# Bevölkerungs-schutz

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Bundesamt für Bevölkerungsschutz BABS**

ZEITSCHRIFT FÜR RISIKOANALYSE UND PRÄVENTION, PLANUNG UND AUSBILDUNG, FÜHRUNG UND EINSATZ

**27 / MÄRZ 2017**

Neue Technologien

## Cyber-Risiken

Seite **7**

Nicoletta della Valle, Direktorin von fedpol

## «Die Polizeiarbeit hat sich massiv verändert»

Seite **4**

Kooperation

**Lernen aus der Flüchtlingskrise**

Seite **20**

Ausbildung

**Jodtabletten für die Botschaft in Wien**

Seite **22**

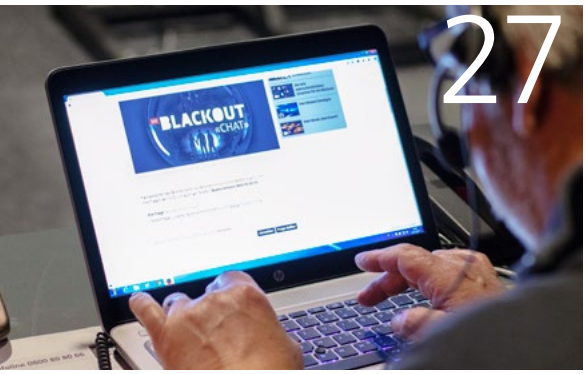
Graubünden

**Grosseinsatz gegen Flammen**

Seite **32**

**www.bevoelkerungsschutz.ch**







**Titelbild: Hacker nutzen die neuen Technologien für kriminelle Zwecke. Fotomontage.**

Liebe Leserin, lieber Leser

Viele Menschen fühlen sich zunehmend unsicher – auch in der Schweiz. Ein wesentlicher Faktor für diese Verunsicherung ist die steigende Komplexität von technischen Systemen, auf die wir im Alltag angewiesen sind. Nahezu alle Bereiche in Wirtschaft, Staat und Gesellschaft sind geprägt von zwei Megatrends: Vernetzung und Digitalisierung. Und auch unser privates Leben wird zu einem grossen Teil bestimmt von Online-Informationen – auch von Algorithmen, die wir nicht verstehen, von Systemen, deren Komplexität wir nicht einmal ansatzweise durchschauen.

**«Unser Leben wird bestimmt von Systemen, deren Komplexität wir nicht einmal ansatzweise durchschauen.»**

Es liegt mir fern, diese neuen Entwicklungen und Technologien zu verteufeln. Sie haben einen grossen Nutzen und bieten riesige Chancen. Wer möchte heute noch darauf verzichten, News, Fahrplanauskünfte oder Öffnungszeiten ständig online und mobil verfügbar zu haben? Vernetzung und Digitalisierung steigern die Effizienz und Produktivität der Unternehmen enorm. Und im Gesundheitswesen können rasche Informationsübermittlung und digitale Vernetzung im Extremfall entscheidend sein, um Leben zu retten. Die Rückkehr in die vordigitale Epoche ist also nicht nur ausgeschlossen – sie würde einen grossen Verlust an Freiheit, Effizienz und Wohlstand bedeuten… und ja: auch einen Verlust an Sicherheit.

Unsere Gesellschaft wird immer leistungsfähiger – der Preis dafür ist jedoch zunehmende Verwundbarkeit. Wir müssen mit einer Paradoxie leben: Einerseits ermöglichen Digitalisierung und Vernetzung mehr Sicherheit. Andererseits setzen sie uns neuen Risiken aus. Damit gewinnt das Thema Cyber-Risiken für den Bevölkerungsschutz an Relevanz. Wir wollen und müssen die Möglichkeiten nutzen, die uns die neuen Technologien eröffnen. Wir müssen aber auch dafür sorgen, dass die Systeme, Daten und Anwendungen, die im Bevölkerungsschutz verwendet werden, sicher sind. Und diese Sicherheit ist heute zunehmend im Cyber-Raum bedroht.

Lesen Sie mehr darüber in unserer Zeitschrift!

**Benno Bühlmann**
Direktor Bundesamt für Bevölkerungsschutz BABS

Nicoletta della Valle, Direktorin von fedpol

# «Die Polizeiarbeit hat sich massiv verändert»

Für Nicoletta della Valle ist fedpol mehr Polizei als Bundesamt. Die fedpol-Direktorin beschreibt im Interview ihre Behörde als Drehscheibe und Dienstleisterin für die Partner in den Kantonen. Nicoletta della Valle über Cybercrime, Terrorismus und ihren Traumjob.

**Sicherheit ist Ihr Beruf. Ist sie Ihnen auch privat besonders wichtig?**
Sicherheit ist für mich so wichtig wie für die meisten: Ich gurte mich im Auto an und trage auf dem Fahrrad und auf den Skiern einen Helm.

**Als oberste Polizistin hegen Sie keine speziellen Ängste?**
Angst ist generell kein besonders guter Ratgeber. Wir leben in einem sicheren Land. Das sieht man auch daran, wie frei sich Bundesräte hier bewegen können. So gesehen leben wir in der Schweiz immer noch auf einer Art Insel. Mein Auftrag ist es, gemeinsam mit meinen Partnerbehörden dazu beizutragen, dass die Schweiz ein sicheres Land bleibt.

**Wie sind Sie zu dieser Aufgabe gekommen?**
Ich habe mich aktiv darum bemüht. Die Leitung von fedpol ist für mich ein Traumjob. Ich finde fedpol die spannendste Behörde des Bundes, weil wir nicht irgendein Amt, sondern eine Polizei sind.

**Was ist denn traumhaft an Ihrem Job?**
Die Spannweite meiner Tätigkeit macht es aus: Ich stehe gegenüber der Politik Rede und Antwort, wenn ich in einer Parlamentskommission das Budget verteidigen muss. Ich verantworte aber auch einen sehr operativen Betrieb mit fast tausend rund um die Uhr engagierten Mitarbeitenden. Ich habe also eine breite Palette von politisch-strategischen und operativen Aufgaben. Das ist eine grosse Verantwortung, aber auch unglaublich spannend.

**Wie sehen die strategischen Aufgaben aus?**
Es gibt keine Polizei auf der Welt, die Ihnen sagt, sie habe genügend Ressourcen. Deshalb ist es eine zentrale strategische Aufgabe, die personellen Ressourcen gezielt einzusetzen und die zahlreichen Aufträge zu priorisieren. Dies erfordert manchmal schwierige Entscheide. Ich muss der Politik aufzeigen, wozu wir da sind, was sie von uns bekommt und was sie von uns nicht bekommt. Dies ist ein Verkaufs- und Übersetzungsjob.

**Und welche operativen Aufgaben hat fedpol?**
Eine ganze Reihe. Beim Besuch ausländischer Ministerinnen und Minister beispielsweise sorgt fedpol zusammen mit der zuständigen Kantonspolizei für den Schutz dieser Gäste und unserer Bundesrätinnen und Bundesräte. Liegt in einem Strafverfahren – etwa gegen mutmassliche Terrorismusunterstützer – die Kompetenz beim Bund, sind wir die Kriminalpolizei des Bundesanwalts. Ausserdem betreiben wir eine 24/7-Einsatzzentrale und sind die «plaque tournante» zwischen den Kantonspolizeien und der ausländischen Polizeibehörde.

## Nicoletta della Valle

Nicoletta della Valle ist seit August 2014 Direktorin von fedpol, wo sie bereits von 2006 bis Anfang 2012 als stellvertretende Direktorin und Chefin der Abteilung Ressourcen gewirkt hat. Dazwischen war sie bei den Universitären Psychiatrischen Diensten Bern (UPD) Direktorin Dienste und Betriebe sowie fast zwei Jahre interimistisch Co-Vorsitzende der Geschäftsleitung. In den 1990er-Jahren arbeitete die Juristin im damaligen Bundesamt für Umwelt, Wald und Landschaft (BUWAL), zuletzt als Leiterin des Rechtsdienstes. Danach war sie Chefin Inspektorat & besondere Aufgaben / Beschwerdedienst im Generalsekretariat des Eidgenössischen Justiz- und Polizeidepartementes (EJPD). Die 55-Jährige lebt in Bern.

**«Es gibt keine Polizei auf der Welt, die Ihnen sagt, sie habe genügend Ressourcen.»**

**Wie beurteilen Sie die Zusammenarbeit mit den Kantonen?**
Sie läuft immer besser. Die innere Sicherheit ist gemäss Verfassung grundsätzlich eine kantonale Angelegenheit. Eine Ausnahme bilden die Ermittlungskompetenzen bei bestimmten Delikten, etwa im Fall von Terrorismus oder kriminellen Organisationen. Kriminalität hört nicht an der Grenze eines Kantons auf, sie macht auch nicht vor der Landesgrenze halt. Deshalb braucht es die Zusammenarbeit aller – der Sicherheitsbehörden des Bundes und der Kantone. Fedpol bietet als Dienstleisterin den Kantonen Koordination, Spezial-Know-how und Unterstützung in der Zusammenarbeit mit dem Ausland. Wir betreiben Informationsysteme, zum Beispiel in den Bereichen Fingerabdruck, DNA-Profile, nationale und Schengen-Fahndung. Um die Bedürfnisse der Kantone zu kennen, stehen wir in regem Austausch mit ihnen. Deshalb bin ich auch Mitglied der Konferenz der kantonalen Polizeikommandanten der Schweiz KKPKS.

**Sie haben kein Problem mit dem Föderalismus?**
Die Entscheidfindung mag manchmal anstrengend sein. Der Föderalismus hat aber wesentliche Vorteile. Käme es in der Schweiz etwa zu einem Attentat wie in Paris, könnten wir auf mehrere Spezialeinheiten zählen – und nicht

## «Ich finde fedpol die spannendste Behörde des Bundes.»

nur auf eine zentrale. Wichtig ist zudem die Nähe zur Bevölkerung. Ich glaube nicht an eine nationale Zentralisierung der Polizei, sie wäre für die Schweiz weder sinnvoll noch realistisch.

**Die Polizei hat auch im Katastrophenfall für Sicherheit zu sorgen. Welche Aufgaben hat da fedpol?**
Sicherheitspolizeilich haben wir im Bevölkerungsschutz einen begrenzten Auftrag, etwa den Schutz von Bundesgebäuden und ausländischen Botschaften. Aber auch bei einer Katastrophe kann ein Kanton unsere Unterstützung benötigen – wenn etwa ausländische Opfer zu beklagen sind. Zählt man Anschläge zum Spektrum der Katastrophen, spielen wir sofort eine zentrale Rolle.

**«Die Herausforderung ist es, den Informationsschutz und die Usability unter einen Hut zu bringen.»**

### Wie ist die Terrorbekämpfung organisiert?

Wenn sich jemand radikalisiert, bemerken dies typischerweise zuerst sein persönliches Umfeld und dann kommunale und kantonale Stellen. Bei einer weiteren Radikalisierung kommt die Person auf den Radar des Nachrichtendienstes. Liegt strafrechtlich relevantes Verhalten vor, übernimmt fedpol den Fall und führt polizeiliche Ermittlungen durch. Konkretisiert sich der Verdacht, stellt fedpol der Bundesanwaltschaft den Antrag, ein Verfahren zu eröffnen. Am Beispiel der Terrorismusbekämpfung sieht man, dass viele Player und Behörden ihre jeweiligen Aufgaben erfüllen müssen. Wenn wir hier nicht gemeinsam funktionieren, geht es nicht. Vor über zwei Jahren hat die Schweiz dazu die Task Force TETRA ins Leben gerufen.

## «Die Bekämpfung von Cybercrime ist ein Schwerpunkt für fedpol.»

### Und wenn es dann doch zu einem terroristischen Anschlag kommt?

Die Ereignisbewältigung vor Ort ist in einem solchen Fall Sache der Kantonspolizei und der lokalen Polizei. Finden gleichzeitig mehrere Ereignisse statt, kann die Kantonspolizei an ihre Grenzen stossen; dann koordiniert der Führungsstab Polizei der Kantone deren Zusammenarbeit und die Ressourcen. In diesen Führungsstab ist auch fedpol mit seiner Einsatzorganisation und seinen internationalen Verbindungen eng eingebunden.

### Wie stark sind Sie international vernetzt?

Die Zusammenarbeit mit dem Ausland ist oft matchentscheidend. Bilateral arbeiten wir mit unseren Nachbarn in Europa zusammen. Ich treffe zum Beispiel jährlich in Den Haag die europäischen Polizeichefs. Es ist sehr wichtig, dass man sich kennt und so auch vertraut. Auf multilateraler Ebene haben wir eine sehr enge Zusammenarbeit mit den Polizeiorganisationen Interpol und Europol. Und als spezielle Instrumente betreiben wir mit Frankreich und Italien in Genf und Chiasso zwei Zentren für Polizei- und Zollzusammenarbeit, in denen die Kantonspolizei, das Grenzwachtkorps und fedpol vertreten sind.

### Kaum eine Rolle spielen Grenzen bei Cyberbedrohungen.

Die Bekämpfung von Cybercrime ist ein Schwerpunkt für fedpol. Da unterscheiden wir zwei Bereiche: Die Alltagskriminalität steht heute fast immer in Verbindung mit Cybermitteln, etwa mit Smartphones oder Notebooks, auch wenn sie nicht direkt im Internet stattfindet. Der zweite Bereich sind Delikte, die sich direkt gegen Computer und IT-Systeme richten.

### Es wird heute viel über Cyberkriminalität geredet.

Die Kriminalität entwickelt sich parallel zu unserem Alltag: Wir handeln immer mehr online, also ist auch die Kriminalität immer mehr online. Das klassische Bild des Bankräubers mit Waffe und Maske wird von jenem des Kriminellen am Bildschirm abgelöst.

### Und kann die Abwehr mithalten?

Leider laufen wir da immer einen Schritt hinterher. Technologisch «up to date» zu sein, ist unglaublich schwierig. Eine Voraussetzung ist, dass unsere Rechtsgrundlagen technologieneutral formuliert sind, damit sie dem raschen technologischen Wandel nicht hinterherhinken. Die Polizeiarbeit hat sich in den letzten zwanzig Jahren massiv verändert. Die Forensik analysiert immer weniger Papier, dafür immer mehr Computerdaten. Es ist anspruchsvoll, aus vielen Terabytes die vom Staatsanwalt benötigten Daten herauszufiltern. Und jede Polizistin, jeder Polizist müsste in der Lage sein, ein Smartphone auszuwerten.

### Wie steht es mit der eigenen IT-Sicherheit?

Das ist ein grosses Thema für uns, weil wir täglich mit sensiblen Daten umgehen. Die Herausforderung ist es, den Informationsschutz und die Usability unter einen Hut zu bringen. Es gilt, intelligente Informationsschutzlösungen zu finden, die die Arbeit der Polizistinnen und Polizisten erleichtern und nicht behindern. Wir müssen zum Beispiel auch von unterwegs und zu jeder Tages- und Nachtzeit mobil und verschlüsselt kommunizieren können.

### Frau della Valle, besten Dank für dieses Gespräch.

Interview:
**Kurt Münger**
Kommunikationschef, BABS

**Überblick**

# Chancen und Risiken neuer Technologien

Neue Technologien verändern unseren Alltag zunehmend. Wir sind dauernd erreichbar und mit unserem digitalen Ich verbunden. Aber nicht nur die Art, wie wir uns informieren und wie wir kommunizieren, hat sich gewandelt. Wir können die Waschmaschine des Ferienhauses aus der Ferne einstellen oder uns gleich selbst in eine virtuelle Realität begeben. Selbstverständlich bringt diese Entwicklung viele Vorteile und Erleichterungen, sie birgt aber auch Risiken, vor allem für die Privatsphäre.


**Dank Sensoren, Aktoren und mobilem Breitband-Internet lassen sich Geräte aus der Distanz überwachen und steuern.**

**Die neuen Technologien haben zu einer globalen Vernetzung geführt – die bis in die Privatsphäre reicht.**

Der wissenschaftliche Fortschritt ist nicht aufzuhalten. Während im Jahre 1995 nur 1 % der Weltbevölkerung Zugang zum Internet hatte, sind es heute 40 %, und Firmen wie Google und Facebook arbeiten unermüdlich daran, Internet in die entlegensten Regionen der Welt zu bringen. In der Schweiz haben über 90 % der Haushalte (meist High-Speed-)Internetzugang.
Zur rasanten Verbreitung und Weiterentwicklung von Technologien, zur Veränderung von Arbeits- und Privatleben und zur Entfaltung neuer Denkweisen hat allerdings in den letzten Jahren nicht nur das Internet beigetragen: Das Homeoffice, flexible Arbeitszeiten und spielerisch gestaltete Büroräume von Internetgiganten sind nur wenige auffallende Beispiele einer neuen Arbeitskultur. Auch im zivilen Schutz und im Krisenmanagement ergeben sich durch neue Technologien Möglichkeiten, die zuvor kaum denkbar waren.

**Das Homeoffice, flexible Arbeitszeiten und spielerisch gestaltete Büroräume von Internetgiganten sind nur wenige auffallende Beispiele einer neuen Arbeitskultur.**

Eine schier endlose Anzahl an Fach- und Modewörtern – meist aus dem Englischen – sind mit den Innovationen und den Anwendungsszenarien neuer Technologien verbunden: «Internet of Things», «Big Data», «Contactless Payments», «Wireless-Technologie», «Cloud-Computing», «Blockchain-Technologie» und «Virtual Reality», um nur einige zu nennen. Die neuen Technologien verändern unseren Alltag und können positive wie negative Einflüsse haben:

### Internet of Things

Der Begriff «Internet of Things» (IoT) beschreibt im Alltag nutzbare, zunehmend intelligente Gegenstände: Drucker, die uns melden, wenn die Tonerkassette auszuwechseln ist, Heizungen, die ihren Verbrauch selbst optimieren usw. Computer werden laufend kleiner, während parallel dazu die Rechen- und Speicherkapazitäten wachsen und die Sensoren – wie GPS, Beschleunigungssensoren und Kameras – immer neue Präzisionsrekorde brechen. Mittels der allgegenwärtigen kabellosen Breitband-Internetverbindungen können immense Datenvolumen ausgetauscht werden. Dies ist eine Voraussetzung für neue Applikationen in der Überwachung und Verwaltung von Gebäuden, Stadt- und Agrarumgebungen.

### Big Data und Cloud-Computing

Die Daten, die etwa über IoT-Sensoren, «Web-Traffic» (Internetverkehr) oder soziale Netzwerke entstehen, bieten Forschern und Unternehmen neue Erkenntnisse über die Gesellschaft und Umwelt. «Big Data» bedeutet, dass wir Zugang zu einer immensen, früher schlichtweg nicht vorstellbaren Anzahl an Daten haben. «Cloud-Computing» ermöglicht es uns, diese riesigen Datenmengen in einfach skalierbaren Rechenzentren zu verarbeiten – Rechenpower kann flexibel «on-demand» gemietet werden.

### Blockchain-Technologie

Ein traditionelles Zahlungssystem setzt eine zentrale Instanz voraus, typischerweise eine Nationalbank. Mit der Erfindung von Bitcoin im Jahre 2008 wurde erstmals bewiesen, dass ein elektronisches Zahlungssystem auch anders funktionieren kann. Bitcoin und die zugehörige Datenbank «Blockchain» ermöglichen es, Prozesse dezentral zu verwalten, die bisher zentral verwaltet wurden. Die Blockchain garantiert, dass Gelder korrekt übermittelt werden und nicht gestohlen werden können.
Interessanterweise erlaubt die Blockchain jedoch weitaus mehr Anwendungen als nur den einfachen Geldaustausch. Dank sogenannter «Smart Contracts» können dezentral Programme ausgeführt werden, die global verifiziert und akzeptiert werden. Smart Contracts ermöglichen zum Beispiel die Verwendung der Blockchain als Entscheidungsinstanz bei Streitschlichtungen.

