für den Auftragseingang. Sie sorgen für die Abwicklung der Aufträge.

Die Produktmanagerinnen und -manager überwachen die Marktentwicklung und erstellen Prognosen, die für den Ausbau und die Weiterentwicklung des sicheren Datenverbundsystems relevant sind. Sie erfassen während der gesamten Projektdauer die Bedürfnisse der Bundesstellen, der Kantone und der Betreiberinnen von kritischen Infrastrukturen.

Die für das Betriebsmanagement zuständigen Personen sorgen in Abstimmung mit den betroffenen Behörden und Organisationen von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen für die Betriebskoordination, Tests und Abnahmen. Sie sind verantwortlich für das Change-, Release- und Konfigurationsmanagement. Sie führen neue Soft- und Hardware-Releases ein. Sie koordinieren den Betrieb im Gesamtnetzverbund mit allen Anwendungen der Nutzer von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen.

Die Verantwortlichen für das Servicemanagement schliessen Dienstleistungsvereinbarungen mit den Leistungserbringern (FUB, Industrie) ab und überwachen die Einhaltung.

Die Network-Operation-Managerinnen und -Manager verwalten und überwachen das sichere Datenverbundnetz und das Zugangssystem. Darunter werden funktionale Aufgaben wie Fehlermanagement, Konfigurationsmanagement, Leistungsmanagement und Sicherheitsmanagement verstanden.

Die Rolle der Service-Assurance-Managerinnen und -Manager beinhaltet die wirksame Sicherstellung der Dienstleistungen gegenüber den Nutzerinnen und Nutzern. Sie sind verantwortlich für die Einhaltung und Steuerung eines effizienten Ereignis- und Problemmanagements mit dem Leistungserbringer sowie für die Kommunikation mit den Nutzerinnen und Nutzern.

Die für das Sicherheits- und Qualitätsmanagement zuständigen Personen konzipieren die sicherheitsrelevanten Vorgaben. Sie setzen die Vorgaben der Nationalen

Strategien vom 27. Juni 2012[9] und vom 18. April 2018 zum Schutz der Schweiz vor Cyber-Risiken um und sorgen für das Qualitätsmanagement. Sie identifizieren während der gesamten Betriebsdauer Verbesserungsmassnahmen und überwachen deren Umsetzung.

Die verantwortlichen Personen für das Vertragsmanagement sorgen für die Verhandlungen und die Vertragsabschlüsse mit den Leistungserbringern (FUB, Industrie) und sämtlichen Nutzern von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen. Zudem sind sie verantwortlich für die Vertragsprozesse und die Einhaltung der Vertragsinhalte.

Für die Projektbegleitung braucht es während der ganzen Dauer eine für das Projekt-Controlling zuständige Person. Diese ist verantwortlich für das Berichtswesen und übernimmt gleichzeitig Querschnittsaufgaben für das Projekt. Sie sorgt für die Koordination mit den Bereichen Finanzen, Beschaffung und Recht.

Die Überwachung bezüglich der Ereignisse und Bedrohungen im Cyber-Raum für die gesamte betroffene IKT-Infrastruktur wird durch die Leistungserbringerin des VBS, d. h. die FUB, sichergestellt.

Das Management der Leistungsbezüger von Bund, Kantonen und Betreiberinnen von kritischen Infrastrukturen wird in der Betriebsphase durch verschiedene Funktionen, die in der Projektphase benötigt werden, aufgebaut (vgl. Tabelle 6).

9 Die Texte der Strategien sind im Internet abrufbar unter: www.isb.admin.ch > Themen > Cyber-Risiken NCS > Strategie NCS 2012–2017 bzw. Strategie NCS 2018–2022.

