Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Bevölkerungsschutz BABS

Bericht zur Zukunft der Alarmierungs- und Telekommunikationssysteme für den Bevölkerungsschutz

Auslegeordnung zu den Führungs- und Einsatzkommunikationssystemen zwischen Behörden und Organisationen für Rettung und Sicherheit (BORS) und den Systemen für die Alarmierung und Information der Bevölkerung

---

29. September 2017

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Bedeutung
ABCN	Atomar, biologisch, chemisch Gefährdungen und Naturgefahren
ASTRA	Bundesamt für Strassen
BABS	Bundesamt für Bevölkerungsschutz
BAKOM	Bundesamt für Kommunikation
BAV	Bundesamt für Verkehr
BAZL	Bundesamt für Zivilluftfahrt
BCM	Business Continuity Management
BK	Bundeskanzlei
B-MPLS-Netz MPLS	IP-Netz, das die Kommunikation zwischen den Polycomnutzern ermöglicht Multiprotocol Label Switching
BORS	Behörden und Organisationen für Rettung und Sicherheit
BOS Austria	Österreich: digitales Bündelfunksystem zur Funkkommunikation für Behörden und Organisationen mit Sicherheitsaufgaben (BOS)
BST ABCN	Bundesstab ABCN
BZG	Bevölkerungs- und Zivilschutzgesetz
CBS	Cell Broadcast Service
DAB+	Digital Audio Broadcast + ist eine digitale Radiotechnologie, die hauptsächlich über die Luft (terrestrisch) verbreitet wird. (Quelle SRG)
dBBK	Drahtlose Breitbandkommunikation
DVB-C	Digital Video Broadcasting – Cable
DVB-S	Digital Video Broadcasting – Satellite
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFK	Eidgenössische Finanzkontrolle
EJPD	Eidgenössisches Justiz- und Polizeidepartement
ELD	Elektronische Lagedarstellung
ENSI	Eidgenössisches Nuklearsicherheitsinspektorat
fedpol	Bundesamt für Polizei
FUB	Führungsunterstützungsbasis
GWK	Grenzwachtkorps
IBBK	Information der Bevölkerung durch den Bund in Krisenlagen mit Radio
ICARO	Information Catastrophe Alarme Radio Organisation
IES-KSD	Einsatz-System des Koordinierten Sanitätsdienstes
IKT	Informations- und Kommunikationstechnik
IP	Internetprotokoll
KKJPD	Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren
KomBV-KTV	Kommunikationsnetz Bundesverwaltung–Kantonalverbund
KTN Bund	Deutschland: sicheres Kerntransportnetz

LO KOVE	Leitungsorgan für die Koordination des Verkehrswesens im Hinblick auf Ereignisfälle
MeteoSchweiz	Bundesamt für Meteorologie und Klimatologie
NAZ	Nationale Alarmzentrale
NDB	Nachrichtendienst des Bundes
NGO	Nichtregierungsorganisation
OSTRAL	Organisation für die Strombewirtschaftung in ausserordentlichen Lagen
OZD	Oberzolldirektion
RK MZF	Regierungskonferenz Militär, Zivilschutz und Feuerwehr
RTVG	Bundesgesetz über Radio und Fernsehen
SBB	Schweizerische Bundesbahnen
SDVN	Sicheres Datenverbundnetz
SED	Schweizerischer Erdbebendienst
SEM	Staatssekretariat für Migration
SMS	short message service
SNB	Schweizerische Nationalbank
SRG	Schweizer Radio und Fernsehen
SVS	Sicherheitsverbund Schweiz
SVU 14	Sicherheitsverbundsübung 2014
UKW	Ultrakurzwelle
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
WEF	World Economic Forum / Weltwirtschaftsforum
WLAN	Wireless Local Area Network

Kurzfassung

Auftrag

Der Bundesrat hat das VBS am 18. Dezember 2015 beauftragt, eine Auslegeordnung über die Telekommunikationsvorhaben zu erstellen, die für den Schutz der Schweizer Bevölkerung wichtig sind. Massgebend sind die Risiken, denen die Bevölkerung in der Schweiz ausgesetzt ist. Zu denken ist dabei an mögliche terroristische Anschläge, Naturkatastrophen wie Erdbeben und Hochwasserereignisse oder technische und gesellschaftliche Katastrophen und Notlagen wie Stromausfälle oder eine Pandemie. Der Bericht soll aufzeigen, welche Systeme für den angemessenen Schutz der Schweizer Bevölkerung unentbehrlich sind und damit kurzfristig realisiert oder weiterentwickelt werden sollen. Ebenso ist darzulegen, welche Systeme eine tiefere Priorität haben und auf welche sogar verzichtet werden könnte. Dabei gilt es die Auswirkungen abzuschätzen, denen die Bevölkerung ausgesetzt ist, wenn diese Systeme den Behörden und Einsatzkräften nicht mehr oder nicht zeitgerecht zur Verfügung stehen. Als Grundlage für eine realistische Beurteilung sind ebenfalls die Kosten für die Realisierung der einzelnen Systeme abzuschätzen sowie Zuständigkeits-, Finanzierungs- und Rechtsfragen zu klären. Es liegt in der Verantwortung der politischen Behörden, die Grundsatzentscheide zu fällen, im Wissen um die damit verbundenen Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen.

Der vorliegende Bericht gibt Auskunft über den Zustand der heutigen bevölkerungsschutzrelevanten Alarmierungs- und Kommunikationssysteme sowie über die aktuellen und zu erwartenden Bedürfnisse von Bund, Kantonen und Betreibern von kritischen Infrastrukturen.

Kommunikationssysteme auf strategischer und operativer Ebene sowie Alarmierungs- und Informationssysteme für die Bevölkerung

Gegenstand des vorliegenden Berichts ist die Kommunikation auf der strategischen Führungsebene und auf der taktischen Ebene der Einsatzorgane. Auch die Alarmierung und Information der Bevölkerung in einer Katastrophensituation sind zu betrachten. Im Ereignisfall ist die Übermittlung von Sprache, Text und Bild zwischen den Behörden über ein sicheres Datenverbundnetz eine Grundvoraussetzung für die Funktionsfähigkeit der strategischen Führungsorgane auf Stufe Bund und Kantone. Dadurch werden diese erst in die Lage versetzt, angemessene Massnahmen für den Schutz der betroffenen oder bedrohten Bevölkerung und von Sachwerten anzuordnen. Dies setzt eine Übersicht über die aktuelle Lage voraus, was wiederum eine elektronische Lagedarstellung und einen gesicherten Lageverbund braucht. Das flächendeckende Sicherheitsfunknetz Polycom hat sich bei den taktischen Einsatzkräften im Alltag und im Ereignisfall bewährt. In Ballungszentren oder bei Grossereignissen haben diese Einsatzkräfte jedoch einen Bedarf nach einer mobilen drahtlosen Breitbandkommunikation (dBBK), um ihre Sicherheits-, Schutz- und Rettungseinsätze zu koordinieren und durchzuführen. Die heutige Alarmierung und Information der Bevölkerung mit Sirenen und Notfallradio soll in Zukunft mit Verhaltensanweisungen über Smartphones ergänzt werden. Damit können die Behörden die Bevölkerung noch direkter und schneller mit relevanten Informationen versorgen und dem veränderten Medienverhalten der Bevölkerung Rechnung tragen. Dies kann unmittelbar Leben retten und die Auswirkungen von Katastrophen und Notlagen reduzieren.

Erkenntnisse aus der Sicherheitsverbundsübung 2014

Die Führungsfähigkeit auf Stufe Bund und Kantone unter den Bedingungen von Stromausfall und Strommangellage war ein zentrales Thema der Sicherheitsverbundsübung 2014 (SVU 14). Dabei zeigte sich, dass vor allem die angenommene mehrmonatige Unterversorgung mit Strom eine komplexe nationale Notlage hervorrufen würde. Ein Merkmal einer solchen nationalen Krise wären technisch bedingte Führungsprobleme. Der Schlussbericht SVU 14 an die Politische Plattform des Sicherheitsverbunds Schweiz SVS hält denn auch fest: «Die untersuchten IKT-Systeme wären in einer mehrwöchigen Strommangellage deutlich eingeschränkt und würden den Ansprüchen der Lage mehrheitlich nicht genügen». Systeme, deren Funktionalität in der Krise eingeschränkt sind, ermöglichen keinen regelmässigen, zeitgerechten und verlässlichen Daten- und Informationsfluss. Sie schränken dadurch Führung, Kommunikation, Information, Alarmierung und die koordinierte Zusammenarbeit zwischen allen Ebenen massiv ein. Die Erkenntnisse aus der SVU 14 führten neben anderem zur Empfehlung, ein sicheres Datenverbundnetz (SDVN) zu realisieren, das auch im Fall einer Strommangellage funktioniert. Ebenfalls seien die Arbeiten zur Entwicklung eines Lageverbunds weiterzuführen.

Sicherheitsdefizite und anzustrebendes Sicherheitsniveau

Im vorliegenden Bericht wird ausgeführt, welche Systeme heute im täglichen Einsatz stehen und die Kommunikation zwischen den Behörden und Organisationen für Rettung und Sicherheit (BORS) sowie die Alarmierung und Information der Bevölkerung sicherstellen. Es wird dargelegt, wie die Systeme bei leichten und massiven Beeinträchtigungen (z. B. grossflächige Panne der Swisscom am 24. Mai 2016) degradieren und die Bedürfnisse der Nutzer nicht mehr erfüllen. Die dadurch entstehenden Sicherheitsdefizite werden aufgezeigt. Das Bundesamt für Bevölkerungsschutz BABS hat zusammen mit den Kantonen, den Einsatzorganisationen, den Betreibern von kritischen Infrastrukturen und verschiedenen Bundesstellen Lösungen geprüft, die diese Sicherheitsdefizite schliessen können. Die Realisierung neuer oder die Weiterentwicklung bestehender Systeme ist mit erheblichen Kosten verbunden. Deshalb ist es angebracht, nicht nur den Nutzen und die Notwendigkeit dieser Systeme für sich alleine zu betrachten, sondern eine Bewertung im Zusammenhang mit dem anzustrebenden Sicherheitsniveau vorzunehmen und auch aufzuzeigen, welchen Risiken man die Bevölkerung im Falle einer Nichtrealisierung dieser Systeme aussetzt. Gestützt auf diese Entscheidungsgrundlagen und unter Berücksichtigung der Finanzierungsmöglichkeiten kann entschieden werden, welche Vorhaben prioritär und welche zu einem späteren Zeitpunkt umgesetzt werden sollen.

Priorisierung

Die Priorisierung der Telekommunikationssysteme beruht auf 72 Stellungnahmen von Bund, Kantonen, Betreibern kritischer Infrastrukturen sowie verschiedenen Verbänden und NGO. Die Realisierung eines sicheren Datenverbundnetzes (SDVN) zusammen mit dem dazugehörigen Datenzugangssystem und geschlossenen Anwendernetz Polydata hat höchste Priorität, verbunden mit der Ablösung des Meldungsvermittlungssystems VULPUS-Telematik (VULPUS). Ausserdem werden die Erarbeitung von Grundlagen für die drahtlose Breitbandkommunikation, allenfalls verbunden mit einem Pilotprojekt der interessierten Kantone und die Entwicklung eines Lageverbundes Schweiz als Vorhaben von sehr hoher Priorität genannt.

Die Realisierung der weiteren Vorhaben wie Polysat, die Alarmierung der Bevölkerung via CBS oder SMS und auch die flächendeckende Umsetzung der drahtlosen Breitbandkommunikation dBBK werden als wichtig eingestuft. Ihre Realisierung ist aber nicht zeitkritisch und bedarf weiterer technischer Abklärungen bei den einzelnen Vorhaben.

Zuständigkeiten und Kostenschlüssel Bund–Kantone–Dritte

Die Kosten für den Aufbau, Betrieb und Werterhalt der zu realisierenden Systeme werden sich Bund, Kantone und die Betreiber von kritischen Infrastrukturen teilen müssen. Die Zuständigkeiten und die Aufgabenteilung zwischen Bund, Kantonen und Dritten muss im Rahmen der anstehenden BZG-Revision geregelt werden. Dies, weil die aktuell gültigen rechtlichen Grundlagen nicht mehr ausreichen oder für neue Systeme wie SDVN/Polydata oder dBBK noch gar nicht vorhanden sind. Das Modell zur Aufteilung von Zuständigkeiten und Kosten sowie die Festlegung der Schnittstellen sollen sich an den bewährten Regeln bei Systemen wie Polycom und Polyalert orientieren. Im vorliegenden Bericht werden entsprechende Ansätze aufgezeigt. Dabei werden die Nutzerbedürfnisse, die föderalen Strukturen, die Vorgaben der Neuen Finanzausgleichsordnung sowie volkswirtschaftliche Überlegungen berücksichtigt. Verbindlich werden die Zuständigkeits- und die damit verbundenen Finanzierungsfragen im Rahmen der anstehenden BZG-Revision geregelt.

1 Einleitung

Ausgangslage

Die Kommunikation und der Informationsaustausch zwischen den Behörden und Organisationen für Rettung und Sicherheit (BORS) in Form von Sprache, Text und Bild sowie die Alarmierung und Information der Bevölkerung im Ereignisfall sind zwei zentrale Instrumente für einen effizienten Schutz der Bevölkerung und ihren Lebensgrundlagen. Kommunikation und Informationsaustausch ermöglichen es den BORS, koordinierte Grundlagen zuhanden der Entscheidungsträger vorzubereiten, damit Massnahmen zum Schutz der Bevölkerung und ihren Lebensgrundlagen ergriffen werden können. Mit der Alarmierung und der Information der Bevölkerung wird sichergestellt, dass diese, beispielsweise bei einem Terroranschlag, einer Katastrophe oder in einer Notlage, rechtzeitig gewarnt und mit Informationen bedient wird, wie sie sich verhalten muss und sich schützen kann.

Die beiden Instrumente tragen wesentlich zur Risikoreduktion bei. Fallen sie aus, hat dies in der Regel gravierende Konsequenzen für die Sicherheit der Bevölkerung. Es ist im Ereignisfall mit grösseren Schäden, mehr Verletzten und mehr Todesopfern zu rechnen.

Für die Kommunikation und den Austausch von Informationen zwischen den BORS stehen heute die Systeme Polycom für Sprache, das Meldungsvermittlungssystem VULPUS-Telematik (VULPUS) für Text und die Elektronische Lagedarstellung (ELD NAZ) für Text- und Bildinformationen im Einsatz. Polycom ist ein Sprachfunksystem für die BORS. Polizei, Feuerwehr, Sanität, Rettungskräfte, das Grenzwachtkorps und verschiedene Betreiber kritischer Infrastrukturen benutzen Polycom täglich bei ihren Einsätzen. Es sind aber auch Behörden auf Stufe Bund (z.B. Naturgefahrenfachstellen) und Kantone mit Polycom ausgerüstet, die erst bei Ereignissen grösseren Ausmasses damit Funkverbindung zu anderen Akteuren haben. VULPUS ist ein geschütztes System für Textmeldungen ziviler und militärischer Stellen von Bund und Kantonen. Die ELD NAZ dient dem Austausch von lagerelevanten Informationen.

Für die Alarmierung und Information der Bevölkerung stehen seit Jahren die Sirenen im Einsatz, die durch das System Polyalert ausgelöst werden. Der Allgemeine Alarm fordert die Bevölkerung auf, Radio zu hören, um Informationen zum Ereignis zu erhalten. Der Wasseralarm fordert die Bevölkerung auf, das gefährdete Gebiet sofort zu verlassen. Falls in der ganzen Schweiz die Rundfunkinfrastrukturen ausfallen, kann mit IBBK, der Information der Bevölkerung durch den Bund in Krisenlagen mit Radio, trotzdem informiert werden.

Die Systeme für Kommunikation und Informationsaustausch stehen tagtäglich bei Ereignissen wie Gewaltdelikten, Verkehrsunfällen, Bränden oder bei grossen Sportanlässen im Einsatz. Sie garantieren eine effiziente Zusammenarbeit der verschiedenen Organisationen, die in diese Ereignisse involviert sind (z. B. Polizei, Feuerwehr, Sanität).

Ereignisse wie der Sturm Lothar 1999, die Hitzewellen 2003 und 2015, die Hochwasser 2005 und 2007, der Stromausfall bei der SBB 2005, die Schweinegrippe 2009 oder der Waldbrand in Visp 2011 erfordern die Zusammenarbeit einer grossen Anzahl von verschiedenen Behörden, Organisationen und Betreibern von kritischen Infrastrukturen, die miteinander Informationen austauschen müssen. Die Hochwasser 2005 machten auch den Einsatz der Sirenen in mehreren Kantonen erforderlich, um die Bevölkerung zu alarmieren, damit sie sich rechtzeitig in Sicherheit bringen konnte.

Obwohl davon ausgegangen werden kann, dass der Sprachfunk als Kommunikationsmittel und die Sirenen als Alarmierungsmittel bestehen bleiben, werden im Bevölkerungsschutz zunehmend die Möglichkeiten des digitalen Informationsaustausches genutzt und nachgefragt.

Der Austausch von grossen Datenmengen und der Einsatz von einsatzbezogenen Applikationen spielen in der täglichen Arbeit der Einsatzkräfte eine zunehmend wichtige Rolle: Sie ermöglichen einen effizienten Austausch von Wissen und Informationen und fördern die Zusammenarbeit der BORS und weiterer Partner im Bevölkerungsschutz im Einsatz.

Der Ausbau bestehender und die Schaffung neuer Informationskanäle wie beispielsweise Apps für Mobilgeräte oder SMS würden es erlauben, die Bevölkerung bei einer unmittelbaren Gefährdung oder in einem betroffenen Gebiet zielgerichtet zu alarmieren und zu informieren, auch ohne dass Sirenen ausgelöst werden müssen. Diese werden aufgrund der Isolierungen in vielen Gebäuden zunehmend nicht mehr gehört. Zudem gibt es immer mehr Schweizerinnen und Schweizer, die auf einen Sirenenalarm nicht oder falsch reagieren. Menschen mit Höreinschränkungen oder geistigen Behinderungen, die die Verhaltensanweisungen via Radio nach einem Sirenenalarm nicht wahrnehmen oder verstehen können, sind auf eine barrierefreie Alarmierung angewiesen. Mit einer Information mittels Smartphone könnten diese Personen in der wichtigen ersten Phase eines Ereignisses überhaupt erreicht

und mit Verhaltensanweisungen unterstützt werden. Dasselbe gilt auch für Ausländerinnen und Ausländer, die das Sirenensignal nicht kennen und unsere Landessprachen nicht verstehen.

Mit der Digitalisierung der Kommunikation zwischen den Behörden und der Bevölkerung entstehen aber auch neue Verletzlichkeiten. Die heute verwendeten Systeme für die Kommunikation und den Informationsaustausch sowie die Alarmierung und Information der Bevölkerung haben markante Sicherheitsdefizite.

Cyberattacken und Cyberkriminalität haben in den vergangenen Jahren stark zugenommen. Sie werden heute global als die grössten Risiken für Nutzer digitaler Kommunikationskanäle eingestuft. Cyberattacken könnten auch in der Schweiz die Netze und Systeme stören oder zum Ausfall bringen. Die BORS und andere sicherheitsrelevante Behörden könnten in einer solchen Situation nicht mehr oder nur noch eingeschränkt miteinander kommunizieren; sie würden auch in ihrem Tagesgeschäft stark eingeschränkt.