### Contactless Payments und Wireless-Technology

Konsumentinnen und Konsumenten können heute bereits in vielen Geschäften zahlen, ohne die Kreditkarte einzuschieben, bei kleineren Einkäufen muss der PIN-Code nicht mehr eingegeben werden. Gezahlt wird kontaktlos.
Unser technisches Umfeld besteht aus immer weniger Kabeln: «Wireless LAN», mobiles Internet, «Bluetooth» und kabelloses Laden von Geräten oder kontaktloses Öffnen eines Autos sind nur einige Beispiele.

Diese Entwicklung wird weitergehen und zu eleganteren und einfacheren Lösungen führen.

### Virtual Reality

Moderne Displays besitzen eine derart hohe Pixeldichte, dass das Auge einzelne Pixel nicht mehr erkennen kann. Dank dieses technischen Fortschrittes ist es beispielsweise möglich, einen realitätsnahen 3D-Effekt zu simulieren, indem für jedes Auge ein Display präzise positioniert wird. Mit «Virtual Reality» werden in der Regel Brillen bezeichnet, die 3D-Inhalte wiedergeben und somit ein vollständiges Eintauchen ermöglichen. Zusammen mit dem realitätsnahen Begleitsound wird so ein beeindruckendes Gefühl des Mittendrinseins erzielt. Die aktuellen Lösungen sind noch verbesserungswürdig, aber es ist absehbar, dass sich diese Technologien in einer Vielzahl von Lebensbereichen – vom Spiel bis zur Medizin – durchsetzen werden.

### Suchmaschinen

Suchmaschinen bieten ein Portal zum unerschöpflichen Inhalt des weltweiten Webs. Eine Internetsuche beginnt in aller Regel mit einem oder mehreren Begriffen, die eine Nutzerin, ein Nutzer der Suchmaschine eingibt – und dabei ganz nebenbei Interessen und Wissen verrät. Indem anschliessend eine bestimmte Webseite aus den vorgeschlagenen ausgewählt wird, erhält die Suchmaschine ein klares Signal darüber, welche Ziel-Webseiten für eine bestimmte Suchanfrage relevant sind. Weil die meisten Suchmaschinen zentralisiert sind und von wenigen Konzernen kontrolliert werden, birgt diese Informationsverarbeitung Probleme mit der Privatsphäre der Nutzenden und der Neutralität des Internets.

### Social Bots

Mit sich laufend verbessernder Spracherkennung und künstlicher Intelligenz können sogenannte «Social Bots» als Assistenten wirken. Ob es sich um einen digitalen Assistenten auf unserem Smartphone, um ein fest installiertes Gerät in unserem Eigenheim oder um einen beweglichen Humanoiden handelt: Diese Assistenten sammeln unentwegt Umgebungsgeräusche und können sich an unsere Gewohnheiten anpassen. Die Chancen dieser Technologien sind eindeutig: Je mehr Aufgaben die digitalen Assistenten übernehmen, umso besser können wir Menschen uns auf wesentliche und interessante Aufgaben konzentrieren.

### Der gläserne Mensch

All die genannten neuen Technologien können uns das Leben erleichtern, sie bergen aber gleichzeitig neue Risiken, die schwer zu kontrollieren oder abzuwenden sind. Wir sind bereits Cybermenschen: Täglich kommunizieren, arbeiten und lernen wir über Computer und Smartphone und hinterlassen dabei einen digitalen Fingerabdruck – und damit einerseits ein absichtlich verbreitetes Eigenbild und andererseits ein implizit vermitteltes Verhalten. Unser absichtlich verbreitetes und ideales Eigenbild zeigen wir etwa in sozialen Netzwerken (wie Facebook, Linkedin, Whatsapp). Die zweite Dimension vermitteln wir implizit, es geht um unser eigentlich privates Verhalten, das grosse Internetkonzerne mit Leichtigkeit analysieren und nutzen können. Unsere Cloud-basierten elektronischen Briefkästen und Terminkalender, Speichermedien, unser Surfverhalten und die benutzten Suchbegriffe im Internet sind wichtige Informationsquellen. Unsere

**Wir sind bereits Cybermenschen.**

Smartphones, die wir häufig nutzen und stets bei uns tragen, verfügen über die Rechenkraft der Computer von vor einigen Jahren und bieten zusätzlich Mikrofon, GPS, Kamera und Beschleunigungssensoren. Viele daraus gewonnene Daten werden zu Analysezwecken an Dritte weitergeleitet. Langjährige Forschung und Erfahrung zeigen, dass es ausserordentlich schwierig ist, die Privatsphäre der Nutzenden zu schützen.
Aufgrund der Digitalisierung haben Informatik-gestützte Systeme zunehmende Entscheidungskraft über die Daten und Informationen, die uns betreffen. Damit werden diese Systeme ebenfalls Ziel von Cyberattacken, und IT-Sicherheit spielt eine immer wichtigere Rolle in unserer Gesellschaft.

### Dringliche Fragen

Obwohl sich neue Technologien immer schneller entwickeln und wir Menschen bereits eng mit der Technik verbunden sind, ist die Verknüpfung zwischen uns und den Maschinen doch noch sehr begrenzt. Mithilfe unserer Sinne, ob mit Augen oder Ohren, können wir eine beträchtliche Bandbreite an Informationen aufnehmen,

**Sobald der Informationsfluss von Mensch zu Maschine effizienter wird, werden auch IT-basierte Applikationen deutlich leistungsfähiger.**

die Schnittstelle von Maschine zu Mensch erlaubt einen reichen Fluss an Informationen. Umgekehrt ist die Übertragung von Mensch zu Maschine weitgehend limitiert auf die Eingabe der Informationen mittels Tastatur oder Sprechen, womit deutlich weniger Informationen übermittelt werden können. Sobald der Informationsfluss von Mensch zu Maschine effizienter wird, werden auch IT-basierte Applikationen deutlich leistungsfähiger. Die Fragen der Sicherheit und des Schutzes der Privatsphäre werden dadurch allerdings in gleichem Masse dringlicher.

**Arthur Gervais**
Wissenschaftlicher Assistent IT-Sicherheit, ETH Zürich

**Meldestelle MELANI**

# Den Internetbetrügern auf der Spur

Datenklau, Hackerangriffe und Erpressungsversuche verunsichern die Computergemeinde. In der Schweiz sorgt die nationale Meldestelle MELANI dafür, dass der Schutz vor und die Abwehr von Cyber-Verbrechen laufend verbessert werden.

Über das genaue Wann, Wo oder Wer streiten sich bis heute die Geister. Doch weil zu einer derart bedeutenden Sache eine ordentliche Geschichte gehört, wurde der 6. August 1991 als offizielle Geburtsstunde des World-Wide-Web gewählt. Vor 25 ½ Jahren ging die Website des Kernforschungsinstituts CERN in Genf als erste überhaupt online. Das Internet, worauf das Surfen seither möglich ist, ist allerdings noch älter: 1977 gelang die Premiere, IT-Netzwerke untereinander kommunizieren zu lassen. Der weltweite Online-Datenaustausch darf dieses Jahr den 40. Geburtstag feiern.
Die Partylaune wird derzeit allerdings getrübt. Anstelle von Lobreden machen Schlagzeilen über klandestine Hackerangriffe auf Staatscomputer oder perfide Online-Erpressungsfälle die Runde. Die Themen «Hacking-Reality» und «Computersicherheit» bestimmten die Agenda am Branchentreffen des Chaos Computer Clubs in Hamburg über den Jahreswechsel. Und Europol warnt vor der «steigenden Aggressivität in der organisierten Internet-Kriminalität». In einzelnen Staaten habe Cybercrime die Schadenswerte aus der «traditionellen Kriminalstatistik» bereits überholt.

## Meldestelle des Bundes

Nach wie vor beeindruckt an der jungen Karriere, wie unverzichtbar das «Netz» im privaten, staatlichen und ökonomischen Alltag geworden ist. Zuletzt haben sich jedoch die negativen Meldungen derart gehäuft, dass das bisherige Vertrauen in die virtuelle Datenwelt in ebenfalls verblüffend kurzer Zeit deutlich geschwunden ist. Der digitalen Kommunikation drohe die Krise, sagen nicht nur Computerfreaks und Zukunftsforscher. Befürchtungen über einen Cyber-Krieg oder von kriminellen Hackern komplett lahmgelegte Systeme haben den zuvor sorglosen Umgang mit dem Internet abgelöst. Die Skepsis, dass das Netz auch eine kriminell verseuchte Zone ist, wächst überall dort, wo mindestens eine Arbeitsstation das Privat- oder Berufsleben erleichtern soll.
Nicht überraschend ist deshalb, dass selbst ein Internetprofi wie Max Klaus das WLAN-Modem zu Hause lieber ausgeschaltet weiss. Andererseits ist beruhigend zu wissen, dass er seine Arbeitszeit im Auftrag der Schweizerischen Eidgenossenschaft nichts anderem als dem bestmöglichen Schutz kritischer Infrastrukturen vor Hackerangriffen widmet. Klaus ist stellvertretender Leiter der Melde- und Analysestelle Informationssicherung MELANI, die die Lage der inländischen Cyber-Sicherheit im Auge behält und möglichst schnell auf Bedrohungen wie Passwortklau, Viren oder Malware reagiert.
Das Informatiksteuerungsorgan des Bundes (ISB) und der Nachrichtendienst des Bundes (NDB) haben diese Fachstelle gemeinsam eingerichtet, damit bestens ausgebildete IT-Spezialisten die wachsende Internet-Bedrohung beobachten und mögliche Angriffsopfer im Inland, darunter Verwaltungsstellen und Unternehmen, vor möglichen Angriffen gezielt warnen können. Seit zwölf Jahren berichtet MELANI halbjährlich über die Bedrohungslage. Für alle Internetuser verständlich, damit dies auch zur weiteren Sensibilisierung beitragen kann.

**Seit zwölf Jahren berichtet MELANI halbjährlich über die Bedrohungslage.**

## Hauptzweck ist die Frühwarnfunktion

Geschäftsrapporte von Ämtern oder Privatfirmen sind meistens trockene, schwer verständliche Lektüre. Die MELANI-Semesterberichte bieten hingegen mindestens so aufregenden Stoff wie Cyber-Kinofilme oder Spionageromane. Anfang 2016 wurde publik, dass die bundesnahe Rüstungsfirma RUAG elektronisch ausspioniert worden war. Monate zuvor konnten Unbekannte eine Schadsoftware in das interne Datennetzwerk einschleusen; Schaden und Täterschaft werden inzwischen, auch dank der von MELANI zusammengetragenen Daten, von der Bundesanwaltschaft untersucht. Kurze Zeit später, im

**Mit der Sicherheit im Internet sollten sich nicht nur Computerspezialisten beschäftigen. MELANI berichtet halbjährlich über die Bedrohungslage – für alle Internetuser verständlich.**

Frühjahr, wurden Tausende von E-Mail-Adressen aus Datenbanken politischer Parteien gestohlen. Und ebenfalls letztes Jahr waren E-Mails mit dem falschen Absender «Bundesamt für Bevölkerungsschutz» und einem vermeintlichen Dokument über «kontaminiertes Trinkwasser» im Umlauf, die nur dazu dienten, mit dem Download des Anhangs eine Malware auf den betreffenden Computern zu installieren.

Jährlich werden unzählige derartige kleine, grosse bis einschüchternde Missbrauchs- und Phishingattacken registriert. Hauptzweck der vom Bund eingerichteten Meldestelle ist die Frühwarnfunktion und Prävention: Mit den an MELANI angeschlossenen Unternehmen werden ausgewählte vertrauliche Informationen ausgetauscht. Und falls nötig werden diese Unternehmen auch bei der Abwehr unterstützt.

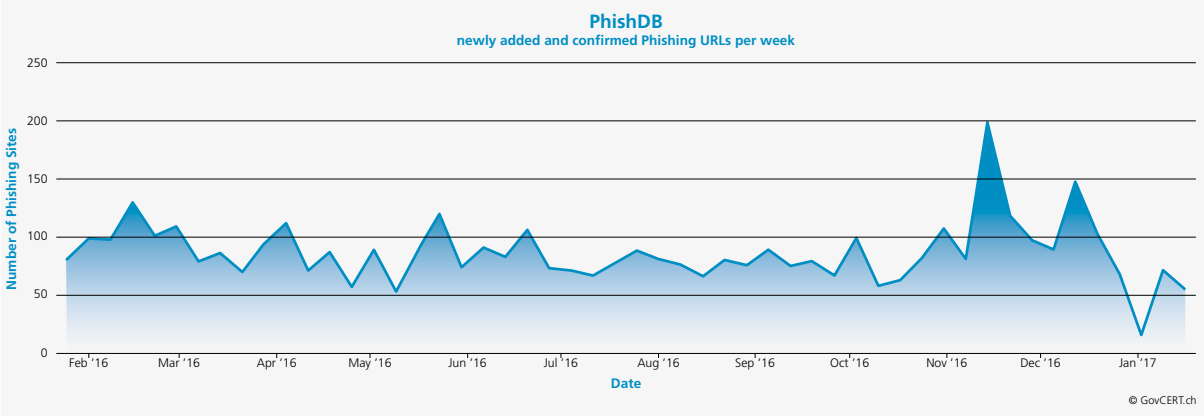
Neben Banken oder Telekommunikationsfirmen sind insbesondere Energieversorger an solchen Informationen interessiert. Und neuerdings geraten Spitäler in den Fokus von Cyber-Kriminellen, weil ihre elektronische Infrastruktur als empfindliches Feld für Erpressungsversuche gilt. «Die meisten Angriffe dienen dazu, mit wenig Aufwand möglichst viel Geld zu verdienen», fasst Max Klaus die Bedrohungsvarianten zusammen.

## Kooperation wird begrüsst

Im Vergleich zu anderen Ländern kennt die Schweiz keine staatliche Meldepflicht; Hinweise auf Hackerangriffe und virtuelle Erpressungsversuche werden von den Betroffenen daher freiwillig weitergegeben. Mit der staatlichen Stelle wird gern kooperiert; das gegenseitige Vertrauen verbessert das bestehende Sicherheitssystem: Letztes Jahr wurden MELANI 6000 E-Mail- und Passwortkombinationen zugespielt, die zuvor durch Hacker gestohlen worden sind. Am 16. März 2016 schaltete MELANI einen öffentlich zugänglichen Check online, um alle möglichen E-Mail-Adressen zu überprüfen. Diesmal entschloss sich das MELANI-Team für den Gang an die breite Öffentlichkeit. Bei anderen Gefährdungsfällen wird jedoch diskreter vorgegangen. «Wir gehen mit den uns angeschlossenen Unternehmen Stillschweigeabkommen ein und dürfen deshalb nicht alles veröffentlichen», ergänzt Klaus.

**Neuerdings geraten Spitäler in den Fokus von Cyber-Kriminellen, weil ihre elektronische Infrastruktur als empfindliches Feld für Erpressungsversuche gilt.**

Anfänglich wurde vor allem vor Viren und Würmern ge-



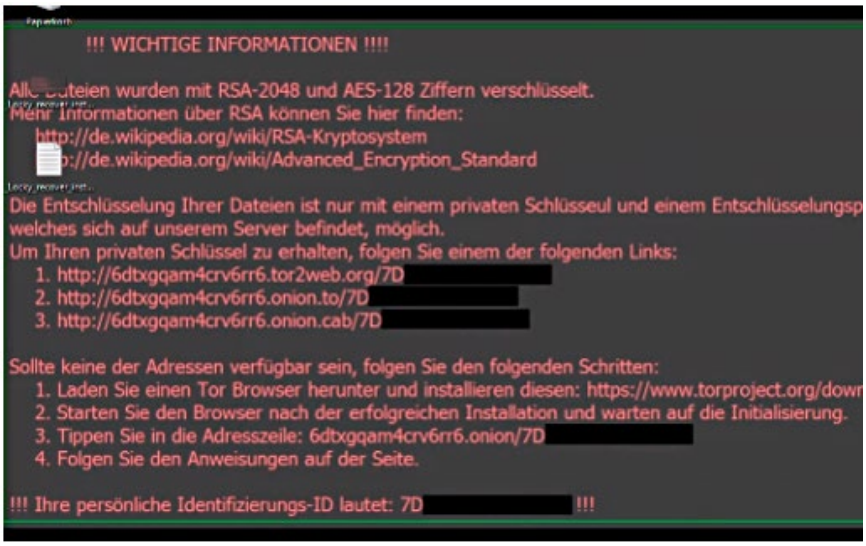

**Für die Zeit der Weihnachtseinkäufe ist eine erhöhte Phishing-Aktivität zu verzeichnen.**

warnt; angegriffen wurden vorwiegend E-Banking- oder andere Bezahlportale, um an Kontodaten, Kreditkartencodes oder Passwörter zu gelangen. Inzwischen ist Erpressung das attraktivste Geschäftskonzept für Cybertäter: Entweder werden heikle Daten von Firmen oder öffentlichen Einrichtungen geklaut oder ihre Verwendung blockiert, damit die Betroffenen ein Lösegeld bezahlen. Von derartigen Angriffen betroffen sind die Finanzbranche, Webshops und, wie erwähnt, selbst Spitäler.
Die MELANI-Mitarbeitenden sind weder Spione noch Polizisten. Sie dürfen nie selbst eingreifen, sind aber so gut wie kaum jemand sonst über die Gefährdungslage im in- und ausländischen Cyber-Umfeld informiert. Eine Vielzahl vergleichbarer IT-Stellen im In- und Ausland gehört zum Beziehungsnetzwerk.

## Sensibilisieren und lernen

Als stellvertretender Leiter der Meldestelle ist Max Klaus ein von Medienschaffenden gerne befragter Experte, wenn ein Beitrag für mehr IT-Sicherheit publiziert werden soll. Auch wenn es um MELANI selbst geht, wird der Zugang nicht geschlossen. Die Büros von Klaus und seinen Arbeitskollegen liegen mitten in der Stadt Bern, umgeben von weiteren Bundesverwaltungsstellen; der Zutritt für angemeldete Besucher ist mit den üblichen Vorkehrungen geschützt. Jeder Kinofilm würde ab hier dichte Schleusen oder ein Abtasten der Handys zeigen; diese Vorsicht braucht es an der Schwarztorstrasse 51 jedoch nicht. «Uns gegen aussen abzuschotten wäre kontraproduktiv», beginnt Klaus. «Denn ohne das Zutun der Öffentlichkeit und der Privatwirtschaft wären wir chancenlos.»
Die Arbeit wird zudem geteilt: MELANI selbst darf keine Internetverbrecher jagen und muss sich peinlich genau an Datenschutz- und die weiteren Gesetze halten. Für die IT-Sicherheit sind einzig und allein die Anwender verantwortlich; die meisten grösseren Betriebe haben eigene Fachkräfte angestellt. Und auch die Polizei verfügt inzwischen über Spezialisten, die für die Strafverfolgung von Cyberverbrechern zuständig sind.
Die MELANI-Fachleute warten aber nicht nur ab: Unbekannte Software wird intern analysiert und die Erkenntnisse werden ausgewählten Partnern zur Verfügung gestellt. Zwar erfolgt kaum ein Angriff gleich wie der vorangegangene. Aber «je besser wir allfällige Sicherheitslücken und Einfallstore kennen und die nötigen Massnahmen einleiten, desto schwieriger wird die Arbeit der Angreifer», fasst Klaus zusammen.
Die Meldestelle MELANI will aber auch sensibilisieren und organisiert gemeinsam mit vielen weiteren Organisationen den «Ransomware-Awareness-Tag». Denn der «Mitarbeiter», der E-Mails verschickt und empfängt, Webseiten besucht, sich dort registriert oder Downloads durchführt, ist inzwischen das grosse Risiko, dass der Zugang zur internen Datenwelt durch Cyber-Kriminelle gehackt werden kann. «Wir dürfen uns weiterhin über viele Neuerungen freuen; aber wir müssen akzeptieren, dass man sich so gut wie möglich vor Bedrohungen schützen muss», fasst Max Klaus die Aussichten zusammen.