Tabelle 6

Personalbedarf und Funktionen pro Jahr bis zum Projektende sowie für den Regelbetrieb

Projektstellen	Projekt	2020	2021	2022	2023	2024	2025	2026	2027	2028
Projektleiter/in	SDVN & DZS (BABS)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
	SDVN & DZS (FUB)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
	Lageverbund/Vulpus (BABS)									
Teilprojektleiter/in	SDVN & DZS (BABS)	3,0	3,0	3,0	2,0	2,0	2,0	1,5	1,5	
	SDVN & DZS (FUB)	1,0	2,0	2,0	2,0	2,0	2,0	1,0	1,0	
	Lageverbund/Vulpus (BABS)	1,0	1,0	1,0	1,0	1,0	1,0	1,0	1,0	
Verantwortliche Auftragsmanagement	SDVN & DZS (BABS)	1,0	1,25	1,5	1,5	1,25				
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)	1,0	1,0	0,75	0,75					
Produktmanager/in	SDVN & DZS (BABS)	1,0	1,0	1,25	1,5	1,0	1,0	1,0	1,0	
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)	1,0	1,0	1,5	1,5					
Betriebsmanager	SDVN & DZS (BABS)	0,5	0,5	0,5						
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)		0,5	0,5						
Verantwortliche/r Service Management	SDVN & DZS (BABS)									
	SDVN & DZS (FUB)		0,5	0,5						
	Lageverbund/Vulpus (BABS)			1,0	1,0					
Network Operation Manager/in	SDVN & DZS (BABS)									
	SDVN & DZS (FUB)		0,5							
	Lageverbund/Vulpus (BABS)									
Sicherheits- und Qualitätsmanager/in	SDVN & DZS (BABS)	1,0	1,0	1,0	0,75	0,75	0,75	0,75	0,75	
	SDVN & DZS (FUB)		1,0	1,0	1,0					
	Lageverbund/Vulpus (BABS)		0,5	0,25						
Verantwortliche Vertragsmanagement	alle Projekte	0,25	1,00	1,25	1,00	0,75	0,25	0,25	0,25	
Verantwortliche Controlling	alle Projekte	0,25	0,25	0,50	0,75	0,75	0,75	1,00	1,00	
Total Projektstellen		13	18	19,5	16,75	11,5	9,75	8,5	8,5	0,0

Fortsetzung Tabelle 6

Betriebsstellen	Betrieb	2020	2021	2022	2023	2024	2025	2026	2027	2028
	SDVN & DZS (BABS)									1,0
Teilprojektleiter/in	SDVN & DZS (FUB)									1,0
	Lageverbund/Vulpus (BABS)									
Verantwortliche Auftragsmanagement	SDVN & DZS (BABS)						1,0	1,0	1,0	1,0
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)					0,5	0,5	0,5	0,5	
Produktmanager/in	SDVN & DZS (BABS)					1,0	1,0	1,0	1,0	1,0
	SDVN & DZS (FUB)									1,0
	Lageverbund/Vulpus (BABS)					1,25	1,25	1,25	1,25	0,75
Betriebsmanager/in	SDVN & DZS (BABS)				1,0	1,0	1,75	2,0	2,0	1,5
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)				0,5	1,0	1,0	1,0	1,0	1,0
Verantwortlicher Service Management	SDVN & DZS (BABS)									1,0
	SDVN & DZS (FUB)				1,5	2,0	2,0	2,0	2,0	2,0
	Lageverbund/Vulpus (BABS)					1,0	1,0	1,0	1,0	1,0
Service Assurance Manager/in	SDVN & DZS (BABS)									
	SDVN & DZS (FUB)					1,0	1,0	2,0	2,0	2,0
	Lageverbund/Vulpus (BABS)									
Network Operation Manager/in	SDVN & DZS (BABS)									
	SDVN & DZS (FUB)			0,5	2,5	8,0	8,0	9,0	9,0	9,0
	Lageverbund/Vulpus (BABS)									
Sicherheits- und Qualitätsmanager/in	SDVN & DZS (BABS)				0,5	0,5	0,5	0,5	0,5	0,5
	SDVN & DZS (FUB)									
	Lageverbund/Vulpus (BABS)				0,25	0,25	0,25	0,25	0,25	0,25
Verantwortliche Vertragsmanagement	alle Systeme									0,25
Verantwortliche Controlling	alle Systeme									0,75
Total Betriebsstellen		0,0	0,0	0,5	6,25	17,5	19,25	21,5	21,5	25,0
Total Stellen pro Jahr (Projekt + Betrieb)		**13**	**18**	**20**	**23**	**29**	**29**	**30**	**30**	**25**