Wenn die Netzknoten und Netzkomponenten nicht mit Energie versorgt werden, fallen sie innert kurzer Zeit aus oder sind erheblich gestört. Bei kleinen, lokalen Ereignissen können die zentralen Kommunikationsfunktionen und der einsatzkritische Informationsaustausch in der Regel auf anderen Wegen mit Einschränkungen kompensiert werden. In der Schweiz muss aber auch mit schwerwiegenden Ereignissen gerechnet werden, wie Risikoanalysen auf nationaler Stufe zeigen:[1] Grossflächige Stromausfälle und langandauernde Strommangellagen, starke Erdbeben, grossflächige Stürme und Überschwemmungen sind für die Schweiz grosse Risiken mit erwarteten Schadenswerten von mehreren bis über 100 Milliarden Franken. Für die Bewältigung solcher Ereignisse mit gravierenden und weitreichenden Konsequenzen ist eine Koordination des Vorgehens von Bund, Kantonen und Betreibern von kritischen Infrastrukturen unabdingbar. Die Wahrscheinlichkeit, dass die heute verwendeten Netze und Systeme in solchen Situationen nicht zur Verfügung stünden, ist aber gross. Sie würden wegen unterbrochener Energieversorgung ausfallen, wären überlastet oder würden im Fall von Terrorereignissen aus Sicherheitsgründen abgeschaltet. Doch genau in diesen Situationen wären die BORS und die Betreiber von kritischen Infrastrukturen auf funktionierende Systeme angewiesen, um sich zu koordinieren, Informationen aufzubereiten und auszutauschen, um damit die Bevölkerung zu schützen, kritische Dienstleistungen aufrechtzuerhalten und rechtzeitig Sicherheitsmassnahmen zu ergreifen. Sie benötigen hochverfügbare Lageinformationen und Führungssysteme, um schnell und umfassend konsolidierte Grundlagen für Beurteilung und Umsetzung von Schutzmassnahmen zu erarbeiten. Die beschriebenen Risiken erfordern, dass rasch und koordiniert Massnahmen ergriffen werden, um Menschenleben zu retten sowie die Bevölkerung und Sachwerte zu schützen.

Die Führungsfähigkeit auf Stufe Bund und Kantone unter den Bedingungen von Stromausfall und Strommangellage war auch ein zentrales Thema der Sicherheitsverbundsübung 2014 (SVU 14). Dabei zeigte sich, dass vor allem die angenommene mehrmonatige Unterversorgung mit Strom eine komplexe nationale Notlage mit technisch bedingten Führungsproblemen herbeiführen würde. Der Schlussbericht SVU 14 an die Politische Plattform des Sicherheitsverbunds Schweiz SVS hält denn auch fest: «Die untersuchten IKT-Systeme wären in einer mehrwöchigen Strommangellage deutlich eingeschränkt und würden den Ansprüchen der Lage mehrheitlich nicht genügen.»[2] Systeme, deren Funktionalität in einer normalen, besonderen oder ausserordentlichen Lage eingeschränkt sind, gewährleisten keinen regelmässigen, zeitgerechten und verlässlichen Daten- und Informationsfluss. Sie schränken dadurch Führung, Kommunikation, Information, Alarmierung und die koordinierte Zusammenarbeit zwischen allen Ebenen massiv ein. Die Erkenntnisse aus der SVU 14 führten neben anderem zur Empfehlung an den Bundesrat, ein sicheres Datenverbundnetz (SDVN) zu realisieren, das auch im Fall einer Strommangellage funktioniert. Ebenfalls seien die Arbeiten zur Entwicklung eines Lageverbunds weiterzuführen.

Da der Verlust der Kommunikations- und Informationsfähigkeit die Arbeit der BORS stark erschweren bis verunmöglichen würde, sind die Verbesserung der Telekommunikationssysteme als zentrale Massnahmen zu verstehen, um das Ausfallrisiko der Systeme zu reduzieren, ihren Schutz gegenüber Cyberrisiken zu erhöhen und damit die Sicherheit der Bevölkerung zu verbessern.

Ohne den Werterhalt und die Weiterentwicklung dieser Systeme wäre bei grösseren Ereignissen mit einer erheblichen Erhöhung der Anzahl Todesopfer, Verletzten und Sachschäden zu rechnen. Die Beurteilung über die Tragbarkeit dieses Risikos und der Entscheid, mit welchen Massnahmen bzw. Systemen (und damit auch Kosten) ein gesellschaftspolitisch akzeptables Mass erreicht werden kann, muss in politischen Gremien geführt werden.

---

1 BABS (2015) Katastrophen und Notlagen Schweiz: Technischer Risikobericht.

2 Projektorganisation SVU 14 (2015) Schlussbericht SVU 14, Sicherheitsverbundsübung 2014 (SVU 14).

Auftrag

Vor dem Hintergrund der eingangs beschriebenen Entwicklungen und dem Bedürfnis der Kantone nach Grundlagen für deren Finanz- und Investitionsplanung hat der Bundesrat das VBS am 18. Dezember 2015 beauftragt, eine Auslegeordnung zu erstellen, die Auskunft gibt über den Kommunikationsbedarf von Bund, Kantonen und Betreibern von kritischen Infrastrukturen bei Katastrophen und Notlagen, über das anzustrebende Sicherheitsniveau der bevölkerungsschutzrelevanten Alarmierungs- und Telekommunikationssysteme, über Varianten zukünftiger Systeme, über die bei einer Realisierung erforderlichen Ressourcen sowie die Ausgestaltung der Rechtsgrundlagen.

Die erste Fassung des vorliegenden Berichtes wurde von September bis November 2016 bei Bundesstellen, Kantonen, Betreibern kritischer Infrastrukturen und weiteren Partnern des Bevölkerungsschutzes konsultiert. Die Konsultation bei Bund, Kantonen und Betreibern kritischer Infrastrukturen sowie die Erfahrungen beim Aufbau von Polycom zeigen, dass die Zuständigkeits- und Finanzierungsfragen insbesondere bei Verbundsystemen, bei denen sich Bund, Kantone und Dritte gemeinsam beteiligen, klar geregelt werden müssen. Der Chef VBS sowie die Präsidenten der KKJPD und RK MZF haben für die Klärung der Zuständigkeiten und Finanzierungsfragen am 10. Januar 2017 eine aus Vertretern von Bund und Kantonen zusammengesetzte Arbeitsgruppe unter der Leitung des Direktors BABS einberufen. Die Resultate dieser Arbeiten sind in den vorliegenden Bericht eingeflossen.

Aufbau des Berichts

Im Anschluss an das einleitende Kapitel werden der Nutzen und die Notwendigkeit der bestehenden Telekommunikationssysteme sowie der Bedarf an neuen Systemen anhand von konkreten Szenarien dargelegt und die bestehenden Sicherheitsdefizite aufgezeigt. Im dritten und vierten Kapitel folgt die Auslegeordnung der einzelnen Systeme für Kommunikation, Informationsaustausch und Alarmierung. Es wird gezeigt, wofür es diese Systeme braucht, was ein Verzicht für die BORS und die Bevölkerung bedeuten würde und welche Lösungsmöglichkeiten bestehen. Ein Priorisierungsvorschlag erfolgt im fünften Kapitel. Das sechste Kapitel widmet sich dem Thema der Zuständigkeiten sowie der Finanzierung in Bezug auf Investition, Werterhalt sowie Unterhalt und Betrieb. Ein Hauptfokus richtet sich auf die Aufgabenteilung und damit auch auf die Kostenteilung zwischen Bund, Kantonen und Dritten. Im siebten Kapitel wird der Zusammenhang zwischen Aufgabenteilung und Finanzierung mit der anstehenden Revision des Bevölkerungs- und Zivilschutzgesetzes erläutert. Im achten Kapitel werden die finanziellen und personellen Auswirkungen thematisiert und im neunten Kapitel die Konsequenzen beschrieben, wenn die Vorhaben nicht umgesetzt werden. Im zehnten Kapitel wird kurz das weitere Vorgehen aufgezeigt.

2 Nutzen und Notwendigkeit der Systeme

2.1 Bedeutung der Telekommunikationssysteme im Ereignisfall

Um Ereignisse wirkungsvoll zu bewältigen und die Sicherheit und den Schutz der Bevölkerung in jeder Lage zu gewährleisten, spielen Kommunikation, Informationsaustausch und Alarmierung der Bevölkerung eine zentrale Rolle. Bereits bei grösseren Ereignissen, wie sie in der Schweiz in den letzten Jahren vorkamen (Lothar 1999, die Hitzewelle 2003 und 2015, Hochwasser 2005 und 2007, Ausfall der SBB 2005, Schweinegrippe 2009, Waldbrand Visp 2011), nimmt die Bedeutung der Zusammenarbeit verschiedener Behörden, Einsatzkräften und Betreibern von kritischen Infrastrukturen zu und fordert eine gute Vernetzung aller Beteiligten.

Die Schweiz ist aber noch grösseren Risiken ausgesetzt (z. B. Terroranschläge, Erdbeben, Strommangellagen), wie Analysen auf nationaler Stufe zeigen (vgl. Abbildung).[3] Solche Ereignisse können grosse Opferzahlen, viele Verletzte, schwere Versorgungsunterbrüche und Sachschäden in Milliardenhöhe verursachen sowie die Sicherheitslage in der Schweiz markant beeinträchtigen. Zudem steht die Reputation der Schweiz auf dem Spiel, wenn die Ereignisbewältigung nicht professionell sichergestellt werden kann. Negative Reputation kann u. a. eine grosse Auswirkung auf wirtschaftliche Bereiche wie Investitionen aus dem Ausland, Tourismus etc. nach sich ziehen und mittel- bis langfristig negative Folgen haben. Die Auswirkungen solcher Ereignisse können rasch eine nationale Dimension erreichen, ihre Bewältigung eine landesweite bis internationale Zusammenarbeit auf den strategischen Führungsebenen und der taktischen Ebene erfordern. Eine zuverlässige Kommunikation, der sichere Informationsaustausch und eine wirkungsvolle Alarmierung der Bevölkerung sind dafür essenziell.

Anhand der drei exemplarischen Szenarien *Terroranschlag*, *Erdbeben* und *Strommangellage* wird im Folgenden verdeutlicht, welche Bedeutung der Zusammenarbeit aller Partner und demnach den Telekommunikationssysteme zukommt.

Beispiel: Terroranschlag in der Schweiz

Bei einem terroristischen Anschlag in der Schweiz zum Beispiel mit mehreren Tatorten in verschiedenen Kantonen wären innert kürzester Zeit alle Sicherheitskräfte im Einsatz und das Ereignis hätte eine nationale Dimension. Die sicherheitspolizeilichen Tätigkeiten (Schutz und Rettung, Sicherung, Absperrung, Opferhilfe, Intervention, Fahndung, Spurensicherung etc.) liegen in den kantonalen Kompetenzen. Jede Kantonspolizei ergreift auf ihrem Hoheitsgebiet die notwendigen Massnahmen. Je nach Ausmass des Ereignisses kommt der nationale Führungsstab Polizei als koordinatives Instrument zum Einsatz und die Armee kann subsidiär Unterstützung leisten. Bei einem Delikt mit terroristischem Hintergrund eröffnet die Bundesanwaltschaft umgehend ein Strafverfahren, da die Strafverfolgungskompetenz beim Bund liegt. Das Bundesamt für Polizei (fedpol) unterstützt die Bundesanwaltschaft und ist in enger Zusammenarbeit mit dem nationalen Führungsstab der Polizei unter anderem für die nationale und internationale Fahndung sowie für die polizeiliche Kooperation mit den ausländischen Polizeibehörden zuständig. Die Oberzolldirektion (GWK) erhöht die Ausreisekontrollen. Der Nachrichtendienst des Bundes (NDB) stellt über die Elektronische Lagedarstellung (ELD NAZ) sicher, dass alle im Nachrichtenverbund des NDB an der ELD NAZ angeschlossenen Stellen über ein einheitliches Lagebild sowie eine laufend aktualisierte Lagebeurteilung verfügen. Für die Kooperation und Koordination im Innern wird auf Stufe Bund unter Einbezug der Kantone zudem ab 2017 ein operatives Koordinationsgremium Terrorismusbekämpfung geschaffen und betrieben.[4] Ebenso rasch werden weitere Akteure wie das Eidgenössische Departement für auswärtige Angelegenheiten (EDA) im Zusammenhang mit ausländischen Opfern oder für die rasche Kooperation auf diplomatischer Stufe aktiv.

---

[3] BABS (2015) Katastrophen und Notlagen Schweiz: Technischer Risikobericht.

[4] Strategie der Schweiz zur Terrorismusbekämpfung vom 18. September 2015

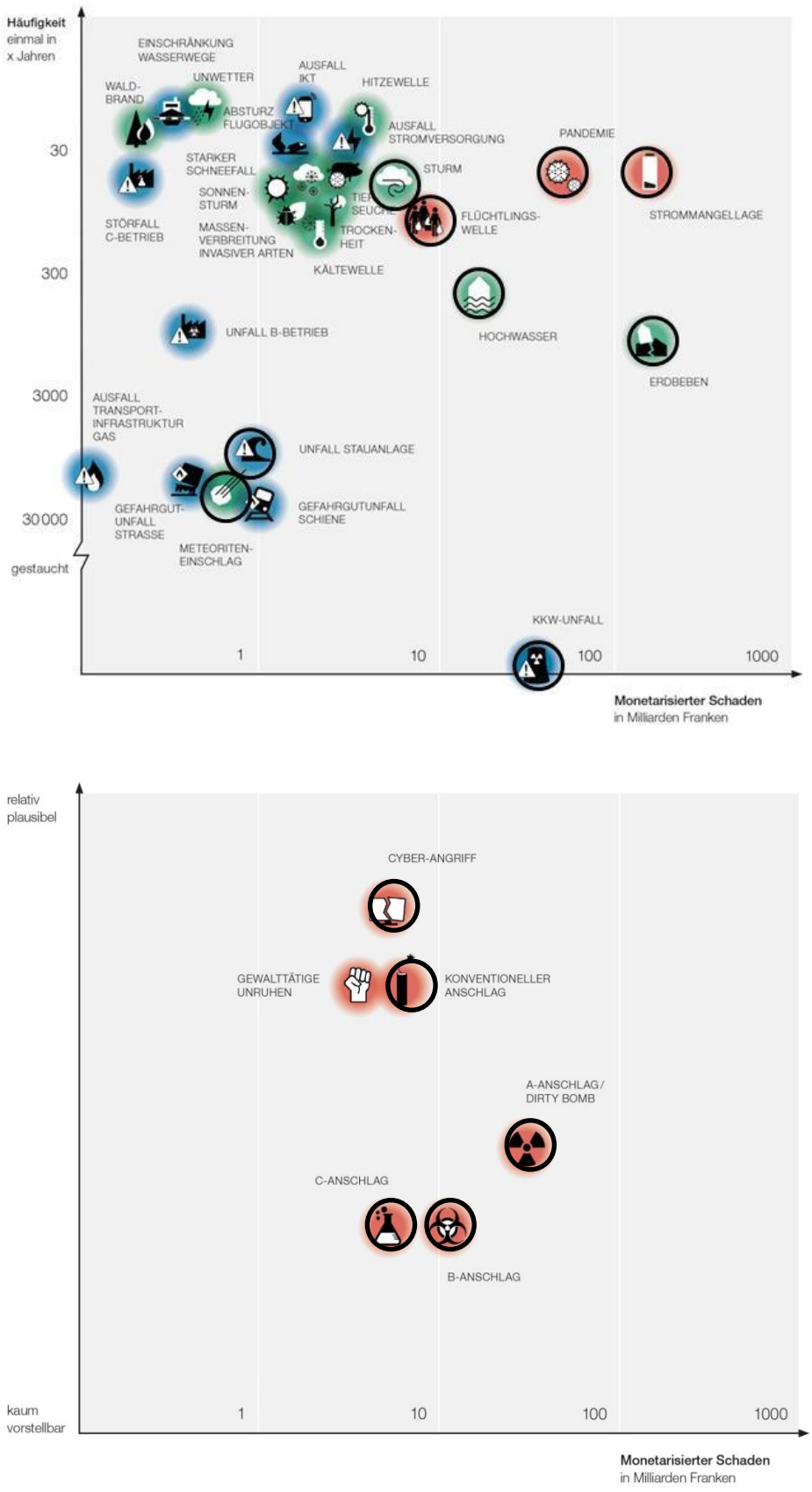

Abbildung: Risikodiagramm der Szenarien, für die eine Häufigkeit (oben) angegeben oder eine Plausibilität (unten) abgeschätzt werden kann. Schwarz umrandet sind Szenarien, bei deren Bewältigung alle Behörden und Organisationen für Rettung und Sicherheit sowie Betreiber von kritischen Infrastrukturen landesweit auf den strategischen Führungsebenen und der taktischen Ebene für den Einsatz zusammenarbeiten müssen, um koordiniert Massnahmen zum Schutz der Bevölkerung zu ergreifen und umzusetzen.

Beispiel: Erdbeben in Basel

Bei einem starken Erdbeben mit zahlreichen heftigen Nachbeben, wie es sich in Basel bereits einmal ereignet hat[5], ist im Schadensgebiet von 160 km Durchmesser mit mehreren tausend Toten und mehreren zehntausend Verletzen zu rechnen. In den ersten Stunden und Tagen ist aufgrund unbewohnbarer Häuser und unterbrochener Wasser- und Nahrungsmittelversorgung über eine halbe Million Menschen auf Unterstützung durch die Behörden angewiesen. Die Stromversorgung und die Kommunikation brechen im Schadensgebiet unmittelbar nach dem Beben zusammen und sind über Wochen bis Monate ausser Betrieb. Die Verkehrswege im Gebiet sind z. T. unpassierbar. Der Verkehr in der ganzen Schweiz ist gestört. Informationen über das Erdbeben (Magnitude, Epizentrum) erfolgen in den ersten Minuten durch den Bund bzw. den Schweizerischen Erdbebendienst (SED) und die Nationale Alarmzentrale (NAZ). Für die Rettung von Personen aus Trümmern, die medizinische Versorgung, für die Sicherung und Absperrungen, die Unterbringung von Obdachlosen etc. sind die betroffenen Kantone verantwortlich. Sie koordinieren den Einsatz und die entsprechenden Massnahmen. Aufgrund des Ausmasses werden zur Unterstützung vor Ort alle verfügbaren Rettungskräfte und Sicherheitseinheiten aus anderen, nicht betroffenen Kantonen ins Schadensgebiet verlegt. Innert Stunden treffen bei der NAZ Hilfsangebote aus dem Ausland ein. Die Einreise von ausländischen Hilfskräften wird vom EDA unter Einbezug des Bundesamtes für Zivilluftfahrt (BAZL), der Oberzolldirektion (OZD), des Flughafenbetreibers und der zuständigen Kantonspolizei koordiniert. Die verfügbaren Ressourcen aus dem In- und Ausland werden vom Bundesstab ABCN (BST ABCN) entsprechend den Bedürfnissen und basierend auf den Zuständigkeiten im Schadensgebiet zugeteilt. Nach ein bis zwei Tagen werden die zivilen Rettungs- und Sicherheitskräfte subsidiär durch die Armee unterstützt. Während der gesamten Ereignisbewältigung liefert das Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz) aktuelle Wetterinformationen für die Rettungskräfte, Behörden und für die massiv erhöhten Helikopteroperationen im Schadensgebiet. Zudem verteilt die NAZ Informationen an alle Behörden von Bund, Kantonen und an die Betreiber von kritischen Infrastrukturen. Für die Abklärung der Sicherheitslage in Kernkraftwerken sowie Störfallbetrieben und Stauanlagen im und in der Nähe des Schadensgebietes ist das Eidgenössisches Nuklearsicherheitsinspektorat (ENSI) bzw. das Departement für Umwelt, Verkehr, Energie und Kommunikation (UVEK) verantwortlich. Sie geben die Informationen an die NAZ bzw. an die kantonalen Führungsorgane weiter, um allfällige Sicherheitsmassnahmen für die Bevölkerung zu ergreifen (Sirenenalarm, Evakuierung). Andere Betreiber von kritischen Infrastrukturen (Bundesamt für Strassen ASTRA, SBB, Swissgrid, Chemiebetriebe etc.) stehen mit Bund und Kantonen in Verbindung und informieren diese über ihre Teillagen. Diese werden vom BST ABCN zu einem nationalen konsolidierten Lagebild (als Resultat des Lageverbundes) zusammengetragen und dienen dem Bundesrat als Entscheidungsgrundlage. Die Bewältigung des Ereignisses zieht sich über mehrere Monate hin.