**Paul Knüsel**
Wissenschaftsjournalist




**Bei Verschlüsselungstrojanern (Erpressungstrojanern) handelt es sich um Schadsoftware, die Dateien auf dem Computer des Opfers verschlüsselt und für das Opfer unbrauchbar macht.**

**Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)**

# Betreiber kritischer Infrastrukturen sind gefordert

Die Digitalisierung und Vernetzung von Wirtschaft und Gesellschaft ist mit vielfältigen Risiken verbunden. Besonders gravierend auswirken können sich Cyber-Angriffe auf kritische Infrastrukturen wie die Strom- oder die Trinkwasserversorgung, das Gesundheitswesen oder den Finanzsektor. Der Bund engagiert sich, um diese Gefährdungen zu erkennen und zu reduzieren.

| Kritische Sektoren (KS) | Koordination NCS Massnahmen | Kritische Teilsektoren (KTS) |
|---|---|---|
| Behörden | BABS | Diplomatische Vertretungen und Sitze internat. Organisationen |
| | BABS | Forschung und Lehre |
| | BABS | Kulturgüter |
| | BABS | Parlament, Regierung, Justiz, Verwaltung |
| Energie | BWL | Erdgasversorgung |
| | BWL | Erdölversorgung |
| | BWL | Stromversorgung |
| Entsorgung | BABS | Abfälle |
| | BWL | Abwasser |
| Finanzen | BABS | Banken |
| | BABS | Versicherungen |
| Gesundheit | BABS | Ärztliche Betreuung und Spitäler |
| | BABS | Labors |
| Industrie | BWL | Chemie- und Heilmittelindustrie |
| | BWL | Maschinen-, Elektro- und Metallindustrie |
| Information und Kommunikation | BWL | Informationstechnologien |
| | BABS | Medien |
| | BABS | Postverkehr |
| | BWL | Telekommunikation |
| Nahrung | BWL | Lebensmittelversorgung |
| | BWL | Wasserversorgung |
| Öffentliche Sicherheit | BABS | Armee |
| | BABS | Blaulichtorganisationen (Polizei, Feuerwehr, Sanität) |
| | BABS | Zivilschutz |
| Verkehr | BWL | Luftverkehr |
| | BWL | Schienenverkehr |
| | BWL | Schiffsverkehr |
| | BWL | Strassenverkehr |

**Die Teilsektoren sind kritisch, weil**

- deren Akteure (lebens)wichtige Leistungen für die Bevölkerung und Wirtschaft erbringen
- Störungen oder Ausfälle in der Erbringung der Leistungen Auswirkungen auf die Bevölkerung und Wirtschaft haben
- sie ein Gefahrenpotential für Mensch, Tier und Umwelt darstellen

Reguläre Kritikalität | Grosse Kritikalität | Sehr grosse Kritikalität

**Gemäss SKI-Strategie sind die kritischen Infrastrukturen Teilsektoren und Sektoren zugewiesen. Insgesamt gibt es zehn kritische Sektoren und 28 kritische Teilsektoren.**

Im Internet lauern viele unsichtbare Gefahren. Dazu gehören beispielsweise Cyber-Attacken auf die Stromversorgung – mit folgenschweren Konsequenzen: Öffentliche Verkehrsmittel stehen still, Telefone und andere Kommunikationsmittel funktionieren nicht mehr, Geschäfte und Banken bleiben geschlossen, Heizungen fallen aus und Wasser kann nicht mehr in die Haushalte gepumpt werden. Cyber-Angriffe könnten gar Menschenleben gefährden, wenn durch sie in Spitälern lebenserhaltende medizinische Geräte oder Patienteninformationen manipuliert würden.
Es ist wichtig, sich der Gefahren aus dem Cyber-Raum bewusst zu sein und die Resilienz (Widerstands- und Regenerationsfähigkeit) kritischer Infrastrukturen mit gezielten Massnahmen zu verbessern. Eine zentrale Rolle spielt dabei der Schutz von Informations- und Kommunikationsinfrastrukturen. Im Juni 2012 hat der Bundesrat die nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) verabschiedet und verschiedene Stellen des Bundes damit beauftragt, sie zusammen mit Partnern aus Behörden, Wirtschaft und Gesellschaft umzusetzen. Die Strategie verfolgt als übergeordnete Ziele:

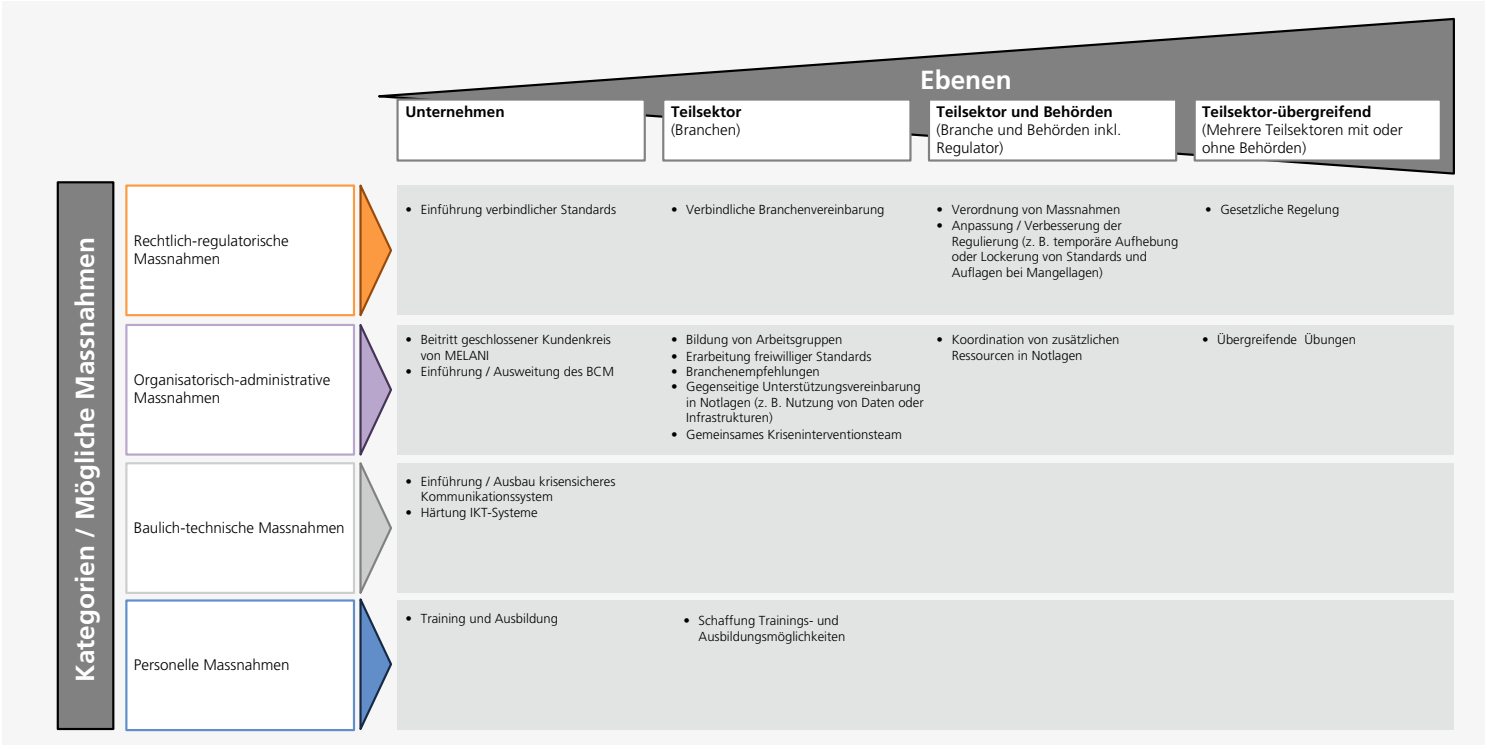
– die frühzeitige Erkennung von Bedrohungen und Gefahren im Cyber-Bereich,
– die Erhöhung der Resilienz von kritischen Infrastrukturen,
– die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.

## Zwei Ämter, zwei Massnahmen

Um diese Ziele zu erreichen, wurden verschiedene Massnahmen definiert – einige davon betreffen kritische Infrastrukturen. Im Auftrag des Bundesrates haben das Bundesamt für wirtschaftliche Landesversorgung BWL und das Bundesamt für Bevölkerungsschutz BABS zwei der Massnahmen aus der NCS umzusetzen. Einerseits soll geprüft werden, ob Risiken bestehen, die zu schwerwiegenden Störungen oder Ausfällen von wichtigen Dienstleistungen und Gütern führen können (etwa zu einem grossflächigen Ausfall des Gesundheitswesens oder der Stromversorgung). Andererseits sollen aufbauend auf den Ergebnissen dieser Untersuchungen weitere Massnahmen erarbeitet werden, mittels derer die Resilienz der kritischen Infrastrukturen verbessert werden kann. Der Fokus der Arbeiten liegt dabei auf den Informations- und Kommunikationstechnologien (IKT) und auf Cyber-Risiken.
Von zentraler Bedeutung sind der frühzeitige Einbezug sowie die enge Zusammenarbeit mit den Behörden, den Betreibern der kritischen Infrastrukturen, den Verbänden und weiteren Stellen. Ebenfalls wichtig ist, dass die Kompetenzen und die Verantwortlichkeiten der Akteure gewahrt bleiben. Insbesondere behalten die Fachbehörden die Regulations- bzw. die Vorgabekompetenz.

## Anbindung an die nationale SKI-Strategie

Das Spektrum der kritischen Infrastrukturen zählt 28 Bereiche (Teilsektoren). Dementsprechend breit ist das Untersuchungsgebiet. Das BWL und das BABS koordinieren die Arbeiten im Rahmen der NCS für je 14 kritische Teilsektoren (siehe Abbildung 1).
Da heute die meisten Ausfälle nicht durch Cyber-Angriffe verursacht werden, ist es wichtig, beim Schutz der kritischen Infrastrukturen weitere relevante Gefährdungen zu




**Massnahmen zur Verbesserung der Resilienz kritischer Infrastrukturen lassen sich auf verschiedenen Ebenen (x-Achse) umsetzen und verschiedenen Kategorien (y-Achse) zuweisen.**

betrachten. Das BABS setzt deshalb die Massnahmen der NCS-Strategie in Kombination mit der übergeordneten Strategie zum Schutz kritischer Infrastrukturen (SKI) um, die der Bundesrat ebenfalls im Juni 2012 verabschiedet hat. In diesem Kontext untersucht das BABS, ob nebst den Cyber-Risiken beispielsweise auch ein grossflächiger Stromausfall, ein schwerwiegendes Erdbeben oder ein gezielter Anschlag zu gravierenden Störungen in den kritischen Teilsektoren führen können.
Methodisch lehnt sich das Vorgehen zur Prüfung und Verbesserung der Resilienz kritischer Teilsektoren weitgehend an den SKI-Leitfaden an, sodass eine Kongruenz zwischen den Arbeiten sichergestellt werden kann. Der SKI-Leitfaden orientiert sich an etablierten Konzepten aus den Bereichen Risiko-, Krisen- und Kontinuitätsmanagement. Im Unterschied zu den Managementsystemen steht jedoch nicht das Wohlergehen der Unternehmen oder der Organisationen im Vordergrund, sondern dasjenige der Bevölkerung und ihrer Lebensgrundlagen.

## Identifikation von Schwachstellen und Risiken

In einem ersten Schritt wird geprüft, wie anfällig ein Teilsektor auf Störungen und Ausfälle ist. Hierzu wird einerseits die Struktur des Teilsektors analysiert: Können sich die Akteure gegenseitig unterstützen (z. B. Übernahme von Patienten durch eine andere medizinische Einrichtung)? Gibt es für eine gewisse Dienstleistung oder ein Produkt mehrere oder nur einen Anbieter? Sind die Akteure in der ganzen Schweiz verteilt oder befinden sie sich an wenigen Standorten – gar nur an einem einzigen? Nebst der Struktur des Teilsektors wird auch untersucht, wie abhängig die Akteure von relevanten Ressourcen wie Arbeitskräften, Energie, IKT, Rohstoffen und Betriebsmitteln sowie Infrastruktur und Logistik sind.
Anhand der Ergebnisse wird in einem zweiten Schritt analysiert, welche Schäden aus relevanten Gefährdungen (Cyber-Angriff, IKT-Ausfall, Ausfall der Stromversorgung etc.) entstehen und welche Risiken sich daraus für die Bevölkerung und Wirtschaft ergeben.

## Verbesserung der Resilienz

Ausgehend von den identifizierten Schwachstellen und Risiken werden Massnahmen zur Verbesserung der Resilienz erarbeitet. Dabei hilft der risikobasierte Ansatz, Massnahmen zu definieren, die kostengünstig sind und die Risiken dennoch stark reduzieren. Nicht angestrebt wird eine Reduktion sämtlicher Risiken und Verwundbarkeiten, da dies mit unverhältnismässig hohen Kosten verbunden wäre.
Die Massnahmen können auf verschiedenen Stufen (Unternehmen, Branche, mehrere Branchen mit und ohne Behörden) umgesetzt und verschiedenen Kategorien (rechtlich-regulatorisch, organisatorisch-administrativ, baulich-technisch, personell) zugeordnet werden (siehe Abbildung 2). Bei der Umsetzung gilt grundsätzlich das Prinzip der Subsidiarität: Der Staat greift nur dort regulatorisch oder unterstützend ein, wo die Unternehmen und Organisationen nicht in Eigenregie ihre Resilienz verbessern (können).

## Bereits zahlreiche Vorkehrungen getroffen

Die Berichte zu den Analysen und Massnahmen müssen bis Ende 2017 für alle 28 Teilsektoren vorliegen. Die bisherigen Arbeiten haben ergeben, dass ein Grossteil der untersuchten Teilsektoren bereits zahlreiche Vorkehrungen getroffen hat, um Ausfällen und Störungen vorzubeugen oder – sollte ein Ereignis eintreten – deren Auswirkungen respektive deren Dauer zu minimieren. Dennoch gibt es Bereiche, in denen Handlungsbedarf besteht und für die Massnahmen zur Verbesserung der Resilienz identifiziert werden konnten.
Dazu gehört beispielsweise die Aufnahme von besonders relevanten Akteuren in den geschlossenen Kundenkreis von MELANI (Melde- und Analysestelle Informationssicherung). Der geschlossene Kundenkreis umfasst ausgewählte Betreiber kritischer Infrastrukturen, und die Aufgabe von MELANI ist es, diese vor Cyber-Risiken zu schützen. Aber auch die Schulung und Sensibilisierung der Mitarbeitenden gegenüber Cyber-Gefahren oder die Erarbeitung von Notfallkonzepten, mittels welcher wichtige Leistungen im Ereignisfall weitergeführt werden können, zählen zu den identifizierten und umzusetzenden Massnahmen.

**Der risikobasierte Ansatz hilft, Massnahmen zu definieren, die kostengünstig sind und die Risiken dennoch stark reduzieren.**

Die Berichte, die zusammen mit den Fachbehörden, Verbänden und Betreibern kritischer Infrastrukturen erarbeitet werden, sind nicht für die Öffentlichkeit vorgesehen. Zur breiteren Information wird jedoch für jeden Teilsektor ein Factsheet erstellt, das die Leistungen, die Akteure und die identifizierten Schwachstellen und Risiken aufzeigt. Diese Factsheets sind auf der Website des Informatiksteuerungsorgans des Bundes ISB zugänglich.

**Angelika P. Bischof**
Wissenschaftliche Mitarbeiterin Schutz kritischer Informationsinfrastrukturen, BABS

*Für weitere Informationen:*
*www.infraprotection.ch*
*www.isb.admin.ch*

**Schutz kritischer Infrastrukturen (SKI)**

# Cyber-Risiken im Bevölkerungsschutz

Kann ein Cyber-Angriff die Einsatzfähigkeit im Bevölkerungsschutz beeinträchtigen? Welche Massnahmen gegen solche Gefährdungen wurden bereits ergriffen? Und welche Herausforderungen und Chancen bringt die Zukunft? Mit Risiko- und Verwundbarkeitsanalysen versucht das Bundesamt für Bevölkerungsschutz BABS diese Fragen zu beantworten.

Im Rahmen der nationalen Strategie zum Schutz kritischer Infrastrukturen (SKI) und der nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) wird derzeit die Resilienz (Widerstands- und Regenerationsfähigkeit) der kritischen Infrastrukturen überprüft und verbessert. Zu den kritischen Infrastrukturen zählen auch die Partner im Bevölkerungsschutz. In Zusammenarbeit mit Behörden, Blaulichtorganisationen und Zivilschutz wurden die Risiken für Störungen bei Polizei, Feuerwehr, Rettungswesen und Zivilschutz untersucht. In die Untersuchung einbezogen wurden ebenfalls wichtige behördliche Aufgaben, etwa im Bereich der Warnung und Alarmierung.
Im Fokus der Arbeiten steht vor allem die Frage, ob es in den genannten Bereichen grossflächige und gravierende Störungen der relevanten Dienstleistungen geben kann. Neben Cyber-Risiken wurden weitere Gefährdungen untersucht, die zu solchen Störungen führen können (Stromausfall, Naturgefahren usw.).

**Die Mobilisierung von Feuerwehr und Zivilschutz geschieht in der Regel via Telefon oder Pager, wobei eine starke Abhängigkeit vom öffentlichen Telekommunikationsnetz besteht.**

An mehreren Workshops und Treffen wurden zunächst die Kernaufgaben der Einsatzorganisationen bei Alltagsereignissen sowie bei Katastrophen und in Notlagen unter die Lupe genommen. Die Analyse berücksichtigte aber auch vorsorgliche und präventive Tätigkeiten wie den Unterhalt von Schutzräumen oder das Betreiben von Mess- und Früherkennungssystemen. Anschliessend wurden ausgewählte Gefährdungen identifiziert, die zu Störungen dieser Aufgaben führen können.

Experten schätzten die Höhe der Schäden, die bei Bevölkerung und Wirtschaft eintreten könnten, sollten die Partnerorganisationen ihre Aufgaben nicht erfüllen. Ziel war es zudem, Schwachpunkte zu erkennen, die einen Cyber-Angriff besonders gefährlich machen. Die möglichen Auswirkungen von Cyber-Angriffen sind vielfältig: Sie könnten die Kommunikation einschränken, elektronische Informationen zerstören oder auch wichtige und sensitive Daten manipulieren.