3.2 Auswirkungen auf die Kantone

Der Bund übernimmt die Investitionskosten für die zentralen Komponenten des Verbundsystems. Für die Investitionskosten der dezentralen Komponenten in den Kantonen, beispielsweise die Härtung ihrer Nutzerstandorte, sind die Kantone selbst zuständig. Die Kantone sorgen über ihre eigenen Netze für den Anschluss von kantonalen Stellen, Gemeinden, Städten usw. an das System. Der Anschluss der dezentralen Komponenten der Kantone an die zentralen Komponenten erfolgt schrittweise. Die Investitionskosten sowie die jährlichen Betriebs- und Unterhaltskosten für die dezentralen Komponenten in den Kantonen hängen von den bestehenden Infrastrukturen und den Bedürfnissen der einzelnen Kantone ab. Zu den Einzelheiten betreffend die Kosten siehe Ziffer 3.1.1.

3.3 Auswirkungen auf die Volkswirtschaft

Die Realisierung des nationalen sicheren Datenverbundsystems hat auch einen nennenswerten volkswirtschaftlichen Nutzen. Sollten die IKT-Dienstleistungen grossflächig ausfallen, wäre die Funktionsfähigkeit der Wirtschaft gefährdet. Viele Unternehmen und insbesondere Betreiberinnen von kritischen Infrastrukturen sind heute mit einer Notstromversorgung auf Stromausfälle in ihren Betrieben vorbereitet. Diese Notstromversorgung garantiert den autonomen Betrieb für eine bestimmte Zeit, nicht aber die Verbindung zu den Partnerorganisationen, Behörden usw. Der elektronische Austausch von Daten zwischen Organisationen und Unternehmen hat in den vergangenen Jahren stark zugenommen und wird im Rahmen der Digitalisierung weiter stark wachsen. Mit der Realisierung des nationalen sicheren Datenverbundsystems wird eine Plattform für alle Behörden und Betreiberinnen von kritischen Infrastrukturen geschaffen, die die Verbindungsfähigkeit ihrer Systeme auch unter Stromausfall sicherstellen wollen oder müssen. Das System kann und soll auch in der normalen Lage genutzt werden. Mit der Realisierung des sicheren Datenverbundsystems kann vermieden werden, dass die verschiedenen Bedürfnisträger redundante Einzellösungen aufbauen. All das stellt einen erheblichen volkswirtschaftlichen Mehrwert dar.

3.4 Auswirkungen auf die Gesellschaft

Die Realisierung des nationalen sicheren Datenverbundsystems verbessert nicht nur die Ausfallsicherheit der Telekommunikationssysteme und des sicheren Datenaustauschs der Führungsorgane, Behörden und Einsatzorganisationen. Letztlich wird die Bevölkerung von einem besseren Sicherheitsniveau profitieren. Damit könnte im Katastrophenfall oder in einer Notlage das mögliche Schadensausmass an Personen, Tieren und Sachwerten erheblich reduziert und ein grosses Sicherheitsdefizit im Bevölkerungsschutz geschlossen werden.

3.5 Auswirkungen auf die Umwelt

Es gibt ausser den aus der Transportlogistik resultierenden Umwelteinwirkungen keine nennenswerten Auswirkungen auf die Umwelt. Das Projekt basiert auf einem Glasfasernetz und es gibt keinen Bedarf für neue Antennenstandorte. Die Emissionen durch nichtionisierende Strahlung werden deshalb nicht zunehmen.

4 Verhältnis zur Legislaturplanung und zu Strategien des Bundesrates

4.1 Verhältnis zur Legislaturplanung

Die Vorlage ist in der Botschaft vom 27. Januar 2016[10] zur Legislaturplanung 2015–2019 unter Ziffer 5.3.5 subsumiert. So sieht die Strategie des Bundesrates vor, die sicherheitspolitischen Instrumente derart auszugestalten, dass die Reaktionsfähigkeit auf eintretende Ereignisse jederzeit gewährleistet ist. Dies erfordert u. a. eine optimale Kooperation aller Partner und ein wirkungsvolles und effizientes Zusammenspiel aller sicherheitspolitischen Akteure. Grundlegendes Instrument dazu ist ein gesicherter Informations- und Lageaustausch aller beteiligten Akteure. Dies soll mit dem sicheren Datenverbundsystem ermöglicht werden.