Beispiel: Strommangellage

Steht zu wenig Strom zur Verfügung, z. B. nach langen Trockenperioden und bei hohem Stromkonsum, muss der verbleibende Strom bewirtschaftet werden.[6] Bei einer solchen Strommangellage werden in der ganzen Schweiz Gebiete alternierend während Stunden nicht mit Strom versorgt. Dabei fallen alle stromabhängigen Systeme und Geräte aus, sofern sie nicht über eine Notstromversorgung verfügen. Ausserdem ist mit unkontrollierten Stromausfällen in anderen Gebieten zu rechnen. Die Organisation für die Strombewirtschaftung in ausserordentlichen Lagen (OSTRAL) ist zusammen mit den kantonalen Energieverteilern für die Umsetzung des Abschaltplans verantwortlich und sie informieren sich gegenseitig über das Funktionieren der Massnahmen. Die Umsetzung von Massnahmen für die Sicherheit in den Gebieten, die von der Stromabschaltung betroffen sind, liegt in der Kompetenz der Kantone. Da eine koordinierte Zusammenarbeit von diversen Bundesbehörden, kantonalen Behörden und Betreibern von kritischen Infrastrukturen, z. B. Swissgrid, erforderlich ist, informieren sie sich gegenseitig über die Lage und die einzuleitenden Massnahmen. Die grossen Verkehrsunternehmen SBB und Postauto informieren das leitende Organ koordinierter Verkehr (LO KOVE) des Bundesamtes für Verkehr (BAV) über die Situation der öffentlichen Verkehrsmittel in der Schweiz. Das Bundesamt für Strassen (ASTRA) verteilt Informationen über die Situation auf den Nationalstrassen an die Kantone. Die Versorgung der Bevölkerung mit wichtigen Gütern (Wasser, Nahrungsmittel) und

---

[5] Beim Erdbeben in Basel von 1356 geht man nach heutiger Einschätzung von einer Magnitude zwischen 6.0 und 7.0 aus. Es handelte sich dabei um das grösste Erdbeben in Europa nördlich der Alpen.

[6] Die nationale Netzgesellschaft Swissgrid gelangte im Dezember 2015 an das Bundesamt für Energie (BFE) und dieses an den BST ABCN, um über Massnahmen zu diskutieren, da aufgrund der tiefen Füllstände bei den Stauseen, geringer Abflussmengen in den Flüssen und des Nichtbetriebs zweier Kernkraftwerke eine Strommangellage nicht auszuschliessen war. Im Laufe des Februars 2016 hat sich die Lage wieder entspannt. 2016/2017 war die Lage ähnlich kritisch.

Dienstleistungen (medizinische Versorgung, Versorgung mit Bargeld, Telekommunikation usw.) ist in der ganzen Schweiz während dieser Zeit massiv gestört oder unterbrochen, weil die Kommunikations- und Steuerungssysteme der Betreiber dieser kritischen Infrastrukturen nicht einwandfrei funktionieren und sie nicht über ausfallsichere Kommunikationsnetze verfügen. Die Schweizerische Nationalbank (SNB) steht mit systemrelevanten Banken in Kontakt, weil die Bargeldversorgung eingeschränkt und der Zahlungsverkehr unterbrochen ist.

Informationsbedürfnisse und Schlüsselinformationen

Beispiel: Terroranschlag

Bei einem solchen Ereignis sind die öffentlichen Kommunikationsnetze sehr schnell überlastet oder werden aus einsatztaktischen Überlegungen abgestellt. Kommunizieren die BORS jedoch über priorisierte drahtlose Breitbandverbindungen, so sind sie von solchen „Netzüberlastungssituationen“ nicht oder weniger betroffen. In Anbetracht der Dimension eines solchen Ereignisses und der Anzahl sich im Einsatz befindlicher Einsatzkräfte ist auch das Sicherheitsfunknetz Polycom überlastet. Die Einsatzkräfte sollten sich über ein gesichertes breitbandiges mobiles Kommunikationsnetz (dBBK) austauschen können. Die Koordination über die Kantonsgrenzen hinweg und zwischen den Führungsorganen von Bund und Kantonen verlangt für alle sich im Einsatz befindlichen Führungsorgane ein aktuell gehaltenes Lagebild. Dieses sollte über ein gesichertes Datenverbundnetz (SDVN) zwischen diesen Behörden und Führungsorganen ausgetauscht werden.

Die Kantonspolizei (Front und Führung), weitere Blaulichtorganisationen, der NDB, der nationale Führungsstab Polizei, das fedpol und der Sonderstab Geiselnahme und Erpressung, das Grenzwachtkorps (GWK) und die Armee benötigen für die effiziente und zielgerichtete Fahndung, Ermittlung und Ereignisbewältigung konsolidierte Lageinformationen. Diese sind aufeinander abzustimmen und den beteiligten Stellen zeitverzugslos und stufengerecht zur Verfügung zu stellen. Heute existieren dazu keine adäquaten, national aufeinander abgestimmte Möglichkeiten.

Zeitkritische Schlüsselinformationen, die innert Minuten bis wenigen Stunden verbreitet werden müssen, sind z. B. Informationen zu Fahndungsmassnahmen und -ergebnissen, Informationen zwischen den Führungsstäben der Polizei, insbesondere bei taktischen Abhängigkeiten der Ereignisse und in Bezug auf Opferinformationen, die sehr rasch aufbereitet und den zuständigen Stellen und Angehörigen im In- und Ausland übermittelt werden müssen, aber auch für das GWK, das Fahndungsmassnahmen an den Grenzen übernimmt.

Weitere Schlüsselinformationen sind Angaben über Mittel (Einsatzkräfte, Einsatzmöglichkeiten, Zustand, Verfügbarkeit), nationale konsolidierte Mitteilungen zu Be- und Überwachungsmassnahmen und die Resultate aus Ermittlungen (Täterabklärungen, Umfeld, Tatmittel, Hausdurchsuchungen). Diese Informationen müssen national möglichst rasch abgeglichen und konsolidiert werden, um Zugriffe auf die Täterschaft synchronisieren zu können. Dazu ist der zeitgerechte Informationsaustausch zwischen den Justizbehörden und ausländischen Behörden via Bundesanwaltschaft und das Bundesamt für Polizei zentral.

Beispiel: Erdbeben

Nach einem starken Erdbeben benötigen Führungsorgane (kantonale Führungsstäbe, Bundesstab) möglichst rasch eine Übersicht über Schadensgebiete und Opferzahlen (Tote und Verletzte) sowie Informationen von Fachstellen (z.B. ENSI, NAZ) und Betreibern von kritischen Infrastrukturen, um Rettungs-, Hilfs und Schutzmassnahmen (Mittel, Einsatzkräfte) effizient und zielgerichtet einzuleiten. Die Lageinformationen sind aufeinander abzustimmen und den beteiligten Stellen zeitverzugslos und stufengerecht zuzustellen, um möglichst viele Menschenleben zu retten und die Rettungskräfte zu schützen. Heute existieren dazu nur unzureichende national aufeinander abgestimmte Möglichkeiten.

Zeitkritische Schlüsselinformationen für Führungsorgane, Rettungsorganisationen aus dem In- und Ausland und weitere Blaulichtorganisationen sind Angaben zu den Schäden an Gebäuden, Verkehrswegen und anderen kritischen Infrastrukturen. Die im Einsatz stehenden Organisationen benötigen möglichst rasch Angaben zu Opferzahlen und Informationen zum Zugang in die entsprechenden Schadensgebiete sowie ständig aktualisierte Informationen zur Wetterlage. Neben den Informationen zu den Auswirkungen auf die Bevölkerung benötigen alle beteiligten Stellen zeitverzugslos Informationen zu Risiken für die Bevölkerung und die Rettungskräfte, die von beschädigten kritischen Infrastrukturen ausgehen. Dazu zählen auch Informationen zur Sicherheitslage an Talsperren und Kernanlagenstandorten sowie zu allfällig notwendigen Schutzmassnahmen für die Bevölkerung infolge eines drohenden Dammbruchs oder einer möglichen Freisetzung von Radioaktivität.

Weitere Schlüsselinformationen betreffen Mittel (Einsatzkräfte, Einsatzmöglichkeiten, Zustand, Verfügbarkeit), Hilfs- und Rettungsmassnahmen sowie Nachbeben und Gefahrengebieten. Diese Informationen müssen national rasch abgeglichen und konsolidiert werden, um die Hilfe optimal zu organisieren und die Sicherheit der Einsatzkräfte zu gewährleisten.

Beispiel: Strommangellage

Die Führungsorgane auf Stufe Bund und Kanton benötigen regelmässig verlässliche Informationen zur Lage im Verkehr, zur Verteilung von Gütern und zur Sicherheitslage in den betroffenen Gebieten. Für die Strombewirtschaftung sind die Führungsorgane auf Stufe Bund im Ereignisfall darauf angewiesen, in regelmässigen Abständen (Stunden und Tage) Informationen zu den geplanten und ausgeführten Gebietsabschaltungen und über die von der Stromkontingentierung betroffenen Energieabnehmer (insbesondere Betreiber von kritischen Infrastrukturen) zu erhalten. Dies ermöglicht, die Strombewirtschaftung anzupassen und möglichst rasch wieder in eine normale Lage zu gelangen.

Zeitkritische Schlüsselinformationen auf kantonaler Stufe sind Informationen für die Führungsorgane und Einsatzkräfte (Blaulichtorganisationen) zu Kollateralschäden durch die Stromabschaltung in einem Gebiet (Verkehrsunfälle, Ausfall von kritischen Infrastrukturen wie z. B. Spitäler, Abwasserreinigungsanlagen), um die Sicherheit und den Schutz der Bevölkerung in diesen Gebieten gewährleisten zu können.

Fazit

Das Risiko und die Plausibilität solcher Ereignisse in der Schweiz sind verhältnismässig gross. Erfahrungen aus dem Ausland haben gezeigt, dass solche komplexe Lagen 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. Im Ereignisfall ist die gegen Stromausfall und Cyberangriffe gesicherte Kommunikation zwischen den Behörden eine Grundvoraussetzung für die strategischen Führungsorgane, um Massnahmen zum Schutz der betroffenen Bevölkerung und Sachwerte anordnen zu können. Die Sprach- und Datenkommunikation muss in diesen oder vergleichbaren Szenarien jederzeit unterbruchfrei sichergestellt sein. Erfahrungsgemäss stehen aber gerade in solchen Fällen die öffentlichen Kommunikationsmittel und -netze für private Endkunden nicht oder nur eingeschränkt zur Verfügung. Bei den jüngsten Terroranschlägen in Paris und Brüssel fielen die Kommunikationsnetze für mehrere Stunden aus, was die Koordination der Einsatzkräfte massiv erschwerte. Bei den Anschlägen in Boston 2013 wurden die Mobilnetze sicherheitshalber abgeschaltet. Dieser Problematik kann durch den Einsatz verfügbarer BORS-Produkte heute entgegengetreten werden. Diese Option ist vertieft zu prüfen. Auch im Fall von starken Erdbeben oder der beschriebenen Strommangellage wäre die Kommunikation von allen relevanten Akteuren stark erschwert, weil die aktuell verwendeten Kommunikationsnetze mit sehr hoher Wahrscheinlichkeit gestört wären oder ganz ausfielen. Kommunikation und Informationsaustausch sind in diesen Situationen aber von zentraler Bedeutung, um die Sicherheit der Bevölkerung mittels koordinierter Führung und Umsetzung von Sicherheitsmassnahmen zu gewährleisten. Nur mit krisensicheren Kommunikations- und Datennetzen können die BORS koordiniert und effizient agieren und Entscheidungsgrundlagen für die strategische Ebene konsolidiert aufbereiten und übermitteln, um weitere Schäden abzuwenden. Dies ist das Ziel SDVN/Polydata auf strategischer Ebene und des Vorhabens dBBK auf operativ-taktischer Ebene.

2.2 Bestehendes Sicherheitsniveau und Sicherheitsdefizite

Die bestehenden Sicherheitssysteme weisen drei wesentliche Defizite hinsichtlich der Kommunikation, des Informationsaustausches und der Alarmierung der Bevölkerung auf:

- Die verwendeten Kommunikationsnetze und -dienste erfüllen die Anforderungen für die Ereignisbewältigung nicht in allen Lagen, d. h. sie sind verletzlich gegenüber Stromausfall und Cyberattacken.
- Basierend auf den bestehenden Systemen ist das Erstellen eines konsolidierten Lagebildes in allen Themenbereichen nicht umfassend und ausfallsicher möglich.
- Die Alarmierung mit Sirenen und Radio allein erreicht heute nur einen Teil der Bevölkerung und ist nicht barrierefrei. Menschen mit Behinderungen, beispielsweise mit Hörbeeinträchtigung, erreicht der Sirenenalarm nicht.

Verwendung von öffentlichen Kommunikationsnetzen und -diensten für die Ereignisbewältigung

Für die Führungs- und Einsatzkommunikation verwenden die BORS Datendienste mit Breitband-Charakter. Der Austausch von grossen Datenmengen (z. B. Fotos, Videos, Messwerte) oder die Nutzung von Applikationen, wie z. B. das Informations- und Einsatz-System des Koordinierten Sanitätsdienstes (IES-KSD), erfolgt zurzeit bei Bund und Kantonen über verschiedene öffentliche Netze und Dienste, für deren Betrieb in der Regel Leistungen der Swisscom oder anderer privater Firmen eingekauft werden. Informationen über Ereignisse sowie Verhaltensanweisungen an die Bevölkerung werden vermehrt via Mobiltelefone verbreitet (z. B. Hochwasser im Matte-Quartier in Bern). Sirenen werden nur im äussersten Notfall ausgelöst.

Die herkömmlichen Kommunikationsplattformen sind verletzlich und daher weniger krisensicher:

- Längere Stromausfälle durch technisches Versagen oder verursacht durch Naturereignisse sowie gezielte Cyberattacken auf die Betreiber der Netze können dazu führen, dass diese Systeme bereits nach kurzer Zeit nicht mehr verfügbar sind.
- Werden bei Grossanlässen und im Ereignisfall in öffentlichen Netzen von BORS-Nutzern nicht priorisierte Mobilfunkangebote eingesetzt, so kann dies dazu führen, dass deren Kommunikation nicht mehr gewährleistet werden kann.
- Bei physischen Schäden durch Naturkatastrophen, Terroranschlägen, Sabotage oder technisches Versagen ist davon auszugehen, dass die Wiederherstellung dieser Kommunikationsnetze im besten Fall Tage, gegebenenfalls aber Wochen bis Monate in Anspruch nehmen würde.

Gerade in diesen Situationen brauchen die BORS sowie die Betreiber von kritischen Infrastrukturen zur Bewältigung der Situation sichere und hochverfügbare Kommunikationssysteme sowie Betriebsorganisationen, die auch im Katastrophenfall rund um die Uhr zur Verfügung stehen. Es sind entsprechende Massnahmen zu ergreifen, um die Verfügbarkeit und Krisenresistenz der vorhandenen Infrastrukturen zu verbessern. So können beispielsweise BORS-Nutzer mittels einer Priorisierung ihrer Kommunikationsverbindungen vermeiden, dass sie bei einer Überlastung öffentlicher Netze (Ereignisfall, Grossanlässe) Einschränkungen in Kauf nehmen müssen.

Fehlendes Instrument für ein konsolidiertes Lagebild

Zurzeit fehlt ein ausfallsicheres und alle Einsätze übergreifendes Instrument, das es bei Katastrophen und Notlagen ermöglicht, konsolidierte Lageinformationen aus verschiedenen Teillagen von Kantonen, Bundesstellen und Betreibern von kritischen Infrastrukturen zu erstellen und den Nutzern drahtgebunden und drahtlos zur Verfügung zu stellen. Ein solches Instrument wäre aber notwendig, um die Zusammenarbeit zwischen den zahlreichen Partnern bei der Bewältigung von Katastrophen und Notlagen umfassend sicherzustellen. Die Führungsorgane auf Stufe Bund (z.B. Bundestab ABCN) und Stufe Kanton benötigen für ihre Entscheidungsprozesse die Übersicht über die Gesamtlage Schweiz. Durch das Zusammenführen von Teillagen beteiligter Partner könnte mit einem konsolidierten Lagebild die Basis für die erforderlichen Führungs- und Entscheidungsgrundlagen bei sicherheits- und bevölkerungsschutzrelevanten Lagen auf nationaler Stufe sichergestellt werden. Mit den heute verwendeten Systemen können insbesondere zeitkritische Informationsbedürfnisse der involvierten Stellen sowie das Bedürfnis nach stufengerechter konsolidierter Lageinformation bei Katastrophen und Notlagen nicht bereitgestellt werden, selbst wenn die Energieversorgung und die Kommunikationsmittel funktionieren.

Nicht barrierefreie Alarmierung

Mit Sirenen und der nachfolgenden Radiomeldung kann nur ein Teil der Bevölkerung alarmiert werden. Für Menschen mit Behinderungen (z.B. Hörbeeinträchtigungen) ist die Alarmierung nicht barrierefrei. Auch Ausländer und Ausländerinnen erreichen die Warnung und Alarmierung nicht, weil sie die Sirenensignal nicht kennen, die Informationen und Verhaltensanweisungen auf Deutsch, Französisch oder Italienisch via Radio nicht verstehen oder nicht empfangen. Es fehlen zurzeit Alarmierungskanäle, mit der mehr Menschen und auch verletzliche Personengruppen erreicht werden und den Informationsgewohnheiten der Bevölkerung entsprechen.

2.3 Anforderungen an Telekommunikationsdienstleistungen und angestrebtes Sicherheitsniveau

Die Risiken, die die Nutzung neuer Kommunikationskanäle und -formen für den Schutz der Bevölkerung einschränken oder gar verunmöglichen, erfordern konkrete Massnahmen. Die mittelfristig geplante Weiterentwicklung der Telekommunikationssysteme des Bevölkerungsschutzes trägt den Bedürfnissen der BORS und der Bevölkerung sowie bereits bestehenden Systemen Rechnung und soll das Sicherheitsniveau in der Schweiz signifikant verbessern. Die im vorliegenden Bericht präsentierten Vorhaben würden die Führung und die Einsatzbewältigung wesentlich optimieren, da in kurzer Zeit umfassende Grundlagen für zu fällende Entscheide erarbeitet und bereitgestellt werden könnten und somit bestehende Sicherheitsdefizite im Bevölkerungsschutz schliessen.