## Aufgebot der Einsatzkräfte

Verwundbarkeiten, aber auch Massnahmen lassen sich an den drei Themenbereichen «Aufgebot der Einsatzkräfte», «Entgegennahme von Notrufen» und «Organisationsübergreifende Kommunikation im Falle einer Katastrophe oder Notlage» aufzeigen:
Dass ein Alltagsereignis oder eine Katastrophe jederzeit eintreten kann, stellt hohe Anforderungen an die Einsatzfähigkeit der Partnerorganisationen des Bevölkerungsschutzes. Die Mehrheit der Angehörigen von Feuerwehr und Zivilschutz übt ihre Aufgaben in einer Milizfunktion aus und muss innerhalb weniger Minuten oder Stunden von zu Hause oder ihrem Arbeitsplatz in den Einsatz gehen können. Die Mobilisierung geschieht in der Regel via Telefon oder Pager, wobei eine starke Abhängigkeit vom öffentlichen Telekommunikationsnetz besteht. Dieses könnte aber beispielsweise aufgrund eines grossflächigen Blackouts ausfallen.
Neu verwalten alle Kantone die Personaldaten der Zivilschutz-Angehörigen mit dem Personalinformationssystem der Armee (PISA). Die Nutzung eines zentralen Systems eröffnet neben Chancen auch Risiken: Die Datenbestände umfassen unter anderem die Strukturen des Zivilschutzes, die Kontaktdaten und die zivilen Kenntnisse der Dienstpflichtigen. Die Verfügbarkeit von PISA wird mittel-


**In der Schweiz gibt es rund 170 Notrufzentralen (im Bild die Einsatzleitzentrale 144/118 von Schutz & Rettung Zürich). Fällt eine davon aus, gewährleistet eine sogenannte dynamische Leitweglenkung, dass ein Notruf in einer anderen Notrufzentrale entgegengenommen werden kann.**

fristig für das Aufgebot an Bedeutung gewinnen, obwohl Alarm- und Notfallaufgebote weiterhin durch die Systeme der Kantone bzw. der Zivilschutzorganisationen ausgelöst werden. Es gilt, ein alternatives Aufgebot der Einsatzkräfte vorzubereiten.

### Notrufe und Breitbandkommunikation

Alarmiert werden die Blaulichtorganisationen in der Regel über die bestehenden Notrufnummern 112, 117, 118 und 144 oder über automatische Brandmelde- und Alarmanlagen. In der Schweiz gibt es für Feuerwehr, Polizei sowie Sanitäts- und Rettungsdienste rund 170 Notrufzentralen, die jeweils für ein definiertes geografisches Gebiet zuständig sind. Die Hilfesuchenden kontaktieren die Zentralen über die öffentlichen Telekommunikationsnetze. In den Notruf- bzw. Einsatzzentralen kommen verschiedene Technologien zum Einsatz: Telefonie, Mobilfunk- und Textmeldungssysteme, aber auch das Sicherheitsfunknetz Polycom. Integrierte Einsatzleitsysteme fassen diese zusammen und steuern sie auf einer einheitlichen Bedienungsoberfläche.

Im Ereignisfall ist es wichtig, dass die eingegangenen Informationen so schnell wie möglich die Einsatzkräfte erreichen, damit diese innerhalb weniger Minuten zum Einsatzort gelangen können. Fällt eine Zentrale aus, gewährleistet eine sogenannte dynamische Leitweglenkung, dass der Notruf in einer anderen Notrufzentrale entgegengenommen werden kann. Ist jedoch ein grösserer Standort von einem Ausfall betroffen, kann eine starke Zunahme von Anrufen zu einer Überlastung der anderen Zentralen führen. Probleme können auch auftreten, wenn Umleitungen über die Sprachgrenzen hinweg notwendig werden.

**Durch die zunehmende Digitalisierung und Zentralisierung wächst allerdings die Gefahr neuer Verwundbarkeiten.**

Das Sicherheitsfunknetz Polycom stellt die Sprachkommunikation zwischen den Partnerorganisationen und Krisenorganen sicher, auch bei einem Ausfall des öffentlichen Kommunikationsnetzes. Der Bevölkerungsschutz benötigt aber zusätzlich eine Breitbandkommunikation für den Austausch von Daten. Beispielhaft zeigt sich dies, wenn bei Hochwassergefahr Niederschlagsprognosen

**Das Sicherheitsfunknetz Polycom funktioniert auch bei einem Ausfall des öffentlichen Kommunikationsnetzes.**

oder im Falle einer radioaktiven Verstrahlung Windausbreitungsmuster berechnet und ausgetauscht werden müssen.

## Einzelne Organisationen gefährdet

Gemäss Risiko- und Verwundbarkeitsanalysen stellen Cyber-Angriffe für einzelne Zivilschutzorganisationen, Kantonspolizeikorps oder Notrufzentralen ein grosses Risiko dar. Treffen Rettungs- und Einsatzkräfte verspätet ein, kann dies bereits bei alltäglichen Ereignissen wie einem Brand oder einem Unfall grosse Sach- und sogar Personenschäden bewirken.
Hingegen ist eine gezielte Störung der Einsatzfähigkeit des gesamten Bevölkerungsschutzes durch einen Cyber-Angriff kaum möglich:

- Eine Störung kann nur dann zu einer landesweiten und/oder gravierenden Schädigung der Bevölkerung und ihrer Lebensgrundlagen führen, wenn sie zeitlich mit einer Katastrophe oder Notlage zusammenfällt.
- In vielen Kantonen bieten die einzelnen Zivilschutz- und Blaulichtorganisationen die Einsatzkräfte direkt auf, eine gleichzeitige Störung mehrerer Organisationseinheiten ist unwahrscheinlich.
- Im Zivilschutz macht die Trennung der Datenverwaltung der Schutzdienstpflichtigen (PISA) und der Aufgebotssysteme eine Zerstörung oder unbemerkte Manipulation von Daten äusserst schwierig.
- Polycom bietet eine gehärtete und organisationsübergreifende Sprachkommunikationsmöglichkeit. Zudem bestehen Eventualplanungen mit Massnahmen wie Kontaktlisten in Papierform.
- Während vieler Einsätze sind vor Ort nur wenige Betriebsmittel nötig. Bei einem Ausfall des übergeordneten Sendenetzes bleibt der Kontakt von Funkgerät zu Funkgerät möglich. Durch die zunehmende Digitalisierung und Zentralisierung wächst allerdings die Gefahr neuer Verwundbarkeiten.

## Gehärtete Systeme auf nationaler Ebene

Bund und Kantone unternehmen bereits grosse Anstrengungen, um Cyber-Risiken zu reduzieren. Aufgrund der Analysen sämtlicher kritischer Teilsektoren konnten verschiedene Handlungsfelder und Massnahmen aufgezeigt werden, die die Resilienz weiter verbessern sollen. Dazu gehören insbesondere ein Informationsaustausch zwischen Organisationen und Fachstellen, eine gemeinsame Sensibilisierung und Schulungsangebote oder auch bauliche und technische Sicherheitsmassnahmen. Angestossen wurden beispielsweise der Aufbau eines Ausweichstandorts für ein Rechenzentrum oder das Anfertigen von regelmässigen Backups von Software und Datenbeständen. Die Umsetzung der Massnahmen ist Aufgabe der jeweiligen Organisationen und Stellen.
Von übergeordneter Bedeutung ist aus SKI- bzw. NCS-Perspektive ein ausfallsicheres Datenkommunikationsnetz, wie das BABS es mit dem Sicheren Datenverbundnetz (SDVN) derzeit vertieft prüft. An das SDVN sollen Stellen von Bund und Kantonen sowie Betreiber von kritischen Infrastrukturen angeschlossen werden. Damit der Bundesrat über das weitere Vorgehen entscheiden kann, hat er das Departement für Verteidigung, Bevölkerungsschutz und Sport VBS mit einer Auslegeordnung beauftragt, die alle bevölkerungsschutzrelevanten Alarmierungs-, Informations- und Kommunikationssysteme umfasst.
Während manche Planungen und Massnahmen, beispielsweise die Aufbewahrung von Kontaktlisten auf Papier, einfach umsetzbar sind, verlangen andere grosse Investitionen. Angesichts der enormen gesellschaftlichen und volkswirtschaftlichen Schäden, die verhindert werden können, lohnen sich aber Investitionen etwa in das gehärtete Kommunikationssystem Polycom oder in ein sichereres Datenverbundnetz.

**Giorgio Ravioli**
Wissenschaftlicher Mitarbeiter Schutz kritische Informationsinfrastrukturen, BABS

*Für weitere Informationen:*
*www.infraprotection.ch*
*www.isb.admin.ch*

**Internationale Konferenz in Abu Dhabi**

# Initiative zum Schutz von Kulturgütern

**Kulturgüter, die durch bewaffnete Konflikte bedroht sind, sollen besser geschützt und auch ins sichere Ausland gebracht werden können. An einer internationalen Konferenz haben über fünfzig Staaten beschlossen, zu diesem Zweck einen neuen Fonds zu gründen. Als erster Staat mit einem Bergungsort nimmt die Schweiz dabei eine Vorreiterrolle ein.**

Auf Initiative und unter der Leitung von Abu Dhabi und Frankreich hat am 2. und 3. Dezember 2016 in Abu Dhabi die erste internationale Konferenz für die sichere Aufbewahrung von Kulturgütern aus Konfliktgebieten stattgefunden. Vertreterinnen und Vertreter von fünfzig Staaten sowie von diversen internationalen Organisationen und privaten Institutionen haben dabei die Deklaration von Abu Dhabi verabschiedet.
Darin erklären die Konferenzteilnehmenden insbesondere ihre Absicht zur Gründung eines internationalen Fonds zum Schutz von Kulturgütern, die durch bewaffnete Konflikte gefährdet sind. Damit sollen Schutzmassnahmen zur Prävention, in einer akuten Gefahrensituation, im Kampf gegen unerlaubten Handel von Kulturgütern sowie die Restaurierung von beschädigten Kulturgütern finanziert werden. Ebenfalls geplant ist der Aufbau eines internationalen Netzwerkes für Bergungsorte, in denen gefährdete Kulturgüter zeitlich beschränkt untergebracht werden können.

## Starkes Engagement der Schweiz

Auf Einladung der Organisatoren präsentierte das Bundesamt für Bevölkerungsschutz BABS in Abu Dhabi wichtige Errungenschaften des Schweizer Kulturgüterschutzes. Mit der Totalrevision des Kulturgüterschutzgesetzes (KGSG) hat die Schweiz 2015 als weltweit erster Staat die Grundlagen für die Einrichtung eines Bergungsorts zur vorübergehenden treuhänderischen Aufbewahrung von in einem anderen Staat akut gefährdeten Kulturgütern geschaffen. Seither sind die entsprechenden Umsetzungsarbeiten vorangeschritten, ein sicherer Bergungsort steht mittlerweile zur Verfügung. Aufgrund des hohen Standards des Schweizer Kulturgüterschutzes ist zudem vorgesehen, dass die Schweiz auch im Rahmen des geplanten internationalen Fonds gewisse Expertenarbeiten übernehmen wird.

**Fachkonferenz in Kreuzlingen (TG)**

# Katastrophenbewältigung an der Landesgrenze

**Mehr als 200 Bevölkerungsschützer und Fachexperten aus Deutschland und der Schweiz trafen sich am 19. Januar 2017 in Kreuzlingen TG. An einer Fachkonferenz wurde die Bewältigung einer grenzüberschreitenden Katastrophe diskutiert. Im Sommer folgt eine vom Bundesamt für Bevölkerungsschutz organisierte Übung.**

Die Partner des Bevölkerungsschutzes in den Grenzregionen Bodensee und Rhein-Schwarzwald pflegen sehr gute Kontakte untereinander. Mit einer grenzüberschreitenden Katastrophenschutz-Übung im Juni soll diese Zusammenarbeit weiter gestärkt werden. In Zusammenarbeit mit den Behörden der Grenzregion hat das Bundesamt für Bevölkerungsschutz BABS eine Übungssequenz entworfen.

Als erster Teil wurde in Kreuzlingen eine Fachkonferenz abgehalten, die für Diskussionen und Absprachen in den Bereichen Koordination von Massnahmen, Ressourcen, Kommunikation und Information genutzt wurde. Ebenso wichtig war das gegenseitige Kennenlernen der Verantwortungsträger aller beteiligter Stellen. Zusätzlich wurden Fachkenntnisse zu den Szenarien vermittelt, die im Juni trainiert werden sollen.

**Internationaler Experten-Workshop in Zürich**

# Aus der Flüchtlingskrise lernen

**In der Flüchtlingskrise von 2015 offenbarten sich in ganz Europa die Stärken und Schwächen der bestehenden Strukturen und Prozesse des Krisenmanagements. Vergangenen Herbst trafen sich in Zürich Fachleute aus Deutschland, Österreich und der Schweiz zu einem Erfahrungsaustausch.**

Die stark gestiegene Zahl von Flüchtlingen in den vergangenen Jahren stellt eine beträchtliche Herausforderung an die europäischen Staaten dar. In der Hochphase der Flüchtlingskrise im Sommer und Herbst 2015 mussten teilweise innerhalb von Tagen oder gar Stunden pragmatische Lösungen gefunden werden. Dabei offenbarten sich die Stärken und Schwächen der bestehenden Strukturen und Prozesse des Krisenmanagements.

**Nur in einzelnen Fällen wurde auf die Strukturen des Bevölkerungsschutzes zurückgegriffen, obwohl hier etablierte Abläufe zur Bewältigung von Krisensituationen vorhanden sind.**

Für den Bevölkerungsschutz stellen die Erfahrungen aus der Flüchtlingskrise eine wertvolle Chance dar, sich auf künftige Katastrophen, Krisen und Notlagen bestmöglich vorzubereiten. Notwendig ist hierfür eine umfassende, zeitnahe und kritische Auswertung der Ereignisse unter Einbeziehung der wichtigsten Akteure. Aus Sicht der Schweiz ist dabei die Zusammenarbeit mit den Nachbarländern besonders relevant, schliesslich handelt es sich beim Flüchtlingswesen um eine grenzübergreifende Herausforderung.
Um diesen Erfahrungsaustausch zwischen Deutschland, Österreich und der Schweiz voranzubringen, veranstaltete das Bundesamt für Bevölkerungsschutz BABS gemeinsam mit dem Center for Security Studies CSS der ETH Zürich Ende Oktober 2016 einen zweitägigen Experten-Workshop in Zürich. Die Veranstalter konnten dabei auf die langjährige Zusammenarbeit der Bevölkerungsschutzbehörden der Nachbarländer aufbauen, die bereits in der Vergangenheit regelmässig sogenannte D-A-CH-Workshops zu unterschiedlichen Fragestellungen im Themenbereich Bevölkerungsschutz (wie Risikoanalyse und Schutz kritischer Infrastrukturen) umfasst hatte.

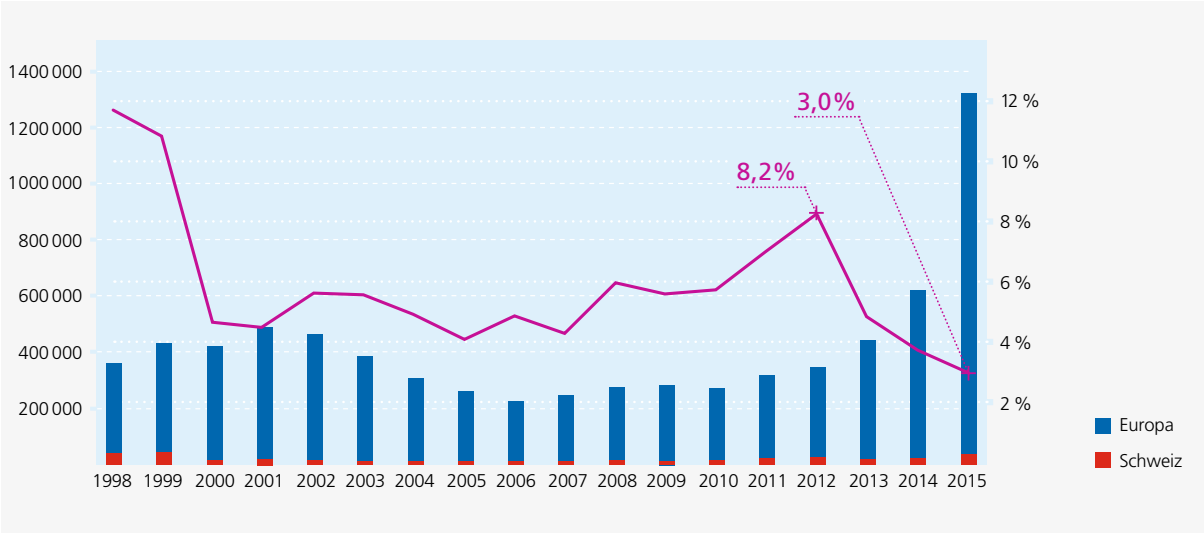

**Diskussion während des Experten-Workshops.**

## Behörden, Hilfsorganisationen und Wissenschaft

Aus Deutschland nahmen am Workshop teil: das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe BBK, das Bundesamt für Migration und Flüchtlinge BAMF, das Bundesamt für Güterverkehr BAG, die Katastrophenforschungsstelle der FU Berlin sowie die Bundesländer Bayern und Baden-Württemberg. Österreich war durch das Bundesministerium für Inneres BMI, das Bundesland Tirol sowie durch das Österreichische Rote Kreuz repräsentiert. Die Schweizer Perspektive brachten das Staatssekretariat für Migration SEM, das Bundesamt für Bevölkerungsschutz BABS, die Eidgenössische Zollverwaltung EZV, die Kantone St. Gallen, Waadt und Zürich sowie das Schweizerische Rote Kreuz in die Diskussion ein.
Zwei Ziele standen im Vordergrund: Zum einen sollten praktische Erfahrungen der letzten Monate ausgetauscht und mögliche Handlungsfelder für die Bewältigung künftiger Herausforderungen diskutiert werden. Zum anderen sollte der Workshop dazu dienen, Auswirkungen für die politisch-strategische Ebene zu identifizieren.

## Stärken und Schwächen

In der Diskussion wurde schnell deutlich, dass die Sicherstellung klarer und verlässlicher Verantwortlichkeiten und Zuständigkeiten eine der anspruchsvollsten Aufgaben im Zuge der Flüchtlingskrise darstellte. Vor allem in der Frühphase der Krise wurde die Bewältigung der stark zunehmenden Migrantenzahlen vielerorts primär als grenzpolizeiliches Problem gesehen. Als später Fragen der Unterbringung und Betreuung immer mehr drängten, wurde die Flüchtlingskrise zunehmend als Aufgabe der Sozialpolitik betrachtet.
Hingegen wurde nur in einzelnen Fällen auf die Strukturen des Bevölkerungsschutzes zurückgegriffen, obwohl hier etablierte Abläufe zur Bewältigung derartiger Krisensituationen vorhanden sind. Stattdessen wurden häufig neue operative Instrumente zur Bewältigung der Krisensi-




**Anteil der Schweiz an Asylsuchenden in Europa (Quelle Staatssekretariat für Migration SEM).**

tuation eingeführt, wodurch es zu Verzögerungen und Koordinierungsproblemen zwischen den zahlreichen involvierten Akteuren kam.
Wie die Teilnehmenden übereinstimmend berichteten, konnten trotz der schwierigen Handlungsbedingungen zumeist pragmatische und effektive Lösungen gefunden werden, um den Geflüchteten ein Mindestmass an Betreuung und Sicherheit zu gewährleisten. Entscheidend waren hierfür in den meisten Fällen enge, häufig informelle Abstimmungen zwischen den involvierten Behörden auf Bundes- und Landesebene bzw. den Kantonen sowie den Hilfsorganisationen. Wie insbesondere die Hilfsorganisationen deutlich machten, wäre es für zukünftige Katastrophen, Krisen und Notlagen jedoch dringend notwendig, geregelte Prozesse und Strukturen zu schaffen, beispielsweise für die Finanzierung von Versorgungs- und Betreuungstätigkeiten der Hilfsorganisationen.