Ziel 16 des Bundesbeschlusses vom 14. Juni 2016[11] über die Legislaturplanung 2015–2019 lautet: «Die Schweiz kennt die inneren und äusseren Bedrohungen ihrer Sicherheit und verfügt über die notwendigen Instrumente, um diesen wirksam entgegenzutreten». Als Massnahme Nr. 65 wird dazu die Verabschiedung der Botschaft zur Änderung des Bevölkerungs- und Zivilschutzgesetzes aufgeführt. In der BZG-Botschaft sind u. a. auch die Rechtsgrundlagen für die Realisierung des nationalen sicheren Datenverbundsystems mit dem nationalen Lageverbundsystem enthalten.

4.2 Verhältnis zu den Zielen des Bundesrates 2018

Der Bundesrat hat aufgrund der Dringlichkeit des Geschäfts die Erarbeitung einer Botschaft in die Ziele des Bundesrates 2018 (Band I und II) vom 23. November 2017[12] aufgenommen und am 1. Dezember 2017 dem BABS den Auftrag erteilt, 2018 eine Botschaft zu erarbeiten.

10 BBl **2016** 1105
11 BBl **2016** 5183
12 Der Text der Ziele ist im Internet abrufbar unter: www.bk.admin.ch > Dokumentation > Führungsunterstützung > Jahresziele.

4.3 Verhältnis zu Strategien des Bundesrates

Aufgrund der Klimaveränderung ist davon auszugehen, dass insbesondere Naturgefahren in Zukunft häufiger und intensiver ausfallen werden,[13] was Anpassungsmassnahmen fordert.[14] Der Schutz der Informations- und Kommunikationsinfrastrukturen vor Cyber-Risiken, die tendenziell zunehmen werden, liegt im nationalen Interesse.[15] Ausfallsichere Telekommunikationssysteme wurden entsprechend im vom Bundesrat am 9. Mai 2012[16] verabschiedeten Bericht zur Strategie Bevölkerungsschutz und Zivilschutz 2015+ als strategisches Ziel formuliert. Gemäss der Strategie «Digitale Schweiz» vom April 2016[17] muss der Staat im digitalen Zeitalter seinen Aufgaben zum Schutz von Gesellschaft und Wirtschaft wirkungsvoll gerecht werden können. Das nationale sichere Datenverbundsystem leistet einen wichtigen Beitrag zur Verbesserung der Resilienz von Telekommunikationssystemen und Betreiberinnen von kritischen Infrastrukturen im Bereich der Sicherheit. Diese Resilienzsteigerung wird in der «Nationalen Strategie zum Schutz kritischer Infrastrukturen 2018–2022»[18] und der «Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken» angestrebt. Ein hochgradig ausfallsicheres Daten- und Kommunikationsnetz, an das die Betreiberinnen von kritischen Infrastrukturen angeschlossen werden können, ist entsprechend ein Ziel und eine explizite Massnahme der Strategie zum Schutz kritischer Infrastrukturen 2018–2022, die der Bundesrat am 8. Dezember 2017 verabschiedet hat. Mit dem nationalen sicheren Datenverbundsystem wird es möglich, bei einem Ausfall der öffentlichen Telekommunikation relevante Prozesse zum Betrieb von kritischen Infrastrukturen aufrechtzuerhalten bzw. die Kommunikation zwischen den Betreiberinnen von kritischen Infrastrukturen und den Organisationen für die Krisenbewältigung auf den Stufen Bund und Kantone sicherzustellen. Ein gegen Ausfälle und Störung gehärtetes Kommunikations- und Datennetz sowie ein Verbund der verschiedenen Lagesysteme wird auch im Bericht des Bundesrates «Umgang mit Naturgefahren in der Schweiz»[19] bzw. in der Naturgefahrenstrategie[20] als Massnahmen aufgenommen, um die Resilienz gegenüber Naturgefahren zu verbessern.

13 Köllner P., Gross C., Schäppi B., Füssler J., Lerch J., Nauser M. 2017: Klimabedingte Risiken und Chancen. Eine schweizweite Synthese. Bundesamt für Umwelt, Bern. Umwelt-Wissen Nr. 1706: 148 S.

14 Vgl. Strategie des Bundesrates zur Anpassung an den Klimawandel in der Schweiz 2014–2019, im Internet abrufbar unter: www.bafu.admin.ch > Themen > Thema Klima > Fachinformationen > Anpassung an den Klimawandel > Strategie des Bundesrates.