Die Behörden und Einsatzkräfte sollen über Kommunikations- und Alarmierungssysteme verfügen, die in sämtlichen bevölkerungsschutzrelevanten Lagen wirksam, sicher und leistungsfähig zur Verfügung stehen. Dies soll sowohl für die Bewältigung von Alltagsereignissen als auch von komplexen Katastrophen und Notlagen gelten. Dazu müssen die Telekommunikationssysteme in folgender Hinsicht verbessert werden:

Sicherheit und Verfügbarkeit der Kommunikations- und Alarmierungssysteme verbessern

Die Sicherheit und Verfügbarkeit der Telekommunikationssysteme ist zu verbessern, damit diese insbesondere gegenüber Cyberangriffen und Stromausfällen ausfallsicherer als bisher sind.

Einsatzbereitschaft der Systeme in allen Lagen gewährleisten

Der Sicherstellung des Business Continuity Management (BCM) dieser Systeme und Prozesse kommt eine herausragende Bedeutung zu. Neben technischen Massnahmen erfordert der Anspruch an eine hohe Verfügbarkeit und Resilienz in allen Lagen zwingend eine Betriebsorganisation, die rund um die Uhr im Einsatz steht, um den unterbruchfreien Betrieb und die schnelle Störungsbehebung sicherzustellen.

Hochverfügbare Lageinformationen für alle Partner im Sicherheitsverbund Schweiz (SVS) sicherstellen

Viele Risiken mit schwerwiegenden Auswirkungen auf die Sicherheit der ganzen Schweiz, die Bevölkerung und ihre Lebensgrundlagen erfordern ein koordiniertes Vorgehen von Bund und Kantonen. Dazu benötigen die Partner im SVS Zugriff auf umfassende Lageinformationen in Echtzeit.

Mobile Breitbandkommunikation für Einsatzkräfte verbessern

Der Zugriff auf Datenbanken, Lageinformationen oder geographische Informationssysteme muss für die Einsatzkräfte jederzeit gewährleistet sein. Die mobile Breitbandkommunikationsinfrastruktur sollte auf nicht oder nicht ausreichend erschlossene Gebiete der Schweiz ausgedehnt werden.

Mobile Endgeräte bei der Alarmierung und Information der Bevölkerung einbeziehen

Der Einbezug von mobilen Endgeräten (z. B. Smartphones, Pager) in die Alarmierung und Ereigniskommunikation ist notwendig, damit die Bevölkerung im Ereignisfall über ihre im Alltag geläufigen Informationskanäle schnell alarmiert und informiert wird, um sich richtig zu verhalten.

3 Kommunikation zwischen den BORS

Die organisationsübergreifende Kommunikation sowie der Austausch von Informationen sind für die Bewältigung von Ereignissen von zentraler Bedeutung. Nur so ist es den BORS möglich, ihr Handeln zu koordinieren und einen effizienten Einsatz zu leisten.

Im Zuge der digitalen Transformation wurden im Ausland bereits verschiedene Entwicklungen für den breitbandigen Datenaustausch vorangetrieben. Nach den Studien über Blackouts und das Abhören von Politikern wurde ab 2014 in Deutschland ein sicheres Kerntransportnetz (KTN Bund) aufgebaut. In Österreich wurde schon 1990 der Grundstein zur Schaffung eines landesweiten Datennetzes gelegt, an das rund 1200 Polizeidienststellen angeschlossen sind. Bis 2010 wurde das Netz mit zusätzlichen Anwendungen wie Telefonie, Digitalfunk BOS Austria ausgebaut und mit den notwendigen Schutzausrüstungen ergänzt. In Finnland und Belgien werden derzeit erste Betriebserfahrungen mit dBBK-ähnlichen Systemen gemacht. In den USA wurde mit FirstNet nach den Kommunikationsproblemen der BORS bei den Terroranschlägen vom 11. September 2001 eine grosse Initiative gestartet, um die mobile Datenkommunikation bei den Rettungs- und Sicherheitsorganisationen durchgängig zu ermöglichen.

Die BORS kommunizieren heute in der ganzen Schweiz über Polycom, einem einheitlichen, digitalen Bündelfunksysteme für Sprache, das speziell auf den Bereich der öffentlichen Sicherheit zugeschnitten ist. Mittlerweile nutzen mehr als 55 000 Angehörige der BORS Polycom bei ihrer täglichen Arbeit, z. B. bei Verkehrsunfällen und Bränden, aber auch bei Grossanlässen wie der Street Parade in Zürich oder dem WEF in Davos, an dem auch Angehörige der Armee subsidiär in den Gesamteinsatz integriert werden. Da Polycom allen BORS in der Schweiz erlaubt, miteinander zu kommunizieren, ist das System auch bei Katastrophen und Notlagen, bei denen sie zusammenarbeiten müssen, einsatzfähig.

Mit der Digitalisierung der Kommunikation und des Informationsaustauschs hat in den letzten Jahren der Bedarf der BORS nach Datendiensten mit einer hohen Datenübertragungsrate (Breitband) zugenommen. Solche Dienste verbessern die Kommunikation und den Informationsaustausch im Einsatz wesentlich. Der Zugang zu Informationen wie Fotos (z. B. Satellitenbilder), geographischen Informationssystemen (z. B. Gefahrenkataster), elektronischen Lagedarstellungsapplikationen (z. B. ELD NAZ) und Datenbanken usw. können von jedem Angehörigen der BORS im Einsatz verwendet werden.

Die Kommunikation von Bund und Kantonen basiert einerseits auf eigenen Netzen (z. B. Bundesverwaltungsnetz, Kommunikationsnetz Bundesverwaltung–Kantonalverbund (KomBV-KTV), Führungsnetz Schweiz der Armee, kantonale Polizeinetze), andererseits auf einer Vielzahl von öffentlichen Netzen und Diensten, für deren Betrieb in der Regel Leistungen der Swisscom oder anderer privater Firmen eingekauft werden. Diese Netze entsprechen allerdings nicht dem angestrebten Sicherheitsniveau im Bereich der Telekommunikationssysteme des Bevölkerungsschutzes.

Nachfolgend werden die für den Bevölkerungsschutz wichtigsten bestehenden und zur Diskussion stehenden neuen Kommunikationssysteme beschrieben. Die Priorisierung dieser Systeme im Lichte der Finanzierungsmöglichkeiten erfolgt im Kapitel 5. Dabei wird ersichtlich, dass die Systeme zwar für die Sicherheit der Schweizer Bevölkerung alle wichtig und deshalb wünschbar sind, aber mindestens zurzeit nicht alle finanzierbar und damit realisierbar sind.

3.1 Polycom 2030[7]

Bei Polycom 2030 geht es um eine Investition für den Werterhalt eines bestehenden Systems. Polycom wurde in verschiedenen Phasen von 2001 bis 2015 in Betrieb genommen; erste Basisstationen müssen in den kommenden Jahren ersetzt werden.

Die Gesamtausgaben des Bundes für den Werterhalt Polycom (nationale Komponenten) belaufen sich im Zeitraum 2016 bis 2030 auf 500 Millionen Franken.

Der Bundesrat beantragte für werterhaltende Massnahmen von Polycom einen Verpflichtungskredit von 159,6 Millionen Franken;[8] dies beinhaltet für Leistungen Dritter 94,2 Millionen Franken zugunsten des BABS und 65,4 Millionen Franken zugunsten des Grenzwachtkorps (GWK). Der Verpflichtungskredit wurde 2016 vom Parlament genehmigt. Dazu kommen Eigenleistungen des BABS mit 45,6 Millionen Franken und des GWK mit 161 Millionen Franken. Die Betriebskosten bis 2030 zulasten des

---

[7] Das Projekt Polycom 2030 wird hier nur der Vollständigkeit halber aufgeführt. Es ist nicht Gegenstand der Priorisierung in diesem Bericht, da der Bundesrat den Entscheid zur Erneuerung des Systems im Dezember 2015 bereits getroffen hat.

[8] Bundesratsbeschluss vom 25. Mai 2016 zur Botschaft Werterhalt Polycom 2030.

BABS betragen für den gleichen Zeitraum 120 Millionen Franken. Für dringliche Entwicklungsarbeiten im 2016 hat das Parlament einen Nachtragskredit von 13,8 Millionen Franken genehmigt. Für das Projekt ist das BABS verantwortlich.

Die Kantone haben neben ihrem Anteil an den Betriebskosten die Kosten für den Werterhalt der dezentralen Komponenten, d.h. die Nachrüstung der Basisstationen, zu übernehmen, die nicht durch das GWK finanziert werden.[9] Der Nachrüstungszeitpunkt ist abhängig vom Alter der technischen Komponenten der Basisstationen. Die Nachrüstung ist bis Ende 2025 abzuschliessen.

3.2 Sicheres Datenverbundnetz und Datenzugangssystem Polydata

Heute erfolgt die festnetzbasierte breitbandige Datenkommunikation der BORS und der Betreiber von kritischen Infrastrukturen über das Bundesverwaltungsnetz, das Kommunikationsnetz Bundesverwaltung–Kantonalverbund, die kantonalen Polizeinetze oder über Netze öffentlicher Anbieter (z. B. Swisscom).

Diese drahtgebundenen Systeme und Netze bieten in der normalen Lage, in der besonderen und in der ausserordentlichen Lage keine Garantie für einen regelmässigen, zeitgerechten und verlässlichen Daten- und Informationsfluss. Sie können im Ereignisfall überlastet werden oder wegen Strompannen oder Cyberattacken ausfallen. Die koordinierte Zusammenarbeit im Ereignisfall zwischen allen Ebenen, d. h. Führung, Kommunikation, Information und Alarmierung, würde damit eingeschränkt oder verunmöglicht. Dies könnte gravierende Folgen für die Bevölkerung haben, wenn im Rahmen der Ereignisbewältigung erforderliche Schutzmassnahmen gar nicht, ungenügend oder zu spät umgesetzt werden könnten.

Mit dem Aufbau von SDVN und Polydata werden die Ausfallsicherheit der Kommunikation und des Datenaustausches der BORS erhöht sowie die Integrität und der Schutz gegenüber Cyberattacken wesentlich verbessert.

Das sichere Datenverbundnetz (SDVN) soll als Transportnetz (Layer 1 und 2) für grosse Datenmengen die Grundlage für alle sicherheitspolitisch relevanten Telekommunikationssysteme des Bevölkerungsschutzes bilden; das heisst, es soll zukünftig zum zentralen Transportnetz im Bevölkerungsschutz und im nationalen Krisenmanagement werden.

Bei der Realisierung von SDVN werden physische Komponenten des Führungsnetzes Schweiz verwendet werden, d. h. Glasfasern und Infrastrukturen. Wo die Erschliessung durch das Führungsnetz ungenügend ist, sollen Glasfasernetze und physische Infrastrukturen von weiteren Netzen eingesetzt werden, z.B. Netze von Bund, Kantonen oder von Betreibern kritischer Infrastrukturen. Der Verbund dieser Glasfasernetze wird als SDVN bezeichnet. Das SDVN soll die Vernetzung zwischen den Bundesstellen, Kantonen und Betreibern von kritischen Infrastrukturen breitbandig auch im Fall einer länger andauernden Strommangellage, bei Stromausfall oder beim Ausfall der kommerziellen Kommunikationsnetze während mindestens zweier Wochen sicherstellen. Darum werden bei der Planung insbesondere diejenigen Netzinfrastrukturen in die Konzeption miteinbezogen, die bereits dieser Anforderung genügen. Ansonsten wird die Stromausfallsicherheit der miteinbezogenen Drittnetze überprüft und unter Umständen verbessert.

Polydata ist ein geschlossenes Anwendernetz (Layer 3). Unter geschlossenen Anwendernetzen werden isolierte logische Netze verstanden, die keine Übergänge ins Internet oder andere IP-Netze haben. Durch das Netz «Polydata» wird den Anwendern 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 IP-Netzen notwendig. Auf dem SDVN können in Kombination mit Polydata alle bevölkerungsschutzrelevanten Applikationen (bestehende und zukünftig entwickelte) in allen Lagen sicher betrieben werden.

Anwendungen in diesem Netz sind Polycom, Polyalert, Polyinform und weitere sicherheitsrelevante Systeme und Applikationen. Durch die Isolation gegenüber allen anderen Netzen (z.B. dem Internet) wird die Resilienz gegenüber Cyber-Angriffen signifikant erhöht. Polydata kann von den Nutzern auch im Tagesgeschäft eingesetzt werden und basiert auf dem sicheren Transportnetz SDVN.

[9] Schreiben ‚Werterhalt Sicherheitsfunknetz der Schweiz Polycom' vom 24.12.15 an die Regierungsräte der Kantone.

SDVN und Polydata sind thematisch eng miteinander verknüpft und können nicht losgelöst voneinander betrachtet, realisiert und betrieben werden.[10] Denn ohne die Realisierung von Polydata ist der sichere und in allen Lagen garantierte Zugang zu den bevölkerungsschutzrelevanten Alarmierungs- und Telekommunikationssystemen nicht gewährleistet. Investitionen ins SDVN ohne Polydata machen deshalb keinen Sinn.

Synergien und Abhängigkeiten

Das schweizweite Behördennetzwerk des Bundes und der Kantone KomBV-KTV (Layer 3) vernetzt den Bund mit den kantonalen und kommunalen Vollzugstellen. Dieses logische IP-Netz basiert heute auf Netzen von öffentlichen Anbietern und Kantonen. Der Betrieb des Netzes ist im Fall eines Stromausfalls oder einer Strommangellage nicht gewährleistet. Bei der Realisierung von SDVN kann KomBV-KTV in Zukunft auf SDVN betrieben und die Ausfallsicherheit dieses Netzes signifikant verbessert werden. Den Nutzern des KomBV-KTV wie auch des Behördennetzes wird somit eine Möglichkeit geboten, Lücken in ihrem BCM zu schliessen.

Auf SDVN können neben Polydata, weitere logische Netze aufgebaut werden, die einen hohen Anspruch an die Verfügbarkeit in Fall von Strom- oder IKT-Ausfällen stellen.

Bei der Realisierung von Polydata können bestehende logische Netze, wie z.B. das B-MPLS-Netz[11] für Polycom weiterentwickelt und auf die neuen Bedürfnisse der Nutzer ausgerichtet werden. Die Nutzung weiterer Synergien zusammen mit dem geplanten Vorhaben des EJPD im Bereich der gerichtspolizeilichen Fernmeldeüberwachung ist noch abzuklären.

Folgen eines Verzichts auf SDVN und Polydata

Ein Verzicht auf SDVN und Polydata würde für die Partner des Bevölkerungsschutzes bedeuten, dass sie bei Ereignissen, die zu Stromausfällen, Strommangellagen oder zu Störungen der öffentlichen Kommunikationsnetze führen, mit hoher Wahrscheinlichkeit nur Zugriff auf ihre lokalen Führungsinstrumente hätten. Dies hätte zur Folge, dass die Organisationen, die bei der Bewältigung eines Ereignisses zusammenarbeiten müssen, nicht mehr in der Lage wären, miteinander zu kommunizieren und Daten sowie Informationen auszutauschen. Die Lagebeurteilung, die Entscheidfassung sowie die Ereignisbewältigung würden damit massiv erschwert. Durch diese stark reduzierte Handlungsfähigkeit der Behörden verschärfen sich die Auswirkungen einer Katastrophe. Daraus resultieren je nach Ereignis gravierende Konsequenzen für die Bevölkerung. Opferzahlen, die Anzahl Verletzte und Sachschäden in Milliardenhöhe könnten in einen direkten Zusammenhang mit der mangelnden Führungs- und Einsatzkommunikation oder einer unzulänglichen Alarmierung und Information der Bevölkerung gestellt werden.

Varianten

Der Bundesrat hat an seiner Sitzung vom 20. Mai 2015 entschieden, bei einer Konkretisierung von SDVN folgende Variante (sogenannte Variante 4) weiterzuverfolgen: SDVN soll auf der Konzeption und den Technologien des Führungsnetzes Schweiz basieren. Auch auf der physischen Ebene (Glasfaserkabel und Standorte) soll es auf dem Führungsnetz Schweiz aufbauen und durch weitere physische Netzkomponenten im Anschlussbereich ergänzt werden (namentlich dem ASTRA-, dem Swissgrid- und dem SBB-Netz, aber auch kantonalen Netzen). Das SDVN soll so realisiert werden, dass der Datenverkehr der Armee auf dem Führungsnetz Schweiz vollständig getrennt ist vom Datenverkehr der Nutzer des SDVN. Damit wird den Sicherheitsbedürfnissen der Armee Rechnung getragen. Gemäss der IKT-Strategie des Bundes 2016 – 2019 soll die FUB den Betrieb und den Service (für SDVN und Polydata) rund um die Uhr sicherstellen. Dies gilt sinngemäss auch für den Betrieb von Polydata. Im Rahmen der geplanten «Netzwerkstrategie des Bundes» soll u.a. festleget werden, welche schweizweiten Telekommunikationsnetze sich auf bundeseigener Infrastruktur abstützen müssen oder (teilweise) als Service auf dem Markt eingekauft werden. Bei den bundeseigenen Netzwerken soll zudem festgelegt werden, von welchen internen IKT-Leistungserbringern diese Netze oder Netzschichten zu betreiben sind und welche Betriebsleistungen davon externen Leistungserbringer übertragen werden.

---

[10] Im Rahmen der konzeptionellen Tätigkeiten werden sie der Einfachheit halber in zwei Arbeitspakete aufgeteilt.

[11] B-MPLS ist ein IP-Netz, das die Kommunikation zwischen den Polycomnutzern ermöglicht.

3.3 Ablösung VULPUS-Telematik

Unter der Ablösung von VULPUS-Telematik werden die Arbeiten zusammengefasst, die notwendig sind, um die Funktionen des derzeit verwendeten Systems VULPUS-Telematik (VULPUS) nach dessen Ausserbetriebnahme sicherzustellen.

VULPUS ist ein geschütztes Meldungsvermittlungssystem ziviler Stellen von Bund und Kantonen und Dritten. Es dient seit rund 30 Jahren dem Informationsaustausch (v.a. Textmeldungen) der Bundesanwaltschaft, der kantonalen Polizeikorps, der Stadtpolizei Zürich, des GWK, der militärischen Sicherheit, der NAZ, dem NDB, verschiedener Sonderstäbe des Bundesrates, des BABS und verschiedener Alarmformationen. VULPUS wird heute bei der Alarmierung, der Alarmfahndung und beim Vermitteln der Naturgefahrenwarnungen der Fachstellen des Bundes unter Einbezug der Medien (Radiostationen) eingesetzt. Die Informationsübertragung erfolgt nicht automatisch, sondern durch einen verantwortlichen Operateur. Sie basiert auf militärischen und zivilen Netzen. Das System wird im Tagesgeschäft der genannten Organisationen und Behörden verwendet. VULPUS wird heute durch die Armee betrieben und auch im Wert erhalten. Die Armee ihrerseits hat keinen Bedarf an VULPUS.

Die Dienstleistungen, die mit VULPUS erbracht werden, sind von zentraler Bedeutung für die Kommunikation der Behörden und müssen auch in Zukunft im Tagesgeschäft sowie in Katastrophen und Notlagen zur Verfügung stehen. VULPUS basiert auf dem analogen Telefonie-Netz der Swisscom, dessen Anschlüsse in absehbarer Zeit ausser Betrieb genommen werden. Der Weiterbetrieb der Anschlüsse ist bis 2022 sichergestellt.

Synergien und Abhängigkeiten

Es existieren heute bereits verschiedene Anwendungen, die ähnliche oder identische Funktionen haben wie VULPUS. Diese Anwendungen könnten die Funktionen des heutigen VULPUS übernehmen, falls daran Anpassungen vorgenommen werden. Nach der Prüfung der technischen Machbarkeit, den Anforderungen an die Sicherheit und der Wirtschaftlichkeit können solche Anwendungen weiterentwickelt und angepasst werden, um die Funktionen von VULPUS nach dessen Ausserbetriebnahme sicherzustellen.

Falls SDVN und Polydata realisiert würden, würde ein Betrieb der Funktionen von VUPLUS auf diesen Systemen die Ausfallsicherheit der neuen Anwendungen und deren Schutz vor Cyber-Angriffen wesentlich verbessern.

Folgen eines Verzichts auf eine VULPUS-Ablösung

VULPUS ist am Ende seines Lebenszyklus und kann aktuell nur noch mit einem unverhältnismässig grossen Aufwand weiterbetrieben werden. Auf das System VULPUS kann grundsätzlich verzichtet werden, nicht aber auf dessen Funktionen wie z.B. die Übermittlung von gesicherten E-Mails. Wird keine VULPUS-Ablösung initiiert, können keine personellen und finanziellen Mittel bereitgestellt werden, um die Funktionen von VULPUS sicherzustellen.

Varianten

Es sind drei Varianten der Ablösung denkbar:

Variante A

Das bestehende System VULPUS wird durch ein neues System vollständig ersetzt.

Variante B

Die Funktionalitäten von VULPUS werden in ein bestehendes System integriert.

Variante C

Bestehende Applikationen der BORS, die auf verschiedenen Systemen betrieben werden, werden so weiterentwickelt und verfügbar gemacht, dass die Funktionen von VULPUS von allen VULPUS-Nutzern weiter genutzt werden können.

3.4 Drahtlose Breitbandkommunikation

Für die drahtlose Datenkommunikation sind die BORS zurzeit auf die Nutzung von öffentlichen drahtlosen Netzsystemen angewiesen (insbesondere der Swisscom). Bei grösseren geplanten Veranstaltungen oder plötzlich auftretenden, ungeplanten Ereignissen mit grossen privaten Kommunikationsbedürfnissen erfolgt die Datenübertragung aufgrund von Netzüberlastung nur mit sehr grosser Verzögerung oder bricht vollständig zusammen, sofern nicht-priorisierte BORS-Produkte eingesetzt werden. Die BORS und ihre Partner benötigen für ihre Einsätze stabile Verbindungen mit garantierter Verfügbarkeit, die resistent gegen Netzüberlastung sind.

Die kommerziellen Netzinfrastrukturen sind nach marktwirtschaftlichen Überlegungen ausgelegt. Heute existieren bei den kommerziell angebotenen Breitbanddiensten besonders entlang der Landesgrenze, im Alpenraum und in nicht dicht bevölkerten Gebieten erhebliche Versorgungslücken bzw. -engpässe. Die BORS benötigen für ihre Einsätze, die in allen Gebieten der Schweiz stattfinden können, eine möglichst lückenlose Abdeckung mit Breitbanddiensten. Die geographischen Versorgungslücken können durch die BORS mit eigenen Infrastrukturen abgedeckt werden.

Die Mobilfunknetze sind nicht stromausfallsicher, d. h. bei einem Stromausfall wäre die Nutzung der Netze nach ca. 1–4 Stunden nicht mehr möglich. Für die Rettungs- und Sicherheitsdienste ist es aber wichtig, dass ein Netz zur Verfügung steht, das nicht durch andere Nutzer ausgelastet wird und auch bei Stromausfall mehrere Tage verfügbar ist.

Mit einem System für drahtlose Breitbandkommunikation (dBBK) könnten hochverfügbare Breitbanddienste für die BORS von Bund (z.B. GWK) und Kantonen sowie für die Betreiber von kritischen Infrastrukturen auch mobil zur Verfügung gestellt werden. Die mobile Vernetzung der BORS und der Betreiber von kritischen Infrastrukturen würde zu einer optimierten Zusammenarbeit beitragen, z. B. zwischen den Einsatzkräften auf dem Schadenplatz und der rückwärtigen Führung. Für dBBK stellt das SDVN als Transportnetz für die Vermaschung der Netzknoten eine optimale Voraussetzung dar. Neben der Möglichkeit der Sprachkommunikation mit Polycom könnten die BORS damit auch grosse Datenmengen, Bildmaterial und Karteninformationen (Lageverbund) mobil austauschen sowie Applikationen mobil nutzen (z. B. Datenbanken, geographische Informationssysteme). DBBK-basierte Anwendungen könnten auch für gesicherte Kommunikation wie z. B. Telefonkonferenzen via Smartphones, genutzt werden. Einsatzunterstützend könnten verschiedene Polizeikorps auch Rapporte vor Ort über Tablets erfassen.

Die BORS nutzen in der Schweiz bereits heute bestehende nationale drahtlose Breitbandinfrastrukturen der öffentlichen Mobilfunkanbieterinnen. Je nach Bedarf können gewisse technische Massnahmen (Härtung und Erschliessung heute nicht versorgter Gebiete, Verhinderung von Cyberattacken) ergriffen werden, um diese sukzessive den Verfügbarkeits- und Sicherheitsanforderungen der BORS anzupassen.

Synergien und Abhängigkeiten

Mit dBBK wird sämtlichen Diensten und Funktionen, die in der vorliegenden Auslegeordnung bei den verschiedenen Vorhaben dargestellt sind, eine mobile Komponente zur Verfügung gestellt. So könnten beispielsweise die Applikationen des Lageverbunds mobil, d. h. im Feld bzw. auf dem Schadenplatz, in die Arbeitsprozesse integriert werden. Ihre Nutzer haben von unterwegs jederzeit sicheren und hochverfügbaren Zugang zu aktuellen Daten, die sie zur Bewältigung in allen Lagen benötigen. Ihre Datenaufnahmen am Schadenplatz könnten in Echtzeit in die Kernsysteme eingespeist werden.

Damit das Bedürfnis für eine sichere und resiliente Datenkommunikation bis zum mobilen Endgerät für sämtliche BORS landesweit harmonisiert abgedeckt werden kann, muss bedarfsorientiert eine mobile Verlängerung des SDVN und des IP-Datenzugangsnetz Polydata mit eingeschränkter Kapazität in Betracht gezogen werden. Da SDVN resilient gegenüber Stromausfällen und Cyberattacken sein soll, hätten die Partner des Bevölkerungsschutzes damit ein durchgängig sicheres und hochverfügbares Transportnetz mit fixem und mobilem Anteil, das in allen Lagen zur Verfügung stünde.

Es ist denkbar, dass dBBK nach 2030/35 Polycom ablöst, sofern die Standardisierung von Sprachfunkanwendungen für die digitale Breitbandkommunikation erfolgt ist. Die Stichverbindungen, deren Kapazität im Rahmen der Weiterentwicklung von Polycom erweitert werden müssen, könnten ohne Mehraufwand so konzipiert werden, dass sie auch für die Übertragung mobiler Daten verwendet werden können. Damit wäre sichergestellt, dass bei einer Erweiterung der bestehenden drahtlosen Breitbandinfrastruktur bereits wesentliche Komponenten für die Datenübertragung zur Verfügung stehen.

Mögliche Synergien zwischen dBBK und Telekommunikation der Armee sind zu prüfen und gegebenenfalls zu nutzen.

Folgen eines Verzichts auf dBBK

Da das Bedürfnis bei verschiedenen BORS für dBBK schon heute gross ist und sie Projekte im Bereich dBBK umsetzen wollen (Feldversuche sind initiiert), könnte ein Verzicht auf dBBK bedeuten, dass verschiedene Kantone und grössere Städte solche Systeme und Infrastrukturen selbstständig aufbauen. Das Resultat wären technisch unterschiedliche Systeme mit unterschiedlichen Verfügbarkeiten, Sicherheitsstandards und einer grossen Anzahl Schnittstellen.

Falls dereinst dBBK Polycom ablösen sollte, müssten diese Systeme mit einem grossen Aufwand sukzessive zu einer landesweiten und einheitlichen technischen Lösung «zusammengebaut» werden. Die Erfahrungen von Polycom haben gezeigt, dass dies mit erheblichen Kosten verbunden sein dürfte.

Für die BORS bedeutet ein Verzicht auf dBBK, dass Einsätze nicht oder nicht effizient bewältigt werden können. Personen- und Sachschäden sowie hohe Kosten aufgrund einer verzögerten Wiederherstellung des Normalzustandes können die Folge sein.

Varianten

Die modernen Übertragungstechnologien ermöglichen die Entwicklung kundengerechter BORS-Lösungen auf der Basis bestehender öffentlicher Mobilfunkinfrastrukturen. Entsprechende kommerzielle Angebote sind auf dem Markt verfügbar. Diese kommen ohne zusätzlichen Frequenzbedarf aus. Dennoch wurden seitens des BAKOM für allfällige, darüber hinausgehende Nutzungen, Frequenzressourcen zugunsten der BORS reserviert. Dieser Ansatz für eine drahtlose Breitbandkommunikation basiert auf einer Einigung zwischen den BORS, dem BABS, der FUB und dem BAKOM und wird im Nationalen Frequenzzuweisungsplan (NaFZ) der Schweiz ausgewiesen.

***Variante A** – Öffentlicher Betreiber mit kommerziellen BORS-Produkten*

Die BORS-Dienstangebote bauen auf öffentlichen Mobilfunknetzen auf und lassen sich beliebig erweitern. Es wird kein neues Netz gebaut, sondern ein Vertrag mit einem kommerziellen Anbieter abgeschlossen, der gegen finanzielle Leistung kommerzielle BORS-Dienste erbringt. Zusätzlich kann bei Bedarf die Abdeckung nicht erschlossener Gebiete vertraglich geregelt werden.

Es werden seitens BORS keine zusätzlichen Frequenzspektren benötigt.

Die Verletzlichkeit gegenüber Stromausfällen und Cyberattacken setzt eine Härtung voraus.

***Variante B** – Gemeinsamer Betrieb privater Mobilfunkanbieter mit BORS-Kernnetz*

Die BORS betreiben ein eigenes Kernnetz. Für die Funknutzung arbeiten die BORS mit einem öffentlichen Mobilfunkanbieter zusammen. Dabei sind unterschiedliche Ausgestaltungsformen (MVNO, RAN-Sharing, etc.) denkbar. Zudem besteht die Möglichkeit mittels der zusätzlich für BORS reservierten Frequenzressourcen (2x3 MHz und 2x5 MHz) komplementäre Bedürfnisse zu realisieren. Solche zusätzliche Standorte lassen sich in die bestehende Netzinfrastruktur der Mobilfunkbetreiberinnen einbinden. Die Verwaltung der Endgeräte und Applikationen und der damit verbundenen Sicherheitsaspekte bliebe in den Händen der BORS.

Die Verletzlichkeit gegenüber Stromausfällen und Cyberattacken setzt eine Härtung voraus.

***Variante C** – Kommerzieller Betreiber mit teilgehärtetem Netz*

Ein Teil der Infrastruktur eines kommerziellen Mobilfunkanbieters würde durch finanzielle und materielle Unterstützung von Bund, Kantonen und Dritte gehärtet und priorisiert, sodass die Resilienz seines Netzes erheblich verbessert würde. Diese Variante könnte skalierbar aufgebaut werden.

Die Verletzlichkeit gegenüber Stromausfällen und Cyberattacken setzt eine Härtung voraus.

3.5 Lageverbund Schweiz

Ein Lageverbund verbindet bestehende Lagesysteme (ELD) zu einem nationalen Gesamtsystem. Ein jederzeit gesicherter Lageverbund zwischen den Führungsorganen von Bund, Kantonen und Betreibern von kritischen Infrastrukturen ist eine zunehmend wichtige Grundlage für die strategische Entscheidungsfindung in Krisensituationen. Das Bedürfnis einer gesamtheitlichen und möglichst umfassenden Übersicht der benötigten und vorhandenen Informationen ist für alle Organisationen und Behörden, welche einen Einsatz führen und koordinieren müssen, zentral. Zurzeit fehlt aber ein Instru-

ment oder ist nur in Teilbereichen ansatzweise realisiert, was eine Lücke im Katastrophenmanagement der Schweiz darstellt.

Dieses Sicherheitsdefizit wurde in der Sicherheitsverbundsübung SVU 14 erkannt. Der Bundesrat hat am 20. Mai 2015 den Schlussbericht der SVU14 zur Kenntnis genommen und den darin vorgeschlagenen Empfehlungen zur Verbesserung der nationalen Krisenvorsorge in der Schweiz zugestimmt. Dem VBS wurde die Federführung in der Umsetzung der Empfehlung 4 (Lageverbund und ELD NAZ) zugewiesen. Damit ist das VBS (BABS) beauftragt, die Massnahmen zur Schaffung des Wissensabgleichs und die Darstellung der Gesamtlage über eine gemeinsame Elektronische Lagedarstellung (ELD) weiterzuentwickeln und insbesondere auch den Informationsfluss zwischen Bund und Kantonen und den Einbezug der Lage kritischer Infrastrukturen weiter zu klären.

Der Lageverbund Schweiz würde die Wissensgrundlagen verfügbar machen, die bei nationalen Katastrophen und Notlagen notwendig sind, um eine konsolidierte Gesamtlage aufzubereiten, die verschiedenen Fachgebiete zu koordinieren, Massnahmen anzuordnen und das Ressourcenmanagement auf Stufe Bund sicherzustellen.

In den Kantonen bestehen bereits heute verschiedene Lösungen. Der Lageverbund Schweiz soll das Zusammenführen dieser verschiedenen Teillagen durch einen automatischen Datenaustausch freigegebener Daten vereinfachen. Damit würde es möglich, einen Überblick über alle verfügbaren Lageinformationen der Partner zu erhalten.

Der Lageverbund Schweiz könnte die Zusammenarbeit zwischen den Partnern auf sämtlichen Stufen bei der Bewältigung von Katastrophen und Notlagen wesentlich vereinfachen und verbessern. Er würde auch den vermehrten Einbezug der Lageinformationen von Betreibern von kritischen Infrastrukturen ermöglichen, was das Lagebild weiter vervollständigen und aussagekräftiger machen würde. Der Lageverbund Schweiz wäre eine zentrale Informationsquelle für die eingesetzten Führungsstäbe (z. B. der Bundestab ABCN), um bei den Entscheidungsträgern (z. B. Bundesrat) die Umsetzung zielführender Massnahmen zu beantragen.

Die Partner (insbesondere die Kantone) könnten weiterhin mit ihren bekannten und bewährten Systemen arbeiten, der Datenaustausch sollte jedoch über neu zu erstellende Schnittstellen und gemeinsame Austauschformate unter Anwendung gemeinsamer Richtlinien stattfinden.

Synergien und Abhängigkeiten

Wichtige Partner im Lageverbund Schweiz, insbesondere die Polizeikorps und der NDB, sind darauf angewiesen, dass sie vertraulich klassifizierte Informationen auf einem gesicherten und ausfallsicheren System austauschen können. Daher müsste ein Lageverbund Schweiz auf der Grundlage von SDVN und dem geschlossenen Anwendernetz Polydata realisiert werden.

Die aktuelle Lagedarstellung des Bundesstabs ABCN, der NAZ und des NDB beruht auf der ELD NAZ. Diese könnte in einer weiterentwickelten Version auch im Lageverbund Schweiz dazu genutzt werden, um die landesweite Lage synoptisch darzustellen. Ohne eine weiterentwickelte ELD NAZ wäre der Lageverbund Schweiz dem Bundesstab ABCN und der NAZ derzeit nicht dienlich, da nicht alle Informationen ausgewertet, dargestellt und verbreitet werden könnten. Bei den Bundesstellen und den Kantonen besteht ebenfalls eine Abhängigkeit zu den existierenden Lageverarbeitungs- und Einsatzleitsystemen.

Folgen eines Verzichts auf den Lageverbund Schweiz

Ein Verzicht auf das Projekt bedeutet, dass auch in Zukunft keine konsolidierte Lageübersicht über Ereignisse in der Schweiz in Echtzeit erstellt werden kann. Der Daten- und Informationsaustausch würde weiterhin weitestgehend manuell (persönliche Absprachen, Telefon, E-Mail) und über nicht ausfallsichere Wege und Systeme stattfinden. Verglichen mit einem Lageverbund ist dies eine sehr ineffiziente Zusammenarbeit in Katastrophen und Notlagen, die mehrere Kantone oder die ganze Schweiz betreffen. Die Führung im Ereignisfall ist damit auf Stufe Bund und auf Stufe Kantone massiv erschwert und die Ereignisbewältigung dadurch beeinträchtigt, weil entscheidrelevante Elemente möglicherweise fehlen. Konkret könnte das Fehlen eines Lageverbunds zur Folge haben, dass beispielsweise im Fall einer Terrorbedrohung oder eines Terroranschlages mit mehreren Tatorten in der Schweiz den Führungs- und Einsatzorganen keine konsolidierte Lagedarstellung zur Verfügung stehen würde.

Varianten

Vorabklärungen bezüglich verschiedener Varianten haben ergeben, dass es problematisch wäre, eine einzige Lagesoftware für alle Partner zu entwickeln oder zu beschaffen. Einerseits haben die im Lageverbund Schweiz involvierten Stellen unterschiedliche Aufgaben und Funktionen. Ihre Prozesse und ihre verwendeten Softwarelösungen sind darauf ausgerichtet und teilweise hoch spezialisiert. Eine einheitliche Lösung könnte diesen Bedürfnissen nicht gerecht werden und wäre eine Verschlechterung gegenüber dem Status quo. Zudem wäre ein Ersatz der existierenden unterschiedlichen Systeme durch ein neues einheitliches System nicht opportun, da es die föderalistischen Zuständigkeiten nicht berücksichtigte sowie dem Investitionsschutz auf den heute genutzten Systemen nicht Rechnung tragen würde.

Aus den oben genannten Gründen haben sich die involvierten Stellen für eine systemverbindende Lösung mittels Schnittstellen und gemeinsamen Austauschformaten ausgesprochen. Angestrebt wird eine dezentrale Lösung mit möglichst wenig zentralen Komponenten (hauptsächlich Zugriffs- und Rechtemanagement sowie Übersichtsfunktionalitäten).

3.6 Werterhalt der elektronischen Lagedarstellung der NAZ[12]

Seit rund 20 Jahren betreibt die NAZ die elektronischen Lagedarstellung (ELD NAZ) zum Austausch von lagerelevanten Informationen. Die heute verwendete Version wurde letztmals im Rahmen der Euro 08 technisch überarbeitet und muss aktualisiert werden. Insbesondere die erhöhten Anforderungen des NDB an die Sicherheit der ELD NAZ erfordern eine Neuprogrammierung.

Die ELD verwenden neben der NAZ und dem NDB auch das fedpol im Bereich Kindsentführungsalarm, das Krisenmanagementzentrum des EDA bei Entführungen von Schweizer Bürgerinnen und Bürgern im Ausland und das Staatssekretariat für Migration SEM im Rahmen der Flüchtlingskrise.

Das Projekt Werterhalt der ELD NAZ befindet sich in der Realisierungsphase. Damit wird sichergestellt, dass die Partner des SVS die bestehenden Funktionalitäten des Systems bis 2020 nutzen können. Gleichzeitig werden mit der Anpassung die Sicherheitsanforderungen des NDB erfüllt. Basierend auf den heutigen konzeptionellen Grundlagen der ELD NAZ wird die Anwendung technologisch auf den aktuellen Stand gebracht. Die NAZ und der NDB setzen das Projekt Werterhalt ELD NAZ unter der Federführung des BABS gemeinsam um.

Synergien und Abhängigkeiten

Die ELD NAZ soll zu einem späteren Zeitpunkt in den Lageverbund integriert werden. Abhängigkeiten zu anderen Vorhaben bestehen keine.

Folgen eines Verzichts auf Werterhalt der ELD NAZ

Das Projekt befindet sich in der Umsetzung.

Varianten

Das Projekt befindet sich bereits in der Umsetzung. Technische Varianten wurden vorgängig geprüft.

3.7 Polysat

Polysat basiert auf der Satellitenübertragung und wäre ein redundanter, breitbandiger Kanal zur Übermittlung von Sprache und Daten. Insbesondere würde Polysat die internationale Vernetzung bei der Bewältigung von Krisen und Katastrophen ermöglichen. Für die Zusammenarbeit mit Organisationen wie z. B. dem European Civil Protection Mechanism, mit dem seit dem Frühjahr 2017 eine Zusammenarbeitsvereinbarung besteht, wäre dies von zentraler Bedeutung.

---

[12] Der Werterhalt der ELD NAZ wird in dieser Auslegeordnung der Vollständigkeit halber aufgeführt, aber nur zusammenfassend erläutert. Das Projekt ist im Weiteren nicht Gegenstand der Priorisierung in diesem Bericht, da es ein bestehendes Projekt ist, das sich in der Umsetzungsphase befindet.

Mit punktuellem Zuschalten von Übertragungskapazitäten, die ebenfalls im Krisen- und Katastrophenfall garantiert wären, könnten gerade im Fall eines grösseren Erdbebens in der Schweiz zusätzliche Übertragungswege für SDVN und dBBK geschaffen werden. Zusatzverbindungen könnten sehr rasch mit mobilen Einheiten geschaffen werden.

Synergien und Abhängigkeiten

Polysat würde eine flexible und standardisierte Anbindung der Führungs- und Einsatzsysteme an internationale Plattformen und Organisationen ermöglichen, die wichtige Informationen auszutauschen haben. SDVN würde die technischen Anschlüsse für Polysat bieten. Mit Polydata könnte die notwendige Authentifizierung und Identifizierung der neu zugeschalteten Aussenposten garantiert werden. Gleichzeitig könnte mit Polysat ein diversitäres System zum Glasfasernetz von SDVN geschaffen werden, das den ununterbrochenen Betrieb sogar in einem Szenario mit sehr grosser Zerstörung (z. B. starkes Erdbeben) ermöglichen würde. Von dieser technischen Anbindung profitierten sämtliche Bedarfsträger des Bevölkerungsschutzes sowie international tätige Organisationen und Fachstellen des Bundes. Grenzkantonen und Einsatzorganisationen im grenznahen Bereich würde eine Anbindung ihrer Kommunikationssysteme ins Ausland ermöglicht.

Folgen eines Verzichts auf Polysat

Ein Verzicht auf Polysat bedeutet, dass die Führungskommunikation nur eingeschränkt international vernetzt werden kann und dass diese redundante Vernetzung und Kapazitätserweiterung im Inland nicht zur Verfügung steht.

Varianten

Bei Katastrophen und Notlagen innerhalb der Schweiz könnten nach einer gewissen Zeit auch die Mittel der Armee im Rahmen der subsidiären Unterstützung für die Wiederherstellung der Kommunikationsnetze (z.B. mobile Richtstrahlsysteme) eingesetzt werden, sofern sie rechtzeitig zur Verfügung stehen und genügend Ressourcen vorhanden sind, mehrere Links zu erstellen.

4 Alarmierung und Information der Bevölkerung

Die Alarmierung und Information der Bevölkerung sind zentrale Prozesse, um die Bevölkerung und ihre Lebensgrundlagen im Ereignisfall schnell und wirksam zu schützen. Die Sirenen sind in der Schweiz zurzeit das einzige Mittel, um die Bevölkerung vor einer akuten Gefährdung im Fall von Katastrophen und Notlagen zu alarmieren und anschliessend via Radio Verhaltensanweisungen innert 15 bis 20 Minuten zu verbreiten. Um die Information der Bevölkerung auch bei einem Totalausfall der gesamten Sendeinfrastruktur der Radioveranstalter zu gewährleisten, steht dem Bund ein UKW-Radio-Notsendernetz zur Verfügung (Information der Bevölkerung durch den Bund in Krisenlagen mit Radio IBBK). Die Alarmierung mit Sirenen, gefolgt von Informationen über Radio und Fernsehen, wird auch in Israel, Schweden, Frankreich und teilweise in Deutschland eingesetzt. Das Fürstentum Liechtenstein ist an das Sirenensystem der Schweiz angeschlossen.

Das Alarmierungssystem mit Sirenen erreicht nur einen Teil der Bevölkerung, da sie der Sirenenalarm und die nachfolgende Radiomeldung nicht erreichen (z. B. Menschen mit Hörbeeinträchtigung) oder es sich um Ausländerinnen und Ausländer handelt, welche die Verhaltensanweisungen auf Deutsch, Französisch oder Italienisch via Radio nicht verstehen. Deshalb sollte die gefährdete Bevölkerung künftig neben dem Sirenenalarm auch mit anderen Mitteln schnell alarmiert und informiert werden können. Im Vordergrund stehen dabei eine Alarmierung und Ereigniskommunikation via Mobiltelefone. Damit sollten insbesondere in einer ersten Ereignisphase Verhaltensanweisungen an die betroffene oder gefährdete Bevölkerung weitergegeben werden können, um noch grössere Schäden und Beeinträchtigungen zu verhindern. Via Mobiltelefone können solche Informationen auch einfach in verschiedenen Sprachen verfasst und anstatt via Radio über das Mobiltelefon zugänglich gemacht werden. Gerade die jüngsten Terrorereignisse im Ausland zeigen den Bedarf eines solchen zusätzlichen Alarmierungs- und Informationssystems. Deutschland verfügt über ein satellitengestütztes Kernsystem, mit dem neben anderen Verbreitungskanälen wie Radio und Fernsehen die Mobiltelefon-App (NINA) bedient werden kann. Neben NINA existiert in Deutschland ein Produkt eines privaten Anbieters namens KATWARN, welches ähnliche Funktionalitäten wie NINA aufweist. In Frankreich wurde nach den Terrorereignissen in Paris und hinsichtlich der Fussball Europameisterschaft eine App namens SAIP entwickelt.

Nachfolgend werden im Rahmen einer Auslegeordnung die für den Bevölkerungsschutz wichtigsten bestehenden und neuen zur Diskussion stehenden Alarmierungs- und Informationssysteme aufgeführt. Die Priorisierung dieser Systeme im Kontext mit den Finanzierungsmöglichkeiten erfolgt in Kapitel 5. Dabei wird ersichtlich, dass diese Systeme zwar für die Sicherheit der Schweizer Bevölkerung wichtig und deshalb wünschenswert sind, aber mindestens zurzeit nicht alles finanzierbar und damit realisierbar ist.

4.1 Polyalert 2030

Polyalert 2030 bezeichnet das Projekt zum Werterhalt und zur Weiterentwicklung des Systems Polyalert zur Alarmierung der Bevölkerung mit Sirenen. Polyalert funktioniert unabhängig von den Netzen der öffentlichen Telekommunikationsanbieter. Aspekte der Sicherheit, der Verfügbarkeit, der Synergienutzung bestehender Netze, des Investitionsschutzes und der maximalen Handlungsfreiheit bei der Weiterentwicklung des Systems haben dazu geführt, dass Polycom als Übertragungsnetz eingesetzt wird. Die Sirenen besitzen eine Stromreserve für eine mehrfache Auslösung des Alarms. Entsprechend ermöglicht das System Polyalert eine krisentaugliche, regionale und nationale Alarmierung der Bevölkerung.

Derzeit werden 5000 stationäre und 2800 mobile Sirenen für die Alarmierung der Bevölkerung betrieben. Besteht eine Gefährdung der Bevölkerung, wird im entsprechenden Gebiet der Allgemeine Alarm ausgelöst. Nach der Alarmierung mit Sirenen erfolgt immer eine Information via Radio (ICARO[13]-Meldung). Der Wasseralarm (sofortige Evakuation) betrifft die Nahzone unterhalb von 65 Stauanlagen.

Die Auslösung der Sirenen erfolgt primär direkt durch die kantonalen Polizei- oder Führungsorgane sowie durch die Betreiber von Stauanlagen. Sirenen können auch bei Unfällen, bei denen chemische Substanzen in die Luft und ins Wasser gelangen, ausgelöst werden, wie z. B. beim Chemieunfall in Schweizerhalle 1986. Auch bei Hochwasser kommen Sirenen zum Einsatz, wie beispielsweise während des Hochwasserereignisses 2005 in den Kantonen Luzern und Obwalden. In den Kantonen Ba-

[13] Information Catastrophe Alarme Radio Organisation. ICRO ist das Informationsangebot der SRG in Krisen- und Katastrophenfällen.

sellandschaft und Zürich wurden 2006 bzw. 2008 die Sirenen nach einer gesundheitsschädlichen Verunreinigung des Trinkwassers eingesetzt, um die Bevölkerung zu warnen. Sie kämen auch im Fall einer Freisetzung von radioaktiven Substanzen zum Einsatz, um die Bevölkerung zu warnen und zum Radiohören anzuweisen.

Zur Weiterentwicklung und zum Werterhalt von Polyalert 2030 gehören technologische Anpassungen des Systems, eine Aktualisierung der Technologie der Funkmodule und Massnahmen, um die Fernsteuerung am Sirenenstandort mit Notstrom zu versorgen.

Synergien und Abhängigkeiten

Polyalert baut auf dem Sicherheitsfunknetz Polycom auf. Anpassungen bei Polycom können Einfluss auf die Konfiguration des Alarmierungssystems haben und müssen fallweise analysiert werden. Der Werterhalt Polyalert wird mit der bereitgestellten Funktionalität von Polycom 2030 synchronisiert.

Als redundanter Auslösungskanal können die Sirenen derzeit über das UKW-Sendernetz der SRG ausgelöst werden. Die Abschaltung dieses analogen Radionetzes wird zur Folge haben, dass die Redundanz voraussichtlich ab 2024 wegfallen wird. Alternativ zu UKW wäre das digitale Radio DAB+ oder die Nutzung von dBBK oder die öffentlichen Netzbetreiber in Betracht zu ziehen. Da sich das bestehende Alarmierungssystem Polyalert 2024 am voraussichtlichen Ende seines Lebenszyklus befindet, ist allenfalls ein Ersatzsystem vorzusehen.

Folgen eines Verzichts auf Polyalert 2030

Ein Verzicht auf den Werterhalt und die Weiterentwicklung des Systems hätte zur Folge, dass die Bevölkerung ab ca. 2025 nicht mehr mittels Sirenen alarmiert werden könnte.

4.2 Information der Bevölkerung mit Notfallradio IBBK-Radio/Polyinform

IBBK-Radio bezeichnet das UKW-Radio-Notsendernetz des Bundes. Damit kann die Bundeskanzlei die Bevölkerung im Auftrag des Bundesrates in allen Lagen über die erste Radio-Senderkette der SRG in allen Landessprachen informieren. Bundeseigene geschützte Radiostudios und UKW-Sendeanlagen mit verstärkter Sendeleistung ermöglichen den Radioempfang auch in den Schutzräumen. Die IBBK-Radio-Sendestandorte können 85 Prozent der Bevölkerung mit den Programmen der SRG versorgen. Das Senden von Informationen ist auch ohne funktionierende Stromversorgung dank Notstromgeneratoren während 40 Tagen möglich. Das Empfangen dieser Informationen setzt aber voraus, dass die Empfänger ein batteriebetriebenes resp. stromnetzunabhängiges UKW-Radioempfangsgerät besitzen und dieses auch zu verwenden wissen.

Polyinform 2030 ist das Vorhaben, das Betrieb, Werterhalt und Weiterentwicklung von IBBK-Radio klären und sicherstellen soll. Ab 2024 wird die Verbreitung von analogen Radiosignalen über UKW in der Schweiz voraussichtlich eingestellt. Mit einer Ausdünnung von UKW wird bereits ab 2019 gerechnet. Der definitive Abschalttermin liegt in der Entscheidkompetenz des Bundesrates. Abhängig von diesem Entscheid kann für IBBK-Radio eine Systemerneuerung notwendig werden, wobei heute davon ausgegangen werden darf, dass das derzeitige System mit den geplanten Werterhaltungsmassnahmen bis ins Jahr 2027 betriebsbereit gehalten werden könnte.

Das Konsumverhalten der jüngeren Bevölkerungsschichten zeigt, dass Radiohören über das analoge Radio an Terrain verloren hat. Zurzeit ist aber noch unklar, ob sich DAB+ oder IP-Broadcast (Streaming über das mobile Netz und Empfang über Smartphones, Tablets etc.) durchsetzen wird. Sobald sich abzeichnet, welche Technologie sich durchsetzen wird, und unter dem Vorbehalt, dass der Bundesrat sich für die Weiterführung eines solchen Notfallradiosystems entscheidet, wird ein entsprechendes Projekt gestartet. Das BABS hat für die Beantwortung dieser Fragen und zwecks Klärung des weiteren Vorgehens eine Studie lanciert, an der sämtliche Bedarfsträger, die in die Information der Bevölkerung durch den Bund involviert sind, beteiligt sind.

Hervorzuheben gilt es den Umstand, dass vor dem Einsatz des gehärteten Systems IBBK-Radio eine gute Zusammenarbeit zwischen der SRG, den Lokalradios und weiteren Informationsquellen besteht und die Informationen des Bundes über sämtliche verfügbaren Rundfunk- und Informationsplattformen (Digitalradio, Digitalfernsehen, Newsportale etc.) an die Bevölkerung weitergeleitet werden. Die hierzu notwendigen Prozesse und Organisationen sind optimal eingespielt.

Synergien und Abhängigkeiten

Das heutige System IBBK-Radio basiert auf dem Führungsnetz Schweiz. Bei einer Realisierung von SDVN/Polydata würde IBBK-Radio oder ein allfälliges Nachfolgesystem auf diese neue Plattform aufgebaut. Mit der SRG besteht schon heute eine sehr effiziente und effektive Zusammenarbeit in Bezug auf die Nutzung der bestehenden Infrastrukturen für die Information der Bevölkerung durch den Bund über Radio.

So wie die Bevölkerung in vielen Situationen über verschiedenste Kanäle und Angebote der SRG informiert werden kann (Digitales Radio DAB+, Internetradio, Digitales Kabelfernsehen DVB-C, Digitales Satellitenfernsehen DVB-S, Internetfernsehen, mobiles Radio und Fernsehen über Smartphones, Internetplattformen etc.), so kann die SRG die IBBK-Radio-Installationen als Redundanz bei Totalausfällen ihrer eigenen Infrastrukturen nutzen (BCM der SRG). Die Zusammenarbeitsprozesse und die entsprechenden Organisationsstrukturen, unter anderem mit der Armee, sind eingespielt.

Folgen eines Verzichts auf IBBK/Polyinform

Bei einem Verzicht auf IBBK-Radio verliert der Bund den heute einzigen, von Dritten entflochtenen Informationskanal, der in allen Lagen einsatzbereit ist und es den Behörden erlaubt, sich direkt an die Bevölkerung zu wenden.

Varianten

Variante A – Weiterbetrieb IBBK-Radio auf bestehender Infrastruktur bis 2027

Bei dieser Variante wird die Infrastruktur IBBK-Radio bis zum Ablauf des Betriebsvertrages zwischen der armasuisse und der Swisscom Broadcast AG weiterbetrieben. Trotz der Migration der SRG auf das digitale Radio DAB+ kann die Senderinfrastruktur ohne Einschränkungen betrieben werden. Es kann davon ausgegangen werden, dass in der Bevölkerung weiterhin eine bestimmte Anzahl von Endgeräten zur Verfügung steht, die das UKW-Signal empfangen können (Autoradios, Doppeltuner-Geräte UKW-DAB+). Der Bund beschränkt sich auf die Sicherstellung des Betriebs und den Werterhalt des bestehenden Systems. In Lagen unterhalb der Einsatzschwelle von IBBK-Radio informiert der Bund die Bevölkerung über sämtliche verfügbaren Rundfunk- und Informationskanäle. Bei dieser Variante wird ab 2024 nur noch ein Teil der Bevölkerung IBBK-Radio-Meldungen empfangen können, weil sie immer weniger über UKW-Empfangsgeräte verfügen.

Variante B – Migration von IBBK-Radio auf IP-Broadcast-Technologie

Schon heute hören 50 Prozent der Radiohörer, die sich für das digitale Radio entschieden haben, ihre Radioprogramme über Smartphones, Tablets oder Computer. Der Empfang wird heute über Fixnet, WLAN und in sehr vielen Fällen mobil über das Mobilfunknetz der öffentlichen Telekommunikationsanbieter sichergestellt, mit dem gewichtigen Vorteil, dass über das persönliche und praktisch immer verfügbare Smartphone nahezu sämtliche Informationsquellen zur Hand sind – vorausgesetzt, der Netzempfang ist sichergestellt. Im Einsatzfall von IBBK, also in Krisenlagen, wird der Netzempfang zum kritischen Faktor und er wird mit grösster Wahrscheinlichkeit nicht mehr zur Verfügung stehen. Sollte dBBK realisiert werden, könnte mit dieser Variante sehr effizient und mit grossem Nutzen für die Bevölkerung ein Informationskanal aufgebaut werden, der dem Anspruch auf Krisentauglichkeit entsprechen kann. Mit dieser Konstellation und unter der Prämisse, dass der Anspruch auf die Versorgungsqualität revidiert wird (kein Empfang im Schutzraum), könnte das bestehende System IBBK-Radio ersetzt werden.

Variante C – Migration auf DAB+

In den kommenden Jahren werden die SRG und die Privatradios mit grossen Investitionen und Marketingaktivitäten den Aufbau des Sendernetzes, die Verbesserung der Empfangsqualität überall in der Schweiz sowie die Penetration der DAB1+-Empfangsgeräte massiv vorantreiben. Das BAKOM ermöglicht dies mit fördernden Rahmenbedingungen im neuen Radio- und Fernsehgesetz (RTVG). Zudem rüstet das ASTRA sämtliche Nationalstrassentunnels mit DAB+ aus. Inwiefern sich DAB+ grossflächig, in Europa durchsetzen kann, ist derzeit nicht abzuschätzen. In der Schweiz hören derzeit 50 Prozent der Radiohörer ihre Radiosendungen über DAB+. Sofern sich DAB+ in den kommenden Jahren durchsetzt, könnte das bis dahin veraltete IBBK-Radio-System mit DAB+-Sendern ausgerüstet und umgebaut werden.

4.3 Weiterentwicklung Alertswiss[14]

Seit Februar 2015 unterhält das BABS eine Webseite unter der Bezeichnung Alertswiss. Sie enthält ausführliche Informationen zu Gefährdungen und Risiken für die Bevölkerung und zur persönlichen Vorsorge und Notfallplanung.

Die gleichzeitig eingeführte App besitzt noch keine aktive Funktion zur Alarmierung und Information der Bevölkerung. Mit einer solchen Funktion könnten Alarmierung und Verhaltensanweisungen rasch und unmittelbar an die Bevölkerung übermittelt werden. Dies wäre eine sinnvolle Ergänzung zum bestehenden System mit Sirenen und Radio. Dadurch kann nicht nur die Reichweite erhöht werden, es wird auch den aktuellen Mediennutzungsgewohnheiten der Bevölkerung Rechnung getragen und die Geschwindigkeit der Informationsverbreitung wesentlich gesteigert.

Eine Ausweitung der Alarmierungs- und Informationsmöglichkeiten wird von breiten Kreisen der Öffentlichkeit ausdrücklich gewünscht. Insbesondere der Schweizerische Gehörlosenbund fordert seit Langem eine Alternative zur Alarmierung über Sirenen und die Vermittlung von Verhaltensanweisungen über Radio. Auch die Polizei und die kantonalen Führungsorgane wollen bei einem Ereignis mit grosser Auswirkung die Bevölkerung schneller und flexibler informieren können, als es heute mit Sirenen und Radio über den ICARO-Prozess der Fall ist. Zudem wäre eine gezieltere Alarmierung der von einem Ereignis betroffenen Bevölkerung in einem definierten Gebiet im Sinne des Bevölkerungsschutzes von grossem Nutzen. Gerade die jüngsten Terroranschläge in Deutschland und Frankreich, wo solche Alarmierungs- und Informationssysteme eingesetzt wurden, zeigen deren Bedarf für die gefährdete Bevölkerung und die Behörden.

Eine solche Alternative bietet sich in der Form einer Push-Funktion für die Alarmierung und Information via Alertswiss App an. Die Alertswiss App als Kanal zur schnellen Information der Bevölkerung soll im Ereignisfall mit zusätzlichen Kanälen ergänzt werden. Als solche Kanäle kommen von breiten Bevölkerungskreisen benutzte Apps in Frage, wie z. B. die App von MeteoSchweiz (5.8 Mio. Nutzer), der SBB oder von 20min, Blick, SRG etc.

Voraussetzung für die Realisierung einer zusätzlichen zeitgemässen und redundanten Alarmierung und Informationsvermittlung ist ein gesamtschweizerisches Kernsystem. Dieses muss die Entgegennahme von Meldungen in einem standardisierten Format und deren Verarbeitung/Aufbereitung sowie ein Front-End für die standardisierte Erfassung mit Vorlagetexten ermöglichen. An dieses Kernsystem sollen primär die Einsatzzentralen der Kantonspolizeien sowie die kantonalen Führungsorgane angeschlossen werden. Mit dem Kernsystem sollen zudem die Alertswiss Website und weitere Verbreitungskanäle, wie z. B. Twitter oder Informationsanzeigen in Bahnhöfen, angesteuert werden können. Dadurch kann eine grösstmögliche Reichweite der Alarmierung und Information der betroffenen Bevölkerung gewährleistet werden.

In einem ersten Schritt wird die bestehende Alertswiss App, basierend auf dem erwähnten Kernsystem, zu einem die Sirenen und das Radio ergänzenden Alarmierungs- und Informationsmittel ausgebaut werden. Da die App auf den öffentlichen Netzen basiert, ist sie nicht in allen Lagen funktionsfähig und es besteht ein hohes Ausfallrisiko. Bei einem Ausfall dieses Systems verbleibt aber als Rückfallebene das bestehende Alarmierungssystem mit Sirenen und Radio.

Synergien und Abhängigkeiten

Die Weiterentwicklung von Alertswiss basiert auf Polyalert, das als Kernsystem genutzt wird. Polyalert wird bereits in den Einsatzzentralen der Kantonspolizeien für die Auslösung der Sirenen sowie für den ICARO-Prozess benutzt. Somit können Synergien optimal genutzt werden. Für die Website Alertswiss soll das Content Management System CMS des VBS als Plattform dienen. Zu den oben erwähnten weiteren Apps wie etwa der MeteoSchweiz können Synergien nach dem Multiplikatorprinzip zur Vergrösserung der Reichweite genutzt werden.

Folgen eines Verzichts auf Alertswiss

Das Projekt zur Weiterentwicklung von Alertswiss befindet sich in der Umsetzung.

---

[14] Die Weiterentwicklung des Informationssystems Alertswiss wird in dieser Auslegeordnung der Vollständigkeit halber aufgeführt, aber nur zusammenfassend erläutert. Das Projekt ist im Weiteren nicht Gegenstand der Priorisierung in diesem Bericht, da es ein bestehendes Projekt ist, das sich in der Umsetzungsphase befindet.

Varianten

Das Projekt zur Weiterentwicklung von Alertswiss befindet sich bereits in der Umsetzung.

4.4 Handyalarm via SMS oder CBS

Eine Alarmierung der Bevölkerung via eine App auf den Mobiltelefonen bedingt, dass die Bevölkerung über die entsprechenden Apps verfügen, d. h. diese auf ihr Mobiltelefon herunterladen und aktivieren. In der Praxis ist diese Hürde unter Umständen sehr nachteilig. Dieses Defizit könnte mit einer Handyalarmierung über Cell Broadcasting (CBS) oder über aufenthaltsgebundene SMS-Dienste behoben werden. Alarmierungssysteme per SMS oder CBS existieren in Europa beispielsweise in den Niederlanden, Schweden, Norwegen, Grossbritannien und demnächst in Belgien.

Beide Technologien verfügen jedoch über Nachteile gegenüber einer App, wie sie im Rahmen von Alertswiss entwickelt wird. Bei einer grossflächigen Alarmierung mit einer hohen Anzahl von Empfängern via SMS würde sich die Übermittlung in zeitlicher Hinsicht stark verzögern. Eine wesentliche Hürde bei einer Alarmierung via CBS würde darin bestehen, dass die Mobiltelefone für diesen Zweck nicht konfiguriert sind. Gemäss einer Studie der Swisscom sind nur 30 Prozent der Endgeräte in der Schweiz grundsätzlich CBS-fähig, die notwendige Konfiguration vorausgesetzt. Die Benutzer müssten diese selber vornehmen, wozu sie jedoch in der Regel ohne Support nicht in der Lage sind. Grundsätzlich ist es aber ohne grössere Anpassungen ab 2018 möglich, von Polyalert Informationen an die Mobilfunkprovider in der Schweiz zu übermitteln, die diese via CBS verbreiten könnten. Voraussetzung dafür ist allerdings, dass die Provider über die notwendigen Infrastrukturen für diesen Prozess verfügen.

Beide Technologien basieren, wie ein technisches Gutachten ergeben hat, zudem auf einem alten Standard. In diesem Kontext sind vorerst die Entwicklungen von künftigen Standards wie die LTE- und 5G-Technologie abzuwarten. Damit werden nicht nachhaltige Investitionen vermieden.

Synergien und Abhängigkeiten

Eine Alarmierung via SMS oder CBS ist abhängig von der Mitwirkung und Preisgestaltung der Mobilfunkanbieter in der Schweiz (Swisscom, Salt, Sunrise, UPC).

Folgen eines Verzichts auf den Handyalarm

Mit der Weiterentwicklung von Alertswiss (Push-Funktion für die Alarmierung und Information) wird den Bedürfnissen der Bevölkerung und der Einsatzorganisationen nach einem alternativen Alarmierungs- und Informationssystem zum Teil bereits Rechnung getragen. Bedürfnisse, die heute mit Alertswiss noch nicht abgedeckt werden können, sollen je nach technologischem Entwicklungsstand in einer späteren Phase geklärt werden.

Varianten

Die technischen Varianten können erst später auf der Basis der künftigen technologischen Standards analysiert und geklärt werden.

5 Priorisierung der neuen Vorhaben

Die Projekte Polycom 2030 sowie die Weiterentwicklung von Alertswiss und der ELD NAZ wurden der Vollständigkeit halber in die Auslegeordnung aufgenommen, um eine Gesamtsicht zu ermöglichen. Diese Projekte befinden sich bereits in der Umsetzungsphase und werden daher keiner Priorisierung unterzogen. Das gleiche gilt für die bestehenden Systeme IBBK und Polyalert. Bei diesen Systemen stehen der Betrieb und der Werterhalt im Vordergrund. Der Weiterentwicklung dieser Systeme ist aus Sicht der BORS grosse Beachtung zu schenken, da sie zentral für die Alarmierung und Information der Bevölkerung sind. Grössere Werterhaltungsmassnahmen werden aber erst ab 2025 notwendig sein und liegen in der Verantwortung des Bundes. Die BORS von Bund, Kantonen und Dritten erachten die Weiterentwicklung dieser Systeme zum jetzigen Zeitpunkt für zentral, insbesondere Polyalert und Alertswiss. Mit der Entwicklung der App für die Ereigniskommunikation und Information der Bevölkerung kann ein wichtiges Sicherheitsdefizit hinsichtlich der Alarmierung der Bevölkerung geschlossen werden. Der Abschluss laufender Projekte und der Werterhalt bestehender Systeme dafür müssen gewährleistet sein. Das BABS soll die Entwicklung in diesen Bereichen aber kontinuierlich beobachten und zu gegebener Zeit Entscheidungsträger von Bund und Kantonen sowie Dritten informieren und entsprechende Grundlagen bereitstellen. Dies entspricht auch einer Empfehlung der Eidgenössischen Finanzkontrolle EFK im Rahmen ihrer Prüfung des IKT-Schlüsselprojektes Polycom 2030.

Priorisierung der neuen Vorhaben

Die aktuelle und absehbare Finanzlage von Bund und Kantonen erfordert eine Priorisierung der neuen Vorhaben, die in der vorliegenden Auslegeordnung erläutert wurden. Im Vordergrund der Priorisierung stehen die Bedürfnisse der BORS von Bund und Kantonen sowie von Betreibern kritischer Infrastrukturen bezüglich der Verbesserung des Sicherheitsniveaus sowie die Finanzierbarkeit der dafür notwendigen Massnahmen im Bereich der Telekommunikation. Die Priorisierung basiert auf 72 Stellungnahmen von Bundesstellen, Kantonen, Betreibern kritischer Infrastrukturen und weiteren Partnern des Bevölkerungsschutzes.

1. Priorität

Aus Sicht der BORS von Bund und Kantonen sowie den Betreibern von kritischen Infrastrukturen sind folgende Vorhaben mit höchster Priorität zu realisieren. Bei allen Vorhaben sind in einem nächsten Schritt die Kosten möglichst zu konkretisieren, sobald der politische Grundsatzentscheid über die Realisierung der Vorhaben getroffen wurde.

SDVN / Polydata

Für die BORS von Bund und Kantonen sowie Betreiber von kritischen Infrastrukturen hat das Vorhaben SDVN höchste Priorität. Hoch verfügbare, stromsichere Verbindungen werden als Voraussetzung für die effiziente und erfolgreiche Ereignisbewältigung erachtet. Durch die Nutzung des Glasfasernetzes und Infrastrukturen des Führungsnetzes Schweiz, das bereits heute eine hohe Energieautonomie aufweist, sowie dessen Verbund mit weiteren bestehenden Glasfaserinfrastruktur von Bundesämtern (z.B. ASTRA) und privaten Organisationen, kann ein verhältnismässig kostengünstiges Netz aufgebaut werden, das dem Anspruch der BORS an die Stromausfallsicherheit gerecht wird.

Das Vorhaben Polydata soll aus Sicht der BORS von Bund und Kantonen zusammen mit dem SDVN in erster Priorität realisiert werden, damit das SDVN im Interesse der BORS genutzt werden kann. Im Vordergrund steht ein geschlossenes Anwendernetz, welches sicheren und hochverfügbaren Zugang zu bevölkerungsschutzrelevanten Anwendungen wie z.B. Polycom und Polyalert gewährleisten soll und den Schutz vor Cyberattacken verbessert.

Der Aufbau von SDVN schafft auch einen Mehrwert über den Nutzerkreis der BORS hinaus. SDVN kann verschiedenen anderen Systemen als Übertragungsplattform dienen und die Ausfallsicherheit dieser Systeme signifikant verbessern. Durch die Nutzung von SDVN kann beispielswiese die Ausfallsicherheit des Datenkommunikationsnetzes KOMBV-KTV, welches den Bund mit kantonalen und kommunalen Vollzugstellen vernetzt, erhöht werden. In Bereichen wie der Energieversorgung und des Finanzplatz Schweiz könnte SDVN als redundantes Datentransportnetz verwendet werden und so die Resilienz dieser kritischen Sektoren gesteigert werden.

Ablösung VULPUS-Telematik

Eine Ablösung der Funktionen von VULPUS-Telematik bis 2022 ist aus Sicht der verschiedenen Bundesstellen, der Kantone und einiger Betreiber kritischer Infrastrukturen zwingend und ist mit höchster Priorität zu realisieren. Falls eine Ablösung der Funktionen bis 2022 nicht eingehalten werden kann, sind grosse Investitionen in ein nicht ausfallsicheres System für die Weiterführung des Betriebes von VULPUS notwendig. Ein rascher Entscheid ist notwendig, damit die Nutzer von VULPUS genügend Zeit haben, preiswerte Alternativen zu prüfen und ihre Meldeprozesse, bei denen derzeit VULPUS verwendet wird, anzupassen. Ein 1:1-Ersatz des Systems scheint aus technischer Sicht nicht mehr sinnvoll. Die notwendigen Ressourcen sollen für die Nutzung von Synergien mit bestehenden Systemen und Anwendungen eingesetzt werden.

Erweiterung der bestehenden drahtlosen Breitbandkommunikationsinfrastruktur

Der Ausbau von dBBK geniesst insbesondere bei Einsatzorganisationen und bei den Kantonen mit grösseren Städten und Agglomerationen höchste Priorität. Mobile Endgeräte wie Smartphones, Tablets und Laptops und die darauf verfügbaren Anwendungen haben sich in den letzten Jahren zu einem unverzichtbaren Führungs- und Einsatzinstrument entwickelt und sind heute aus dem Alltag der Blaulichtorganisationen nicht mehr wegzudenken. DBBK könnte dereinst das System Polycom ersetzen. Die Sicherstellung der Koordination und einheitlicher landesweiter Standards müsste durch das BABS erfolgen.

Lageverbund

Das Bedürfnis einer gesamtheitlichen und möglichst umfassenden Übersicht der benötigten und vorhandenen Informationen zum Ereignis, seine Auswirkungen und den getroffenen Massnahmen, ist für alle Organisationen und Behörden, die einen Einsatz führen und koordinieren müssen, zentral. Diese Einschätzung deckt sich mit den Sicherheitsdefiziten, die im Rahmen der SVU 14 identifiziert wurden. Darum wird der Entwicklung eines solchen Führungsinstrumentes von den BORS von Bund und Kantonen und von einigen Betreibern von kritischen Infrastrukturen (z.B. SBB) eine sehr hohe Priorität beigemessen. Im Vordergrund steht eine systemverbindende Lösung, d.h. ein Lösung, die bestehende Lagedarstellungssysteme der Kantone bedarfsorientiert vernetzt. Die Lösung soll möglichst wenige zentrale Komponenten aufweisen. Um den Nutzen eines Lageverbundes weiter zu steigern, ist eine Einbindung des grenznahen Auslandes in den Lageverbund zu prüfen.

2. Priorität

Für nachfolgende Vorhaben müssen noch vertiefte Abklärungen auf technischer Ebene und in Bezug auf die Bedürfnisse der Partner durchgeführt werden. Eine allfällige Realisierung wird dementsprechend erst zu einem späteren Zeitpunkt in Frage kommen.

Flächendeckende Umsetzung dBBK

Bei der Realisierung von dBBK wird von den BORS eine Lösung mit einem dedizierten Kernnetz bevorzugt, das an die Netze der öffentlichen Mobilfunkanbieter angeschlossen wird. Abstriche bei der Ausfallsicherheit würden in Kauf genommen werden. Ob diese Lösung zum besten Resultat für die BORS führt, werden Pilotversuche in den Kantonen zeigen. Die flächendeckende Realisierung von dBBK hat aber vorläufig zweite Priorität und soll erst angegangen werden, wenn klare Vorgaben im Rahmen eines Pilotprojekts erarbeitet wurden und damit solide Grundlagen vorhanden sind. Auch aus Kostengründen soll dBBK im Rahmen eines geographisch beschränkten Pilotprojektes, aber nicht flächendeckend umgesetzt werden.

Handyalarm via SMS und CBS

Die Alarmierung der Bevölkerung via SMS oder CBS stellt gemäss den BORS zufolge eine nutzenbringende Ergänzung zur Alarmierung via die Alertswiss-App dar. Beide Technologien verfügen gegenüber der App neben den technischen Nachteilen (Konfiguration, Alarmierungsgeschwindigkeit) auch über Vorteile. Die Alarmierung via CBS funktioniert auch bei Überlastung der öffentlichen Mobilfunknetze und die Alarmierungsinformation kann geographisch zugeteilt werden. Aus Kostengründen

soll die Alarmierung via SMS und CBS aber vorerst zurückgestellt werden. Das BABS soll die Entwicklungen in diesem Bereich weiter untersuchen und zu gegebener Zeit Entscheidungsgrundlagen erarbeiten.

Polysat

Aus Sicht der BORS kann auf eine flächendeckende Realisierung von Polysat vorläufig verzichtet werden. Die Vorteile einer Anbindung an internationale Plattformen oder als diversitäres System zu anderen Kommunikationskanälen (z.B. im Fall eines Erdbebens) werden zwar erkannt, es bestehen aber heute bereits Lösungen wie z.B. mobile Polycom-Basisstationen oder mobile Richtstrahlsysteme der Armee, welche die Vorteile von Polysat teilweise abdecken. Satellitenverbindungen sollen einstweilen nur beschränkt dort realisiert werden, wo es keine sinnvollen Alternativen gibt und die Umsetzung kostengünstig realisiert werden kann.

Fazit

Basierend auf den Konsultationsergebnissen und unter Berücksichtigung der Finanzierbarkeit sieht das VBS das weitere Vorgehen wie folgt:

- Sicherstellung von Betrieb und Werterhalt der bestehenden Systeme.
- Realisierung des SDVN mit dem Datenzugangssystem Polydata und der Ablösung von VULPUS in erster Priorität.
- Konzeptionelle Klärung beim künftigen möglichen Vorhaben des nationalen Lageverbundsystems und dem Ausbau der drahtlosen Breibandkommunikation.
- Bereitstellung der erforderlichen Entscheidungsgrundlagen betreffend den weiteren Betrieb, den Werterhalt oder Ersatz, respektive den Verzicht auf diese bestehenden Systeme.

6 Zuständigkeiten und Finanzierung

Der Bevölkerungsschutz ist ein Verbundsystem zwischen Bund und Kantonen. Die Zuständigkeiten und damit verbunden auch die Finanzierung sind grundsätzlich im BZG und den zugehörigen Verordnungen geregelt. Die Zuständigkeit für bevölkerungsschutzrelevante Alarmierungs- und Telekommunikationssysteme und ihre Finanzierung sind bis anhin aber nur teilweise geregelt, und die Regelungen unterscheiden sich teilweise je nach System. Für die geplanten Vorhaben bestehen noch keine Regelungen.

Die Konsultation bei Bund, Kantonen und Betreibern kritischer Infrastrukturen sowie die Erfahrungen beim Aufbau von Polycom zeigen, dass die Zuständigkeits- und Finanzierungsfragen insbesondere bei Verbundsystemen, bei denen sich Bund, Kantone und Dritte gemeinsam beteiligen, klar geregelt werden müssen. Bei Verbundsystemen werden zentrale und dezentrale Komponenten unterschieden. Die zentralen Komponenten vernetzen die Nutzer miteinander und werden von diesen gemeinsam beansprucht. Bei den dezentralen Komponenten handelt es sich um diejenigen Komponenten, welche proprietär von Bundesstellen, z.B. dem GWK, Kantonen und Dritten genutzt werden und diesen die Nutzung der zentralen Komponenten ermöglicht.

Der Chef VBS sowie die Präsidenten der KKJPD und RK MZF haben für die Klärung der Zuständigkeiten und Finanzierungsfragen am 10. Januar 2017 eine aus Vertretern von Bund und Kantonen zusammengesetzte Arbeitsgruppe einberufen. Die Arbeitsgruppe schlägt folgendes Zuständigkeits- und Finanzierungsmodell vor, das sich an den bewährten Modellen bei Polycom oder Polyalert orientiert:

- Das Notfallradio IBBK, das System Alertswiss zur Information der Bevölkerung im Ereignisfall und weitestgehend auch das Meldevermittlungssystem VULPUS sowie das Sirenenalarmsystem Polyalert sind Bundessysteme. Bei diesen Systemen ist gemäss den gesetzlichen Grundlangen der Bund alleine zuständig und sorgt für deren Finanzierung. Die Bedingungen und Vorgaben für die Nutzung der Systeme, den Betrieb und technische Anpassungen werden aber zusammen mit den Nutzern beraten und ausgearbeitet.
- Bei Verbundsystemen ist der Bund für die zentralen Komponenten zuständig. Für die dezentralen Komponenten sind Bund (Bundesstellen), Kantone sowie Dritte zuständig.
- Unter dem Begriff «Investition» werden alle Aufwände verstanden, die für den Aufbau und die Einführung eines neuen Systems notwendig sind. Darunter sind beispielsweise im Rahmen von SDNV und Polydata Investitionen für Gebäude, Kabel, Hardware, Software, Notstromaggregate, Klimaanlagen usw. zu verstehen (vgl. Tab. 1). Die zentralen Komponenten werden durch den Bund finanziert. Investitionen fallen einmalig an und erfordern in der Regel einen politischen Entscheid (Bundesrat, Parlament). Die Investitionen der dezentralen Komponenten finanzieren die Kantone und Dritte. Soweit es sich um Anschlüsse der dezentralen Komponenten von Bundesstellen handelt, werden diese durch den Bund selber finanziert.
- Nach Ablauf des Lebenszyklus eines Systems fallen erfahrungsgemäss Werterhaltungsmassnahmen an. Diese haben Investitionscharakter. Unter Werterhalt werden dementsprechend grössere Reinvestitionen verstanden, die innerhalb von 6 bis 8 Jahren nach der Erstinvestition anfallen können. Die Kosten dafür entsprechen etwa 60 Prozent der relevanten Erstinvestitionskosten und werden für die zentralen Komponenten durch den Bund finanziert. 60 Prozent deshalb, weil z. B. nicht das ganze Gebäude, die Klimaanlage o. ä. nach 8 Jahren ersetzt werden müssen, primär aber gewisse Hardware- und Softwarekomponenten. Die Kantone und Dritte tragen ihrerseits die Werterhaltungskosten für die dezentralen Komponenten. Dies gilt auch für Bundesstellen, soweit diese über dezentrale Komponenten verfügen.
- Als jährlichen Betriebs- und Unterhaltskosten werden die Aufwendungen für Leistungen zur Sicherstellung des unterbruchfreien 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, aber auch Mietkosten. 15 Prozent der jährlich anfallenden Betriebs- und Unterhaltskosten werden für werterhaltende Massnahmen während des Lebenszyklus der Systeme eingesetzt.
- Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten werden beim mobilen Sicherheitsfunksystem (Polycom), beim Alarmierungssystem (Polyalert), beim System für die Ereigniskommunikation (Alertswiss) und beim Notfallradio IBBK durch den Bund finanziert. Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten von SDVN, Polydata und der VULPUS-Ablösung, des mobilen breitbandigen Sicherheitskommunikationssystems dBBK und des nationalen Lageverbundsystems werden durch alle angeschlossenen Nutzer anteilmässig finanziert. Der Betrieb und der Unterhalt der dezentralen Komponenten werden bei den Bundessyste-

men wie Alarmierungssystem, Ereigniskommunikation und Notfallradio durch den Bund, bei den andern Systemen durch die Kantone bzw. Dritte sowie bei angeschlossenen Bundesstellen ebenfalls durch den Bund finanziert.

- Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten von SDVN und Polydata inkl. der Funktionen, die VULPUS ersetzen, sollen zu 30 Prozent durch die Kantone und zu 70 Prozent durch den Bund getragen werden. Die Kantone werden damit berechtigt, maximal 36 Anschlüsse an dieses System zu realisieren. Die Kostenaufteilung zwischen den Kantonen ist durch diese selbst festzulegen. Der Bund hat seinerseits das Recht für maximal 84 Anschlüsse und sorgt dabei auch für die Anschlüsse der Betreiber kritischer Infrastrukturen oder Dritter, wie beispielsweise der Anschluss des Fürstentums Liechtenstein. Deren Finanzierungsbeiträge kommen dem Bund zugute. Wenn über das jeweilige Anrecht hinaus zusätzliche Anschlüsse realisiert werden, wird der Kostenschlüssel nach dem gleichen Prinzip angepasst.

Tabelle 1: Übersicht über Mitteleinsatz, Fälligkeit und Zuständigkeit der Finanzierung bzgl. Investition, Werterhalt (Reinvestition) sowie Betrieb und Unterhalt am Beispiel von SDVN und Polydata.

	Investition	**Werterhalt (Reinvestition)**	**Betrieb und Unterhalt**
Bestehend aus	Gebäude, Klimaanlage, Notstromaggregat, Hardware, Software, Lizenzgebühren usw.	Grundsätzlicher Wechsel, Hardware (z. B. Router), Software usw.	Wartung, Software-Release/Update, Ersatzteile, Mietkosten usw.
Fällt … an	einmalig[15]	ca. alle 6–8 Jahre	jährlich
Bezahlt durch	Zentrale Komponenten: Bund Dezentrale Komponenten: Bundesstellen, Kantone und Dritte	Zentrale Komponenten: Bund Dezentrale Komponenten: Bundesstellen, Kantone und Dritte	Zentrale Komponenten: Nutzer (Bund mit ten[16]/Kantone: 70/30) Dezentrale Komponenten: Bundesstellen, Kantone und Dritte

- Bei einer Realisierung des nationalen Lageverbundsystems sollen die gleichen Zuständigkeits- und Finanzierungsregeln wie beim nationalen sicheren Datenverbundsystem zur Anwendung gelangen.
- Der Verteilschlüssel beim mobilen breitbandigen Sicherheitskommunikationssystem bleibt noch offen, da insbesondere das Interesse der Beteiligung der Kantone an diesem System zurzeit noch sehr unterschiedlich ist und auch noch die Ergebnisse eines allfälligen Pilotprojekts fehlen.
- Die Sicherstellung der Finanzierung der Kosten die dem Bund entstehen sollte gemäss den betroffenen Bundesstellen über eine zentrale Budgetierung erfolgen. Der Bundesrat wird darüber im Rahmen der jeweiligen Botschaften zu entscheiden haben.

7 Gesetzliche Grundlagen

In der anstehenden BZG-Revision werden die Aufgabenteilung zwischen Bund, Kantonen und Dritten sowie die Finanzierungfragen im Bereich der bevölkerungsschutzrelevanten Alarmierungs- und Telekommunikationssysteme rechtlich verankert, auch wenn die Realisierung der Vorhaben zum Teil erst wesentlich später erfolgen kann. Die Nutzerbedürfnisse, die föderalen Strukturen und volkswirtschaftliche Überlegungen wurden dabei berücksichtigt.

Es ist vorgesehen, dem Bundesrat im 2. Quartal 2018 eine Botschaft für die Bereitstellung des notwendigen Verpflichtungskredites für ein nationales Sicheres Datenverbundnetz (SDVN) zusammen mit der Botschaft zur Revision des BZG vorzulegen und diese in der Folge im Parlament beraten zu lassen.

Um zu vermeiden, dass Kantone und Dritte verschiedene eigene Systeme realisieren, die später wie bei 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 unter Berücksichtigung der Anliegen weiterer Nutzer

[15] Respektive sehr lange Zyklen von Jahrzehnten, z. B. Gebäudeerneuerung.

[16] Bund mit Betreibern kritischer Infrastrukturen und FL.

die Möglichkeit erhalten, technische und terminliche Vorgaben bei solchen Verbundsystemen zu machen.

8 Finanzielle Konsequenzen für Bund und Kantone

Der Werterhalt bestehender Alarmierungs- und Telekommunikationssysteme im Bevölkerungsschutz oder die Realisierung neuer Systeme ist zum Teil nur mit zusätzlichen personellen und finanziellen Ressourcen möglich. Die Konzeptionierung der Vorhaben, die detaillierte Aufstellung der Kosten und notwendigen Ressourcen für Bund, Kantone und Dritte sind bereits mit einem Aufwand und Kosten verbunden, der das Budget des BABS übersteigt. Diese Vorinvestitionen sollen erst getätigt werden, wenn ein politischer Grundsatzentscheid vorliegt, welche Vorhaben zu welchem Zeitpunkt zu konkretisieren sind. Die Genehmigung und Sicherstellung der Ressourcen erfolgt im Rahmen von projektspezifischen Botschaften des Bundesrates zuhanden des eidgenössischen Parlaments, wie es beispielsweise für den Werterhalt von Polycom 2030 der Fall war. Für die Sicherstellung der Betriebsbereitschaft des Systems Polycom bis 2030 waren zusätzliche finanzielle Mittel des Bundes für die nationalen Komponenten erforderlich, die vom Parlament 2016 bewilligt wurden.

Die Kosten für den Betrieb und den Werterhalt von Polycom, Polyalert und IBBK sowie die Kosten für den Werterhalt der ELD NAZ und des Informationssystems Alertswiss sind in den Budgets der zuständigen Bundesstellen (BABS, FUB, GWK, NDB) eingestellt. An den Betriebskosten von Polycom und Polyalert beteiligen sich auch die Kantone gemäss festgelegtem Kostenschlüssel, gestützt auf die geltende Rechtslage.

Der Ressourcenbedarf für die Realisierung, den Betrieb und Werterhalt von SDVN und Polydata sowie die Ablösung von VULPUS können zum jetzigen Zeitpunkt nur grob geschätzt werden. Die Investitionskosten für die gemäss vorgeschlagener Zuständigkeitsregelung vom Bund zu finanzierenden zentralen Komponenten belaufen sich auf rund 150 Millionen Franken. Im Vergleich zu den früheren Kostenschätzungen von 60 Millionen Franken (nur SDVN) sind neu auch die Kosten von Polydata (25 Mio.) und der VULPUS-Ablösung von 25 Millionen eingerechnet. Neu sind zusätzlich die Risiken bei SDVN mit 25 Prozent (15 Mio.) und die Projektmanagementkosten (25 Mio.) berücksichtigt. Die Investitionskosten der dezentralen Komponenten sind durch die jeweiligen Eigentümer und Nutzer selber zu klären und zu finanzieren. 2014 wurde ebenfalls eine Kostenschätzung für die Betriebs- und Unterhaltskosten von SDVN (ohne Polydata und VULPUS-Ablösung) für die nationalen Komponenten vorgenommen. Im Vergleich zu dieser Kostenschätzung muss unter den heutigen Voraussetzungen von höheren Betriebs- und Unterhaltskosten für die zentralen Komponenten von SDVN, Polydata und VULPUS-Ablösung ausgegangen werden. Die Gründe dafür sind Folgende: (a) die heutigen Kostenschätzungen beinhalten neu nicht nur SDVN, sondern zusätzlich die Kosten für Polydata und die VULPUS-Ablösung, (b) die Preise, die für einen Anschluss bezahlt werden müssen, sind für Bund und Kantone gleich, (c) es werden nur noch Anschlüsse mit grösserer Leistung (10 statt 2.5GBit/s) und ein 24/7-Service bei der Kostenberechnung einkalkuliert und (d) es werden neu die Kosten für werterhaltende Massnahmen während des Lebenszyklus mitberechnet (15 Prozent der Betriebs- und Unterhaltskosten). Die jährlichen Betriebs- und Unterhaltskosten der zentralen Komponenten werden auf 20 Millionen Franken geschätzt. Diese Kosten sollen anteilsmässig durch alle angeschlossenen Nutzer finanziert werden. Die Projektumsetzung und der Betrieb des Systems werden nicht ohne zusätzliche Stellen beim Bund zu realisieren sein. Der Betrieb der dezentralen Komponenten ist Sache der jeweiligen Eigner bzw. Nutzer.

Detailliertere Ressourcenangaben sind im Rahmen einer geplanten Botschaft vorgesehen. Für eine Ressourcenabschätzung der anderen Vorhaben sind noch weitere konzeptionelle Abklärungen erforderlich.

Die den Kantonen entstehenden Kosten sind abhängig von ihren Bedürfnissen und der Aufgaben- und Finanzierungsverteilung im Bereich der bevölkerungsschutzrelevanten Alarmierungs- und Telekommunikationssysteme zwischen Bund, Kantonen und Dritten. Falls die Realisierung des Vorhabens SDVN/Polydata beschlossen wird, könnte ein Grundnetz mit Erstanschluss bei allen Kantonen im Zeitraum von 2020 bis 2023 realisiert werden. Die zweite Phase der Realisierung würde von 2024 bis 2027 dauern. Allfällige Kosten auf Kantonsseite dürften voraussichtlich ab 2021 anfallen. Die Nutzungsgebühren für die in der ersten Phase realisierten Anschlüssen wären ab 2024 geschuldet. Deren Höhe hängt auch von den jeweiligen Kantonsbedürfnissen und vom interkantonalen Finanzierungsschlüssel ab.

Falls die Realisierung des Vorhabens VULPUS-Ersatz beschlossen wird, könnte ein Grundnetz mit Erstanschluss bei allen Kantonen bis 2022 realisiert werden. Die Nutzungsgebühren wären ab 2023 geschuldet.

Die allfälligen spezifischen Kantonskosten für das Vorhaben dBBK hängen wesentlich von den jeweiligen Bedürfnissen der einzelnen Kantone und der noch festzulegenden Aufgaben- und Finanzierungsverteilung zwischen Bund und Kantonen ab.

Je nach Massgabe ihres Interesses werden sich auch Dritte wie beispielsweise Betreiber von kritischen Infrastrukturen den Vorhaben SDVN/Polydata und die Ablösung VULPUS-Telematik beteiligen. Entsprechend würden sie gemäss der festzulegenden Finanzierungsregelung auch einen Teil der Kosten zu übernehmen haben.

9 Konsequenzen bei Nichtrealisierung

Werden der Werterhalt und der Betrieb von bestehenden Systemen wie Polycom, Polyalert, ELD NAZ und Alertswiss nicht gesichert, drohen diese ihre Funktionstauglichkeit zu verlieren. Die Konsequenz daraus wäre, dass Einsatzkräfte und Behörden über keinen gemeinsamen Sprachfunk mehr verfügen und bereits bei Alltagsereignissen nicht mehr miteinander kommunizieren könnten. Sie müssten neue Kommunikationswege etablieren und das Risiko in Kauf nehmen, dass bei einem gemeinsamen Einsatz nicht alle über die gleichen Informationen verfügen bzw. diese rechtzeitig erreichen. Beim Terroranschlag am 11. September 2001 auf die World Trade Center in New York führte genau die fehlende Kommunikationsfähigkeit zwischen den verschiedenen Einsatzkräften zu gravierenden Fehlentscheiden, was den Einsatz der Intervention verschlechterte und im Anschluss an die Ereignisse eine Untersuchung auslöste. Beim Verlust des Sirenenalarms würde sich die Reaktionszeit der Bevölkerung auf eine drohende Gefahr massiv verlängern, weil sie nicht mehr rechtzeitig alarmiert werden kann. Menschen mit Höreinschränkungen würden weiterhin von der Alarmierung ausgeschlossen sein, falls der Sirenenalarm mit ICARO-Meldung via Radio nicht mit einem alternativen Alarmierungs- und Informationskanal, d. h. Alertswiss, ergänzt wird. Der Bedarf nach einer schnellen Alarmierung und Information der Bevölkerung hat sich gerade bei den Terrorereignissen der letzten Jahre im Ausland gezeigt.

Werden neu Vorhaben wie SDVN/Polydata nicht realisiert, bleiben der Datenaustausch und wichtige bevölkerungsschutzrelevante Anwendungen weiterhin gegenüber Stromausfall und der Störungen öffentlicher Kommunikationsnetze verletzlich. Wird kein geschlossenes Anwendernetz realisiert, bleiben die Telekommunikationssysteme gegenüber Cyber-Risiken ungenügend geschützt. Bekannte und mehrmals bemängelte Defizite (z.B. Empfehlungen aus der SVU 14) werden nicht behoben. Im Ereignisfall besteht weiterhin das Risiko, dass die strategischen Führungsebenen von Bund, Kanton und Betreibern kritischer Infrastrukturen keine breitbandigen Informationen und Daten austauschen können. Ein koordiniertes und schnelles Vorgehen – insbesondere bei Ereignissen mit landesweiten Auswirkungen – wird damit verunmöglicht. Es besteht ein grosses Risiko, dass Fehlentscheide, späte Anordnung von Massnahmen oder ein ineffizienter Ressourceneinsatz zu Schäden führt, die hätten vermieden werden können.

Ohne einen funktionierenden Lageverbund Schweiz, der alle Ereignisformen und -informationen abdeckt, fehlen den Führungsorganen auf Stufe Bund, Kantone und Betreiber kritischer Infrastrukturen landesweit konsolidierte Lageinformationen. Diese sind aber wichtige Grundlagen für übergeordnete und aufeinander abgestimmte strategische Führungsentscheide, beispielsweise bei einer akuten terroristischen Bedrohung in verschiedenen Landesgebieten oder beim Ressourcenmanagement Bund im Fall einer ausgedehnten nationalen Katastrophensituation.

Für Einsatzkräfte wie GWK, Polizei, Feuerwehr, Rettung und Sanität bedeutet ein Verzicht auf dBBK, dass Einsätze nicht oder nicht effizient bewältigt werden können. Smartphones, Tablets und Notebooks sind bereits heute ein unverzichtbares Instrument der taktischen Ebene. Die sicheren Kommunikationsmöglichkeiten für den Austausch von Informationen oder bei der Übermittlung von Lagebildern, Videos oder der Zugriff auf Datenbanken (z.B. für Fahndung, Ein- und Ausreise) würden fehlen. Personen- und Sachschäden sowie hohe Kosten aufgrund einer verzögerten Wiederherstellung des Normalzustandes können die Folge sein.

Die Behebung der erkannten Sicherheitsdefizite verbessert nicht nur allein die Ausfallsicherheit der Telekommunikationssysteme und des Datenaustauschs der Führungs- sowie Einsatz- und Rettungsorganisationen. Letztlich soll die Bevölkerung von einem besseren Sicherheitsniveau profitieren. Damit könnte im Katastrophenfall oder in einer Notlage das mögliche Schadensausmass erheblich reduziert werden. Ohne die neuen Systeme bliebe die Bevölkerung in der Schweiz einem erhöhten Risiko ausgesetzt.

10 Weiteres Vorgehen

Das weitere Vorgehen sieht wie folgt aus:

1. Die vorliegende Auslegeordnung inkl. Konsultationsauswertung und Antrag wird dem Bundesrat vorgelegt (gleichzeitig mit der Vernehmlassungsvorlage der BZG-Revision).
2. Der Bundesrat entscheidet über die Priorisierung und das weitere Vorgehen.