## Langfristige Lehren

Diskutiert wurde auch, welche mittel- und langfristigen Lehren sich ziehen lassen. Es wurde deutlich, dass es sich bei der Flüchtlingsthematik keineswegs um ein abgeschlossenes Ereignis handelt. Vielmehr ist in den kommenden Jahren mit einem erneuten starken Anstieg der Migrationsbewegungen nach Europa zu rechnen. Gleichzeitig ist zu erkennen, dass die Strukturen des Krisenmanagements nach und nach wieder zurückgefahren werden. Wichtig ist deshalb, jetzt rechtzeitig Vorkehrungen zu treffen, um gegebenenfalls rasch auf Veränderungen im Handlungsumfeld reagieren zu können. Die Organisationen des Bevölkerungsschutzes sollten hierbei eine aktive Rolle spielen.

Damit zusammen hängt ein weiterer, wiederholt genannter Punkt: die Früherkennung. Aufgrund mangelnder Koordination und Kommunikation fehlte den Akteuren während der Hochphase der Flüchtlingskrise zeitweise ein klares Lagebild, wodurch sie stellenweise nur noch sehr kurzfristig auf Ereignisse reagieren konnten, anstatt proaktiv Massnahmen einleiten zu können. Um dies zu verbessern, wäre es insbesondere wichtig, die Zusammenarbeit der Akteure sowohl auf den unterschiedlichen administrativen Ebenen als auch zwischen den Nachbarländern weiter zu institutionalisieren und zu stärken, etwa durch regelmässige grenzüberschreitende Übungen.

**Florian Roth**
Senior Researcher, Risk and Resilience Research Team, Center for Security Studies CSS, ETH Zürich

## Bevölkerungsschutz in der Flüchtlingsbetreuung

Die Bewältigung grosser Flüchtlingszahlen erfordert, dass eine Vielzahl staatlicher und nichtstaatlicher Akteure zusammenwirken, etwa aus den Bereichen Gesundheitsversorgung, Sozial- und Jugendwesen, öffentliche Sicherheit und Asylwesen. Auch die Organisationen des Bevölkerungsschutzes leisten einen wichtigen Beitrag, vor allem in den Bereichen Transport und Registrierung, Aufbau von Notunterkünften, Bereitstellung von Nahrung und Kleidung sowie medizinische Versorgung und psychosoziale Betreuung.

**Übung EMMA II**

# Messgeräte und Jodtabletten für die Botschaft in Wien

**Das Bundesamt für Bevölkerungsschutz BABS und das Eidgenössische Departement für auswärtige Angelegenheiten EDA haben die rasche Versorgung einer Botschaft mit Schutzmitteln bei einem Kernkraftwerksunfall im Ausland geübt. Im Ernstfall könnte so der Schutz des Botschaftspersonals und der Schweizer Gemeinde vor Ort verbessert werden.**

Im Nachgang zum Reaktorunfall im japanischen Kernkraftwerk Fukushima Daiichi im März 2011 hat der Bundesrat 56 Massnahmen zur Optimierung der Notfallschutzmassnahmen bei Extremereignissen (NOMEX) beschlossen. Heute verfügt der Bund über Material, um Schweizer Bürgerinnen und Bürger im Ausland rasch zu unterstützen. Mit der Ende November 2016 durchgeführten Übung EMMA II (Emergency Management MAterial) wurde die ganze Prozesskette für den Versand und Einsatz des Notfallmaterials überprüft.

## Übungsszenario aus Österreich

Geübt wurde mit der Schweizer Botschaft in Wien. In die Übung involviert waren neben der Botschaft das Krisenmanagement-Zentrum KMZ des Eidgenössischen Departements für auswärtige Angelegenheiten EDA, die humanitäre Hilfe des Bundes, die in der Direktion für Entwicklung und Zusammenarbeit DEZA im EDA angesiedelt ist, die Armeeapotheke sowie vom Bundesamt für Bevölkerungsschutz BABS die Nationale Alarmzentrale NAZ, das Nationale Operations- und Koordinationszentrum und der Bereich Ressourcen.

**Das Szenario mit einem Kernkraftwerksunfall in Mittel- bzw. Osteuropa basierte auf der österreichischen Strahlenschutzübung INTREX 12 vom Oktober 2012.**

In der Vorbereitung wurde mit den österreichischen Behörden zusammengearbeitet: Das Szenario mit einem Kernkraftwerksunfall in Mittel- bzw. Osteuropa basierte auf der österreichischen Strahlenschutzübung INTREX 12 vom Oktober 2012. Damit konnte auch das Verhalten der österreichischen Behörden realistisch ins Übungsdrehbuch eingearbeitet werden.
Wie in einem Ernstfall erfuhren die Botschaft und die NAZ fast gleichzeitig aus den Medien von einem möglichen Unfall. Die NAZ kontaktiert bei Meldungen jeweils die Internationale Atomenergieagentur IAEA, gleichzeitig vernetzt sie sich mit dem Krisenmanagement-Zentrum des EDA, das bei Krisen für die Unterstützung des EDA-Personals vor Ort zuständig ist.

## Schutz- und Messmittel für die Botschaft

Gemäss Übungsszenario war rasch klar, dass es sich nicht um eine Falschmeldung handelte und eine Freisetzung von Radioaktivität nicht ausgeschlossen werden konnte. Das KMZ kontaktierte die Botschaft, worauf diese ein grobes Mengengerüst für das benötigte Material angab. In der Übung wurde mit einer Personengruppe von ca. 40 000 Schweizerinnen und Schweizer gerechnet.
Das zum Versand vorgesehene Schutzmaterial umfasst Dosimeter, Dosisleistungsmessgeräte und Jodtabletten. Dosimeter sollen von besonders exponierten Personen getragen werden und geben Auskunft über die Strahlung, die diese Personen aufnehmen. Die gemessenen Werte werden im Einsatz regelmässig der NAZ mitgeteilt und von dieser beurteilt. Die NAZ kann aufgrund der Daten präzise Empfehlungen zum Schutz der betroffenen Personen liefern. Diese Personen können somit bis zum Erreichen gewisser Dosisschwellen ihre Aufgaben wahrnehmen und dann einen geschützten Raum aufzusuchen.
Die Dosisleistungsmessgeräte werden als Sensoren verwendet, um die Strahlenbelastung in der Luft zu messen oder festzustellen, ob Oberflächen oder Gegenstände kontaminiert wurden. Die Jodtabletten schliesslich verhindern – rechtzeitig eingenommen – die Aufnahme von radioaktivem Jod, das bei Kernkraftwerksunfällen freigesetzt wird.

## Logistik für den Materialversand

In Absprache mit der NAZ und dem KMZ wurde der Versand des Materials in die Wege geleitet. Der Prozess folgt dem Standardvorgehen des Ressourcenmanagements Bund (ResMaB), das bei allen dringlichen Ressourcenbegehren im Bevölkerungsschutz zur Anwendung kommt. Die Messgeräte des BABS und die Jodtabletten der Armeeapotheke wurden zur DEZA in Wabern gebracht und mit Diplomatenkurier verschickt. Hier könnte im Ernstfall auf die Erfahrung der humanitären Hilfe des Bundes zurückgegriffen werden, um die Güter auch auf anderen Kanälen ins Ausland zu senden. Je nach Bedarf bestünde zudem die Möglichkeit, Mitglieder des Schweizerischen Korps für humanitäre Hilfe SKH für den Einsatz aufzubieten. Ein Thermome-

**Botschaftsangehörige kontrollieren den Inhalt des Materialpakets aus der Schweiz, mit dem Dosimeter, Radioaktivitätsmessgeräte und Jodtabletten nach Wien geliefert wurden.**

ter zeigte auf, welchen Temperaturunterschieden die heikle Fracht auf dem Weg nach Wien ausgesetzt war.

## Im Krisenstab in Wien

Die Botschaft in Wien bildete für die Übung einen Krisenstab, der Bürgerbegehren, Schutz des eigenen Personals, psychologische Faktoren und die Kontakte zu österreichischen und Schweizer Behörden parallel koordinieren musste. Das Paket aus der Schweiz stellte die Mitarbeitenden vor eine ungewohnte Situation: Kaum jemand war geschult in der Inbetriebsetzung und im Umgang mit Radioaktivitätsmessgeräten.

Die Botschaftsangehörigen konnten mit den Dosimetern einfach herausfinden, ob sie ihre Aufgabe weiterhin erfüllen könnten, falls die Radioaktivität erhöht wäre. Nicht definitiv festgelegt war der Einsatz der Radioaktivitätsmessgeräte. Sie können sowohl als Messsonde auf dem Botschaftsgelände verwendet werden, als auch etwa an der Eingangstür zur Kontrolle, damit keine kontaminierten Personen das Gebäude betreten.

Klar war der Einsatz der Jodtabletten: Sie waren nur für Fälle vorgesehen, bei denen über die offiziellen österreichischen Kanäle keine Tabletten erhältlich wären. Keinesfalls sollte eine Doppelspurigkeit aufgebaut werden.

## Verbesserungen

Eine erste Auswertung der Übung zeigt, dass die Logistik funktionierte und die Botschaft trotz der vielen involvierten Stellen rasch mit dem benötigten Material versorgt werden konnte. Verbesserungsbedarf besteht bei der Beratung des Botschaftspersonals und beim direkten Kontakt zwischen der NAZ und der Botschaft. So gingen aus der Übung allgemeine praktische Fragestellungen hervor: Wie wird die Verteilung der Jodtabletten innerhalb des Gastlandes sichergestellt? Welche Informationen erhalten Schweizer Staatsangehörige mit den versendeten Jod-Tabletten? Wie wird der Einnahmezeitpunkt kommuniziert? Wer erhält wie viele Tabletten? Eine Arbeitsgruppe der NAZ und des KMZ wird sich nun mit diesen Punkten befassen.

Weiter ist zu beachten, dass die Sicherstellung der logistischen Mittel nach einem realen Reaktorunfall eine zusätzliche Herausforderung darstellen könnte. Da es selten Grund für eine direkte Zusammenarbeit gibt und die Kommunikation im Alltag über das KMZ läuft, ist es umso wichtiger, im Ereignisfall rasch aufeinander zuzugehen, Informationsbedarf zu erkennen und in diesen Bereichen einfache, praxisbezogene Unterstützung anzubieten. So kann ein möglichst guter Schutz für die Botschaftsangehörigen und die Schweizer Gemeinde vor Ort sichergestellt werden.

**Christian Fuchs**
Chef Ereigniskommunikation,
Nationale Alarmzentrale NAZ, BABS

Aus dem Bundesrat

# Zugang zu Vorläuferstoffen für Explosivstoffe reglementieren

**Der Bundesrat ist sich des Risikos bewusst, dass Terroristen sich in der Schweiz mit Chemikalien zur Herstellung von Sprengstoffen eindecken können, und will den Zugang zu diesen Substanzen daher erschweren. An seiner Sitzung vom 9. Dezember 2016 hat er das Eidgenössische Justiz- und Polizeidepartement EJPD beauftragt, die erforderlichen gesetzlichen Grundlagen auszuarbeiten.**

Die jüngsten Attentate in Europa haben es gezeigt: Terroristen verwenden zur Herstellung von Sprengsätzen Substanzen, die in Produkten des täglichen Gebrauchs wie Düngemittel, Reinigungsmittel für Schwimmbäder oder Unkrautvertilgungsmittel zu finden sind. Diese Chemikalien wie etwa Wasserstoffperoxid, Aceton oder auch Nitrate sind sogenannte Vorläuferstoffe für Explosivstoffe. Während der Handel mit diesen Produkten in der Europäischen Union eingeschränkt ist, sind sie in der Schweiz im freien Verkauf erhältlich. Es besteht deshalb ein Risiko, dass sich Kriminelle solche Substanzen in der Schweiz beschaffen.

## Zusammenarbeit mit den betroffenen Branchen

Im Auftrag des Bundesrates hat sich eine von fedpol geleitete Expertengruppe mit der Frage befasst, wie der Zugang zu Vorläuferstoffen erschwert werden kann. Die betroffenen Branchen wurden von der Expertengruppe konsultiert.

Um eine solche Regelung umsetzen zu können, bedarf es eines neuen Bundesgesetzes. Der Bundesrat hat deshalb das EJPD beauftragt, eine Vernehmlassungsvorlage zu einem Gesetz auszuarbeiten und sie ihm bis Ende 2017 zu unterbreiten.

## Eine differenzierte Regelung

Die vorgeschlagene Regelung setzt beim Kauf bestimmter Vorläuferstoffe im Fachhandel an: Je höher die Konzentration der Substanzen, desto stärker soll der Verkauf geregelt werden. Die Regelungen gelten lediglich für Privatpersonen. Berufsleute wie Landwirtinnen oder Landwirte sind davon nicht betroffen. Der Bundesrat setzt auf die Eigenkontrolle und Sensibilisierung der professionellen Anwender, um allfälligem Missbrauch entgegenzutreten.

Aus dem Bundesrat

# Versorgungssicherheit betrifft viele Akteure

**Die wirtschaftliche Landesversorgung muss interdisziplinär tätig sein. Nur dann können komplexe Gefährdungen rechtzeitig identifiziert und Versorgungslücken überbrückt werden. Zu diesem Schluss kommt der «Bericht zur wirtschaftlichen Landesversorgung 2013–2016», den der Bundesrat am 2. Dezember 2016 zur Kenntnis genommen hat.**

In der Berichtsperiode von 2013 bis 2016 hat die wirtschaftliche Landesversorgung gemäss ihrem Strategieprozess die Gefährdungen der Versorgungsprozesse neu evaluiert. Weiter wurden die strategische Ausrichtung vertieft überprüft sowie ihre Instrumente und Massnahmen bezüglich Wirksamkeit und Einsatzbereitschaft analysiert. Dieser vierjährige Prozess wird mit dem Bericht zur wirtschaftlichen Landesversorgung abgeschlossen. Der Bericht liefert einen Rückblick auf die zentralen Aktivitäten, einen Überblick über den bestehenden Handlungsbedarf und einen Ausblick auf die anstehenden Herausforderungen.

Die Versorgungsprozesse stehen zunehmend schwer vorhersehbaren Gefährdungen gegenüber. Von 2013 bis 2016 musste die wirtschaftliche Landesversorgung aufgrund eines Mineralölengpasses sowie mehrerer Versorgungslücken bei Medikamenten eingreifen. In allen Fällen kamen Pflichtlagerwaren zum Einsatz. Der Engpass bei Mineralölprodukten im Herbst 2015 hat zudem gezeigt, wie ganz unterschiedliche Faktoren in ihrer Gesamtheit zu einem Versorgungsproblem führen können.

**Bericht zum Hitzesommer 2015**

# Gut bewältigt, Potenzial für Verbesserungen erkannt

**Die Schweiz erlebte im Sommer 2015 zum zweiten Mal nach 2003 eine markante Hitzeperiode und eine ausgeprägte Trockenheit. Der Juli war in einigen Landesteilen der heisseste je gemessene Monat. Besonders stark betroffen waren Menschen in den Städten. Der nun veröffentlichte Bericht des Bundes «Sommer 2015: Hitze, Trockenheit und Auswirkungen auf Mensch und Umwelt» analysiert diese Ereignisse, zeigt Auswirkungen auf und zieht Lehren für die Zukunft.**

Die Trockenheit im Sommer 2015 konnte dank der seit 2003 ergriffenen Massnahmen insgesamt besser bewältigt werden als in dieser letzten grossen Hitzeperiode. Starke Auswirkungen hatte die Hitzewelle aber auf die Gesundheit. So waren im Sommer 800 Todesfälle mehr zu beklagen als in einem normalen Jahr. Die Sterblichkeit in den Sommermonaten 2015 liegt damit in etwa auf dem Niveau des Hitzesommers 2003.
Es gab aber auch Erfolge beim Umgang mit der Sommerhitze. So konnte in der Genferseeregion, wo nach 2003 Hitzepläne erstellt wurden, dank spezieller Betreuung gefährdeter Personen die Hitzesterblichkeit gegenüber 2003 deutlich gesenkt werden. Aufgrund des Klimawandels ist davon auszugehen, dass es in Zukunft mehr Hitzewellen geben wird. Umso wichtiger ist es, die Massnahmen der Kantone und Gemeinden genau zu analysieren und von den erfolgreichen Massnahmen zu lernen. Dazu gehören zum Beispiel das Informieren von Risikogruppen (z. B. ältere Personen) sowie des Betreuungspersonals über richtiges Verhalten bei Hitzewellen wie zum Beispiel ausreichendes Trinken oder das Vermeiden körperlicher Anstrengungen. Weiter soll es eine einheitliche Hitzewarnung für die Schweiz geben. Die zum Teil sehr unterschiedlichen Massnahmen gegen Hitze sollen zudem koordiniert und Hitzepläne in den Kantonen mit hohem Risiko auch wirklich umgesetzt werden.

## Backofeneffekt in den Städten

Unter Sommerhitze leidet vor allem die Bevölkerung in den Städten und Agglomerationen. Städte mit ihren versiegelten Böden speichern die Wärme und verstärken dadurch die Hitze. In der Nacht kühlt es zudem kaum ab. Als Massnahme gegen diese zunehmenden Hitzeinseln braucht es genügend Grünflächen und Schattenplätze. Zudem muss in belasteten Gebieten die Zufuhr und Zirkulation von Frischluft aus dem Umland gewährleistet oder verbessert werden – trotz des Anliegens des verdichteten Bauens in Städten. Bund, Kantone und Städte arbeiten momentan an einer Ideensammlung über die klimaangepasste Stadtentwicklung.
Die Auswirkungen von Hitze und Trockenheit auf Pflanzen und Tiere können erst in einigen Jahren beurteilt werden. Je nach Witterung in den kommenden Jahren wird die Natur das Extremjahr 2015 mehr oder weniger ausgleichen können. Um die Trinkwasserversorgung überall auch in Trockenperioden zu gewährleisten, empfiehlt der Bund eine entsprechende Nutzungsplanung, die Vernetzung der Wasserversorgungen sowie je mindestens zwei unabhängige Bezugsquellen.


## Klimaschutz statt Symptombekämpfung

Alle Anpassungsmassnahmen dienen letztlich nur der Symptombekämpfung. Der wichtigste Hebel im Kampf gegen die Zunahme von Hitze und Trockenheit ist und bleibt die Reduktion des Treibhausgasausstosses. Nur wenn es gelingt, den Klimawandel zu begrenzen, sind Anpassungsmassnahmen möglich und bezahlbar.

*Der Bericht ist zugänglich unter:*
*www.bafu.admin.ch/uz-1629-d*

**TWK 2017**

# Neue technische Weisungen für Schutzbauten

**Anfang Jahr sind die neuen technischen Weisungen für die Konstruktion und Bemessung von Schutzbauten des Bevölkerungsschutzes (TWK 2017) in Kraft getreten. Bereits begonnene Projekte können noch nach den alten Vorgaben realisiert werden.**

Die Schutzbauten müssen einen Basisschutz gegen die Wirkungen moderner Waffen aufweisen. Grundsätzlich hat sich daran nichts geändert. Das Bundesamt für Bevölkerungsschutz hat aber die technischen Weisungen für die Planung und Bemessung von Schutzbauten dem heutigen Kenntnisstand, den aktuellen Normen und den geltenden technischen Vorschriften angepasst. Eine Überarbeitung der bisher geltenden technischen Weisungen (TWK 1994) wurde insbesondere aufgrund der Einführung neuer SIA-Normen erforderlich. Seit 1994 werden Schutzbauten einheitlich gemäss den TWK 1994 erstellt. Die Weisungen basieren zwar auf einem eigenständigen Bemessungskonzept, berücksichtigen jedoch die Normen des SIA.
Die TWK 2017 sind massgebend für die Planung der Schutzbauten, beispielsweise beziffern sie die maximale Höhe der sich über den Schutzräumen befindenden Gebäude oder führen die Massnahmen auf, die bei der Überprüfung der Erdbebensicherheit von Gebäuden zusätzlich zu treffen sind. Strenger geworden sind hauptsächlich die Anforderungen an den Nachweis der Schubtragfähigkeit.
Die vor dem 1. Juli 2017 begonnenen Projekte können noch gemäss den TWK 1994 geplant und realisiert werden.

**Sirenentest 2017**

# 99 Prozent funktionierten einwandfrei

**Beim Sirenentest vom 1. Februar 2017 funktionierten 99 Prozent der Sirenen einwandfrei. Entdeckte Mängel werden nun behoben. Die Alarmierung der Bevölkerung bei einer Katastrophe bleibt damit sichergestellt.**

In der Schweiz gibt es zum Schutz der Bevölkerung rund 7200 Sirenen für den Allgemeinen Alarm; davon sind ca. 5000 Sirenen stationär und ca. 2200 Sirenen mobil eingesetzt. Von den stationären Sirenen werden ca. 600 als Kombisirenen gleichzeitig für den Allgemeinen Alarm und den Wasseralarm eingesetzt. Dank dem neuen Steuerungssystem Polyalert konnten die Ergebnisse des Sirenentests noch gleichentags erhoben werden.
Die Auswertung des Bundesamtes für Bevölkerungsschutz BABS zeigt, dass 99 Prozent der getesteten stationären Sirenen einwandfrei funktioniert haben. Bei insgesamt 61 Sirenen wurden Fehler festgestellt. Dieses Ergebnis liegt im Bereich der Vorjahresergebnisse.
Die Kantone und Gemeinden sind nun gehalten, die defekten Anlagen umgehend zu reparieren bzw. zu ersetzen. Da die Sirenen jedes Jahr getestet und festgestellte Mängel im Anschluss behoben werden, kann die Funktionssicherheit auf sehr hohem Niveau gehalten werden.

**Swisstopo-Vitrine im BABS**

# Ausgezeichnetes Geoportal

In den letzten Jahren hat map.geo.admin.ch, das Geoportal des Bundes, diverse Preise erhalten. Die Daten des Kulturgüterschutzinventars (KGS Inventar 2009) sind Bestandteil der nationalen Geodaten; unter dem Titel «SwissGuesser» steht auch ein Ratespiel zur Verfügung, bei dem die Standorte von Kulturgütern in der Schweiz herausgefunden werden können.
Seit geraumer Zeit ist eine mobile Vitrine mit den Preisen von geo.admin.ch als Exponat und «Dankeschön» unterwegs bei den beteiligten Bundesämtern. Die Wanderausstellung von swisstopo macht vom 1. bis 28. April 2017 Halt im Bundesamt für Bevölkerungsschutz BABS.

*Weiterführende Informationen zur Wanderausstellung und den Auszeichnungen finden sich auf: www.geo.admin.ch/awards*

**SRF1 Thementag «Blackout»**

# Das BABS vor und hinter der Kamera

Gleich zu Jahresbeginn bot das Deutschschweizer Fernsehen SRF1 den Zuschauerinnen und Zuschauern ein aussergewöhnliches Fernseherlebnis: Im Rahmen einer neunstündigen Sondersendung am 2. Januar 2017 wurde die Gefährdung unseres privaten und öffentlichen Lebens durch einen grossen Stromausfall bzw. eine langandauernde Strom-Mangellage dargestellt. Das Ziel bestand darin, die Bevölkerung dafür zu sensibilisieren, wie wichtig eine funktionierende Stromversorgung für unsere stark vernetzte Gesellschaft ist – gerade unter dem Aspekt der Sicherheit.

Das Bundesamt für Bevölkerungsschutz BABS hat das SRF-Produktionsteam bei der Planung, Vorbereitung und Realisierung des Thementags stark unterstützt: Vom BABS erarbeitete Gefährdungsanalysen waren Grundlage für den Dokumentarfilm mit fiktivem Szenario, in dem die Auswirkungen eines grossen Blackouts eindrücklich dargestellt wurden. Ein Filmteam konnte Aufnahmen in der Nationalen Alarmzentrale des BABS realisieren. BABS-Fachpersonen haben das Redaktionsteam beratend begleitet und Kontakte zu anderen Fachleuten vermittelt. In der Sendung selber standen der Direktor BABS, Benno Bühlmann, sowie der Chef Risikogrundlagen und Forschungskoordination, Stefan Brem, dem Moderator Urs Gredig Rede und Antwort.

## Fragen der Zuschauerinnen und Zuschauer

Ein spezieller Einsatz des BABS erfolgte hinter der Kamera: 15 Expertinnen und Experten des BABS beantworteten während der gesamten Dauer der Thementag-Sendung an einer Telefon-Infoline und in einem Online-Chat Fragen der Zuschauerinnen und Zuschauer. Dabei wurde deutlich, wie stark das Thema die Bevölkerung beschäftigt. Zu keiner anderen Fernsehsendung hat SRF bisher so viele Fragen beantwortet. Inhaltlich waren die Fragen und Bemerkungen fast ausnahmslos sachlich und konstruktiv – viele Zuschauerinnen und Zuschauer haben sich explizit für die wichtigen und guten Informationen bedankt. Sowohl für das SRF-Team als auch für das BABS hat sich der grosse Aufwand damit vollumfänglich gelohnt.


**Zusammenarbeit von Zivilschutz Basel-Stadt und Industrielle Werke Basel IWB**

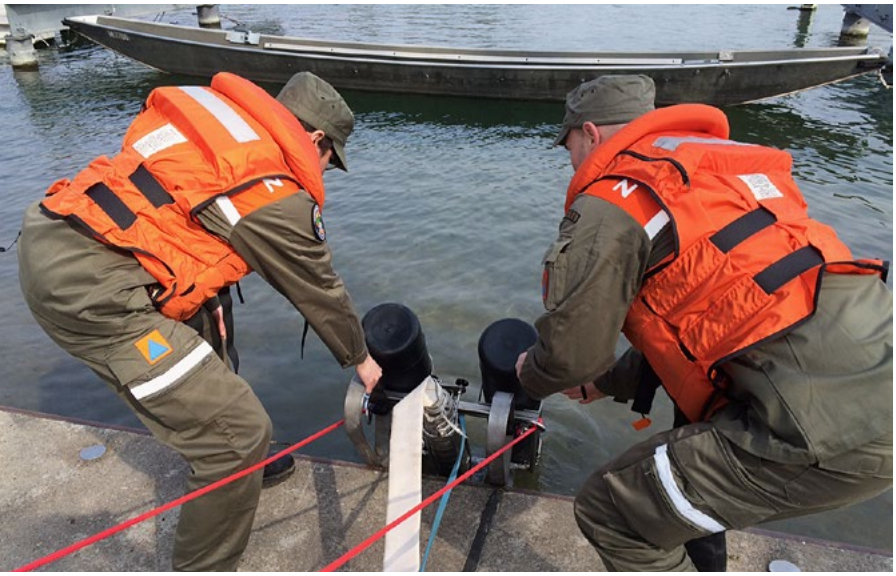
# Mit mobilen Trinkwasser-aufbereitungsanlagen

**Für eine Notlage verfügt der Kanton Basel-Stadt über mobile Trinkwasseraufbereitungsanlagen. Damit können die Industriellen Werke Basel IWB und der Zivilschutz Basel-Stadt innert weniger Stunden bis zu 160000 Personen mit dem nötigen Trinkwasser versorgen.**

In der Schweiz haben die Kantone die Versorgung der Bevölkerung mit Trinkwasser sicherzustellen. Im Hinblick auf eine Notlage definiert die Verordnung über die Sicherstellung der Trinkwasserversorgung in Notlagen (VTN) die Rahmenbedingungen und die Menge an Trinkwasser, die verfügbar sein muss. Von einer Notlage wird gesprochen, wenn die normale Versorgung mit Trinkwasser durch ein Naturereignis, einen Störfall, eine Sabotage oder kriegerische Handlungen erheblich gefährdet, eingeschränkt oder verunmöglicht ist. Die Verordnung legt fest, dass die normale Trinkwasserversorgung so lange wie möglich aufrechterhalten bleiben, auftretende Störungen so schnell wie möglich behoben und die zum Überleben notwendige Trinkwassermenge jederzeit verfügbar sein müssen:

- bis zum 3. Tag: so viel Wasser wie möglich,
- ab dem 4. Tag: 4 Liter pro Person und Tag (Nutztiere: 60 Liter pro Grossvieheinheit und Tag),
- ab dem 6. Tag: 15 Liter pro Person und Tag (Spital/Pflegeheim: 100 Liter pro Person und Tag; Betriebe, die lebenswichtige Güter herstellen: so viel wie nötig).

Für den Kanton Basel-Stadt beträgt die zum Überleben notwendige Menge rund 800000 Liter Trinkwasser pro Tag. Zum Vergleich: Der normale Tagesverbrauch liegt bei 70 Millionen Litern und kann in den Sommermonaten auf das Doppelte anwachsen.



**Der Zivilschutz Basel-Stadt unterhält einen eigenen «Trinkwasserzug», der innert Stunden aufgeboten werden kann.**

## Kantonale Krisenorganisation führt

Um die Vorgaben zur Trinkwasserversorgung in Notlagen umzusetzen, erstellen die Kantone Notwasserkonzepte, die an ihre spezifischen Rahmenbedingungen angepasst sind. Der Schweizerische Verein des Gas- und Wasserfaches SVGW hat als praktisches Hilfsmittel die Wegleitung für die Planung und Realisierung der Trinkwasserversorgung in Notlagen (TWN) erarbeitet. Diese Wegleitung dient auch als Grundlage für das Basler Konzept, das die Zuständigkeiten und Verantwortlichkeiten in einer Notlage definiert.

Nicht nur im Alltag sind die IWB, die Industriellen Werke Basel, für die Trinkwasserversorgung im Kanton Basel-Stadt zuständig – auch bei einer eingeschränkten Netzversorgung bleiben die IWB Wasserversorger und der Betrieb wird möglichst lange aufrechterhalten. Das Ziel ist dann die schnellstmögliche Wiederherstellung der normalen Netzversorgung. Bei einem Ausfall der normalen Wasserversorgung (unterbrochene Netzversorgung) übernimmt die Kantonale Krisenorganisation (KKO) die Führung. Sie entscheidet über die Einrichtung der Notwasserversorgung.

Das Notwasserkonzept dient der KKO als wichtige Entscheidungshilfe und fasst die möglichen Massnahmen in einer Matrix zusammen: Abhängig von der Anzahl der betroffenen Personen, den örtlichen Begebenheiten, dem zeitlichen Umfang und der Dringlichkeit werden unterschiedliche Massnahmen vorgeschlagen. Die Verteilung von Flaschenwasser, die Versorgung mit Zisternenwagen und die Einspeisung von Trinkwasser aus dem Versorgungsnetz der Nachbargemeinden gehören ebenso dazu wie die Nutzung der vorhandenen Grundwasserbrunnen (Notbrunnen) und, damit verbunden, die Aufbereitung des Wassers durch mobile Trinkwasseraufbereitungsanlagen.

## Notwasserkonzept setzt auf mobile Aufbereitungsanlagen

Basel hat sich für die Beschaffung mobiler Aufbereitungsanlagen entschieden, da es bei einem Ausfall der Trinkwasserversorgung zu Versorgungslücken kommen kann, die nur schwer mit anderen Massnahmen abzudecken


**Eine mobile Aufbereitungsanlage produziert Trinkwasser für bis zu 40 000 Personen.**

sind. Die vier mobilen Aufbereitungsanlagen, mit denen je bis zu 40 000 Personen versorgt werden können, bieten gleich mehrere Vorteile: Dank der im Stadtgebiet verfügbaren Notbrunnen kann die Bevölkerung dezentral mit Trinkwasser versorgt werden. Bei einer Verschmutzung der Notbrunnen können die mobilen Anlagen auf alternative Standorte und auf Oberflächenwasser ausweichen. Zudem lässt sich mit den mobilen Anlagen in grosser Menge Brauchwasser aufbereiten, mit dem ausgefallene Wasserversorgungsanlagen gereinigt werden können.
Der Nachteil von mobilen Aufbereitungsanlagen ist, dass die Bevölkerung das zum Überleben notwendige Trinkwasser selbst abholen muss. Die mobilen Anlagen kommen allerdings erst zum Einsatz, wenn andere Massnahmen nicht mehr greifen, womit der Vorteil dieses flexiblen Mittels für den Notfall sicher überwiegt.

## Trinkwasserzug Zivilschutz Basel-Stadt

Mobile Aufbereitungsanlagen haben in Basel Tradition. Dies ist unter anderem darauf zurückzuführen, dass die Trinkwasserversorgung im Kanton Basel-Stadt zu einem hohen Prozentsatz mit Rheinwasser erfolgt. Fällt der Rhein für längere Zeit (Monate) als Rohwasserquelle aus, ist die Trinkwasserversorgung im Kanton Basel-Stadt eingeschränkt. Dank der mobilen Aufbereitungsanlagen kann in einem solchen Fall auf alternative Rohwasserquellen wie die Basler Notbrunnen (Grundwasser) ausgewichen werden.
Der Zivilschutz Basel-Stadt spielt im Notwasserkonzept eine wichtige Rolle: Er unterhält einen eigenen «Trinkwasserzug», der innert Stunden aufgeboten werden kann. Die Ausbildung sowie den Einsatz der Anlagen stellt der Zivilschutz selbst sicher, IWB-Mitarbeitende unterstützen ihn fachlich. Ohne diese Zusammenarbeit wäre der Einsatz der mobilen Aufbereitungsanlagen wohl nicht möglich. Bei einem Ausfall der Wasserversorgung sind die IWB-Mitarbeitenden primär mit der Instandsetzung der Wasserversorgungsanlagen beschäftigt und können nicht gleichzeitig die mobilen Aufbereitungsanlagen betreiben.

## «Blackout»

Wie gut das «Ersteinsatzteam Trinkwasser Zivilschutz Basel-Stadt» funktioniert und mit den IWB zusammenarbeitet, konnte das Schweizer Radio und Fernsehen (SRF) im letzten Jahr mit der Kamera verfolgen. Mit dem in Basel gedrehten Beitrag zeigte SRF zum Thementag «Blackout» vom 2. Januar 2017 auf, was ein längerer Stromausfall in der Schweiz für die Wasserversorgung bedeutet. Im Vorfeld und bei den Dreharbeiten selbst wurde allen Beteiligten vor Augen geführt, dass ein «Blackout» von mehreren Tagen nicht nur jederzeit möglich ist, sondern mit einschneidenden Auswirkungen auf die Wasserversorgung einhergeht. Das Basler Notwasserkonzept bildet die Grundlage dafür, eine solche Notlage im Kanton zu bewältigen.

**Das Schweizer Fernsehen filmt, wie eine Zisterne (grüner Lastwagen im Hintergrund) mit Trinkwasser gefüllt wird.**

**Franz Näf**
Teamleiter Ausbildung/Einsatz,
Militär und Zivilschutz Basel-Stadt

Kanton Aargau

# Erneuerung des geschützten Führungsstandortes

**Der Kanton Aargau ist daran, den geschützten Führungsstandort des Regierungsrates und des Kantonalen Führungsstabes zu sanieren. Im ersten Quartal 2018 soll die modernisierte und ausgebaute Anlage zur Verfügung stehen.**

**Mit dem Spatenstich vom 8. Dezember 2016 leitete der Kanton Aargau die Sanierung des geschützten Führungsstandortes des Regierungsrates und des Kantonalen Führungsstabes feierlich ein.**

Die Abklärungen zur künftigen Nutzung des geschützten Führungsstandortes des Kantonalen Führungsstabes (KFS) starteten 2014. Die Gefährdungsanalyse Aargau zeigte dabei deutlich auf, dass der KFS bei Szenarien wie einem grossflächigen Stromausfall, einem Erdbeben oder einem KKW-Störfall auf einen geschützten Standort und zudem auf funktionierende Kommunikationsmittel angewiesen ist.

## In die Jahre gekommen

Aufgrund des Alters der Schutzanlage (Baujahr 1978) besteht ein grosser Erneuerungsbedarf, da verschiedene notwendige bauliche und technische Massnahmen vor den Abklärungen zurückgestellt worden waren. Damit der KFS jederzeit führen kann, müssen die in die Jahre gekommenen Systeme und Einrichtungen sowie die Notstromversorgung auf den neuesten technischen Stand gebracht werden.
Nachdem die zuständige Vorsteherin des Departements Gesundheit und Soziales der Weiterverwendung und somit der Sanierung der Schutzanlage zugestimmt hatte, konnten die ersten Abklärungen mit dem Bundesamt für Bevölkerungsschutz BABS getroffen werden. In einem nächsten Schritt galt es, den Zustand zu erfassen und die Sanierungsmassnahmen festzulegen. Während der Projektausarbeitung wurde entschieden, dass im Führungsstandort auch der Notstandort der Kantonalen Notrufzentrale der Kantonspolizei Aargau integriert werden soll. Eine ganze Reihe von Massnahmen müssen nun umgesetzt werden:

- Sanierung der Gebäudehülle,
- Ersatz der Telefonzentrale,
- Aufwertung der Informatik- und Telematikeinrichtungen,
- räumliche Anpassungen an die Bedürfnisse des KFS,
- Einrichtung eines Notstandortes für die Kantonale Notrufzentrale,
- Einrichtung einer redundanten Auslösestelle der Sirenen (Fernsteuerung Polyalert),
- energietechnische Optimierungen aufgrund der vermehrten Nutzung für Rapporte und Übungen,
- Aufwertung der Versorgungsräume (Küche) gemäss Lebensmittelvorschriften,
- Verstärkung der Notstromversorgung.

## Verpflichtungskredit von 3,9 Mio. Franken

Auf Antrag des Regierungsrates stimmte der Grosse Rat des Kantons Aargau am 22. November 2016 dem Brutto-Verpflichtungskredit von rund 3,9 Mio. Franken für die Realisierung des Sanierungsprojektes zu. Das BABS leistet an die Sanierungsarbeiten einen Beitrag in der Höhe von 2,1 Mio. Franken, die Kantonspolizei einen Beitrag von 130 000 Franken.
Bereits am 8. Dezember 2016 konnte der Bau offiziell starten – im Beisein von Vertreterinnen und Vertretern des BABS, der Standortgemeinde Gränichen, der Landwirtschaftlichen Schule Liebegg in Gränichen, den Planern sowie des Kantons Aargau und des KFS Aargau. Im gleichen Monat wurde als weiterer Schritt das Baugesuch für eine Polycom- und GSM-Antenne sowie für das neue Zu- und Abluftbauwerk der Gemeinde zur Prüfung und Beschlussfassung eingereicht. Die Terminplanung sieht vor, dass die Sanierungsarbeiten noch in diesem Jahr abgeschlossen werden und die Anlage im ersten Quartal 2018 dem KFS übergeben wird.

**Bevölkerungsschutz im Kanton Bern**

# Gefahrenanalyse 2015 abgeschlossen

**Unter dem Projekttitel «Gefahrenanalyse 2015» hat der Kanton Bern für seine 352 Gemeinden eine systematische Risikoanalyse durchgeführt. Um Lücken in kommunalen Notfallplanungen zu schliessen, wurde ein Leitfaden entwickelt.**

Der Kanton Bern führt seit 1995 auf kommunaler Ebene Gefahrenanalysen (andernorts Gefährdungsanalysen genannt) durch. Die kantonale Gesetzgebung verpflichtet die Gemeinden, periodisch ihre spezifische Gefährdungssituation zu ermitteln.
Mit der Gefahrenanalyse 2015 hat das Amt für Bevölkerungsschutz, Sport und Militär BSM zusammen mit den kantonalen Fachstellen und -spezialisten für alle Berner Gemeinden 20 Gefährdungen beurteilt. Nun verfügen die Gemeinden über eine Gefahrenanalyse nach heutigen methodischen Standards. Im Gegensatz zu früheren Analysen kann sowohl zwischen den Gemeinden als auch zwischen unterschiedlichen Gefährdungen verglichen werden. Zudem lässt sich jede Bewertung auf klare Kriterien zurückführen.
Die Resultate der Gefahrenanalyse 2015 sollen im Geoportal des Kantons Bern aufgeschaltet und somit als Kartenanwendung der Öffentlichkeit zugänglich gemacht werden. Damit gibt das BSM nicht nur den offiziellen Abschluss des Projekts bekannt, sondern stärkt auch das Risikobewusstsein der Bevölkerung.

## Online-Leitfaden «Notfallplanung»

Die Gefahrenanalyse dient den zivilen Führungsorganen auf Stufe Gemeinde und Verwaltungskreis bei den Planungen im Hinblick auf die relevanten Risiken. Zur Unterstützung hat das BSM einen «Leitfaden Notfallplanung» entwickelt, der bei der Gefahrenanalyse und der damit verbundenen Risikobewertung ansetzt und hilft, anhand von einfachen Fragen Planungsdefizite zu eruieren und Lücken in der kommunalen Notfallplanung zu schliessen. Zu jeder erfassten Gefährdung liegen weitere Informationen, Mustervorlagen oder Behelfe vor, die in Zukunft ergänzt werden sollen.

*Weitere Informationen: www.be.ch/geoportal*

**Die Berner Gemeinden verfügen über eine Gefahrenanalyse nach heutigen methodischen Standards.**

**Kooperation zwischen Glarus und Graubünden**

# Gemeinsame Zivilschutzausbildung

**Die Angehörigen des Glarner Zivilschutzes werden künftig gemeinsam mit ihren Bündner Kameraden in Chur ausgebildet. Die beiden Kantone haben eine entsprechende Absichtserklärung unterzeichnet.**

Als Bergkantone haben Graubünden und Glarus ähnliche Bedürfnisse im Zivilschutz. Entsprechend gab es bereits viele Überschneidungen und Synergien, was die Ausrichtung der Zivilschutzorganisationen beider Kantone betrifft. Beispielsweise basiert der derzeitige Aufbau der Seuchenwehrpioniere im Kanton Glarus auf dem Bündner Konzept und erfolgt in enger Zusammenarbeit.
Die Kooperation ist eine grosse Chance, um die Zivilschutzorganisationen der beiden Kantone gemeinsam weiterzuentwickeln und den Standort Meiersboden in Chur als Ausbildungsort für den Zivilschutz zu stärken. Zudem erwarten die Kantone Kosteneinsparungen. Für die Glarner Schutzdienstpflichtigen, die bislang in Schwyz, Cham und Sempach ausgebildet wurden, verkürzt sich die Reisezeit und lässt sich die Ausbildung flexibler planen.

**Zufriedene Gesichter: vorne die Regierungsräte Christian Rathgeb (GR, links) und Andrea Bettiga (GL), hinten (von links) Martin Bühler, Leiter Amt für Militär und Zivilschutz Graubünden, Daniel Spadin, Departementssekretär (GR), und Andrea Bottoni, Hauptabteilungsleiter Militär und Zivilschutz Glarus.**

**Waldbrände im Kanton Graubünden**

# Grosseinsatz gegen Flammen und Glut

**Vom 27. Dezember 2016 bis am 12. Januar 2017 bekämpften täglich bis zu 100 Einsatzkräfte mit Unterstützung von militärischen und zivilen Löschhelikoptern die Waldbrände im Misox und im Calancatal (GR). Die Zusammenarbeit zwischen den betroffenen Gemeinden und den beteiligten Partnern Kantonspolizei, Feuerwehr, Forstdienst, Sanität, Zivilschutz und Schweizer Armee erfolgte sehr kooperativ und war von gegenseitigem Vertrauen geprägt.**

Am 27. und 28. Dezember 2016 brachen aufgrund der seit Mitte November anhaltenden Trockenheit zuerst zwischen Mesocco und Soazza im Misox und anderntags in Braggio im Calancatal Waldbrände aus. In Mesocco mussten vier Personen aus zwei Wohnhäusern evakuiert werden, ein drittes Gebäude war wegen Steinschlaggefahr nicht mehr zugänglich. Die Autostrasse A13 und die Kantonsstrasse H13 waren zeitweise wegen Steinschlaggefahr gesperrt. In Braggio näherte sich das Feuer den Wohnhäusern bis auf fünfzig Meter. Die Brände beschädigten insgesamt weit über hundert Hektaren Schutzwald. Glücklicherweise kamen keine Menschen zu Schaden und auch die Hochspannungsleitung Sils–Soazza, eine wichtige europäische Linie für den Stromtransport, blieb dank raschem Eingreifen unversehrt.
Feuerwehr und Löschhelikopter konnten die offenen Brände innert kurzer Zeit fast vollständig löschen. Während der darauffolgenden Tage galt es, in mühseliger Kleinarbeit im nur sehr schwierig zugänglichen Gelände die unzähligen Glutnester aufzuspüren und zu löschen, um das Wiederaufflammen der Brände zu verhindern.

## Mit vereinten Kräften

Im Verlauf des Einsatzes leisteten Angehörige der Schweizer Armee, der Bündner Kantonspolizei, der Feuerwehren aus ganz Graubünden, des Forstdienstes, des regionalen Rettungsdienstes, der technischen Betriebe der Gemeinden und des Kantons sowie des Zivilschutzes in enger Kooperation insgesamt weit über 1000 Diensttage zur Rettung der betroffenen Schutzwälder.
Anhand der Phase der Glutnester-Bekämpfung lässt sich eindrücklich das Zusammenspiel der beteiligten Akteure aufzeichnen. Gestützt auf die Resultate der Wärmebildkameras des von der Armee zur Verfügung gestellten Aufklärungszuges und des FLIR-Helikopters, bearbeiteten die örtlichen Förster gemeinsam mit den Feuerwehrleuten und den Angehörigen des Zivilschutzes Quadratmeter um Quadratmeter verbrannten Waldbodens. Die Löschhelikopter der Armee wässerten derweil grossräumig die Flanken der Schutzwälder und die zivilen Helikopter flogen nebst punktuellen Löscheinsätzen vor allem Mannschafts- und Materialtransporte. Zusätzlich zur Unterstützung der Löscharbeiten kümmerten sich die Angehörigen des Zivilschutzes um die Verpflegung der Einsatzkräfte und um den Betrieb der Unterkunft. Soldaten, Zivilschützer und Feuerwehrleute teilten sich kameradschaftlich die Zivilschutzanlage der Gemeinde Soazza.

## Regionale Einsatzverantwortung – kantonale Koordination

Die Leitung blieb für die gesamte Dauer des Einsatzes in der Hand der regionalen Führungskräfte. Während der ersten etwa 48 Stunden führte der Chef der Regionenpolizei Mesolcina den Einsatz. Nachdem die Verkehrsachsen wieder durchgehend geöffnet und die Hochspannungsleitungen in Betrieb genommen werden konnten, übergab er die Einsatzleitung an den heimischen Feuerwehrinspektor.
Für die Schwergewichtsbildung bei den Löscheinsätzen zeichnete sowohl im Misox als auch im Calancatal ab Beginn der Löscheinsätze der jeweils zuständige Regionalforstingenieur mitverantwortlich. Die für Feuerwehr sowie Militär und Zivilschutz verantwortlichen Mitglieder des Kantonalen Führungsstabs waren vor Ort und standen der Einsatzleitung beratend und unterstützend zur Seite. Sie stellten die Anträge um Unterstützung durch die Armee und sorgten für die Nachführung zusätzlicher Einsatzkräfte und -mittel der Feuerwehren und des Zivilschutzes aus Nordbünden.

## Erste Erkenntnisse und Konsequenzen

Der erfolgreich abgeschlossene Einsatz zum Jahresübergang 2016/2017 zeigt, dass die Zusammenarbeit zwischen Blaulichtorganisationen, Forstdienst, Zivilschutz und Armee in Graubünden gut funktioniert und sich bewährt. Die Beteiligten werden den Einsatz während der kommenden Monate detailliert auswerten, um die Lehren daraus zu ziehen und die Fähigkeit zur Bewältigung von Ereignissen weiter zu verbessern. Erste Erkenntnisse und Konsequenzen lassen sich aber bereits festhalten:

– Die ersten Reaktionen und Massnahmen der lokalen und regionalen Einsatzelemente der Polizei, Feuerwehr und Rettungsdienste sowie der Regionalforstingenieure und örtlichen Förster waren für den weiteren Verlauf der Ereignisbewältigung von entscheidender Bedeutung. Es gilt, diese Akteure in Bezug auf solche Grossereignisse weiter auszubilden. Die Verantwortlichen der Regionen müssen kantonsweit in der Lage sein, selbständig und zeitgerecht die ersten Massnahmen zu treffen und rasch die notwendige Führungsinfrastruktur bereitzustellen.

**Die Pioniere der Zivilschutz-Kompanie Surselva bekämpfen oberhalb des Dorfes Mesocco im steilen Gelände die Glutnester**


**Anhand der von der Armee gelieferten Information erstellt der Regionalforstingenieur Karten für die Einsatzkräfte von Feuerwehr und Zivilschutz.**

**Die Feuerwehr Calanca verhindert dank intensivem Einsatz während der Nacht das Übergreifen des Feuers auf das Dorf Braggio. Etwa 12 Hektaren Schutzwald werden beschädigt.**

**Ohne die Unterstützung der Löschhelikopter der Armee wären die Schutzwälder von Soazza und Messoco zerstört worden. Die Luftwaffe wirft im Verlauf der Einsätze gegen die Waldbrände insgesamt über 2400 Tonnen Wasser ab.**

– Der Bündner Zivilschutz konnte beweisen, dass er zeitnah und polyvalent die Einsatzkräfte der Feuerwehr und des Forstdienstes zu unterstützen vermag. Er stellte die Durchhaltefähigkeit sicher. Die Möglichkeiten zur raschen und einsatzbezogenen Mobilisierung müssen weiterentwickelt und optimiert werden.
– Ohne den Einsatz der Löschhelikopter der Armee hätten die Schutzwälder von Soazza und Mesocco nicht geschützt werden können. Die Schweizer Armee leistete den grössten Löscheinsatz seit 20 Jahren. Sie präsentierte sich dabei als unkomplizierter, verlässlicher und unverzichtbarer Partner. Der guten Zusammenarbeit mit der Armee, nicht nur im Ereignisfall, ist gerade in Graubünden ein hoher Stellenwert beizumessen.

**Martin Bühler**
Chef Kantonaler Führungsstab Graubünden

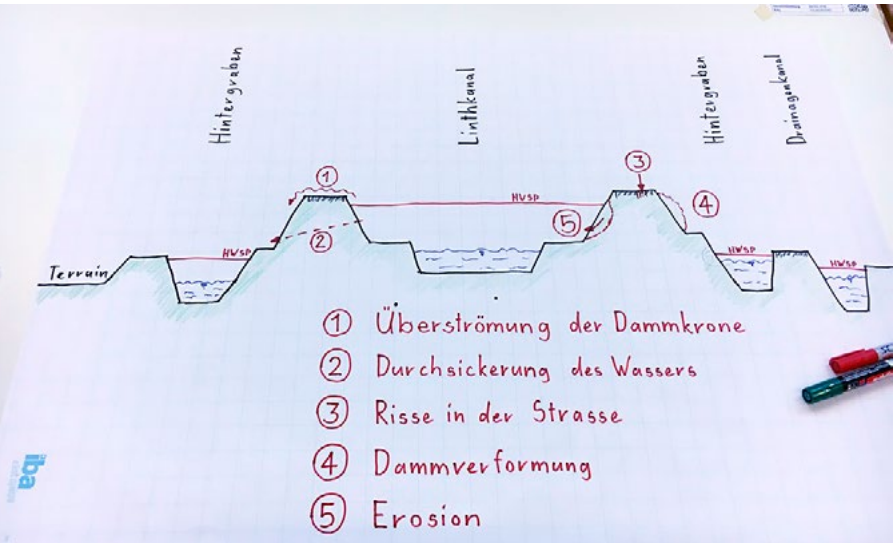
Stabsrahmenübung IKS Linth 16

# Grenzereignisse gemeinsam bewältigen

**Die Herausforderungen eines Unwetter- und Hochwasserereignisses koordiniert angehen: Dies war die Aufgabe des interkantonalen Koordinationsstabs Linth (IKS Linth) in der Stabsrahmenübung IKS LINTH 16.**

Der Linthkanal verbindet den Walensee mit dem Zürichsee und durchzieht in der Linthebene das Grenzgebiet der Kantone Glarus, Schwyz und St. Gallen. Aufgrund der hohen Bedeutung von Ereignissen im Abflussbereich des Linthkanals und des Escherkanals haben die drei Kantone Notfallplanungen erstellt, den interkantonalen Koordinationsstab Linth (IKS Linth) gegründet und diesen mit der Bewältigung von Ereignissen in der Linthebene beauftragt. Der Führungsstandort befindet sich in Kaltbrunn (SG) und ist mit modernster Infrastruktur ausgestattet.

**Für die Bewältigung von Ereignissen in der Linthebene haben die Kantone Glarus, Schwyz und St. Gallen den interkantonalen Koordinationsstab Linth gegründet.**




**Neben der elektronischen Lagedarstellung war auch Handarbeit gefragt.**

## Unterstützung von BABS und BAFU

Dass der IKS Linth einsatzbereit für die Ereignisbewältigung ist und die Zusammenarbeit mit den drei kantonalen Führungsstäben (KFO) funktioniert, konnten alle Beteiligten Ende November 2016 in der Stabsrahmenübung IKS Linth 16 beweisen. Geleitet wurde die Übung vom Bundesamt für Bevölkerungsschutz BABS, einbezogen waren Fachspezialisten aus den drei Kantonen und des Bundesamtes für Umwelt BAFU.
Das Szenario sah ein aussergewöhnliches Hochwasser der Linth vor, entstanden nach anhaltenden Starkniederschlägen und zunehmend milden Temperaturen, die eine Schneeschmelze bewirkten. Bei solchen Ereignissen sind in grossen Teilen der betroffenen Kantone massive Einschränkungen und Schäden zu erwarten. Nebst den Schadenereignissen an der Linth mussten die kantonalen Führungsorganisationen zahlreiche weitere Ereignisse in den Kantonen bewältigen.

## Informationsaustausch

Die eintägige Übung beinhaltete eine ganze Reihe von Aufgaben: die Verbindungen zwischen den kantonalen Führungsstäben (an ihren Standorten) und dem IKS sicherzustellen, die Lageeinschätzungen und Informationen auszutauschen, den Mitteleinsatz zu planen, sich mit dem Werkschutz Linth fachlich zu beraten und die Führungsprozesse situationsbezogen anzuwenden. Dabei galt es im Besonderen, das Sicherheitsfunksystem Polycom und das Informations- und Einsatz-System (IES) einzusetzen. Zudem sollte die Dammüberwachung überprüft werden.

## Zivilschutz und IES haben sich bewährt

Die Beurteilung der Übung fällt positiv aus: Die Zivilschutz-Führungsunterstützung erbrachte einen wertvollen Beitrag zur Sicherstellung der Führungsfähigkeit des Stabes, und der Einsatz der elektronischen Lageführung- und Lagedarstellung mittels IES bewährte sich. Jederzeit konnte die Stabsleitung IKS Linth ein aktuelles Lagebild der drei Kantone und die Ergebnisse der Dammüberwachung abrufen. Der Zivilschutz stellte die Dammüberwachung hervorragend sicher.
Die Übungsleitung konstatierte, dass die Zusammenarbeit zwischen den betroffenen Kantonen gut funktioniert und dass der IKS Linth solche Ereignisse erfolgreich bewältigen kann. Die Übungsbesprechung wurde mittels Skype in alle Führungsstandorte der drei KFO Glarus, Schwyz und St. Gallen live übertragen.

**Militärisch-zivile Katastrophenübung im Appenzellerland**

# Grosses Turngerät für die Zivilen

**Während der Volltruppenübung «Technico 16» vom 25. bis 28. Oktober 2016 standen mehr als 1000 Personen im Einsatz – zivile Einsatzkräfte und Armee, Hand in Hand. Die Übung wurde von der Armee lanciert und von den zivilen Übungspartnern wesentlich mitgestaltet.**

Angenommen wurde bei der Übung «Technico 16» eine flächendeckende Schadenlage im Appenzellerland, verursacht durch einen Meteoritenschauer. Die Folgen der zahlreichen Einschläge und Brände waren zerstörte Gebäude und Strassen, viele Opfer und Obdachlose, grosse Schäden in Wäldern und Feldern. Grundsätzlich war es eine militärische Übung der Territorialregion 4, im Wesentlichen ausgeführt vom Katastrophenhilfebataillon 4 – mit Unterstützung des Zivilschutzes.

## Nur gemeinsam macht es Sinn

Schon bei der Übungsvorbereitung, die rund ein Jahr vor der Durchführung begonnen hatte, wurde eines deutlich: Das volle Potenzial liess sich nur ausschöpfen, wenn bereits die Planung der Übung gemeinsam mit den zivilen Behörden, Stäben und Einsatzorganisationen erfolgte. Die Übungsobjekte mussten von den zivilen Partnern vorbereitet und bis zum Ende der Aktion betreut werden.
Die Bewältigung eines Katastrophenereignisses beginnt in aller Regel bei den Blaulichtorganisationen. Die Armee kommt subsidiär zum Einsatz – wenn die zivilen Einsatzkräfte des Kantons nicht mehr ausreichen und der Bund um Verstärkung ersucht werden muss. Dieser Weg musste auch in der Übung gegangen werden.
Das Übungsszenario beginnt bei den Notrufzentralen und wird mit Lage-Inputs einer Regie unterlegt. Zivile Führungsorgane mit ihrer Führungsunterstützung erkunden die Schadenplätze, beurteilen sie und bestimmen die Hilfeleistungen. Der subsidiäre Einsatz der Armee beruht auf einem klar definierten Hilfsgesuch des Kantons an das Kommando der Territorialregion. Ist die Truppe vor Ort, müssen die Aufträge abgesprochen und die Schadenplätze von den zivilen Einsatzkräften übernommen werden.

**Ausserrhoder Zivilschützer präparieren das ehemalige Munitionsdepot in Teufen für die Übung «Technico 16».**

**Die Armee nutzt das vom Zivilschutz vorbereitete Trümmergebäude in Teufen für eine Rettungsübung.**

## Jede Menge Schnittstellen

Bei der Arbeit auf dem Schadenplatz zählt die Fachkompetenz der Einsatzkräfte. Diese kann durchaus isoliert, von jeder Organisation einzeln, trainiert werden. Alleingänge wären aber nicht nur eine Verschwendung von Ressourcen, sondern ergäben einen unrealistischen Ablauf des Einsatzes. Über den Erfolg eines Katastropheneinsatzes entscheidet die Effizienz und Qualität der Zusammenarbeit aller beteiligten Organisationen und Ebenen.
Die Prozesse dieser Kooperation sind besonders aufmerksam und bewusst zu üben. Das ist aber nur möglich, wenn die entsprechenden Schnittstellen partnerschaftlich definiert und vorbereitet werden. Insbesondere gilt dies auch für die Kommunikation über und aus der Übung – im Ernstfall wird sie immer von den zivilen Behörden geführt.

## Grosser Gewinn für die Zivilen

Der Kanton Appenzell Ausserrhoden hat diese Chance des Austausches und der Zusammenarbeit wahrgenommen und von der Planung der Übung über die Durchführung bis zur Schlussbesprechung aktiv und mit beträchtlichem Engagement mitgewirkt. Der Gewinn war dank des Entgegenkommens der Armee so gross wie die Übung selbst!

**Gunnar Henning, Zonenkoordinator des Schweizerischen Zivilschutzverbandes SZSV**

# Rückzug nach erfolgreicher Rekrutierung

**Nun, da im neuen Organigramm des Schweizerischen Zivilschutzverbandes SZSV die Kästchen der Zonen-Verantwortlichen besetzt sind, zieht sich «Mister Zivilschutz» Gunnar Henning langsam zurück: 2018 ist für ihn Schluss mit der Verbandsarbeit.**

Nach gut drei Jahren sagt Gunnar Henning: «Hurra, alle Zonen sind besetzt!» Es sei nicht immer einfach gewesen, interessierte wie kompetente Leute für die Posten zu finden. Zum Glück seien zu Beginn der Umstrukturierung mit den drei Zonendelegierten und mit ihm aus dem SZSV-Vorstand bereits vier Personen mit an Bord gewesen. «Das hat vieles erleichtert.»

## Gute Argumente

Schlagende Argumente hat der Zonenkoordinator für alle Kandidaten parat, die auf kantonaler Ebene im Bevölkerungsschutz tätig sind. «Wer beim SZSV in einer Zone mitmacht, kriegt garantiert alle relevanten News aus der Bundesverwaltung mit.» Gunnar Henning sagt, manche Kantone würden Neuigkeiten aus Bern nur gefiltert weitergeben. Der Zonenkoordinator unterstützt die Zonen mit Rat und Tat und trägt ihre Anregungen von der Zivilschutzbasis bis in die höchsten Gremien hinein.
Bei den Mitgliedervertretern auf der dritten Hierarchiestufe sind wenige Posten noch vakant. Vor allem sind aber die Kästchen zweier Kantone im Organigramm rot angezeichnet: Graubünden und Schaffhausen sind noch nicht Mitglied. «Das ist ihr gutes Recht, aber schade», sagt Henning. «Wir sollten im Zivilschutz noch mehr miteinander reden und kooperieren. Es macht, überspitzt gesagt, keinen Sinn, dass bei uns 26 verschiedene Kompressoren im Einsatz sind.»
Der Mitgliederbeitrag von rund 3 Rappen pro Einwohner lohne sich. Nebst Informationen aus erster Hand, dem Zugang zu hilfreichen Netzwerken und dem Angebot von Veranstaltungen, Fachtagungen und Seminaren erhielten die Mitglieder auch Stimmrechte, liefert Henning weitere Argumente zum Mitmachen beim nationalen Verband.
Seit Jahrzehnten engagiert er sich mit sehr viel Herzblut für den Zivilschutz. Viele Reformen hat «Mister Zivilschutz», wie der Ostschweizer von einer Zeitung in seiner Heimat einmal betitelt wurde, angestossen und begleitet. Er hat sich für alltagsnahe und intensive Ausbildungen, besseres Material und professionellere Instruktoren eingesetzt. Als Kommandant war ihm Leerlauf zuwider.


**Gunnar Henning, seit Jahren im Einsatz für den Zivilschutz – und den Schutz der Bevölkerung.**

## Grosse Akzeptanz

Wenn Henning von seinen Anfängen beim Zivilschutz erzählt, klingt es, als ob es gestern gewesen sei. «Wir sind damals dahergekommen, als seien wir von der Bourbaki-Armee», berichtet er. Doch die einst belächelte Truppe ist längst nicht mehr: «Ich spüre inzwischen eine grosse Akzeptanz. Wir sind zwar nicht so schnell wie die Feuerwehr, können aber etwa bei Naturkatastrophen mit mehr Leuten helfen und länger bleiben. Das schätzt die Bevölkerung.» Auch die Motivation in den Korps sei heute viel besser.
Beruflich hat der 66-Jährige nichts mehr mit dem Bevölkerungsschutz zu tun – er ist seit 2013 pensioniert. Und auch das Ende des ehrenamtlichen Engagements für den Zivilschutz ist absehbar. An der Generalversammlung 2018 in Luzern will Gunnar Henning als Vorstandsmitglied, Zonenleiter und Zonenkoordinator verabschiedet werden. Einerseits hat er seinen Nachfolger als Zonenkoordinator – natürlich – schon gefunden. Und andererseits sagt er: «Ich bin nicht mehr an der Front tätig. Die Gefahr steigt, dass ich nur noch von früher rede und nicht mehr glaubhaft bin.»

**Nutzung ziviler Drohnen**

# REDOG geht in die Luft

**Die Suchhunde von REDOG erhalten Unterstützung aus der Luft: Drohnen des Schweizerischen Verbandes ziviler Drohnen SVZD werden künftig bei der Suche nach vermissten Menschen in der Schweiz eine Übersicht von oben liefern. Damit wird die Suche in unübersichtlichem, unwegsamem und grossflächigem Gebiet schneller und einfacher.**

Für einmal ein Joint Venture, das nicht hohe Gewinne im Visier hat, sondern das Ziel, Menschenleben zu retten: Wenn die Teams des Schweizerischen Vereins für Such- und Rettungshunde REDOG nach Vermissten suchen, nutzen sie – vom Boden aus – Wärmebildkameras und Nachtsichtgeräte. In weitem und manchmal unwegsamem Gelände ist diese technische Unterstützung nur beschränkt wirksam. Die Zusammenarbeit mit dem Schweizerischen Verband ziviler Drohnen (SVZD) erlaubt es nun, dieses Manko zu beheben. Drohnen, bestückt mit Wärmebildkameras, werden die Geländesuche aus der Luft ergänzen.


**Die Teams des Schweizerischen Vereins für Such- und Rettungshunde REDOG können bei ihrer Suche nach Vermissten künftig auf Unterstützung aus der Luft zählen.**

## Zwei Partner ergänzen sich

Dabei haben sich zwei Partner mit unterschiedlicher Ausrichtung zu einem gemeinsamen Zweck verbunden. REDOG ist eine humanitäre Freiwilligenorganisation des Schweizerischen Roten Kreuzes SRK und bildet Teams von Mensch und Hund zur Rettung von Vermissten und Verschütteten aus; die Freiwilligenorganisation, die rund 240 Mitglieder zählt, kann schweizweit und international wirken. Der SVZD setzt sich – als Vertreter von Pilotinnen und Piloten, Operatorinnen und Operatoren, Händlerinnen und Händlern sowie Herstellerinnen und Herstellern in der Schweiz – für Drohnen und deren Sicherheit ein, für die Akzeptanz in der Bevölkerung und die Integration in den Luftraum.
Der SVZD bringt in die Zusammenarbeit die Technologie und die Erfahrung ein, REDOG stellt seine bewährten Alarmierungsstrukturen über die Notrufnummer 0844 441 144, die Einsatzleitung und einsatzfähige Teams zur Verfügung. Die Ausbildung und das Training der Fachleute der Technischen Ortung von REDOG und des SVZD werden für diese gemeinsame Arbeit angepasst. Im Einsatz bilden die Pilotin oder der Pilot mit der Einsatzkraft von REDOG ein Team.

## «Nicht kommerziell»

«Zwei grosse Freiwilligenorganisationen schliessen sich zugunsten vermisster Menschen zusammen, das erhöht die Effizienz, denn im Ernstfall zählt jede Minute», freut sich Romaine Kuonen, Zentralpräsidentin von REDOG, und betont: «Die Zusammenarbeit ist nicht kommerziell.» Ueli Sager, Präsident des SVZD ergänzt: «Search and Rescue ist ein Bereich, in dem mit Drohnen zukünftig viel bewegt werden kann. Durch die Zusammenarbeit des SVZD mit REDOG wird die Erfahrung und Expertise des Suchhunde-Vereines mit dem technischen Know-how und der Qualitätssicherung der Drohnenpiloten verbunden. Wir sind sicher, dass damit ein optimales Resultat zugunsten vermisster Personen erzielt werden kann, das auch über die Landesgrenzen hinaus strahlt.»
«Up in the air» heisst es somit künftig für REDOG. Die fliegenden Spürhunde werden die Hundenasen am Boden allerdings nicht ersetzen können.

*Für weiterführende Informationen:*
*www.redog.ch*
*www.drohnenverband.ch*


**KGS Forum 27/2016**

# Eine «tierische» Publikation

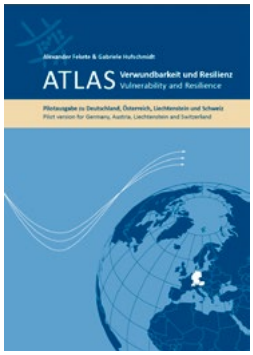
Tier und Kulturgut – ein Zusammenspiel, das es in unterschiedlichsten Kombinationen zu entdecken gilt. Seit frühesten Zeiten hat das Tier für den Menschen eine grosse Bedeutung, ob als Bedrohung, Nahrungslieferant, Symbolträger oder treuer Begleiter. Wir sind fasziniert von Tieren in Bildern, in Zoos, in Museen oder in Freiheit. Die enge Beziehung spiegelt sich nicht zuletzt in Malereien, Skulpturen und figürlichen Darstellungen, die auf unterschiedlichsten Materialien eine Bedeutung als Kulturgut erlangt haben. Museen, Archive, Bibliotheken beherbergen eine Vielzahl Beispiele. Tiere findet man aber auch an Hausfassaden, auf Möbeln und Transportmitteln, als Wappenträger und in Namen, in Fabeln und Märchen, im täglichen Wortschatz und in der Psychologie. Und auch im «KGS Forum 27/2016».

**Internationale Fachtagung Psychosoziale Notfallversorgung 2017**

# «Aus der Praxis – für die Praxis»

Die Schweizerische Vereinigung Psychosoziale Notfallversorgung SV-PSNV organisiert am 20. Mai 2017 im Campus Sursee (LU) die 3. internationale Fachtagung Psychosoziale Notfallversorgung. Das Motto der Tagung lautet: «Aus der Praxis – für die Praxis». Die Informations- und Weiterbildungsveranstaltung für Einsatzkräfte in der Psychosozialen Notfallversorgung PSNV sowie für Kriseninterventions-Organisationen und Rettungseinsatzkräfte bietet nicht nur praxisorientierte Referate, sie fördert ebenfalls die Vernetzung und den Erfahrungsaustausch unter den Teilnehmenden.

*Weitere Informationen: www.sv-psnv.ch*




**Fachpublikation**

# Atlas der Verwundbarkeit und Resilienz

In welchem Masse sich Gefahren auf eine Gesellschaft auswirken, wird im Bevölkerungsschutz mit den Begriffen Verwundbarkeit und Resilienz beschrieben. Projekte und Praxisbeispiele zur vielfältigen Anwendung und Umsetzung der beiden Konzepte haben die Technische Hochschule Köln und die Universität Bonn jetzt im «Atlas VR» zusammengestellt. Der zweisprachige Übersichtsband (deutsch und englisch) enthält 46 Fallstudien aus Deutschland, Österreich, Liechtenstein und der Schweiz.

*Kostenlos zugänglich: www.atlasvr.de*

**IMPRESSUM**

**Bevölkerungsschutz 27** / März 2017 (10. Jahrgang)

Die Zeitschrift *Bevölkerungsschutz* ist in der Schweiz kostenlos erhältlich in Deutsch, Französisch und Italienisch.

**Herausgeber:** Bundesamt für Bevölkerungsschutz BABS

**Koordination und Redaktion:** P. Aebischer

**Redaktionsteam:** A. Bucher, Ch. Fuchs, D. Häfliger, M. Haller, K. Münger, N. Wenger

**Übersetzungen und Lektorat:** Sprachdienste BABS

**Kontakt:** Bundesamt für Bevölkerungsschutz, Kommunikation, Monbijoustr. 51A, CH-3003 Bern, Telefon +41 58 462 51 85, info@babs.admin.ch

**Fotos:** S. 1, 7, 9 und 11 Fotolia, S. 17 Schutz & Rettung Zürich; übrige BABS / zVg

**Layout:** Zentrum elektronische Medien ZEM, Bern



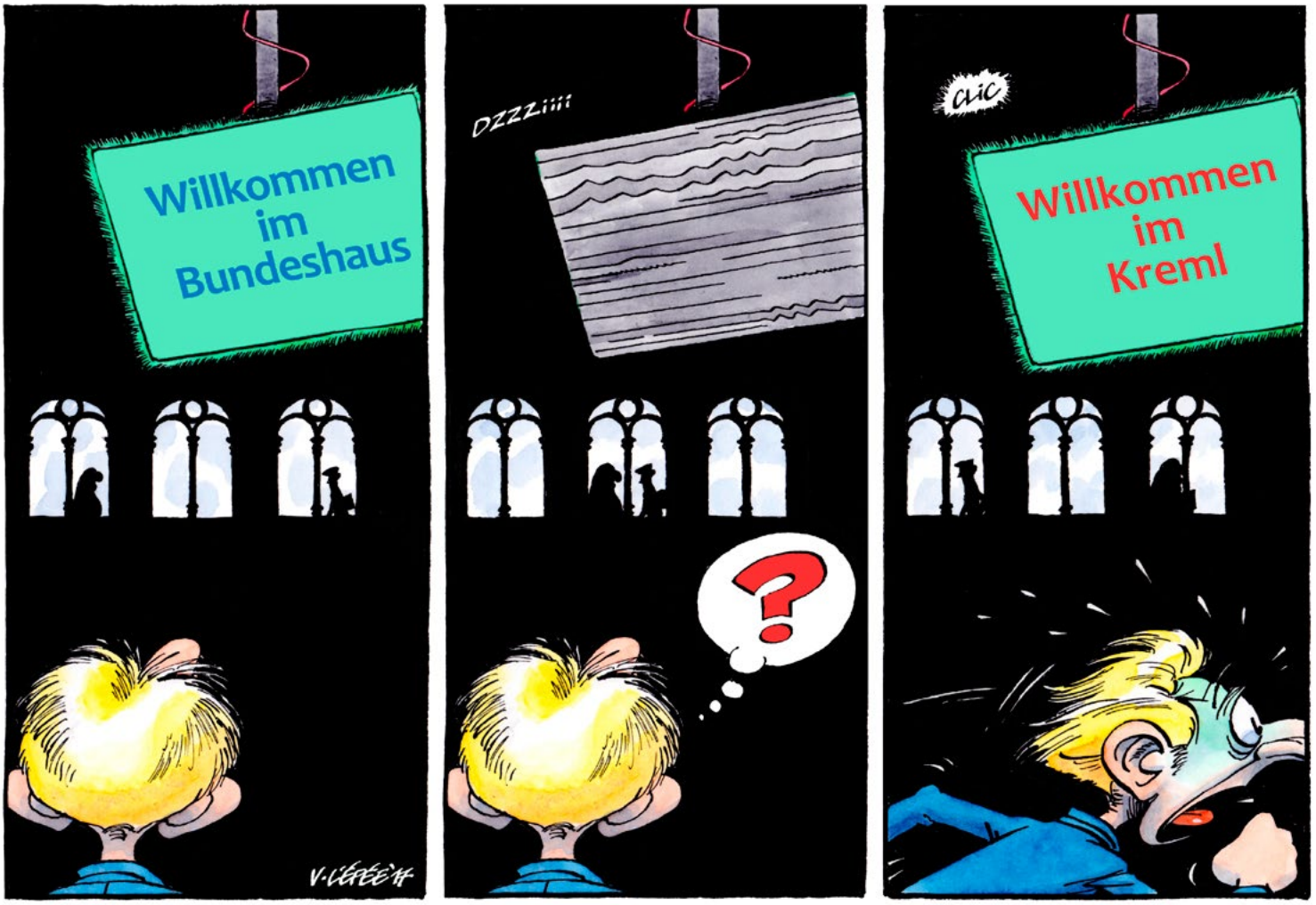
**Auflagen:** Deutsch 8100 Ex., Französisch 3100 Ex., Italienisch 800 Ex.

Das BABS ist Herausgeber von *Bevölkerungsschutz*. Die Zeitschrift ist aber keine offizielle Publikation im engeren Sinn, sondern eine Plattform; die Beiträge geben somit nicht in jedem Fall den Standpunkt des BABS wieder.

Cyber-Risiken

# So sieht es V. L'Épée

Vincent L'Epée zeichnet für die Westschweizer Tageszeitungen «L'Express», «L'Impartial» und «Le Journal du Jura». Seine Arbeiten sind auch in der zweimonatlich erscheinenden Zeitschrift «Edito+Klartext» und gelegentlich im Wochenblatt «Courrier international» zu sehen. Er wohnt in Neuenburg.




## Ausblick Nr. 28, Juli 2017

Dossier

**Partnerorganisation Gesundheitswesen**

## Was meinen Sie?

Wir freuen uns über Ihre Rückmeldungen und Anregungen für kommende Ausgaben!

*info@babs.admin.ch*

## Jetzt bestellen

Die Zeitschrift des Bundesamtes für Bevölkerungsschutz erscheint dreimal pro Jahr in Deutsch, Französisch und Italienisch.

*Gratishefte und -abonnements können bestellt werden unter www.bevoelkerungsschutz.ch oder info@babs.admin.ch.*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Bundesamt für Bevölkerungsschutz BABS**

**«Die Herausforderung ist es, den Informationsschutz und die Usability unter einen Hut zu bringen.»**

Nicoletta della Valle, Direktorin fedpol
Seite 6

**«Wir dürfen uns weiterhin über viele Neuerungen freuen; aber wir müssen akzeptieren, dass man sich so gut wie möglich vor Bedrohungen schützen muss.»**

Max Klaus, stv. Leiter Melde- und Analysestelle Informationssicherung MELANI
Seite 12

**«Wir sind damals dahergekommen, als seien wir von der Bourbaki-Armee.»**

Gunnar Henning, Zonenkoordinator Schweizerischer Zivilschutzverband SZSV
Seite 36

**Bundesamt für Bevölkerungsschutz BABS**
**Monbijoustrasse 51A**
**CH-3003 Bern**
**Telefon +41 58 462 51 85**
**info@babs.admin.ch**
**www.bevoelkerungsschutz.ch**