15 Vgl. Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken 2012–2017 bzw. 2018–2022, im Internet abrufbar unter: www.isb.admin.ch > Themen > Cyber-Risiken > Strategie NCS 2018–2022 bzw. Strategie NCS 2012–2017.

16 BBl **2012** 5503

17 BBl **2016** 3985

18 Der Text der Strategie vom 8. Dez. 2017 ist im Internet abrufbar unter: www.babs.admin.ch > Weitere Aufgabenfelder > Schutz kritischer Infrastrukturen > Nationale SKI-Strategie.

19 Der Bericht ist im Internet abrufbar unter: www.bafu.admin.ch > Themen > Thema Naturgefahren > Dossiers > Naturgefahren in der Schweiz – was tun für unsere Sicherheit > Bundesratsbericht «Naturgefahren Schweiz 2016».

20 Die Strategie ist im Internet abrufbar unter: www.planat.ch > Strategie 2018.

20 Die Strategie ist im Internet abrufbar unter: www.planat.ch > Strategie 2018.

Am 4. Dezember 2015 hat der Bundesrat die IKT-Strategie 2016–2019 verabschiedet.[21] Im Rahmen der Stossrichtung «S03 – Erbringung der IKT-Leistung» dieser Strategie wurde eine Strategie «Netzwerke des Bundes» erarbeitet. Der Bundesrat hat diese gleichzeitig mit der vorliegenden Botschaft verabschiedet. Sie zeigt auf, welche Anforderungen an die Netzwerke des Bundes gestellt werden, und legt fest, mit welchen landesweiten Netzwerken diese Anforderungen künftig erfüllt werden sollen. Das Projekt «sicheres Datenverbundsystem» ist Bestandteil der IKT-Strategie «Netzwerke des Bundes» und mit dieser abgestimmt. Die Feinabstimmung erfolgt im Rahmen der weiteren Projektarbeiten.

Grundsätzlich werden gemäss der Strategie «Netzwerke des Bundes» bei den optischen Datentransportnetzwerken im Weitverkehr vom Bund zwei Infrastrukturen angestrebt. Bei der ersten handelt es sich um das Führungsnetz Schweiz, das robuste und hochsichere Leistungen zugunsten der Armee erbringt. Bei der zweiten handelt es sich um das sogenannte Optische Behördennetz Bund. Dieses Netz stellt Bundesstellen, Kantonen, Betreiberinnen kritischer Infrastrukturen und zugelassenen Dritten, die für ihre Zusammenarbeit Netzverbindungen benötigen, stromresiliente und hochsichere optische Datenverbindungen zur Verfügung. Dieses optische Behördennetz wird in einer ersten Phase im Rahmen von drei Vorhaben bzw. Projekten aufgebaut: dem nationalen sicheren Datenverbundsystem (SDVS), der Vernetzung der Betriebs- und Sicherheitsausrüstungen entlang der Nationalstrassen und der Vernetzung der zivil genutzten Rechenzentren.

Diese optischen Datentransportnetzwerke nutzen soweit möglich die bestehende Glasfaserinfrastruktur des Führungsnetzes Schweiz und der Nationalstrassen. Mit dieser Lösung können verschiedene Synergien genutzt werden. Zum einen werden weitgehend vorhandene bundeseigene Infrastrukturen mehrfach genutzt. Zum anderen werden die Betriebsleistungen für diese beiden Infrastrukturen von einem Leistungserbringer (der FUB) wahrgenommen. Die FUB verfügt über die Ressourcen und Fähigkeiten für den Betrieb von optischen Datentransportnetzen und stellt diesen Betrieb auch in der besonderen und ausserordentlichen Lage sicher.

Bei den IP-Netzwerken, die für die Verbindungen Bund – Kantone und zwischen den Kantonen benötigt werden, soll mittel- bis langfristig soweit möglich eine integrierte IP-Plattform aufgebaut und betrieben werden. Damit soll die Erhöhung der Komplexität der Übergänge bzw. Schnittstellen zu den Kantonen verhindert und sollen Synergien im Bereich der Infrastrukturen und dem Betrieb genutzt werden.

Auf dieser integrierten IP-Plattform können mehrere voneinander isolierte IP-Teilnetze oder Verbindungen implementiert und betrieben werden. Die Betriebsrolle dieser integrierten IP-Plattform und der darauf basierenden Teilnetze muss erst noch bestimmt werden. Die FUB und das BIT erarbeiten dazu zusammen und unter Beizug des BABS bis Ende 2019 ein Betriebs- und Zusammenarbeitsmodell. Dabei müssen auch die organisatorischen und prozessualen Aufgaben und Schnittstellen, Kompetenzen und Verantwortlichkeiten festgelegt werden. Dies unter Berücksichtigung der für verschiedene sicherheitsrelevante Anwendungen verlangten Anforderungen (Betrieb auch in der besonderen und ausserordentlichen Lage), der im neuen

21 Der Text der Strategie ist im Internet abrufbar unter: www.isb.admin.ch > Themen > Strategie und Planung IKT Bund > IKT-Strategie Bund 2016–2019.

Bevölkerungs- und Zivilschutzgesetz (BZG) und in der Bundesinformatik vorgegebenen Randbedingungen und der in den Standarddiensten etablierten Regelungen.

5 Rechtliche Aspekte

5.1 Verfassungs- und Gesetzmässigkeit

Die Zuständigkeit der Bundesversammlung für den vorliegenden Kreditbeschluss ergibt sich aus Artikel 167 der Bundesverfassung (BV).

Der Vorschlag für die Zuständigkeitsregelung und die Aufgabenteilung zwischen Bund, Kantonen und Dritten sowie die Aufteilung der Kosten für diese Systeme (vgl. Ziff. 2.2.7) ist in der BZG-Botschaft berücksichtigt worden. Die BZG-Botschaft wird dem Parlament in einem separaten Antrag zeitlich koordiniert mit der vorliegenden Botschaft unterbreitet. Um zu vermeiden, dass Kantone und Dritte verschiedene eigene Systeme realisieren, die später wie beim Polycom nur mit grossem Zeitaufwand und Ressourceneinsatz zu einem nationalen System zusammengebaut werden können, ist auch vorgesehen, dass der Bund Vorgaben für Standards für die Systeme festlegen kann. Zudem soll der Bund die Möglichkeit erhalten, technische und terminliche Vorgaben bei solchen Verbundsystemen machen zu können.

5.2 Erlassform

Nach Artikel 163 Absatz 2 BV und Artikel 25 Absatz 2 des Parlamentsgesetzes vom 13. Dezember 2002[22] ist für den vorliegenden Erlass die Form des einfachen Bundesbeschlusses vorgesehen. Dieser untersteht somit nicht dem Referendum.

5.3 Unterstellung unter die Ausgabenbremse

Nach Artikel 159 Absatz 3 Buchstabe b BV bedarf Artikel 1 des Bundesbeschlusses zum Verpflichtungskredit der Zustimmung der Mehrheit der Mitglieder beider Räte, da dieser einmalige Ausgaben von mehr als 20 Millionen Franken nach sich zieht.

22 SR **171.10**

Abkürzungsverzeichnis

ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAFU	Bundesamt für Umwelt
BCM	Business Continuity Management
BFE	Bundesamt für Energie
BSTB	Bundesstab Bevölkerungsschutz
BZG	Bevölkerungsschutz- und Zivilschutzgesetz
DZS	Datenzugangssystem
EFK	Eidgenössische Finanzkontrolle
ELD	Elektronische Lagedarstellung
EZV	Eidgenössische Zollverwaltung
fedpol	Bundesamt für Polizei
FinDel	Finanzdelegation
FTE	Vollzeitäquivalent
FUB	Führungsunterstützungsbasis der Armee
IBBK (-Radio)	Information der Bevölkerung durch den Bund in Krisenlagen
IKT	Informations- und Kommunikationstechnologie
IP	Internet-Protokoll
GWK	Grenzwachtkorps
IKT	Informations- und Kommunikationstechnologie
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KomBV–KTV	Kommunikationsnetz Bundesverwaltung–Kantonalverbund
MeteoSchweiz	Bundesamt für Meteorologie und Klimatologie
NAZ	Nationale Alarmzentrale
NCC	Network Control Center
NDB	Nachrichtendienst des Bundes
PRZ	Prüf- und Referenzzentrum
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
SDVS	Sichere Datenverbundsystem
SFU	Strategische Führungsübung
SOC	Security Operation Center

SVU	Sicherheitsverbundsübung
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport