Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

**Office fédéral de la protection de la population OFPP**

# Rapport sur l'avenir des systèmes d'alarme et de télécommunication pour la protection de la population

Évaluation des systèmes permettant la communication au niveau de la conduite et en cas d'intervention entre les autorités et les organisations chargées du sauvetage et de la sécurité (AOSS) et des systèmes d'alarme et d'information de la population

---

29 septembre 2017 (traduction du 20 octobre 2017)

**Table des matières**

## Liste des abréviations

| Abréviation | Signification |
|---|---|
| ABCN | Menaces atomiques, biologiques et chimiques et dangers naturels |
| AOSS | Autorités et organisations responsables du sauvetage et de la sécurité |
| BAC | Base d'aide au commandement |
| BCM | Business Continuity Management |
| BNS | Banque nationale suisse |
| BOS Austria | Österreich: digitales Bündelfunksystem zur Funkkommunikation für Behörden und Organisationen mit Sicherheitsaufgaben (BOS) |
| CBS | Cell Broadcast Service |
| CCDJP | Conférence des directrices et directeurs des départements cantonaux de justice et police |
| CDF | Contrôle fédéral des finances |
| CENAL | Centrale nationale d'alarme |
| CFF | Chemins de fer fédéraux |
| CG MPS | Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers |
| Cgfr | Corps des gardes-frontière |
| ChF | Chancellerie fédérale |
| CSFLB | Communication sans fil à large bande |
| DAB+ | Digital Audio Broadcast +<br>est une technologie de radiodiffusion numérique par voie hertzienne via des stations émettrices terrestres. (source SSR) |
| DDPS | Département fédéral de la défense, de la protection de la population et des sports |
| DETEC | Département fédéral de l'environnement, des transports, de l'énergie et de la communication |
| DFAE | Département fédéral des affaires étrangères |
| DFJP | Département fédéral de justice et police |
| DGD | Direction générale des douanes |
| DVB-C | Digital Video Broadcasting – Cable |
| DVB-S | Digital Video Broadcasting – Satellite |
| EMF ABCN | État-major fédéral ABCN |
| ERNS 14 | Exercice du Réseau national de sécurité 2014 |
| fedpol | Office fédéral de la police |
| ICARO | Information Catastrophe Alarme Radio Organisation |
| IFSN | Inspection fédérale de la sécurité nucléaire |
| IIS-SSC | Système d'information et d'intervention du Service sanitaire coordonné |
| IP | Protocole Internet |
| IPCC | Information de la population par la Confédération en cas de crise |
| KomBV-KTV | Réseau de communication des autorités entre la Confédération et les cantons |
| KTN Bund | Deutschland: sicheres Kerntransportnetz |

| | |
|---|---|
| LPPCi | Loi sur la protection de la population et sur la protection civile |
| LRTV | Loi fédérale sur la radio et la télévision |
| MétéoSuisse | Office fédéral de météorologie et de climatologie |
| OD CTE | Organe directeur pour la coordination des transports dans l'éventualité d'événements |
| OFAC | Office fédéral e l'aviation civile |
| OFCOM | Office fédéral de la communication |
| OFPP | Office fédéral de la protection de la population |
| OFROU | Office fédéral des routes |
| OFT | Office fédéral des transports |
| ONG | Organisation non gouvernementale |
| OSTRAL | Organisation pour l'approvisionnement en électricité en cas de crise |
| OUC | Onde ultracourte |
| PES | Présentation électronique de la situation |
| RDS | Réseau de données sécurisé |
| Réseau B-MPLS | Réseau IP permettant aux utilisateurs Polycom de communiquer entre eux |
| MPLS | Multiprotocol Label Switching |
| RNS | Réseau national de sécurité |
| SEM | Secrétariat d'État aux migrations |
| SMS | short message service |
| SRC | Service de renseignement de la Confédération |
| SSR | Société suisse de radiodiffusion |
| SSS | Service sismologique suisse |
| TIC | Techniques d'information et de communication |
| WEF | World Economic Forum / Forum économique mondial |
| WLAN | Wireless Local Area Network |

## Condensé

### Mandat

Le 18 décembre 2015, le Conseil fédéral a chargé le DDPS d'effectuer une évaluation des projets de télécommunications importants pour la protection de la population. Les risques auxquels est exposée la population de la Suisse sont à cet égard déterminants : attentats terroristes, catastrophes naturelles telles que séismes et crues, catastrophes d'origine technique ou sociétale et situations d'urgence telles que panne d'électricité ou pandémie. Le rapport doit indiquer quels sont les systèmes indispensables pour la protection adéquate de la population suisse et devant par conséquent être réalisés ou développés à court terme. Il convient également d'établir quels sont les systèmes présentant une priorité moindre, voire ceux auxquels il serait possible de renoncer. À cet égard, on évaluera les conséquences pour la population d'une indisponibilité totale ou partielle de ces systèmes. Afin de pouvoir procéder à une estimation réaliste, il faut également étudier les coûts de réalisation des différents systèmes, les questions liées à la répartition des compétences, ainsi que les aspects financiers et juridiques. Il incombe ensuite aux autorités politiques de prendre des décisions de principe en ayant connaissance de leurs répercussions sur la population et ses bases d'existence.

Le présent rapport renseigne sur l'état des systèmes actuels d'alarme et de communication importants pour la protection de la population ainsi que sur les besoins actuels et futurs côté Confédération, cantons et exploitants d'infrastructures critiques.

### Systèmes de communication aux niveaux stratégique et opérationnel et systèmes d'alarme et d'information de la population

L'objet du présent rapport est la communication au niveau de la conduite stratégique et au niveau tactique des organes d'intervention. La transmission de l'alarme et l'information à la population sont aussi prises en compte. En cas d'événement, la transmission d'informations orales, de textes ou d'images entre les autorités sur un réseau de données sécurisé est indispensable pour que les organes de conduite stratégique aux échelons fédéral et cantonal puissent fonctionner. Ces organes sont dès lors à même d'ordonner les mesures adéquates pour la protection de la population et des biens touchés ou menacés. Cela suppose d'avoir une vue d'ensemble de la situation en cours, ce qui n'est possible qu'en disposant d'une présentation électronique de la situation et d'un suivi de la situation. Le réseau radio suisse de sécurité Polycom a fait ses preuves dans le cadre de son utilisation par les organisations d'intervention tactiques en situation normale et en cas d'événement. Dans les centres urbains, ces organisations ont toutefois besoin, en cas d'événement majeur, d'une communication mobile sans fil à large bande pour pouvoir coordonner et mener à bien leurs interventions de sécurité, de protection et de sauvetage. La transmission actuelle de l'alarme et l'information à la population par sirènes et radio d'urgence devront à l'avenir être complétées par la diffusion de consignes de comportement par smartphone. Les autorités seront ainsi en mesure de transmettre les informations importantes plus directement et plus rapidement à la population et de prendre en compte l'évolution du comportement de celle-ci face aux médias. Cela permettra éventuellement de sauver des vies et de réduire les effets des catastrophes et situations d'urgence.

### Enseignements de l'exercice du Réseau national de sécurité 2014

L'exercice du Réseau national de sécurité 2014 (ERNS 14) visait essentiellement à vérifier la capacité à maîtriser la conduite aux échelons fédéral et cantonal dans des conditions impliquant une panne de courant ou une pénurie d'électricité. Il s'est avéré qu'une pénurie d'électricité de plusieurs mois notamment pouvait entraîner une situation d'urgence d'envergure nationale, complexe à gérer. Une telle situation de crise serait caractérisée par des problèmes d'ordre technique au niveau de la conduite. Le rapport final ERNS 14 dresse d'ailleurs le constat suivant à l'intention de la plate-forme politique du Réseau national de sécurité (RNS) : « Les systèmes TIC examinés auraient été nettement limités dans le cas d'une pénurie de courant durant plusieurs semaines. Ils n'auraient en grande partie pas été en mesure de répondre aux exigences posées ». Les systèmes dont la fonctionnalité est réduite en cas de crise ralentissent ou empêchent la circulation des données à temps, de manière régulière et fiable. De ce fait, ils préjudicient sensiblement à la conduite, la communication, l'information et l'alarme à chaque niveau et entre les partenaires. En tirant les enseignements de l'ERNS 14, il est notamment préconisé la réalisation d'un réseau de données sécurisé (RDS), capable de fonctionner même en situation de pénurie d'électricité, ainsi que de poursuivre les travaux visant à mettre en place un réseau de suivi de la situation.

**Lacunes en matière de sécurité et niveau visé**

Le présent rapport décrit les systèmes actuels, utilisés au quotidien pour garantir la communication entre les autorités et organisations chargées du sauvetage et de la sécurité (AOSS) de même que la transmission de l'alarme à la population et l'information de celle-ci. On y explique également la détérioration des systèmes lors d'atteintes légères ou importantes qui auraient pour effet de les rendre inopérants. Les lacunes qui en résulteraient en termes de sécurité y sont détaillées. En collaboration avec les cantons, les organisations d'intervention, les exploitants d'infrastructures critiques et divers services fédéraux, l'Office fédéral de la protection de la population OFPP a examiné plusieurs solutions qui permettraient de combler ces lacunes. La réalisation de nouveaux systèmes ou le perfectionnement de systèmes existants occasionnerait des coûts considérables, c'est pourquoi il convient d'évaluer l'utilité et la nécessité de ces systèmes sous l'angle du niveau de sécurité à atteindre, en montrant aussi les risques auxquels la population serait exposée si ces systèmes n'étaient pas réalisés. On pourra fixer sur cette base, compte tenu des possibilités de financement, un ordre de priorité pour la réalisation des projets.

**Ordre de priorité**

La classification des systèmes de télécommunications par priorités se fonde sur 72 prises de position de la Confédération, des cantons, des exploitants d'infrastructures critiques et de différentes associations et ONG. La priorité absolue est donnée à la réalisation du réseau de données sécurisé (RDS) avec son système d'accès aux données et réseau d'utilisateurs fermé Polydata, en coordination avec le remplacement du système de transmission de messages VULPUS-Télématique (VULPUS). En outre, une importance hautement prioritaire est attachée à l'élaboration de bases pour la communication sans fil à large bande, éventuellement dans le cadre d'un projet pilote des cantons intéressés, et à la mise en place d'un réseau national de suivi de la situation.

La réalisation des autres projets, comme Polysat, la transmission de l'alarme à la population via CBS ou SMS mais aussi la mise en œuvre généralisée de la Communication sans fil à large bande (CSFLB), est également jugée importante. Elle ne dépend cependant pas impérativement du facteur temps et ces projets doivent encore être davantage étudiés sous l'aspect technique.

**Compétences et répartition des coûts Confédération – cantons – tiers**

Les coûts d'installation, d'exploitation et de maintien de la valeur des systèmes à mettre en place devront être répartis entre la Confédération, les cantons et les exploitants d'infrastructures critiques. Les compétences et la répartition des tâches entre la Confédération, les cantons et les tiers doivent être réglées dans le cadre de la révision en cours de la LPPCi, puisque les bases juridiques actuelles ne sont plus suffisantes ou que les bases juridiques font carrément défaut pour les nouveaux systèmes prévus, tels que RDS/Polydata ou CSFLB. Le modèle de répartition des compétences et des coûts ainsi que la définition des interfaces doivent être conformes aux règles éprouvées pour des systèmes tels que Polycom et Polyalert. Le présent rapport contient des propositions tenant compte des besoins des utilisateurs, des structures fédérales, de la réforme de la péréquation financière et de la répartition des tâches entre la Confédération et les cantons (RPT) et des principes économiques. Sur le plan juridique, les compétences et le financement seront définis dans le cadre de la révision prochaine de la LPPCi.

# 1 Introduction

## Contexte

La communication et l'échange d'informations entre les autorités et les organisations chargées du sauvetage et de la sécurité (AOSS) sous la forme de conversations, de textes et d'images, d'une part, et la transmission de l'alarme et d'informations à la population en cas d'événement, d'autre part, représentent deux instruments essentiels d'une protection efficace de la population et de ses bases d'existence. La communication et l'échange d'informations permettent aux AOSS de coordonner la fourniture aux décideurs des éléments sur lesquels ils se fondent pour prendre des mesures afin de protéger la population et ses bases d'existence. En outre, l'alarme et l'information de la population garantissent à celle-ci la possibilité d'adopter en temps utile le comportement adéquat et ainsi de se protéger, par exemple en cas d'attaque terroriste, de catastrophe ou de situation d'urgence.

Ces deux instruments contribuent largement à réduire les risques. Leur absence aurait d'une manière générale de graves conséquences pour la sécurité de la population qui se traduiraient par des dommages accrus et davantage de blessés et de morts.

La communication et l'échange d'informations entre les AOSS reposent actuellement sur les systèmes suivants : Polycom pour les conversations radio, VULPUS-Télématique pour la transmission de messages écrits et la Présentation électronique de la situation (PES CENAL) pour les textes et images. Polycom est un système de transmission radio à disposition des AOSS. La police, les sapeurs-pompiers, les premiers secours, les services de sauvetage, le Corps des gardes-frontière (Cgfr) et divers exploitants d'infrastructures critiques l'utilisent quotidiennement. Lors d'événements majeurs, les autorités fédérales (p. ex. les organes chargés des dangers naturels) et cantonales en sont également équipées pour communiquer avec d'autres intervenants. VULPUS est un système protégé de transmission de messages textes entre les organes civils et militaires de la Confédération et des cantons. Quant à la PES CENAL, elle sert à l'échange d'informations sur la situation.

L'alarme et l'information de la population utilisent depuis des années les sirènes déclenchées désormais par le système Polyalert. L'alarme générale invite la population à écouter la radio afin d'obtenir des informations sur l'événement. Quant à l'alarme eau, elle exhorte les riverains à quitter immédiatement la zone dangereuse. Si l'infrastructure de transmission radio tombe en panne dans toute la Suisse, la Confédération peut tout de même informer la population par l'intermédiaire de l'IPCC (Information de la population en cas de crise par la Confédération).

Les systèmes de communication et d'échange d'informations sont utilisés quotidiennement lors d'événements aussi divers que des attaques à main armée, des accidents de la route, des incendies ou des manifestations sportives. Ils garantissent une collaboration efficace des différentes organisations d'intervention engagées (p. ex. la police, les sapeurs-pompiers, les premiers secours).

Des événements comme l'ouragan Lothar en 1999, les canicules de 2003 et 2015, les crues de 2005 et 2007, la panne d'électricité des CFF en 2005, la grippe porcine en 2009 ou encore l'incendie de forêt de Viège en 2011 exigent la collaboration d'un grand nombre d'autorités, organisations et exploitants d'infrastructures critiques qui doivent pouvoir s'échanger des informations. Les crues de 2005 ont en outre nécessité l'emploi de sirènes dans plusieurs cantons afin d'avertir la population qu'elle devait se mettre rapidement à l'abri.

On continuera certes à utiliser la radio comme moyen de communication et les sirènes pour donner l'alarme, mais de nos jours la protection de la population fait de plus en plus appel aux possibilités de l'échange d'informations sur support numérique.

Dans leurs activités quotidiennes, les organisations de première intervention sont de plus en plus appelées à échanger de grandes quantités de données et à faire usage d'applications liées aux différents types d'interventions. Ces moyens permettent la transmission efficace de données et d'informations et favorisent la collaboration des AOSS et d'autres partenaires de la protection de la population.

Le développement de canaux existants et la création de nouvelles ressources comme les applications pour smartphones ou les SMS permettraient d'alerter et d'informer de façon ciblée la population d'un secteur menacé ou touché même sans devoir recourir aux sirènes, lesquelles ne sont pas perçues dans de nombreux bâtiments à cause de l'isolation phonique. Par ailleurs, de plus en plus de Suisses réagissent de manière inadéquate – si tant est qu'ils réagissent – à l'alarme par sirènes. Les malentendants ou les personnes souffrant de handicaps mentaux, auxquels il est impossible de percevoir ou de comprendre les consignes de comportement diffusées par radio à la suite d'une alarme donnée par des sirènes, dépendent d'un mode de diffusion d'alarme qui leur est accessible. Il serait possible

d'atteindre ces personnes durant la première phase d'un événement en leur donnant des informations par smartphone et en leur transmettant des consignes de comportement. Le problème de l'accessibilité se pose aussi pour les résidents étrangers qui ne connaissent pas le signal émis au moyen des sirènes et ne comprennent pas nos langues nationales.

Cependant, la numérisation de la communication entre les autorités et la population s'accompagne aussi de nouvelles vulnérabilités. Les systèmes actuels de communication et d'échange d'informations, de même que l'alarme et l'information de la population présentent de sérieuses lacunes de sécurité.

Ces dernières années, les cyberattaques et la cybercriminalité se sont considérablement développées. Elles représentent aujourd'hui le plus grand risque pour les utilisateurs de canaux de communication numériques. Les réseaux et systèmes utilisés en Suisse ne sont pas à l'abri d'une perturbation, voire d'une défaillance sciemment provoquée. Dans une telle situation, les AOSS et les autorités en charge de la sécurité ne pourraient plus communiquer ou seulement de manière très limitée et verraient leur capacité d'action réduite, en temps normal aussi.

Si les nœuds et les composants des réseaux ne sont plus alimentés en énergie, ils tombent rapidement en panne ou subissent des dérangements considérables. Lors de petits événements à l'échelle locale, les fonctions de communication centrales et l'échange d'informations nécessaire à l'intervention peuvent généralement être assurées, même partiellement, par d'autres canaux. Mais les analyses des risques montrent que la Suisse doit aussi s'attendre à faire face à des événement graves[1] : pannes de courant touchant une grande partie du pays, pénuries d'électricité de longue durée, séismes de forte intensité, tempêtes et inondations à grande échelle représentent des risques importants pouvant occasionner des dommages pour plus de 100 milliards de francs. De tels événements et leurs conséquences néfastes et étendues ne sauraient être maîtrisés sans coordination de l'action de la Confédération, des cantons et des exploitants d'infrastructures critiques. Il est cependant fort probable que les réseaux et systèmes utilisés aujourd'hui fassent défaut dans de telles situations, pour différentes raisons : interruption de l'alimentation en énergie, surcharge ou déconnexion préventive en cas d'alerte terroriste. Or c'est précisément lors de pareils événements que les AOSS et les exploitants d'infrastructures critiques ont besoin de systèmes qui fonctionnent afin de coordonner leurs activités, de préparer et d'échanger des informations, ce qui permettra de protéger la population, d'assurer les prestations vitales et de prendre à temps les mesures de sécurité qui s'imposent. Ils ont besoin d'informations sur la situation en permanence et de systèmes de conduite à haute disponibilité afin de pouvoir fournir dans les meilleurs délais des bases de décision consolidées qui permettront d'évaluer et de prendre les mesures de protection adéquates. Les risques décrits exigent des réactions rapides et coordonnées pour sauver des vies et protéger la population et les biens matériels.

La capacité de la Confédération et des cantons à diriger les opérations en cas de panne et de pénurie d'électricité constituait l'un des thèmes centraux de l'exercice du Réseau national de sécurité 2014 (ERNS 14). Il en était ressorti qu'une pénurie d'électricité durant plusieurs mois engendrerait une situation d'urgence complexe à l'échelle nationale mettant les autorités face à des problèmes techniques entravant les capacités de conduite. Le rapport final sur l'ERNS 14 à l'attention de la plateforme politique du Réseau national de sécurité (RNS) tire le constat suivant : « Les systèmes TIC examinés auraient été nettement limités dans le cas d'une pénurie de courant durant plusieurs semaines. Ils n'auraient en grande partie pas été en mesure de répondre aux exigences posées. »[2] Des systèmes dont les fonctionnalités sont limitées en situation normale, particulière ou extraordinaire empêchent un flux de données et d'informations régulier, fiable et ponctuel. Ce faisant, ils entravent gravement la conduite, la communication, l'information, l'alarme et la coordination à tous les échelons. Les enseignements tirés de l'ERNS 14 ont notamment débouché sur la recommandation, adressée au Conseil fédéral, de créer un réseau de données sécurisé (RDS) fonctionnant même en cas de pénurie d'électricité. Il convient en outre de poursuivre les travaux visant à mettre en place un réseau de suivi de la situation.

L'optimisation des systèmes de télécommunication de la protection de la population représente une mesure fondamentale pour réduire le risque de défaillance des systèmes, renforcer leur protection contre les cyberrisques et ainsi améliorer la sécurité de la population, étant entendu que la perte de la capacité de communiquer et d'informer perturberait gravement, voire empêcherait le travail des AOSS.

---

1 OFPP (2015) Catastrophes et situations d'urgence en Suisse : rapport technique sur les risques.

2 Organisation du projet ERNS 14 (2015), rapport final sur l'ERNS 14 (Exercice du Réseau national de sécurité).

Faute de maintenir la valeur de ces systèmes et de les développer, il faudrait s'attendre à voir le bilan des événements s'alourdir, tant sur le plan humain (morts et blessés) que sur celui des dommages matériels. Il appartient aux responsables politiques de juger jusqu'à quel point un tel risque est supportable et de déterminer les mesures et les moyens (notamment financiers) permettant de l'endiguer à une échelle acceptable pour la société.

### Mandat

Compte tenu des développements décrits plus haut et du besoin des cantons de disposer de bases pour leur planification financière et la planification de leurs investissements, le Conseil fédéral a confié au DDPS, le 15 décembre 2015, la mission de faire le point sur les besoins de la Confédération, des cantons et des exploitants d'infrastructures critiques en matière de communication en cas de catastrophe ou de situation d'urgence, sur le niveau de sécurité souhaitable, pour les systèmes d'alarme et de télécommunication importants pour la protection de la population, sur des solutions de remplacement, sur les ressources nécessaires et sur les bases légales. Le rapport doit être soumis au Conseil fédéral d'ici la fin de l'année 2016.

De septembre à novembre 2016, la première version du présent rapport a été mise en consultation auprès des organes fédéraux concernés, des cantons, des exploitants d'infrastructures critiques et des autres partenaires de la protection de la population. Cette consultation, de même que les expériences faites au moment de la mise en place de Polycom montrent la nécessité de régler clairement les questions de compétences et de financement avant tout dans le cas de systèmes mixtes, auxquels la Confédération, les cantons et des tiers participent conjointement. Pour définir avec précision les compétences et la répartition des coûts, le chef du DDPS et les présidents de la CCDJP et de la CG MPS ont institué, le 10 janvier 2017, un groupe de travail composé de représentants de la Confédération et des cantons et dirigé par le directeur de l'OFPP. Ses résultats ont été intégrés dans le présent rapport.

### Structure du rapport

Après une introduction, le chap. 2 expose l'usage et la nécessité des systèmes de télécommunication actuels ainsi que le besoin de nouveaux systèmes sur la base de scénarios concrets et met en évidence les lacunes existantes en matière Les chap. 3 et 4 font le point sur les différents systèmes de communication, d'échange d'informations et d'alarme. Il y est montré pourquoi ces systèmes sont nécessaires, quelles seraient les conséquences d'une non-réalisation pour les AOSS et la population et quelles sont les solutions possibles dans ce domaine. On trouvera au chap. 5 une proposition d'ordre de priorité. Le chap. 6 est consacré aux compétences et au financement en matière d'investissement, de maintien de la valeur, d'entretien et d'exploitation. La répartition des tâches et des coûts entre la Confédération, les cantons et les tiers est un thème central. Le chap. 7 explique le lien entre la répartition des tâches et le financement à la lumière de la révision en cours de la loi sur la protection de la population et la protection civile. Le chap. 8 porte sur les conséquences financières et les effets sur le personnel, alors que le chap. 9 a pour objet les conséquences d'une non-réalisation des projets. La suite des travaux est brièvement présentée dans le chap. 10.

# 2 Utilité et nécessité des systèmes

## 2.1 Importance des systèmes de télécommunication en cas d'événement

La communication, l'échange d'informations et la transmission de l'alarme à la population sont essentiels à la gestion efficace d'un événement ainsi qu'à la sécurité et à la protection de la population en toute situation. Lors d'événements majeurs tels qu'ils sont survenus en Suisse durant les deux dernières décennies (Lothar en 1999, les canicules en 2003 et 2015, les crues en 2005 et 2007, la panne des CFF en 2005, la grippe porcine en 2009, l'incendie de forêt au-dessus de Viège en 2011), la collaboration entre les différentes autorités, les organisations de première intervention et les exploitants d'infrastructures critiques revêt une importance accrue et exige une interopérabilité de toutes les parties.

Cependant, la Suisse reste exposée à des risques dont les conséquences seraient encore plus graves (p. ex. acte terroriste, séisme, pénurie d'électricité), comme le montrent des analyses au niveau national (cf. diagrammes ci-après)[3]. De tels événements peuvent en effet causer un grand nombre de morts et de blessés, d'importantes perturbations de l'approvisionnement de même que des dommages matériels se chiffrant en milliards de francs. Ils sont également susceptibles de détériorer sensiblement la sécurité en Suisse. De plus, la réputation de la Suisse est en jeu lorsque la maîtrise d'un événement ne peut être assurée de manière professionnelle. Une réputation négative peut avoir d'importantes répercussions sur des branches de l'économie telles les investissements étrangers, le tourisme, etc. et avoir des conséquences négatives à moyen et long terme. Les effets de tels événements peuvent rapidement atteindre une dimension nationale. Leur maîtrise peut exiger une coopération nationale, voire internationale à l'échelon stratégique, pour les organes de conduite, et et à l'échelon tactique. A cet effet, une communication fiable, un échange d'informations sécurisé et une transmission efficace de l'alarme à la population sont indispensables.

L'importance de la collaboration entre tous les partenaires et, partant, des systèmes de télécommunication, est illustrée ci-après à l'aide des trois scénarios *acte terroriste*, *séisme* et *pénurie d'électricité*.

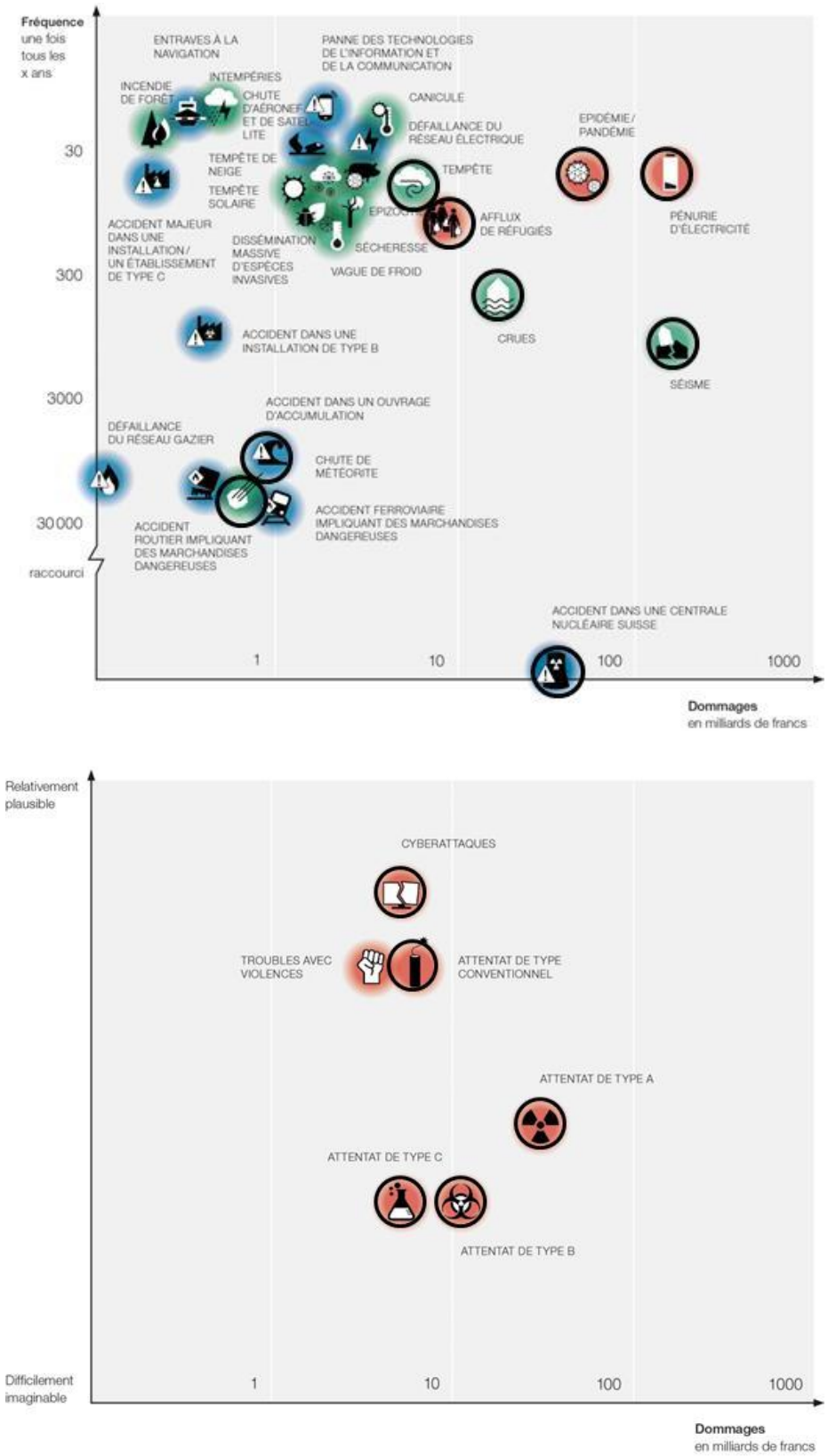
*Exemple : acte terroriste en Suisse*

Lors d'une vague d'attentats terroristes perpétré par exemple dans plusieurs cantons, toutes les forces de sécurité sont intégrées en très peu de temps aux opérations d'intervention et l'événement prendrait rapidement une ampleur nationale. Les activités policières en matière de sécurité (protection et sauvetage, bouclage de zones, aide aux victimes, intervention, recherche, préservation des preuves, etc.) relèvent des cantons. Chaque police cantonale prend sur son territoire les mesures qui s'imposent. Selon l'ampleur de l'événement, l'état-major national de conduite de la police intervient pour coordonner les actions et la police cantonale peut recevoir l'aide subsidiaire de l'armée. Soutenant le Ministère public de la Confédération, l'Office fédéral de la police (fedpol) est chargé de la recherche aux plans national et international de même que de la coopération avec les autorités policières d'autres pays en collaboration étroite avec l'état-major national de conduite de la police. La Direction générale des douanes (Cgfr) accroît les contrôles de sortie. Le Service de renseignement de la Confédération (SRC) veille à ce que tous les organes raccordés à la présentation électronique de la situation (PES CENAL) par le renseignement intégré du SRC disposent, par l'intermédiaire de la PES CENAL, d'une vue d'ensemble uniforme ainsi que d'une évaluation de la situation régulièrement mise à jour. Pour servir la coopération et la coordination internes, un comité de coordination opérationnel pour lutter contre le terrorisme est créé à partir de 2017 au niveau fédéral avec le concours des cantons[4]. D'autres organismes, comme le Département fédéral des affaires étrangères (DFAE), sont également mobilisés dans un bref délai (victimes étrangères, coopération rapide au niveau diplomatique).

---

[3] OFPP (2015) Catastrophes et situations d'urgence en Suisse : rapport technique sur la gestion des risques.

[4] Stratégie de la Suisse pour la lutte antiterroriste du 18 septembre 2015




**Légende** : Diagramme des risques pour les scénarios dont on peut estimer la fréquence (en haut) ou la plausibilité (en bas). Les scénarios dont la gestion nécessite la collaboration nationale, aux niveaux de la conduite (stratégique) et de l'intervention (tactique), de toutes les autorités et organisations responsables du sauvetage et de la sécurité et des exploitants d'infrastructures critiques sont entourés d'un cercle noir. Cette collaboration est requise pour coordonner les mesures de protection de la population.

*Exemple : tremblement de terre à Bâle*

Lors d'un fort séisme suivi par de nombreuses répliques intenses, comparable à celui de 1356 à Bâle[5], il faut s'attendre, dans la zone sinistrée d'un rayon de 160 km, à plusieurs milliers de morts et plusieurs dizaines de milliers de blessés. Au cours des premières heures et des premiers jours qui suivent la catastrophe, plus d'un demi-million de personnes ont besoin de l'aide des autorités, leurs maisons étant inhabitables et l'approvisionnement en eau et en vivres interrompu. Dans la zone touchée, l'alimentation électrique et le réseau de communication tombent en panne immédiatement après le tremblement de terre et restent hors service pendant plusieurs semaines, voire plusieurs mois. Les voies de communication y sont en partie coupées. Les transports sont perturbés dans l'ensemble du pays. Durant les premières minutes qui suivent le séisme, la Confédération, par l'entremise du Service sismologique suisse (SED) et de la Centrale nationale d'alarme (CENAL), diffuse des informations à ce sujet (magnitude, épicentre). Le sauvetage des personnes ensevelies dans les décombres, les soins médicaux, le bouclage des voies d'accès, l'hébergement des sans-abri et autres mesures entrent dans les compétences des cantons concernés, qui coordonnent l'intervention et les mesures ad hoc. En fonction de l'étendue de la catastrophe, toutes les forces de sauvetage et de sécurité disponibles dans les autres cantons sont déplacées dans la zone sinistrée en vue de renforcer les équipes d'intervention sur place. En l'espace de quelques heures, la CENAL reçoit des offres d'aide de l'étranger. L'entrée en Suisse d'organisations de secours étrangères est coordonnée par le DFAE avec l'aide de l'Office fédéral de l'aviation civile (OFAC), de la Direction générale des douanes (DGD), de l'exploitant de l'aéroport concerné et de la police cantonale compétente. Les ressources disponibles à l'échelon national et international sont attribuées par l'Etat-major fédéral ABCN (EMF ABCN) conformément aux besoins et en fonction des compétences prévues dans la zone sinistrée. Au bout d'un ou deux jours, les forces de sauvetage et de sécurité civiles sont soutenues par l'armée dans le cadre de son engagement subsidiaire. Pendant toute la durée de gestion de l'événement, l'Office fédéral de météorologie et climatologie (MétéoSuisse) fournit des informations météorologiques destinées aux équipes de sauvetage, aux autorités aux très nombreuses opérations héliportées de la zone sinistrée. De plus, la CENAL diffuse des informations à tous les organes fédéraux et cantonaux et aux exploitants d'infrastructures critiques. La détermination de la situation en matière de sécurité dans les centrales nucléaires et les autres entreprises soumises à l'ordonnance sur les accidents majeurs ainsi que dans les ouvrages d'accumulation situés dans la zone sinistrée ou à proximité de celle-ci est de la compétence de l'Inspection fédérale de la sécurité nucléaire (IFSN) et du Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), respectivement, qui transmettent leurs informations à la CENAL et aux organes de conduite cantonaux chargés de prendre d'éventuelles mesures de sécurité pour la population (alarme par sirènes, évacuation). D'autres exploitants d'infrastructures critiques (Office fédéral des routes [OFROU], CFF, Swissgrid, usines chimiques, etc.) sont en contact avec la Confédération et les cantons, qu'ils informent de la situation dans leur domaine respectif. Ces données sont agrégées par l'EMF ABCN pour constituer un tableau consolidé de la situation nationale (résultat du réseau de suivi de la situation).(puis transmises au Conseil fédéral, qui se fonde sur elles pour prendre des décisions. Toutes les activités visant à maîtriser l'événement s'étendront ainsi sur plusieurs mois.

*Exemple : pénurie d'électricité*

En cas de pénurie d'électricité, par exemple après une période de sécheresse prolongée ou en période de surconsommation électrique, le courant restant doit être géré[6]. Dans une telle situation, des régions définies de l'ensemble du pays sont à tour de rôle privées d'énergie électrique pour quelques heures. Il en résulte que tous les systèmes et appareils à fonctionnement électrique seront hors service pendant cette durée et dans les zones concernées, à moins qu'ils ne disposent d'une alimentation de secours. En outre, des coupures de courant incontrôlées sont prévisibles dans les régions qui ne sont pas touchées par cette mesure. L'Organisation chargée de l'approvisionnement électrique lors de situations extraordinaires (OSTRAL) est responsable, avec les fournisseurs d'électricité cantonaux, de l'application du plan d'interruption. L'OSTRAL et les distributeurs cantonaux s'informent mutuellement du déroulement des mesures. La mise en œuvre des mesures en faveur de la sécurité des ré-

---

[5] Selon les critères d'estimation utilisés aujourd'hui, le séisme survenu en 1356 à Bâle a atteint une magnitude de 6,0 à 7,0. Il s'agit du plus fort tremblement de terre jamais enregistré en Europe au nord des Alpes.

[6] En décembre 2015, Swissgrid, la société nationale pour l'exploitation du réseau électrique, avait adressé une requête à l'Office fédéral de l'énergie (OFEN), qui l'a transmise à l'EMF ABCN, pour discuter de mesures qu'elle jugeait utiles en raison d'un risque réel de pénurie d'électricité dû aux bas niveaux de remplissage des lacs de retenue, aux faibles débits des rivières et à l'interruption de la production électrique dans deux centrales nucléaires. Cette situation critique s'est détendue au cours du mois de février 2016. La situation était également critique en 2016/2017.

gions touchées par la mise hors circuit temporaire relève des cantons. Une collaboration coordonnée entre les diverses autorités fédérales et cantonales et les exploitants d'infrastructures critiques, par exemple Swissgrid, étant requise, les parties se tiennent mutuellement informées de l'évolution de la situation et des mesures à prendre. Les principales entreprises de transports publics, CFF et CarPostal Suisse, informent l'organe directeur de la Coordination des transports en cas d'événement (CTE), rattaché à l'Office fédéral des transports (OFT), sur la situation des transports publics en Suisse. L'OFROU informe quant à lui les cantons de la situation sur les routes nationales. Pendant toute la durée de pénurie, l'approvisionnement de la population en biens (eau, denrées alimentaires) et services (soins médicaux, espèces, télécommunications, etc.) importants est perturbé ou interrompu dans l'ensemble du pays, puisque les systèmes de communication et de commande des exploitants de ces infrastructures critiques ne fonctionnent pas normalement et qu'ils ne sont pas raccordés à un réseau à toute épreuve. La Banque nationale suisse (BNS) est reliée à des banques d'importance systémique du fait que l'approvisionnement en numéraire est restreint et que les services de paiements sont interrompus.

**Besoins en information et informations-clef**

*Exemple : attaque terroriste*

Lors d'un tel événement, les réseaux de communication publics sont très vite surchargés ou sont mis hors service pour des raisons tactiques. Cependant, si les AOSS utilisent pour leurs communications des connexions priorisées sans fil à large bande, elles évitent plus ou moins complètement de telles situations de surcharge. Vu la dimension de l'événement et le nombre d'intervenants, le réseau Polycom est lui aussi surchargé. Les intervenants doivent donc pouvoir échanger sur un réseau de communication mobile à large bande sécurisé (CSFLB). La coordination des cantons entre eux et des organes de conduite de la Confédération avec les cantons nécessite en outre un suivi de la situation actualisé pour tous les organes de conduite concernés. Les autorités et les organes de conduite devraient échanger ces informations via un réseau de données sécurisé (RDS).

La police cantonale (front et conduite), d'autres organisations d'intervention d'urgence, le SRC, l'Etat-major de conduite Police, fedpol et l'Etat-major « Prise d'otage et chantage », le Corps des gardes-frontières (Cgfr) et l'armée ont besoin d'informations concrètes sur la situation pour effectuer des recherches, communiquer et gérer des événements efficacement. Ces informations doivent être coordonnées et transmises à temps aux échelons correspondants des services concernés. A l'heure actuelle, aucune solution adéquate n'existe à l'échelle nationale.

Les informations-clef doivent pouvoir être diffusées en l'espace de quelques minutes voire quelques heures concernent par exemple la recherche de personnes, les investigations en cours ou encore des informations entre les états-majors de conduite de la police, en particulier sur les interdépendances tactiques des événements et sur les victimes. Ces informations doivent être traitées rapidement et pouvoir être transmises aux services concernés en Suisse comme à l'étranger mais aussi au Cgfr, chargé d'effectuer des mesures de recherches aux frontières.

Parmi les autres informations importantes on compte également les données sur les moyens à disposition (organisations de première intervention, possibilités d'intervention, état, disponibilité), les communications nationales sur le contrôle et la surveillance et les résultats d'enquêtes (vérification de l'identité de l'auteur, environnement, moyens utilisés, perquisition). Ces informations doivent être rapidement comparées et consolidées à l'échelon national afin de pouvoir synchroniser l'arrestation de l'auteur du délit. L'échange rapide d'informations entre les autorités judiciaires et les autorités étrangères via le Ministère public de la Confédération et l'Office fédéral de la police est essentiel.

*Exemple : séisme*

Après un important séisme, les organes de conduite (états-majors de conduite cantonaux, état-major fédéral) ont besoin rapidement d'une vue d'ensemble des régions touchées et du nombre approximatif des victimes (morts et blessés) ainsi que d'informations de la part des services spécialisés (IFSN, CENAL) et des exploitants d'infrastructures critiques pour mettre en place des mesures de sauvetage, de secours et de protection (moyens, organisations de première intervention) efficaces. Les informations sur la situation doivent être coordonnées et transmises à temps aux échelons correspondants des services concernés afin de sauver autant de vies que possible et protéger les équipes de sauvetage. A l'heure actuelle, aucune solution adéquate n'existe à l'échelle nationale.

Parmi les informations importantes qui doivent être transmises aux organes de conduite, aux organisations du sauvetage suisses et étrangères et à d'autres organisations de secours, on trouve des

informations sur les dommages causés aux bâtiments, aux routes et à d'autres infrastructures critiques. Les organisations d'intervention ont besoin d'obtenir rapidement des informations régulièrement mises à jour sur le nombre de victimes, sur l'accès aux zones sinistrées et sur la météo. Outre les informations sur les conséquences d'un événement pour la population, les services concernés ont aussi besoin de recevoir au plus vite des renseignements sur les risques que constituent les infrastructures critiques endommagées pour la population et les services de sauvetage. Parmi ces informations figurent également des renseignements concernant la sécurité des barrages ou des centrales nucléaires ainsi que les éventuelles mesures de protection à prendre par la population suite à une rupture de barrage ou à une possible dissémination radioactivité.

Les informations sur les moyens (organisations de première intervention, possibilités d'intervention, état, disponibilité), les mesures de sauvetage et de secours ainsi que sur les répliques et les zones de danger sont aussi de grande importance. Ces informations doivent être rapidement comparées et consolidées à l'échelon national afin de pouvoir organiser au mieux les secours et garantir la sécurité des organisations de première intervention.

*Exemple : pénurie d'électricité*

Les organes de conduite aux échelons fédéral et cantonal ont besoin d'obtenir régulièrement des informations sur la situation en matière de trafic, de sécurité et de distribution des biens dans les régions concernées. Pour gérer l'électricité en cas d'événement, les organes de conduite fédéraux ont besoin d'obtenir régulièrement (chaque heure / chaque jour) des informations sur les coupures prévues et effectuées ainsi que sur les utilisateurs concernés par le contingentement de l'électricité (en particulier les exploitants d'infrastructures critiques). Cela permet d'adapter la gestion de l'électricité et un retour rapide à la normale.

Les informations urgentes à l'échelon cantonal sont destinées aux organes de conduite et aux organisations de première intervention. Elles concernent les dommages collatéraux occasionnés par les coupures d'électricité dans une région donnée (accidents de la route, panne d'infrastructures critiques comme les hôpitaux, les stations d'épuration). Elles permettent de garantir la sécurité et la protection de la population dans les régions touchées.

**Conclusions**

Le risque et la plausibilité de tels événements en Suisse sont relativement élevés. L'expérience faite à l'étranger a montré que tous les intervenants ont besoin de disposer dans les plus brefs délais d'une vue d'ensemble de la situation pour maîtriser rapidement et efficacement des situations aussi complexes, et les empêcher de faire d'autres blessés, victimes et dommages matériels. C'est à cela que sert un réseau de suivi de la situation. En cas d'événement, un système de communication destiné aux autorités qui soit à l'épreuve d'une panne d'électricité et protégé contre les cyberattaques est une condition sine qua non pour que les organes de conduite stratégiques puissent ordonner des mesures visant à protéger la population concernée et les biens matériels importants. Pour faire face à un tel scénario, la communication vocale et la transmission de données doivent à tout moment être garanties sans aucune interruption. Or l'expérience nous apprend que précisément dans de tels cas, les moyens et réseaux de communication publics ne sont pas disponibles ou, le cas échéant, qu'avec certaines restrictions. Lors des récents attentats terroristes à Paris et à Bruxelles, les réseaux de communication sont tombés en panne pour plusieurs heures, ce qui a considérablement entravé la coordination des organisations de première intervention. Lors des attentats de Boston en 2013, les réseaux ont été mis hors service pour des raisons de sécurité. Cette situation peut être évitée de nos jours par l'utilisation de produits des AOSS. Il convient d'examiner attentivement cette option. Dans le cas de forts tremblements de terre ou d'une pénurie d'électricité telle qu'elle est décrite ci-dessus, la communication entre les organes concernés serait encore compliquée par le risque de perturbation, voire de panne des réseaux. Dans une telle situation, la communication et l'échange d'informations revêtent cependant une importance primordiale pour assurer la sécurité de la population au moyen d'une coordination de la gestion et de la mise en œuvre des mesures requises. Seuls des réseaux de communication et de données résistant aux crises permettent aux AOSS d'agir de manière coordonnée et efficace et de préparer et transmettre des bases décisionnelles consolidées à l'échelon stratégique afin de prévenir des dommages supplémentaires. Tel est l'objectif du RDS/Polydata à l'échelon stratégique et du projet CSFLB à l'échelon opérationnel et tactique.

## 2.2 Niveau et lacunes de sécurité actuels

Pour trois raisons importantes, le niveau de sécurité actuel est insuffisant sur les plans de la communication, de l'échange d'information et de la transmission de l'alarme à la population :

- Les réseaux et services de communication utilisés ne satisfont pas dans toutes les situations aux exigences relatives à la gestion d'un événement en raison de leur vulnérabilité aux pannes d'électricité et aux cyberattaques.
- Il n'est pas possible au moyen des systèmes actuels d'obtenir dans tous les domaines une vue d'ensemble consolidée de la situation qui soit complète et à l'épreuve des pannes.
- De nos jours, l'alarme par sirènes et radio n'atteint qu'une partie de la population. Les personnes souffrant de certains handicaps, par exemple les malentendants, ne la perçoivent pas.

**Utilisation de réseaux et de services de communication publics pour la gestion d'un événement**

Pour communiquer au niveau de la conduite et dans le cadre des interventions, les AOSS ont recours à des services de données à large bande. Pour l'échange de grandes quantités de données (p. ex. photos, vidéos, valeurs mesurées) ou l'utilisation d'applications telles que le système d'information et d'intervention du Service sanitaire coordonné (SII du SSC), la Confédération et les cantons font actuellement appel à divers réseaux et services publics dont le fonctionnement exige généralement l'achat de prestations de Swisscom ou d'autres fournisseurs privés. De plus en plus, les informations sur des événements et les consignes de comportement destinées à la population sont diffusées par téléphone mobile (p. ex. crues de l'Aar dans le quartier de la Matte à Berne). Les sirènes ne sont déclenchées que dans une situation d'urgence extrême.

Les plates-formes de communication courantes sont vulnérables dans la mesure où elles ne sont pas à l'abri d'une crise.

- Des pannes d'électricité prolongées, qu'elles soient dues à une défaillance technique ou à un événement naturel ou encore à une cyberattaque ciblée contre les exploitants des réseaux, peuvent avoir pour effet que ces systèmes ne sont plus disponibles après une brève durée déjà.
- Lors de manifestations de grande ampleur et en cas d'événement, la communication des AOSS risque de ne plus être garantie si elles ne disposent pas de canaux prioritaires.
- Lors de dommages physiques dus à des catastrophes naturelles, des attentats, des sabotages ou des défaillances techniques, on peut supposer que ces réseaux de communication ne seraient dans le meilleur cas pas rétablis avant quelques jours, voire plusieurs semaines ou mois.

Or, c'est justement pour maîtriser ces situations que les AOSS et les exploitants d'infrastructures critiques ont besoin de systèmes de communication à toute épreuve et donc hautement disponibles, de même que d'organisations d'exploitation disponibles en continu, donc également en cas de catastrophe. Il faut prendre les mesures nécessaires pour améliorer la disponibilité et la résistance aux crises des infrastructures existantes. Les AOSS peuvent ainsi faire prioriser leurs communications afin d'éviter le risque de limitations en cas de surcharge des réseaux publics (en cas d'événement majeur ou de grande manifestation).

**Absence d'un instrument servant à obtenir une vue d'ensemble consolidée de la situation**

A l'heure actuelle, il manque un outil à l'épreuve des défaillances et polyvalent permettant, en cas de catastrophe et de situation d'urgence, d'établir une vue d'ensemble consolidée de la situation à partir des informations des cantons, des organes fédéraux et des exploitants d'infrastructures critiques, et qui soit accessible avec ou sans fil aux utilisateurs. Un tel système serait toutefois nécessaire à la collaboration entre les nombreux partenaires chargés de la gestion de catastrophes et de situations d'urgence. Les organes de conduite de la Confédération (p. ex. l'EMF ABCN) et des cantons ont besoin d'un aperçu de la situation à l'échelle suisse pour leurs processus de décision. En regroupant les informations concernant la situation individuelle des partenaires concernés, un tableau ainsi étayé pourrait fournir aux organes de conduite les bases de décision dont ils ont besoin lors d'événements mettant en jeu la sécurité et la protection de la population au plan national. Les systèmes actuellement utilisés ne permettent pas de couvrir les besoins en informations urgentes des services concernés en cas de catastrophe ou de situation d'urgence ni les besoins en informations sur le suivi aux échelons donnés même si l'approvisionnement en énergie et les moyens de communication fonctionnent.

Manque d'accessibilité de l'alarme

L'alarme par les sirènes et les informations radio consécutives ne touche qu'une partie de la population. Elle n'est pas accessible à certaines personnes en situation de handicap (p. ex. les malentendants). C'est aussi le cas des étrangers non résidants qui ne connaissent pas les signaux d'alarme et ne comprennent pas forcément les messages diffusés dans les langues officielles ni ne les captent. Il manque actuellement des canaux d'alarme permettant d'atteindre davantage de personne ainsi que des groupes vulnérables et correspondent aux habitudes de la population en matière d'information.

## 2.3 Exigences en matière de prestations de télécommunication et niveau de sécurité visé

Les risques qui limitent, voire excluent l'utilisation de nouveaux supports et formes de communication servant à la protection de la population appellent des mesures concrètes. Le développement des systèmes de télécommunication de la protection de la population, tel qu'il est planifié à moyen terme, tient compte des besoins des AOSS et de la population ainsi que des systèmes existants et devrait relever le niveau de sécurité en Suisse. Les projets de télématique décrits dans le présent rapport devraient améliorer sensiblement la conduite des interventions en mettant à disposition des bases de décision complètes en peu de temps et combler les lacunes existantes en matière de sécurité dans le système de protection de la population.

Les autorités et organisations d'intervention doivent disposer, pour toutes les situations mettant en jeu la protection de la population, de systèmes de communication et d'alarme efficaces, sûrs et performants. Ceux-ci doivent en effet pouvoir servir aussi bien à maîtriser des événements non exceptionnels qu'à gérer des catastrophes et des situations d'urgence autrement plus complexes. À cet effet, les systèmes de télécommunication doivent être améliorés sous les aspects suivants :

*Améliorer la sécurité et la disponibilité des systèmes de communication et d'alarme*

La sécurité et la disponibilité des systèmes de télécommunication doivent être améliorées, en améliorant leur résistance aux cyberattaques et aux pannes d'électricité.

*Garantir la disponibilité opérationnelle des systèmes en toute situation*

La capacité de ces systèmes et processus de garantir la continuité de la gestion des activités (*business continuity management*, BCM) revêt une importance primordiale. Outre des mesures techniques, une haute disponibilité et la résilience des systèmes en toute situation supposent une organisation d'exploitation disponible en permanence afin de pouvoir assurer un fonctionnement ininterrompu du réseau et une élimination rapide des dérangements.

*Garantir l'accessibilité des informations sur la situation pour tous les partenaires du RNS*

De nombreux risques ayant des conséquences graves pour la sécurité de toute la Suisse et de la population et de ses bases d'existence requièrent une procédure coordonnée de la part de la Confédération et des cantons. A cet effet, les partenaires intégrés au RNS doivent pouvoir accéder en temps réel à des informations complètes sur la situation.

*Augmenter la communication mobile à large bande pour les organisations d'intervention*

L'accès aux banques de données, aux informations sur la situation ou aux services d'information géographique (SIG) doit être garanti à tout moment aux organisations d'intervention. L'infrastructure de communication mobile à large bande doit être étendue aux régions peu ou non desservies.

*Inclure les terminaux mobiles dans la transmission de l'alarme à la population et son information*

Il est nécessaire d'intégrer les terminaux mobiles (p. ex. smartphones, pagers) en tant que supports pour l'alarme et la communication en cas d'événement afin que la population puisse, dans une telle situation, être avertie et informée par les canaux utilisés au quotidien et ainsi adopter un comportement adéquat.

# 3 Communication entre les AOSS

La communication entre les organisations et l'échange d'informations sont d'une importance cruciale pour la maîtrise d'événements. À défaut, les AOSS ne sont pas en mesure de coordonner leurs activités et d'assurer un engagement efficace.

À l'étranger, la transformation numérique a déjà amené différentes innovations relatives à l'échange de données par large bande. Suite aux études sur des pannes électriques majeures et les écoutes téléphoniques de responsables politiques, l'Allemagne a procédé à l'installation d'un réseau de transport central sécurisé, le « KTN Bund ». C'est en 1990 déjà que l'Autriche a jeté les bases d'un réseau de données national reliant environ 1200 postes de police. Il a été étendu jusqu'en 2010 par des applications supplémentaires comme la téléphonie et la radiocommunication numérique BOS Austria et équipé des dispositifs de protection nécessaires. La Finlande et la Belgique font leurs premières expériences dans l'utilisation de systèmes proches de la CSFLB. Les États-Unis ont entamé d'importants travaux suite aux problèmes de communication rencontrés par les AOSS lors des attaques terroristes du 11 septembre 2001 : FirstNet doit permettre d'assurer auprès des organisations de sauvetage et de sécurité une communication mobile de données ininterrompue.

Aujourd'hui, les AOSS communiquent dans toute la Suisse via Polycom, un réseau radio numérique homogène, à ressources partagées, spécialement adapté à la sécurité publique. Plus de 55 000 membres des AOSS y recourent dans leur travail quotidien, par exemple en cas d'accident de la circulation et d'incendie, ainsi que lors de grandes manifestations comme la Street Parade à Zurich, ou le WEF à Davos, lequel intègre aussi à titre subsidiaire des militaires dans l'intervention globale. Vu que Polycom permet à toutes les AOSS de Suisse communiquer entre elles à travers tout le pays, elles y recourent aussi en cas de catastrophe et de situation d'urgence exigeant leur collaboration.

Pour les AOSS, la numérisation de la communication et de l'échange d'informations des dernières années a entraîné un accroissement des besoins en services de données offrant un débit de transfert élevé (à large bande). De tels services améliorent nettement la communication et l'échange d'informations dans le cadre d'une intervention. L'accès à des informations comme des photos (p. ex. images satellitaires), des systèmes d'information géographique (p. ex. cadastres des dangers), des applications de présentation électronique de la situation (p. ex. PES CENAL) et des banques de données notamment, peut être utilisé par chaque organe lors d'une intervention.

La communication de la Confédération et des cantons se base d'une part sur des réseaux propres (p. ex. réseau de l'administration fédérale, réseau de transmission de données entre les cantons et l'administration fédérale [KomBV-KTV], réseau de conduite suisse mis en place par l'armée, réseaux de police cantonaux) et, d'autre part, sur de nombreux réseaux et services publics pour l'exploitation desquels des prestations de Swisscom ou d'autres sociétés privées sont généralement achetées. Ces réseaux ne présentent toutefois pas le niveau de sécurité visé dans le domaine des systèmes de télécommunication de la protection de la population.

Les principaux systèmes de communication existants et les projets mis en discussion sont exposés en détail ci-après.

L'ordre de priorité compte tenu des possibilités de financement est exposé au chapitre 5. Comme on peut le voir, ces systèmes sont importants pour la sécurité de la population et leur réalisation est souhaitable, mais tous ne peuvent pas être financés et donc réalisés, actuellement du moins.

## 3.1 Polycom 2030[7]

Le projet destiné à maintenir la valeur de Polycom jusqu'en 2030 représente un investissement dans le système existant. Comme Polycom a été mis en service en plusieurs phases, de 2001 à 2015, les premières stations de base devront être remplacées ces prochaines années.

Les dépenses de la Confédération pour le maintien de la valeur de Polycom (composants nationaux) s'élèvent pour la période 2016 à 2030 à 500 millions de francs.

Le Conseil fédéral a proposé au Parlement un crédit d'engagement de 159,6 millions de francs pour le maintien de la valeur de Polycom[8] qui comprend, pour les prestations de tiers, 94,2 millions de francs

---

[7] Le projet Polycom 2030 est mentionné par souci d'exhaustivité. Il ne fait pas l'objet des mesures prioritaires du présent rapport car son financement a déjà été décidé en décembre 2015.

[8] Décision du Conseil fédéral du 25 mai 2016 concernant le message relatif au maintien de la valeur de Polycom jusqu'en 2030.

en faveur de l'OFPP et 65,4 millions de francs en faveur du Corps des gardes-frontières (Cgfr). Le crédit d'engagement a été approuvé par la Parlement en 2016 A cela s'ajoutent les prestations propres de l'OFPP pour un montant de 45,6 millions de francs et celles du Cgfr pour 161 millions de francs. Les coûts d'exploitation à la charge de l'OFPP jusqu'en 2030 s'élèvent à 120 millions de francs. Le Parlement a approuvé pour 2016 un crédit supplémentaire de 13,8 millions de francs pour les travaux de développement urgents. L'OFPP est responsable de ce projet.

Outre leur participation aux coûts d'exploitation, les cantons doivent prendre en charge les coûts liés au maintien de la valeur des composants décentralisés, à savoir le rééquipement des stations de base, qui n'est pas financé par le Cgfr[9]. Le rééquipement se fait selon l'âge des composants techniques des stations de base. Il devrait être terminé d'ici fin 2025.

## 3.2 Réseau de données sécurisé et système d'accès aux données Polydata

Aujourd'hui, la communication de données à large bande sur le réseau fixe des AOSS et des exploitants d'infrastructures critiques passe par le réseau de l'administration fédérale, le réseau de transmission de données entre les cantons et l'administration fédérale, les réseaux de police cantonaux ou via des réseaux de fournisseurs de prestations publics (p. ex. Swisscom).

En situation normale, particulière ou extraordinaire les systèmes et les réseaux par fil ne garantissent pas un flux de données et d'informations fiable, régulier et disponible en temps utile. En cas d'événement, ils peuvent être hors service à cause d'une surcharge, d'une panne d'électricité ou de cyberattaques. La collaboration coordonnée en cas d'événement entre tous les niveaux, à savoir la conduite, la communication, l'information et la transmission de l'alarme, peut donc s'en trouver limitée, voire empêchée. Cela pourrait avoir de graves conséquences pour la population si des mesures de protection nécessaires dans le cadre de la maîtrise de l'événement ne pouvaient pas être mises en œuvre, ou de manière insuffisante ou trop tardive.

La mise en place du RDS et de Polydata augmenterait la sécurité de la communication et de l'échange de données entre les AOSS en cas de panne ainsi que l'intégrité et la protection en cas de cyberattaque.

Le RDS (couches 1 et 2) est appelé à constituer la base de tous les systèmes de télécommunication de la protection de la population qui ont trait à la politique de sécurité. Il s'agit d'un réseau de transport à large bande permettant la transmission de grandes quantités de données. Ce réseau servira de réseau central de transport pour la protection de la population et pour la gestion nationale des crises.

Le RDS se base sur des composants physiques du réseau de conduite suisse, à savoir les fibres optiques et les infrastructures. Lorsque le réseau de conduite suisse est insuffisant, le raccordement est réalisé en utilisant les fibres optiques et les infrastructures physiques des réseaux existants de la Confédération, des cantons et des exploitants d'infrastructures critiques. Le RDS doit assurer la liaison à large bande entre les organes fédéraux, les cantons et les exploitants d'infrastructures critiques pendant au moins deux semaines, même en cas de pénurie d'électricité de longue durée, de panne de courant ou de défaillance des réseaux publics de communication. C'est pourquoi les infrastructures de réseaux qui répondent déjà à ces exigences seront intégrées dans la conception. Dans les autres cas, il convient de vérifier et d'améliorer le cas échéant la sécurité d'alimentation électrique de réseaux tiers.

Polydata est un réseau d'utilisateurs fermé (couche 3). On entend par là un réseau logique isolé dépourvu de connexion avec l'internet ou d'autres réseaux IP. Cet isolement augmente sensiblement la sécurité contre les cyberattaques. Le réseau Polydata garantira aux utilisateurs un accès sûr en toute situation aux systèmes d'alarme et de télécommunication dont la protection de la population a un besoin impérieux. L'utilisation des applications se fait à l'aide de terminaux dédiés. Étant donné qu'il s'agit d'un réseau fermé, aucune coordination avec d'autres réseaux IP n'est requise. Toutes les applications nécessaires à la protection de la population, existantes et futures, pourront être utilisées en toute sécurité sur le RDS, en combinaison avec Polydata.

Les applications de ce réseau sont Polycom, Polyalert, Polyinform et d'autres systèmes et applications importants pour la sécurité. La résilience par rapport aux cyberattaques est sensiblement augmentée par l'isolement vis-à-vis des autres réseaux (p. ex. l'internet). Polydata peut également être utilisé en temps normal et est basé sur les réseau de transport sécurisé RDS.

---

[9] Document « Maintien de la valeur du réseau de communication sécurisé Polycom » du 24.12.15 aux gouvernements cantonaux.

Le RDS et Polydata sont étroitement liés et ne peuvent être considérés, réalisés ou exploités séparément[10]. En effet, la réalisation de Polydata est indispensable pour assurer en tout temps l'accès sécurisé aux systèmes d'alarme et de télécommunication importants pour la protection de la population. Pour cette raison, investir uniquement dans le RDS, sans Polydata, n'aurait pas de sens.

### Synergies et interdépendances

Le réseau national des autorités de la Confédération et des cantons (KomBV-KTV, couche 3) relie la Confédération aux services cantonaux et communaux. Ce réseau IP logique se base sur des réseaux publics et des cantonaux. Son exploitation n'est pas garantie en cas de panne ou de pénurie d'électricité. En cas de réalisation du RDS, le réseau KomBV-KTV peut être exploité sur le réseau de données sécurisé, ce qui augmente considérablement sa sécurité en cas de défaillance. Les utilisateurs du réseau KomBV-KTV et du réseau des autorités peuvent combler ainsi des lacunes dans leur BCM.

Il est possible d'installer d'autres réseaux logiques sur le RDS, en plus de Polydata. Il s'agirait de réseaux qui exigent également une disponibilité optimale en cas de panne d'électricité ou d'infrastructure critique.

La réalisation de Polydata permet de développer des réseaux logiques existants, tel le réseau B-MPLS pour Polycom, et de les adapter aux nouveaux besoins des utilisateurs.

Les autres synergies restent à déterminer dans le cadre du projet du DFJP sur la surveillance des télécommunications aux fins d'enquêtes de police judiciaire.

### Conséquences d'une non-réalisation du RDS et de Polydata

Pour les partenaires de la protection de la population, renoncer au RDS et à Polydata signifierait qu'en cas d'événements causant des pannes ou des pénuries d'électricité ou encore des dysfonctionnements des réseaux de communication publics, ils n'auraient très vraisemblablement accès qu'à leurs instruments de conduite locaux. Cela aurait pour effet que les organisations qui doivent collaborer pour maîtriser un événement ne seraient plus en mesure de communiquer entre elles et d'échanger des informations. L'évaluation de la situation, la prise de décision ainsi que la maîtrise de l'événement en seraient considérablement entravées. Cela réduirait les capacités d'intervention des autorités, ce qui aurait pour conséquence une augmentation des effets dommageables d'une catastrophe. Suivant la nature de l'événement, il peut en résulter des conséquences graves pour la population. Le nombre de victimes et de blessés et des milliards de francs de dommages matériels pourraient être directement liés aux lacunes de la communication pour la conduite et les interventions ou à une transmission insuffisante de l'alarme à la population et à l'information lacunaire de celle-ci.

### Variantes

Lors de sa séance du 20 mai 2015, le Conseil fédéral a choisi la solution suivante (« solution 4 ») pour développer le RDS : la conception et les technologies du réseau de conduite suisse doivent soustendre le RDS. Au niveau physique (câble à fibre optique et stations), ce dernier doit se baser sur le réseau de conduite suisse et être complété par d'autres composants physiques de réseau dans le domaine du raccordement (notamment le réseau de l'OFROU mais aussi Swissgrid, le réseau des CFF, des réseaux cantonaux, etc.). Le RDS doit être réalisé de telle sorte que le trafic de données de l'armée sur le réseau de conduite suisse soit totalement séparé du flux de données des utilisateurs du RDS. On tiendrait ainsi compte des besoins de sécurité de l'armée. Conformément à la stratégie informatique de la Confédération 2016 – 2019, la BAC est chargée d'assurer l'exploitation et l'entretien (du RDS et de Polydata) 24 heures sur 24. Cela s'applique donc aussi à l'exploitation de Polydata. Dans le cadre de la future stratégie fédérale en matière de réseaux, il faudra désigner notamment les réseaux nationaux de télécommunication qui doivent s'appuyer sur une infrastructure appartenant à la Confédération ou seront (en partie) acquis sur le marché sous la forme de services. Dans le premier cas de figure, il faudra également désigner les prestataires de services informatiques internes exploitant ces réseaux ou ces couches de réseaux ainsi que les prestations d'exploitation qui pourraient être confiées à des fournisseurs externes.

[10] Pour simplifier, le RDS et Polydata ont été répartis entre deux lots de travail dans le cadre des tâches de conception.

## 3.3 Remplacement de VULPUS-Télématique

Le remplacement de VULPUS-Télématique comprend tous les travaux nécessaires au maintien des fonctions de l'actuel système télématique VULPUS après sa mise hors service.

VULPUS est un système protégé servant à la transmission de messages entre les autorités civiles de la Confédération et des cantons et des tiers. Il est employé depuis une trentaine d'années pour échanger des informations (principalement des messages) entre le Ministère public de la Confédération, les polices cantonales, la police municipale de Zurich, le Cgfr, la Sécurité militaire, la CENAL, le SRC, différents états-majors spéciaux du Conseil fédéral, l'OFPP et diverses unités d'alarme. Actuellement, VULPUS est utilisé pour la transmission de l'alarme ou de messages d'alerte en cas de danger naturel ainsi que dans le cadre d'opérations de recherche. Les informations ne sont pas transmises automatiquement mais par un opérateur responsable. Basé sur des réseaux civils et militaires, VULPUS est utilisé quotidiennement par les organisations et autorités mentionnées plus haut. VULPUS est actuellement exploité par l'armée, qui veille également au maintien de la valeur. L'armée n'a pour sa part pas besoin de VULPUS.

Les services apportés par VULPUS sont fondamentaux pour la communication des autorités et devront être disponibles au quotidien mais aussi en cas de catastrophe ou de situation d'urgence. VULPUS utilise actuellement le réseau de téléphonie analogique de Swisscom, dont les raccordements seront mis hors service dans un proche avenir. L'exploitation des raccordements est garantie jusqu'en 2022.

### Synergies et interdépendances

Il existe à l'heure actuelle plusieurs applications proposant des fonctions comparables ou identiques à celles de VULPUS. Moyennant quelques adaptations, elles pourraient remplacer VULPUS. D'après une étude portant sur la faisabilité technique ainsi que sur les exigences relatives à sécurité et à l'efficacité, de telles applications peuvent être développées et adaptées pour assurer les fonctions de VULPUS après sa mise hors service.

La réalisation du RDS et de Polydata et par conséquent l'exploitation des fonctions de VULPUS sur ces systèmes permettraient d'améliorer sensiblement la sécurité en cas de défaillance des nouvelles applications qui seraient également mieux protégées contre des cyberattaques.

### Conséquences de l'abandon du remplacement de VULPUS

VULPUS est arrivé au terme de son cycle de vie et son fonctionnement actuel nécessite des investissements trop élevés. S'il est possible d'abandonner le système VULPUS, on ne peut pas se passer de ses fonctionnalités, notamment la transmission de courriels sécurisés. Sans projet de remplacement de VULPUS, il n'est pas possible de mettre à disposition des ressources humaines et financières pour assurer les fonctionnalités de VULPUS.

### Variantes

Pour le remplacement de VULPUS, trois variantes peuvent être envisagées :

*Solution A*

L'actuel système VULPUS est entièrement remplacé par un nouveau système.

*Solution B*

Les fonctionnalités de VULPUS sont intégrées dans un système existant.

*Solution C*

Les applications utilisées par les AOSS, qui sont exploitées sur différents systèmes, sont développées et mises à disposition de sorte que les utilisateurs de VULPUS conservent un accès aux fonctionnalités de VULPUS.

## 3.4 Communication sans fil à large bande

Vu l'importance croissante de la communication de données sans fil pour les AOSS, les organisations doivent recourir actuellement à des réseaux publics, notamment ceux de Swisscom. Lors de manifestations planifiées de grande envergure ou en cas d'événements imprévus et soudains entraînant un important besoin en communications privées, les réseaux sont vite saturés, ce qui ralentit la transmission de données. Lors de l'utilisation de produits d'AOSS non prioritaires, le réseau peut même être entièrement mis hors service. En cas d'intervention, les AOSS ainsi que leurs partenaires doivent pouvoir disposer de connexions solides dont la disponibilité est garantie et qui résistent en cas de saturation du réseau.

Les infrastructures de réseaux commerciales sont conçues selon des considérations économiques. Les services à large bande des prestataires commerciaux offrent actuellement une couverture largement insuffisante surtout le long des frontières suisses, dans les régions alpines ainsi que dans des zones à faible densité d'habitation. Or, les AOSS qui interviennent dans toutes les régions de Suisse doivent pouvoir disposer de services à large bande qui assurent une couverture aussi complète que possible. Les lacunes géographiques peuvent être comblées par les AOSS au moyen de leurs propres infrastructures.

Les réseaux radio mobiles ne sont pas à l'épreuve d'une panne d'électricité, mais ne disposeraient que d'une autonomie d'une à quatre heures dans un tel cas. Les services de sauvetage et de sécurité ont cependant besoin de réseaux qui ne soient pas saturés par d'autres utilisateurs et qui restent disponibles plusieurs jours en cas de panne d'électricité.

La communication sans fil à large bande (CSFLB) pourrait donner aux AOSS de la Confédération (p. ex. Cgfr) et des cantons ainsi qu'aux exploitants d'infrastructures critiques l'accès à des services à large bande à haute disponibilité, également sur des réseaux mobiles. Cette interconnexion mobile des AOSS et des exploitants d'infrastructures critiques contribuerait à optimiser la collaboration, par exemple entre les organisations de première intervention sur la place sinistrée et la conduite à l'arrière. La CSFLB aurait impérativement besoin du Le RDS représente une excellent solution pour doter la CSFLB d'un réseau de transport pour le maillage des nœuds d'interconnexion. Les AOSS pourraient non seulement communiquer oralement avec Polycom mais aussi échanger de grands volumes de données, des photos et des cartes (réseau de suivi de la situation) et utiliser des applications (banques de données, systèmes d'information géographique etc.) sur des réseaux mobiles. On pourrait également utiliser des applications basées sur la CSFLB comme les conférences téléphoniques par smartphones. Différents corps de police recourent également à des tablettes pour tenir des rapports sur le terrain.

Actuellement, les AOSS utilisent déjà des infrastructures nationales à large bande sans fil mises à disposition par les opérateurs publics de téléphonie mobile. Selon les besoins, il est possible de les adapter progressivement aux exigences des AOSS en matière de disponibilité et de sécurité par des mesures techniques (renforcement et raccordement de zones non couvertes actuellement, protection contre les cyberattaques).

### Synergies et interdépendances

La CSFLB met une composante mobile à la disposition de tous les services et fonctions représentés dans les différents projets faisant l'objet du présent rapport. Les applications du réseau de suivi de la situation pourraient par exemple être intégrées dans les processus de travail sur le terrain, soit sur la place sinistrée. Cela assure en tout temps un accès sûr et à haute disponibilité aux données actuelles dont leurs utilisateurs ont besoin pour remplir leur mission dans toutes les situations. Les données qu'ils recueillent sur la place sinistrée peuvent en outre être enregistrées dans les systèmes de base en temps réel.

Afin de pouvoir offrir à toutes les AOSS une solution harmonisée pour couvrir leur besoin de disposer d'une communication des données sûre et résiliente jusqu'au terminal mobile, il convient d'envisager, en fonction des besoins, une extension mobile du RDS et du réseau IP d'accès aux données de Polydata à capacité réduite. Le RDS étant résilient en cas de panne électrique ou de cyberattaque, les partenaires de la protection de population disposeraient avec ce système en tout temps et en toute circonstance d'un réseau de transport sécurisé à haute disponibilité avec une composante fixe et une composante mobile.

La CSFLB pourrait remplacer Polycom après 2030/35, à condition que les applications de radiocommunication soient standardisées pour la communication numérique à large bande. Les liaisons de branchement, dont la capacité doit être élargie dans le cadre du développement de Polycom, pour-

raient être conçues de manière à pouvoir transmettre également les données mobiles et ce sans générer de coûts supplémentaires. Ainsi, en cas d'extension de l'infrastructure à large bande sans fil existante, des composants essentiels seraient déjà en place.

Il convient d'étudier les synergies potentielles entre la CSFLB et la télécommunication de l'armée et de les mettre à profit le cas échéant.

**Conséquences d'une non-réalisation de la CSFLB**

Les besoins de certaines AOSS étant d'ores et déjà importants, tout comme leur volonté de concrétiser des projets dans le domaine de la CSFLB (des tests sur le terrain sont déjà en cours), la non-réalisation de ce projet à l'échelle nationale pourrait inciter plusieurs cantons et grandes villes à mettre eux-mêmes en place de tels systèmes et infrastructures. Il en résulterait une coexistence de solutions techniquement différentes présentant aussi des différences au niveau de la disponibilité et des normes de sécurité ainsi qu'un grand nombre d'interfaces

Si la CSFLB devait remplacer Polycom, ces systèmes devraient être intégrés successivement dans une solution techniquement uniforme et applicable à l'échelon suisse, ce qui occasionnerait probablement à nouveau des frais importants, comme l'a montré l'expérience de Polycom.

Une non-réalisation de la CSFLB signifierait pour les AOSS qu'elles seraient empêchées de maîtriser certains événements ou que leur intervention serait moins efficace. Il pourrait en résulter des dommages aux personnes et aux biens ainsi que des coûts élevés dus à des retards dans le retour à la normale.

**Variantes**

Les technologies de transmission modernes permettent de développer des solutions répondant aux besoins des clients, en l'occurrence des AOSS, sur la base des infrastructures mobiles des opérateurs privés. On en trouve déjà sur le marché. Bien qu'elles ne requièrent pas l'attribution de nouvelles fréquences, l'OFCOM a néanmoins réservé des ressources en termes de fréquences à l'intention des AOSS pour d'éventuelles utilisations supplémentaires. Cette ébauche de communication sans fil à large bande se fonde sur un accord entre les AOSS, l'OFPP, la BAC et l'OFCOM. Elle est inscrite dans le Plan national d'attribution des fréquences (PNAF).

Solution A – *Opérateur public avec des produits commerciaux pour les AOSS*

Les prestations des AOSS se basent sur des réseaux de communication mobile publics et peuvent être étendues au besoin. Aucun nouveau réseau n'est installé. À la place, un accord est conclu avec un opérateur commercial qui fournit des prestations commerciales pour les AOSS en étant rémunéré. De plus, la couverture de zones qui ne disposant pas de raccordements peut être réglée par contrat.

Les AOSS n'ont pas besoin de spectres de fréquences supplémentaires.

La vulnérabilité par rapport aux coupures de courant et aux cyberattaques exige un renforcement.

Solution B – *Exploitation commune avec des opérateurs de réseaux mobiles privés sur la base d'un réseau de base AOSS*

Les AOSS exploitent leur propre réseau de base. Pour les communications radio, elles collaborent avec des opérateurs publics. Plusieurs options sont envisageables (MVNO, RAN-Sharing, etc.). Les fréquences supplémentaires réservées pour les AOSS (2x3 MHz et 2x5 MHz) peuvent en outre être utilisées pour couvrir des besoins complémentaires. Ces emplacements supplémentaires peuvent être intégrés dans des infrastructures de réseau existantes des opérateurs de téléphonie mobile. La gestion des terminaux et des applications ainsi que les aspects relatifs à la sécurité restent du domaine des AOSS.

La vulnérabilité par rapport aux coupures de courant et aux cyberattaques exige un renforcement.

Solution C – *Opérateur commercial avec réseau partiellement renforcé*

Une partie de l'infrastructure du réseau d'un opérateur commercial serait renforcée avec l'aide matérielle et financière de la Confédération, des cantons et des tiers, afin d'augmenter sensiblement sa résilience. Cette solution pourrait être développée de manière modulable.

La vulnérabilité par rapport aux coupures de courant et aux cyberattaques exige un renforcement.

## 3.5 Réseau national de suivi de la situation

Un réseau de suivi de la situation réunit les systèmes existants (PES) dans un tout. Les décisions stratégiques en situation de crise dépendent de plus en plus d'un réseau de suivi de la situation utilisable en permanence par les organes de conduite de la Confédération, les cantons et les exploitants d'infrastructures critiques. Toutes les organisations et autorités qui sont appelées à conduire et coordonner une intervention doivent pouvoir disposer d'une vue d'ensemble aussi complète que possible des informations nécessaires et disponibles. Un instrument fait cependant actuellement défaut ou n'est réalisé que partiellement dans des sous-secteurs, ce qui constitue une lacune dans la gestion de catastrophes en Suisse.

Ce déficit en matière de sécurité a également été identifié à l'occasion de l'ERNS 14. Le Conseil fédéral a pris connaissance, le 20 mai 2015, du rapport final concernant l'ERNS 14 et a approuvé les recommandations faites pour améliorer la préparation de la Suisse en cas de crise. Il a confié au DDPS la responsabilité de mettre en œuvre la recommandation 4 (suivi coordonné de la situation et PES CENAL). L'OFPP est ainsi chargé de prendre les mesures nécessaires pour comparer les informations et développer un outil commun (PES) pour présenter la situation générale et notamment étudier dans quelle mesure le flux des informations entre la Confédération et les cantons ainsi que la situation des infrastructures critiques peuvent y être intégrées.

Le réseau national de suivi de la situation fournirait les bases de connaissances requises en cas de catastrophe ou de situation d'urgence pour obtenir une vue d'ensemble consolidée de la situation, coordonner les divers services spécialisés, ordonner des mesures et garantir la gestion des ressources par la Confédération.

Différentes solutions existent d'ores et déjà au niveau cantonal. Le réseau national de suivi de la situation simplifierait la synthèse entre ces informations partielles grâce à un échange automatique de données validées et fournirait ainsi une vue d'ensemble des informations dont disposent les partenaires.

Le Réseau national de suivi de la situation permettrait d'améliorer et de simplifier sensiblement la collaboration des partenaires dans la maîtrise des catastrophes et des situations d'urgence à tous les échelons. Avec lui, il serait également possible de tirer davantage profit des informations fournies par les exploitants d'infrastructures critiques, ce qui rendrait la vue d'ensemble de la situation plus complète et plus pertinente. Le réseau devrait servir de source d'information centrale aux états-majors de conduite engagés (p. ex. l'État-major fédéral ABCN), qui pourraient ainsi proposer en connaissance de cause des mesures ad hoc aux décideurs tels que le Conseil fédéral.

Les partenaires, dont notamment les cantons, pourraient conserver leurs outils, qu'ils connaissent et qui ont fait leurs preuves, mais l'échange de données devrait se faire sur de nouvelles interfaces restant à créer et dans des formats communs tout en appliquant les directives communes.

### Synergies et interdépendances

Des partenaires importants du réseau national de suivi de la situation, en particulier les corps de police et le SRC, ont besoin de pouvoir échanger des informations classées confidentiel sur un système sécurisé. Ce réseau devrait donc être réalisé sur la base du RDS et du réseau fermé des utilisateurs de Polydata.

La présentation de la situation de l'État-major fédéral ABCN, de la CENAL et du SRC, dans sa configuration actuelle, repose sur la PES CENAL. Cette dernière devrait pouvoir être utilisée aussi dans le cadre du réseau national de suivi de la situation dans une version optimisée, afin de permettre une présentation synoptique de la situation à l'échelle nationale. Celui-ci ne pourrait actuellement pas être utilisé par l'État-major fédéral ABCN, et notamment par la CENAL, sans cette optimisation de la PES CENAL, car il serait impossible d'évaluer, de présenter ou de diffuser toutes les informations.. Les organes fédéraux et les cantons sont également dépendants des systèmes existants de traitement du suivi de la situation et de gestion des interventions.

### Conséquences d'une non-réalisation du réseau national de suivi de la situation

Si le projet n'était pas réalisé, cela rendrait impossible une vue d'ensemble consolidée en temps réel d'évènements survenant en Suisse. L'échange de données et d'informations continuerait de se faire en grande partie manuellement (par contacts personnels, téléphone, courriel) via des canaux et des systèmes non sécurisés. Comparée au réseau national de suivi de la situation, cette solution serait inefficace en termes de collaboration en cas de catastrophe ou de situation d'urgence touchant plu-

sieurs cantons ou la totalité du pays. Dans de telles situations, la conduite à l'échelon fédéral et cantonal serait considérablement entravée, ce qui se répercuterait sur la gestion des événements, car des éléments décisifs pourraient faire défaut. Concrètement, le manque de coordination dans le suivi de la situation signifierait que, dans le cas d'une menace ou d'une vague d'actes terroristes commis en plusieurs lieux en Suisse, par exemple, les organes de conduite et d'intervention ne disposeraient d'aucun outil consolidé pour la présentation de la situation.

**Variantes**

Selon les études préalables portant sur les différentes variantes, la création ou l'acquisition d'un même logiciel de suivi de la situation pour tous les partenaires poserait problème. D'une part, les organes concernés ont des tâches et des fonctions extrêmement différentes, d'où une grande diversité de processus et de solutions informatiques parfois très spécialisées. Une solution unique ne saurait répondre à tous ces besoins et représenterait une régression par rapport au statu quo. D'autre part, il ne serait pas opportun de remplacer les différents systèmes existants par un système unique en raison de la structure fédérale du pays et des investissements consentis dans les solutions actuellement utilisées.

Pour les raisons citées plus haut, les organes concernés se sont prononcés pour une solution permettant de relier les différents systèmes par des interfaces et des formats d'échange communs. L'objectif visé est d'aboutir à une solution décentralisée avec un minimum de composants centraux (principalement la gestion des droits et accès et des fonctionnalités de vue d'ensemble).

## 3.6 Maintien de la valeur de la présentation électronique de la situation de la CENAL[11]

La CENAL utilise la présentation électronique de la situation (PES) depuis une vingtaine d'années pour échanger des informations concernant le suivi de la situation. La version actuelle a connu sa dernière mise à jour technique lors de l'Euro 08 et doit être actualisée. Les exigences élevées du SRC en matière de sécurité rendent notamment nécessaire une reprogrammation.

La PES est également employée par fedpol pour les alertes en cas de kidnapping, par le centre de gestion de crises du DFAE en cas d'enlèvement de citoyens suisses à l'étranger et par le SEM dans le cadre de la crise migratoire.

Le maintien de la valeur de la PES CENAL a déjà été décidé afin de garantir aux partenaires du RNS l'utilisation des fonctionnalités actuelles du système jusqu'en 2020. Il permet également de l'adapter aux exigences du SRC en matière de sécurité. L'application sera mise à niveau afin de correspondre à l'état de la technique sans changer fondamentalement. Le projet de maintien de la valeur de la PES CENAL est mis en œuvre conjointement par la CENAL et le SRC sous la direction de l'OFPP.

**Synergies et interdépendances**

Il est prévu d'intégrer ultérieurement la PES CENAL au suivi de la situation. Il n'existe aucune interdépendance avec d'autres projets.

**Conséquences d'une non-réalisation du maintien de la valeur de la PES CENAL**

Le projet est actuellement mis en œuvre.

**Variantes**

Le projet se trouve déjà en phase de mise en œuvre. Les différentes solutions technologiques ont été étudiées préalablement.

[11] Le maintien de valeur de la PES CENAL est mentionné dans le présent état des lieux dans un souci d'exhaustivité. C'est pourquoi elle est présentée de manière succincte. Le projet ne fait en outre pas l'objet d'une priorisation au sein de ce rapport étant donné qu'il se trouve dans la phase de mise en œuvre.

## 3.7 Polysat

Polysat est un canal satellite à large bande qu'il est prévu d'utiliser de manière redondante pour la communication vocale et la transmission de données. Il permettrait notamment une connexion internationale de première importance dans la gestion de crises et de catastrophes. Celle-ci est très importante pour la coopération avec des organisations comme le mécanisme de protection civile de l'Union européenne (MPC UE), avec lequel un accord de collaboration a été conclu au printemps 2017.

L'ajout ponctuel de capacités de transmission garanties également en cas de crise et de catastrophe permettrait de créer des canaux supplémentaires pour le RDS et la CSFLB lors d'un séisme de grande ampleur survenant en Suisse. Des liaisons supplémentaires pourraient être établies très rapidement grâce à des unités mobiles.

### Synergies et interdépendances

Polysat permettrait une connexion souple et standardisée des systèmes de conduite et d'intervention aux plates-formes et organisations internationales qui ont des informations importantes à échanger. Le RDS offrirait les raccordements pour Polysat et Polydata garantirait l'authentification et l'identification requises des postes extérieurs nouvellement connectés. En même temps, Polysat créerait un système alternatif au réseau de fibre optique du RDS, assurant un fonctionnement sans interruption de celui-ci, même dans un scénario impliquant des destructions à grande échelle (p. ex. séisme de forte intensité). L'ensemble des partenaires de la protection de la population en profiteraient, de même que les organisations internationales et les organes de la Confédération. Les cantons frontaliers et les organisations d'intervention affectées aux zones frontalières auraient en outre la possibilité de connecter leurs systèmes de communication avec ceux des pays voisins.

### Conséquences d'une non-réalisation de Polysat

La non-réalisation de Polysat limiterait la connexion internationale de la communication en matière de conduite et empêcherait la redondance et l'augmentation des capacités à l'intérieur du pays.

### Variantes

En cas de catastrophe ou de situation d'urgence touchant la Suisse, les moyens de l'armée pourraient également être engagés après une certaine période afin d'offrir une aide subsidiaire pour le rétablissement des réseaux de communication (p.ex. systèmes d'ondes mobile), à condition que ces moyens soient disponibles à temps et que les ressources suffisent à établir plusieurs liens.

# 4 Alarme et information de la population

La transmission de l'alarme et l'information de la population sont des processus centraux visant à agir rapidement et efficacement en cas d'événement pour protéger celle-ci et ses bases d'existence. En Suisse, actuellement, les sirènes sont le seul moyen permettant d'avertir la population d'un danger imminent en cas de catastrophe ou de situation d'urgence et de diffuser ensuite par radio des consignes de comportement dans les 15 à 20 minutes qui suivent. Afin de pouvoir informer la population même si l'infrastructure émettrice des radiodiffuseurs est hors service, la Confédération dispose d'un réseau de diffusion d'urgence par radio OUC (information de la population par la Confédération en cas de crise, IPCC). La transmission de l'alarme par sirènes suivie de la diffusion d'informations à la radio et à la télévision a également cours en Israël, en Suède, en France et, en partie, en Allemagne. La Principauté de Liechtenstein est quant à elle raccordée au système de sirènes installé en Suisse.

Le système d'alarme par sirènes n'atteint qu'une partie de la population, car l'alarme sirène et la communication radio qui s'ensuit ne sont pas accessibles pour certaines personnes, telles que les malentendants ou les étrangers qui ne comprennent pas les consignes de comportement diffusées à la radio dans les trois langues officielles. C'est pourquoi il devrait être possible à l'avenir de transmettre l'alarme à la population menacée et d'informer celle-ci rapidement en se servant d'autres moyens qui viendraient s'ajouter à l'alarme par sirènes. Il s'agirait en premier lieu d'alarme et de communication par téléphone mobile, afin de transmettre les consignes de comportement aux personnes touchées ou menacées en particulier pendant la phase initiale de l'événement et de limiter ainsi autant que possible les dommages et répercussions éventuels. La téléphonie mobile permet de rédiger de telles informations en plusieurs langues. Les récents actes terroristes à l'étranger soulignent encore le besoin d'un tel système d'alarme et d'information supplémentaire. L'Allemagne dispose d'un système central soutenu par satellite qui permet, outre d'autres canaux de diffusion comme la radio et la télévision, d'utiliser également l'application sur téléphone mobile (NINA). Mis à part NINA, l'Allemagne connaît encore un produit d'un fournisseur privé, disponible sous l'appellation KATWARN, qui propose des fonctionnalités similaires à celles de NINA.

En France, une application baptisée SAIP (Système d'alerte et d'information des populations) a été développée après les actes terroristes de Paris et en prévision du Championnat d'Europe de football.

Les principaux systèmes d'alarme et d'information existants et les projets mis en discussion sont énumérés ci-après. L'ordre de priorité compte tenu des possibilités de financement est exposé au chapitre 5. Comme on peut le voir, ces systèmes sont importants pour la sécurité de la population et leur réalisation est souhaitable, mais tous ne peuvent pas être financés et donc réalisés, actuellement du moins.

## 4.1 Polyalert 2030

Polyalert 2030 désigne le projet visant à assurer le maintien de la valeur et le développement du système Polyalert, qui permet d'alerter la population au moyen des sirènes. Polyalert fonctionne indépendamment des réseaux de fournisseurs publics de télécommunications. Les aspects liés à la sécurité, à la disponibilité, à l'utilisation des synergies entre les réseaux existants, à la protection des investissements et le souci de disposer d'une liberté de manœuvre totale dans le cadre du développement du système ont conduit à utiliser Polycom comme réseau de transmission. Les sirènes disposent d'une réserve de courant pour un déclenchement multiple de l'alarme. Polyalert représente ainsi un système d'alarme utilisable en temps de crise, à l'échelle régionale ou nationale.

À l'heure actuelle, quelque 5000 sirènes fixes et 2800 sirènes mobiles sont exploitées pour transmettre l'alarme à la population. Lorsque la population est menacée, l'alarme générale est déclenchée dans la zone concernée. Elle est toujours suivie d'une communication à la radio (message ICARO[12]). La diffusion de l'alarme-eau (évacuation immédiate) se limite aux zones menacées situées en aval de 65 ouvrages d'accumulation.

Le déclenchement des sirènes est effectué en premier lieu directement par les organes de police et de conduite cantonaux ainsi que par les exploitants d'ouvrages d'accumulation. Les sirènes peuvent également être déclenchées en cas d'accident entraînant le rejet de substances chimiques dans l'atmosphère ou dans les eaux, comme lors de celui survenu dans l'usine chimique de Schweizerhalle en 1986. Elles peuvent l'être aussi en cas de crue, comme en 2005 dans les cantons de Lucerne et d'Obwald. Dans les cantons de Bâle-Campagne et de Zurich, les sirènes ont retenti en 2006 et en

[12] Information Catastrophe Alarme Radio Organisation. ICARO désigne le service d'information de la SSR dans les situations de crise et de catastrophe, mais aussi en cas d'événements exceptionnels ne revêtant pas un caractère de catastrophe.

2008 pour alerter la population à la suite d'une contamination ayant rendu l'eau potable insalubre. Elles seraient aussi déclenchées en cas de dissémination de substances radioactives pour alerter la population et l'inciter à écouter la radio.

Le développement et le maintien de la valeur visés dans le cadre de Polyalert 2030 impliquent des adaptations technologiques du système, une mise à jour de la technologie des modules radio et la mise en œuvre de mesures destinées à alimenter la télécommande à l'emplacement des sirènes en courant de secours.

**Synergies et interdépendances**

Polyalert s'appuie sur le réseau radio de sécurité Polycom. Des adaptations touchant Polycom peuvent influer sur la configuration du système d'alarme et doivent être analysées dans chaque cas. Le maintien de la valeur du système Polyalert est synchronisé avec la fonctionnalité préparée en vue de Polycom 2030.

Le réseau émetteur OUC de la SSR peut être utilisé actuellement comme canal redondant pour le déclenchement des sirènes. La désactivation de ce réseau radio analogique aura pour conséquence la suppression du système redondant probablement à partir de 2024. À titre d'alternative aux OUC, une intégration de DAB+, la radio numérique, ou l'utilisation de la CSFLB ou le recours à des opérateurs privés pourraient être envisagés. Comme le système d'alarme Polyalert existant sera probablement arrivé à la fin de son cycle de vie en 2024, un système de remplacement doit être éventuellement prévu.

**Conséquences d'une non-réalisation de Polyalert 2030**

Si l'on renonçait au maintien de la valeur et au développement du système, la population ne pourrait plus être alertée par le biais des sirènes à partir de 2025 environ.

## 4.2 Information de la population par la radio d'urgence IPCC/Polyinform

Par radio IPCC, on entend le réseau d'urgence par radio OUC de la Confédération. La Chancellerie fédérale peut ainsi, sur mandat du Conseil fédéral, informer la population en toutes situations sur la première chaîne radio SSR dans toutes les langues nationales. Grâce aux studios radios protégés et aux émetteurs OUC (à puissance d'émission accrue) de la Confédération, l'information peut être captée jusque dans les abris. Les emplacements d'émetteurs radio IPCC peuvent diffuser les programmes de la SSR auprès de 85 % de la population. Même si l'alimentation électrique est hors service, l'émission d'informations est possible pendant 40 jours grâce aux générateurs de secours. La réception de ces informations suppose toutefois des récepteurs radio OUC fonctionnant avec des piles et pouvant être maniés par les utilisateurs.

Polyinform 2030 est le projet visant à étudier et à garantir l'exploitation, le maintien de la valeur et le développement de la radio IPCC. À partir de 2024, la diffusion de signaux radio analogiques par OUC sera probablement abandonnée en Suisse. Cet abandon progressif devrait commencer dès 2019. La décision quant à la date de désactivation définitive relève du Conseil fédéral. En fonction de cette décision, une modernisation du système utilisé pour la radio IPCC pourra s'avérer nécessaire. En l'état actuel, on peut cependant admettre que le système en place puisse demeurer opérationnel jusqu'en 2027 avec les mesures prévues de maintien de la valeur.

Le comportement des jeunes couches de la population en matière de consommation montre une diminution de la réception de programmes radio analogiques. On ne peut encore dire pour l'instant si c'est DAB+ ou IP-Broadcast (streaming par réseau mobile et réception via smartphone, tablette, etc.) qui tend à s'imposer. En fonction de la technologie qui s'imposera et sous réserve que le Conseil fédéral décide de poursuivre l'exploitation d'un tel système de radio d'urgence, un projet adapté pourra être envisagé. Pour être au clair sur la situation et définir la marche à suivre, l'OFPP a lancé une étude à laquelle participent tous les organismes intéressés par l'information de la population par la Confédération.

Il importe de mettre en évidence les conditions suivantes : en vue du recours au système de radio IPCC renforcé, la SSR, les radios locales et d'autres sources d'information doivent interagir efficacement et les informations de la Confédération doivent être transmises à la population par l'intermédiaire de toutes les plates-formes de radiodiffusion et d'information disponibles (radio numérique, télévision

numérique, portails de nouvelles, etc.). Les processus et organisations requises à cet effet doivent être parfaitement rodés.

**Synergies et interdépendances**

Le système radio IPCC actuel s'appuie sur le réseau de conduite suisse. En cas de réalisation du RDS/Polydata, tant la radio IPCC qu'un système de remplacement éventuel seraient développés sur cette nouvelle plate-forme. Déjà, à l'heure actuelle, une collaboration efficace a été mise en place avec la SSR concernant l'utilisation des infrastructures existantes pour l'information de la population par la Confédération via la radio.

Alors que la population peut être informée dans de nombreuses situations par le biais de divers canaux et offres de la SSR (radio numérique DAB+, radio sur internet, télévision numérique par câble DVB-C, télévision numérique par satellite DVB-S, télévision par internet, radio et télévision mobiles sur smartphone, plate-forme internet, etc.), la SSR peut quant à elle utiliser les installations radio IPCC comme réseau redondant en cas de panne totale de ses propres infrastructures (BCM de la SSR). Les processus de collaboration et les structures d'organisation correspondantes, notamment avec l'armée, sont bien rodés.

**Conséquences d'un abandon d'IPCC/Polyinform**

En cas d'abandon de la radio IPPC, la Confédération perdrait le seul canal d'information indépendant prêt à être utilisé en toutes situations et permettant aux autorités de s'adresser directement à la population.

**Variantes**

*Solution A : Poursuivre l'exploitation de la radio IPCC sur l'infrastructure existante jusqu'en 2027*

Dans le cadre de cette solution, l'infrastructure radio IPCC serait exploitée jusqu'au terme du contrat d'exploitation signé entre armasuisse et Swisscom Broadcast SA. Bien que la SSR étende son offre en matière de radio numérique DAB+, l'infrastructure d'émetteurs pourra fonctionner sans restriction. On peut supposer que la population continuera de disposer d'un certain nombre de terminaux capables de recevoir le signal OUC (autoradios, appareils à double syntoniseur OUC-DAB+). Le cas échéant, la Confédération se limitera à garantir le fonctionnement du système existant et le maintien de sa valeur. Dans les situations ne nécessitant pas le recours à la radio IPCC, la Confédération informera la population au moyen de tous les canaux de radiodiffusion et d'information disponibles. Si cette solution était choisie, seule une partie de la population pourrait encore, dès 2024, capter les messages par radio IPCC, vu que les récepteurs OUC se feraient de plus en plus rares.

*Solution B : Migration de la radio IPCC sur la technologie IP-Broadcast*

D'ores et déjà, 50 % des auditeurs qui ont opté pour la radio numérique captent leurs programmes via smartphone, tablette ou ordinateur. La réception de ceux-ci est aujourd'hui assurée par l'entremise du réseau fixe, du réseau local sans fil (wifi) et, dans de très nombreux cas, à l'aide du réseau de téléphonie mobile des opérateurs de télécommunication. Ils bénéficient ainsi d'un avantage important dans la mesure où ils peuvent, grâce à leur smartphone personnel, pratiquement disponible en permanence, accéder à quasiment toutes les sources d'information, sous réserve de la couverture du réseau. Dans le cas requérant le recours à IPCC, c'est-à-dire en situation de crise, la couverture du réseau devient un facteur critique et risque fort de ne plus être garantie. Si la CSFLB devait être réalisée, cette solution permettrait de mettre en place un canal d'information efficace et de grande utilité pour la population qui pourrait répondre aux exigences en matière d'utilisation en cas de crise. Dans ces circonstances et à condition de revoir les prétentions en termes de qualité de la couverture radio (pas de réception à l'intérieur des abris), il serait possible de remplacer le système actuel de radio IPCC.

*Solution C : Migration sur DAB+*

Ces prochaines années, la SSR et les radios privées consentiront d'importants investissements pour accélérer, à grand renfort d'activités de marketing, la mise en place du réseau d'émetteurs, l'amélioration de la qualité de réception dans toute la Suisse et la pénétration des appareils de réception DAB1+. L'OFCOM favorisera cette évolution en inscrivant les conditions-cadres nécessaires dans

la nouvelle loi sur la radio et la télévision (LRTV). En outre, l'OFROU veillera à ce que tous les tunnels des routes nationales soient équipés de la technologie DAB+. La mesure dans laquelle DAB+ pourra s'étendre à l'échelle européenne n'est pas prévisible à l'heure actuelle. En Suisse, près de la moitié des auditeurs utilisent actuellement cette technologie pour capter leurs programmes. Si DAB+ devait réussir à s'imposer au cours des années à venir, le système de radio IPCC, qui sera dépassé d'ici là, pourrait être équipé d'émetteurs DAB+.

## 4.3 Développement du système Alertswiss[13]

L'OFPP exploite depuis février 2015 sous l'appellation Alertswiss une application et un site internet, qui donnent des informations détaillées sur les dangers et risques potentiels pour la population ainsi que sur les mesures de précaution personnelles et la planification des mesures d'urgence.

L'application n'est toutefois pas encore dotée d'une fonction active d'alarme et d'information de la population. Une telle fonction permettrait de transmettre rapidement et directement l'alarme et les consignes de comportement à la population. Elle complèterait judicieusement le système de sirènes et radio existant. Elle permettrait non seulement une portée plus étendue, mais elle tiendrait également compte des habitudes actuelles de la population dans l'utilisation des médias et aboutirait à une augmentation considérable de la vitesse de diffusion des informations.

Une extension des moyens d'alarme et d'information est expressément souhaitée par un très large public. La Fédération suisse des sourds en particulier demande depuis longtemps une alternative à la transmission de l'alarme par les sirènes et à la diffusion des consignes de comportement à la radio. La police et les organes de conduite cantonaux souhaitent également, en cas d'événement de grande ampleur, pouvoir informer la population plus rapidement et plus simplement qu'actuellement avec le processus ICARO (par sirènes et radio). En outre, une alarme plus ciblée dans un secteur donné s'avérerait plus efficace pour la protection de la population touchée par un événement. Les récents attentats commis en Allemagne et en France, lors desquels de tels systèmes d'alarme et d'information ont été utilisés, montrent à l'évidence que ceux-ci sont nécessaires pour la population menacée et les autorités.

Une telle alternative se présente sous la forme d'une fonction push pour l'alarme et l'information via l'application Alertswiss. L'application Alertswiss en tant que canal pour une information rapide de la population devrait être complétée par d'autres canaux en cas d'événement. Les applications utilisées par une large part de la population pourraient par exemple entrer en ligne de compte comme celles de MétéoSuisse (5,8 millions d'utilisateurs), des CFF, de 20min, de Blick, de la SSR, etc.

La condition nécessaire pour la réalisation d'un canal supplémentaire moderne et redondant de transmission de l'alarme et de l'information est un système central à l'échelle nationale. Il permettra la réception des messages dans un format standardisé et leur traitement ainsi qu'un frontal pour la saisie standardisée avec des modèles de textes. Il s'agira de raccorder en premier lieu les centrales d'intervention des polices cantonales et les organes de conduite cantonaux à ce système central. Le site internet d'Alertswiss et d'autres canaux de diffusion, comme Twitter et les panneaux d'information dans les gares, pourraient également être commandés par ce système central, qui garantirait que le plus grand nombre possible de personnes touchées lors de la transmission de l'alerte et de l'information soient atteintes.

Dans une première étape, l'application Alertswiss existante, reposant sur le système central mentionné, viendrait compléter le système par sirènes et radio. Utilisant les réseaux publics, cette application ne fonctionnerait pas dans toutes les situations et présente un risque de défaillance élevé. En cas d'indisponibilité d'Alertswiss, le système de transmission de l'alarme existant (par sirènes et radio) resterait toutefois une solution de secours.

### Synergies et interdépendances

L'optimisation d'Alertswiss s'appuie sur Polyalert, qui est utilisé comme système central. Polyalert est déjà utilisé à l'heure actuelle dans les centrales d'intervention des polices cantonales pour le déclenchement des sirènes ainsi que pour le processus ICARO. Les synergies peuvent ainsi être mises à profit de manière optimale. Il est prévu que le système CMS DDPS serve de plate-forme au site inter-

[13] L'optimisation du système d'information Alertswiss est mentionnée dans le présent rapport par souci d'exhaustivité mais est abordée de manière sommaire. Ce projet n'est par ailleurs pas l'objet premier du présent rapport étant donné qu'il s'agit d'un projet existant, qui se trouve en phase de mise en œuvre.

net Alertswiss. Concernant les autres applications mentionnées plus haut, comme celle de MétéoSuisse, les synergies peuvent être mises à profit pour un effet multiplicateur en vue d'une plus large diffusion.

**Conséquences d'une non-réalisation d'Alertswiss**

Le projet visant à optimiser Alertswiss est en cours de mise en œuvre.

**Variantes**

Le projet visant à optimiser Alertswiss est déjà en cours de mise en œuvre.

## 4.4 Alarme par téléphone portable (SMS ou CBS)

La transmission de l'alarme à la population via une application sur téléphone mobile suppose que la population dispose des applications correspondantes, autrement dit qu'elles aient été téléchargées et activées sur les téléphones mobiles. Dans la pratique, cela peut poser un grave problème, qui pourrait néanmoins être résolu au moyen d'une alarme par téléphone portable via Cell Broadcasting (CBS) ou des services SMS liés au lieu de résidence. De tels systèmes d'alarme existent déjà en Europe, par exemple aux Pays-Bas, en Suède, en Norvège et en Grande-Bretagne et seront prochainement introduits en Belgique.

Ces deux technologies présentent toutefois des inconvénients par rapport à une application telle qu'elle est développée dans le cadre d'Alertswiss. Dans le cas d'une alarme à grande échelle avec un nombre élevé de destinataires par SMS, la transmission pourrait être sensiblement retardée. Dans le cas d'une alarme via CBS, le fait que les téléphones mobiles ne soient pas configurés à cet effet représenterait un obstacle majeur. Selon une étude réalisée par Swisscom, seuls 30% des terminaux utilisés en Suisse sont en principe compatibles avec CBS, sous réserve de la configuration requise. Les utilisateurs devraient faire eux-mêmes cette opération, qui nécessite généralement une assistance technique. En principe, il devrait être possible dès 2018, sans adaptations majeures, de transmettre via Polyalert des informations aux opérateurs de téléphonie mobile en Suisse, qui pourraient les diffuser par le canal CBS. Ceux-ci devraient cependant disposer de l'infrastructure requise pour ce processus.

Ces deux technologies s'appuient par ailleurs, comme le montre une expertise technique, sur une norme obsolète. Dans ce contexte, il faut attendre les normes à venir comme la technologie LTE ou 5G. On évitera ainsi des investissements qui ne porteraient pas sur le long terme.

**Synergies et interdépendances**

La transmission de l'alarme par SMS ou CBS dépendra de la participation des opérateurs de téléphonie mobile en Suisse (Swisscom, Salt, Sunrise) et de leurs tarifs.

**Non-réalisation de l'alarme par téléphone portable**

Avec l'optimisation d'Alertswiss (fonction push pour l'alarme et l'information), les besoins de la population et des organisations d'intervention quant à une solution de remplacement pour l'alarme et l'information sont déjà partiellement pris en compte. Les besoins qui ne sont pas couverts pour l'instant par Alertswiss seront étudiés dans une phase ultérieure sur la base des avancées technologiques.

**Variantes**

Des solutions techniques ne pourront être étudiées et définies qu'à un stade ultérieur sur la base des normes technologiques à venir.

# 5 Ordre de priorité des nouveaux projets

Les projets Polycom 2030 ainsi que le développement d'Alertswiss et de la PES CENAL ont été intégrés dans l'état des lieux afin de permettre une vue d'ensemble. Comme ils se trouvent déjà en phase de mise en œuvre, ils ne sont pas soumis à un ordre de priorité. C'est également le cas des systèmes IPCC et Polyalert, qui fonctionnent déjà. En ce qui les concerne, l'accent est mis sur l'exploitation et le maintien de la valeur. Pour les AOSS, il est primordial de continuer d'optimiser ces systèmes car ils jouent un rôle central en matière d'alarme et d'information de la population. La Confédération devra prendre dès 2025 des mesures d'envergure pour maintenir leur valeur. Les AOSS de la Confédération, des cantons et des tiers considèrent actuellement l'extension de ces systèmes, en particulier de Polyalert et d'Alertswiss, comme indispensable. Le développement d'une application pour la communication en cas d'événement et l'information de la population est à même de compenser un important déficit de sécurité en matière d'alarme. Il faut garantir l'achèvement des projets en cours et le maintien de la valeur des systèmes existants. L'OFPP doit toutefois observer en permanence l'évolution de ces domaines, informer en temps utile les responsables fédéraux et cantonaux ainsi que les tiers et fournir des documents à l'appui des décisions à prendre. Cela va dans le sens d'une recommandation du Contrôle fédéral des finances dans le cadre de son examen du projet Polycom 2030.

## Ordre de priorité des nouveaux projets

La situation financière actuelle de la Confédération et des cantons et son évolution probable exigent la définition d'un ordre de priorité pour les nouveaux projets détaillés dans le présent document. Cet ordre de priorité se fonde en premier lieu sur les besoins des AOSS de la Confédération et des cantons ainsi que des exploitants d'infrastructures critiques en ce qui concerne l'amélioration du niveau de sécurité et la possibilité de financer les mesures requises en matière de télécommunications. Il s'appuie sur 72 prises de position émanant d'organes fédéraux, de cantons, d'exploitants d'infrastructures critiques et d'autres partenaires de la protection de la population.

## 1re priorité

Pour les AOSS de la Confédération et des cantons et pour les exploitants d'infrastructures critiques, les projets ci-après doivent être réalisés avec la plus haute priorité. Dans tous les cas, les coûts devront être estimés le plus précisément possible dans une prochaine étape, dès qu'une décision politique de principe aura été prise quant à la réalisation des projets.

### RDS / Polydata

Pour les AOSS de la Confédération et des cantons et pour les exploitants d'infrastructures critiques, c'est le projet RDS qui a la première priorité. Afin de maîtriser des événements, il faut en effet pouvoir s'appuyer sur des liaisons à haute disponibilité et à l'épreuve des coupures d'électricité. On pourra mettre en place un réseau à un coût relativement modeste et conforme à ces exigences en utilisant le réseau de fibre optique et les infrastructures du Réseau de conduite Suisse, lequel bénéficie d'ores et déjà d'une large autonomie d'alimentation électrique, et en se connectant à d'autres réseaux de fibre optique appartenant à des offices fédéraux (p. ex. l'OFROU) et à des organisations privées.

De l'avis des AOSS de la Confédération et des cantons, le projet Polydata doit être réalisé en première priorité conjointement au RDS afin que celui-ci puisse être utilisé conformément à leurs besoins. Il s'agit principalement d'un réseau d'utilisateurs fermé assurant un accès sécurisé et hautement disponible à des applications importantes pour la protection de la population, comme Polycom et Polyalert, tout en améliorant la protection contre les cyberattaques.

La mise en place du RDS apporte également une plus-value au-delà du cercle des utilisateurs des AOSS. Il peut en effet servir de plateforme à d'autres systèmes et améliorer sensiblement leur sécurité d'exploitation. En utilisant le RDS, on peut par exemple augmenter la résistance aux pannes du réseau de données KOMBV-KTV, qui relie la Confédération aux organes d'exécution cantonaux et communaux. Le RDS pourrait aussi être utilisé comme réseau de données redondant pour l'approvisionnement énergétique ou la place financière suisse et ainsi améliorer la résilience de ces secteurs critiques.

### Remplacement de VULPUS-Télématique

Différents organes fédéraux, les cantons et quelques exploitants d'infrastructures critiques estiment indispensable de remplacer les fonctions de VULPUS-Télématique d'ici 2022, donc en première priorité. Dans le cas contraire, il faudrait consentir des investissements importants dans un système qui n'est pas à l'épreuve des pannes en vue de poursuivre l'exploitation de VULPUS. Il faut prendre une décision rapidement afin de donner aux utilisateurs de VULPUS le temps nécessaire pour examiner des alternatives avantageuses et adapter leurs processus de communication. Un remplacement 1:1 du système n'apparait plus souhaitable pour des raisons techniques. Les ressources nécessaires doivent être engagées dans le but de permettre des synergies avec les systèmes et applications existants.

Extension de l'infrastructure actuelle de communication sans fil à large bande

L'extension de la CSFLB profitera essentiellement aux organisations d'intervention et aux cantons les plus urbanisés. Les terminaux mobiles (smartphones, tablettes, ordinateurs portables) et les applications qu'ils utilisent se sont imposés ces dernières années et sont devenus des outils indispensables pour la conduite et l'intervention. Les organisations à feux bleus les emploient quotidiennement et un retour en arrière ne serait plus envisageable. La CSFLB pourrait un jour remplacer le système Polycom. L'OFPP devrait assurer la coordination et la normalisation au plan national.

Réseau de suivi de la situation

Toutes les organisations et autorités ayant à mener et coordonner une intervention jugent indispensable de disposer d'une vue d'ensemble la plus complète possible des informations requises et disponibles concernant un événement, ses conséquences et les mesures prises. Cet avis coïncide avec les déficits de sécurité identifiés à l'occasion de l'ERNS 14. Une très haute priorité est donc accordée au développement d'un tel instrument de conduite par les AOSS de la Confédération et des cantons ainsi que par certains exploitants d'infrastructures critiques (p. ex. les CFF). Il s'agit principalement d'une solution mettant en réseau les systèmes cantonaux existants de présentation de la situation. Elle doit fonctionner avec un minimum de composants centraux. On examinera par ailleurs la possibilité d'intégrer dans le système des organes de pays limitrophes afin de tirer un profit encore plus grand du réseau de suivi de la situation.

**2e priorité**

Les projets ci-après nécessitent encore des études supplémentaires concernant les aspects techniques et les besoins des partenaires. Une réalisation éventuelle serait par conséquent envisagée ultérieurement.

Mise en œuvre à grande échelle de la CSFLB

S'agissant de la réalisation de la CSFLB, les AOSS privilégient une solution reposant sur un réseau central dédié, relié à ceux des opérateurs privés. Il convient de tenir compte du fait qu'une telle solution serait plus sensible aux défaillances. Des essais pilotes seront effectués avec les cantons pour déterminer si elle peut offrir le meilleur résultat pour les AOSS. La réalisation à grande échelle de la CSFLB n'est cependant pas prioritaire pour le moment. Elle ne sera envisagée que sur la base de directives claires élaborées dans le cadre d'un projet pilote. Si elle doit être réalisée sous la forme d'un projet pilote géographiquement limité, c'est aussi pour des raisons de coûts.

Alarme par SMS et CBS

Pour les AOSS, l'alarme par SMS ou CBS représente un complément utile à l'alarme via l'application Alertswiss. Les deux technologies présentent aussi bien des avantages que des inconvénients (configuration, rapidité) par rapport à l'application. L'alarme par CBS fonctionne aussi en cas de surcharge des réseaux d'opérateurs privés. L'information peut en outre être répartie géographiquement. Il faut cependant mettre provisoirement de côté ces solutions pour des raisons de coûts. L'OFPP poursuivra les études dans ce domaine et fournira des bases de décision en temps utile.

Polysat

Les AOSS estiment que l'on peut renoncer pour le moment à la réalisation à grande échelle de Polysat. Il y a certes des avantages à être relié à des plateformes internationales ou à d'autres canaux de communication en tant que système diversitaire (p. ex. en cas de tremblement de terre), mais des solutions actuellement en fonction comme les stations de base mobiles de Polycom ou les systèmes mobiles à ondes dirigées de l'armée présentent en partie les mêmes avantages que Polysat. Pour le moment, les liaisons par satellite ne devraient être réalisées que de manière limitée, en l'absence d'alternative judicieuse et à des coûts avantageux.

**Récapitulation**

Sur la base des résultats de la consultation et compte tenu des possibilités de financement, le DDPS préconise de procéder comme suit :

- assurer l'exploitation et le maintien de la valeur des systèmes existants ;
- réaliser le RDS avec le système d'accès aux données Polydata et le remplacement de VULPUS en première priorité ;
- étudier la conception possible du projet de réseau national de suivi de la situation et de l'extension de la communication sans fil à large bande ;
- préparer les bases de décision nécessaires à la poursuite de l'exploitation, au maintien de la valeur, au remplacement ou à la suppression des systèmes existants.

# 6 Compétences et financement

La protection de la population se fonde sur un système coordonné de la Confédération et des cantons. Les compétences et, par conséquent, le financement sont en principe fixés dans la LPPCi et les ordonnances correspondantes. S'agissant des systèmes d'alarme et de télécommunication importants pour la protection de la population et de leur financement, les attributions ne sont à ce jour que partiellement définies et les réglementations peuvent différer selon les systèmes. Aucune réglementation n'a été établie jusqu'à présent pour les projets en question.

La consultation de la Confédération, des cantons et des exploitants d'infrastructures critiques de même que les expériences faites lors de la mise en place de Polycom ont montré la nécessité de régler clairement les questions de compétences et de financement, avant tout lorsqu'il s'agit de systèmes mixtes, auxquels la Confédération, les cantons et des tiers participent conjointement. Dans le cas de tels systèmes, on distingue entre composants centraux et composants décentralisés. Les composants centraux relient tous les utilisateurs, qui s'en servent en commun. Quant aux composants décentralisés, ils sont utilisés spécifiquement par des organes fédéraux, tels que le Cgfr, des cantons et des tiers, qui peuvent ainsi se servir des composants centraux.

En vue de régler les questions en matière de compétences et de financement, le chef du DDPS et les présidents de la CCDJP et de la CG MPS ont institué le 10 janvier 2017 un groupe de travail composé de représentants fédéraux et cantonaux. S'inspirant des modèles éprouvés appliqués à Polycom et Polyalert, celui-ci propose le modèle suivant pour la réglementation des compétences et le financement:

- La radio d'urgence IPCC, le système Alertswiss servant à informer la population en cas d'événement et, pour l'essentiel, le système de transmission de messages Vulpus et le système d'alarme par sirènes Polyalert sont des systèmes fédéraux. Conformément aux bases légales, les systèmes de ce type relèvent exclusivement de la Confédération, qui veille aussi à leur financement. Les conditions et les prescriptions relatives à l'utilisation des systèmes, à leur exploitation et à leurs adaptations techniques sont toutefois établies en concertation avec les utilisateurs.
- Lorsqu'il s'agit de systèmes mixtes, la compétence en matière de composants centraux incombe à la Confédération. Quant aux composants décentralisés, ils relèvent de la Confédération (organes fédéraux), des cantons et des tiers.
- On entend par investissement toutes les dépenses nécessitées par la mise en place d'un nouveau système. À propos de RDS et de Polydata, il s'agit par exemple des montants investis pour les bâtiments, les câbles, le matériel informatique, les logiciels, groupes électrogènes, installations de climatisation, etc. (voir le tableau 1). Les composants centraux sont financés par la Confédération. Les investissements sont uniques et requièrent en principe une décision politique (Conseil fédéral ou Parlement). En ce qui concerne les composants décentralisés, les frais d'investissement sont supportés par les cantons et les tiers. Dans la mesure où les raccordements concernent des composants décentralisés d'organes fédéraux, les investissements sont à la charge de la Confédération elle-même.
- Une fois arrivés au terme de leur cycle de vie, les composants d'un système nécessitent des mesures de maintien de la valeur ayant un caractère d'investissement. On entend ainsi par maintien de la valeur d'importants réinvestissements qui peuvent être indispensables 6 à 8 ans après le premier investissement. Ces coûts représentent environ 60 % de ce premier investissement et sont assumés par la Confédération pour ce qui est des composants centraux. Ce taux est estimé à 60 %, c'est parce qu'il n'est pas nécessaire, après 8 ans, de remplacer tout le bâtiment, l'installation de climatisation entière, etc. mais en premier lieu uniquement certains éléments du matériel informatique ou des logiciels. Les cantons et les tiers supportent pour leur part les coûts du maintien de la valeur des composants décentralisés. Lorsqu'ils disposent de composants décentralisés, les organes fédéraux doivent eux aussi en assumer de tels réinvestissements.
- On entend par coûts d'exploitation et d'entretien les dépenses nécessaires au fonctionnement ininterrompu et sécurisé des systèmes. Cela recouvre notamment la maintenance des systèmes, leur surveillance, la gestion des services et des urgences, la mise à jour des logiciels et les patches de sécurité mais aussi les frais de location. Les mesures de maintien de la valeur mises en œuvre durant le cycle de vie des systèmes représentent 15 % des coûts annuels d'exploitation et d'entretien.
- En ce qui concerne le système radio de sécurité Polycom, le système de transmission d'alarme Polyalert, le système de communication en cas d'événement Alertswiss et la radio d'urgence IPCC, les coûts annuels d'exploitation et d'entretien des composants centraux sont à la charge de la Con-

fédération. Quant aux coûts annuels d'exploitation et d'entretien des composants centraux en rapport avec RDS, Polydata, les fonctions destinés à remplacer Vulpus, le système mobile de communication sécurisée à large bande CSFLB et le réseau national de suivi de la situation, ils sont pris en charge au prorata par tous les utilisateurs connectés. L'exploitation et l'entretien des composants décentralisés sont financés par la Confédération dans le cas de systèmes fédéraux comme les systèmes d'alarme, de communication en cas d'événement et la radio d'urgence et par les cantons ou les tiers lorsqu'il s'agit d'autres systèmes. Si de tels composants sont utilisés par des organes fédéraux raccordés aux systèmes précités, les coûts d'exploitation et d'entretien des composants sont également assumés par la Confédération.

- Il est prévu que les coûts annuels d'exploitation et d'entretien des composants centraux du RDS, de Polydata, y compris les fonctions destinées à remplacer VULPUS, soient assumés pour 30 % par les cantons et pour 70 % par la Confédération. Cette part autorise les cantons à réaliser au maximum 36 raccordements à ce système. La répartition des coûts entre les cantons sera fixée par ceux-ci. De son côté, la Confédération a droit à 84 raccordements au plus et s'occupe de ceux des exploitants d'infrastructures critiques ou de tiers comme la Principauté de Liechtenstein, dont elle encaisse les contributions financières. En cas de réalisation de raccordements supplémentaires par rapport aux droits accordés, la clé de répartition des coûts sera adaptée selon le même principe.

Tableau 1: Vue d'ensemble de l'engagement des moyens, des échéances et des compétences en matière de financement de l'investissement, du maintien de la valeur (réinvestissement), de l'exploitation et de l'entretien de RDS et Polydata.

| | **Investissement** | **Maintien de la valeur (réinvestissement)** | **Exploitation et entretien** |
|---|---|---|---|
| Objet | Bâtiments, installations de climatisation, groupes électrogènes, matériel informatique, logiciels, licences | Changement complet, matériel informatique, (p. ex. routeurs), logiciels | Maintenance, mise à jour de logiciels, pièces de rechange, locations |
| Échéances | unique[14] | tous les 6 à 8 ans | annuelle |
| Payé par | Composants centraux : Confédération<br>Composants décentralisés : organes fédéraux, cantons et tiers | Composants centraux : Confédération<br>Composants décentralisés : organes fédéraux, cantons et tiers | Composants centraux : utilisateurs (Confédération et tiers[15]/cantons : 70/30)<br>Composants décentralisés : organes fédéraux, cantons et tiers |

- En cas de réalisation du Réseau national de suivi de la situation, la réglementation des compétences et du financement établie pour le Réseau national de données sécurisé s'appliquera par analogie.
- La clé de répartition du système de communication mobile de sécurité à large bande reste à définir, en particulier parce que l'intérêt à y participer varie actuellement d'un canton à l'autre. En outre, il faudra attendre les résultats d'un éventuel projet pilote.
- Selon les organes fédéraux concernés, le financement des coûts incombant à la Confédération devrait être garanti au titre d'une budgétisation centralisée. Le Conseil fédéral devra en décider dans le cadre des messages respectifs.

[14] Ou très longs cycles de plusieurs décennies, p. ex. pour la rénovation des bâtiments.

[15] Avec les exploitants d'infrastructures critiques et le Liechtensetin.

## 7 Bases juridiques

La révision en cours de la LPPCi inscrit dans la loi la répartition des tâches entre la Confédération, les cantons et des tiers et le financement des systèmes d'alarme et de télécommunication de la protection de la population, quand bien même une partie des projets ne pourront être réalisés que bien plus tard. Il est tenu compte des besoins des utilisateurs, des structures fédérales et des aspects économiques.

Il est prévu de remettre au Conseil fédéral, au deuxième trimestre 2018, un message à l'appui du crédit d'engagement pour la réalisation d'un réseau national de données sécurisé (RDS) en même temps que le message relatif à la révision de la LPPCi et de les transmettre ensuite au Parlement.

Afin d'éviter que les cantons et des tiers ne réalisent chacun de son côté différents systèmes dont la réunion ultérieure au sein d'un système national exigerait beaucoup de temps et de ressources, à l'instar de Polycom, il est également prévu de confier à la Confédération la possibilité d'imposer des normes. Elle doit également pouvoir édicter des prescriptions techniques et fixer des délais concernant de tels réseaux, en tenant compte des demandes des autres utilisateurs.

## 8 Conséquences financières pour la Confédération et les cantons

Le maintien de la valeur des systèmes existants d'alarme et de télécommunication de la protection de la population ou la réalisation de nouveaux systèmes dépend en partie de ressources humaines et financières supplémentaires. La conception des projets et la présentation détaillée des coûts et des ressources nécessaires pour la Confédération, les cantons et les tiers exigent déjà une augmentation du budget de l'OFPP. Ces investissements préalables ne seront effectués que sur la base d'une décision politique de principe désignant les projets à réaliser et leur calendrier. Les ressources demandées doivent être acceptées et garanties dans le cadre de messages du Conseil fédéral spécifiques à chaque projet et transmis au Parlement, comme ce fut le cas pour Polycom 2030. La Confédération a dû débloquer des moyens financiers supplémentaires pour les composants nationaux afin d'assurer la disponibilité de Polycom jusqu'en 2030. Le Parlement a donné son aval en 2016.

Les coûts du fonctionnement et du maintien de la valeur de Polycom, Polyalert et IPCC ainsi que les coûts du maintien de la valeur de la PES CENAL et du système d'information Alertswiss sont inscrits aux budgets des organes fédéraux compétents (OFPP, BAC, Cgfr, SRC). Les cantons participent aussi aux coûts de fonctionnement de Polycom et de Polyalert selon une clé de répartition établie en fonction du droit en vigueur.

Les ressources nécessaires pour la réalisation, l'exploitation et le maintien de la valeur du RDS, de Polydata et du remplacement de VULPUS ne peuvent pour l'instant faire l'objet que d'une estimation sommaire. Selon la répartition des compétences proposée, les coûts d'investissement à la charge de la Confédération pour les composants centraux s'élèveraient à quelque 150 millions de francs. Une précédente estimation chiffrait à 60 millions de francs les coûts du seul RDS, à quoi s'ajoutent désormais ceux de Polydata (25 millions) et du remplacement de VULPUS (25 millions). Il faut dorénavant tenir compte des risques liés au RDS à hauteur de 25 % (15 millions) et des coûts de gestion du projet (25 millions). Il appartient aux propriétaires et aux utilisateurs des composants décentralisés d'évaluer et de financer les coûts liés à ceux-ci. Une estimation des coûts d'exploitation et d'entretien des composants nationaux du RDS (sans Polydata ni le remplacement de VULPUS) a par ailleurs été effectuée en 2014. Dans les conditions actuelles, ces coûts seraient certainement plus élevés, pour les raisons suivantes : (a) il faut inclure également les coûts de Polydata et du remplacement de VULPUS ; (b) la Confédération et les cantons doivent payer le même prix pour un raccordement ; (c) seuls des raccordements de grande capacité (10 Gbit/s au lieu de 2,5) avec un service 24 heures sur 24 doivent être pris en considération et (d) les coûts du maintien de la valeur sont désormais calculés pendant le cycle de vie (15 % des coûts d'exploitation et d'entretien). Les coûts annuels d'exploitation et d'entretien des composants centraux sont estimés à 20 millions de francs. Ils doivent être financés au prorata par tous les utilisateurs raccordés. La réalisation du projet et l'exploitation du système nécessiteront la création de postes supplémentaires auprès de la Confédération. L'exploitation des composants décentralisés est l'affaire de leurs propriétaires et utilisateurs.

Il est prévu de donner des informations détaillées sur les ressources dans le cadre d'un message. S'agissant des autres projets, des études supplémentaires doivent encore être menées.

Les coûts incombant aux cantons dépendent de leurs besoins et de la répartition des tâches et des coûts entre la Confédération, les cantons et les tiers en ce qui concerne les systèmes d'alarme et de télécommunication importants pour la protection de la population. S'il est décidé de réaliser le projet RDS/Polydata, un réseau de base avec premier raccordement pour tous les cantons pourrait être réalisé entre 2020 et 2023. La deuxième phase de réalisation durerait de 2024 à 2027. Les éventuels coûts à supporter par les cantons seraient probablement effectifs à partir de 2021. Quant aux droits d'utilisation des raccordements réalisés dans la première phase, ils seraient dus à partir de 2024. Leur montant sera également fonction des besoins respectifs des cantons et de la clé de financement intercantonale.

S'il est décidé de réaliser le projet de remplacement de VULPUS, un réseau de base avec premier raccordement pour tous les cantons pourrait être réalisé d'ici 2022. Les droits d'utilisation seraient dus à partir de 2023.

Les éventuels coûts que le projet CSFLB occasionnera à l'échelon cantonal seront déterminés essentiellement par les besoins de chaque canton et de la répartition des tâches et du financement à fixer entre la Confédération et les cantons.

Selon leur intérêt, des tiers (p. ex. exploitants d'infrastructures critiques) pourraient également participer au projet RDS/Polydata et au remplacement de VULPUS-Télématique. Par conséquent, ils devraient aussi assumer une partie des coûts conformément à la règle de financement à établir.

## 9 Conséquences d'une non-réalisation

Si le maintien de la valeur et l'exploitation de systèmes existants comme Polycom, Polyalert, la PES CENAL et Alertswiss ne sont pas assurés, ceux-ci risquent de ne plus être aptes à fonctionner. En conséquence de quoi les forces d'intervention et les autorités ne pourraient plus communiquer ensemble par radio, même en situation normale. Elles devraient mettre en place de nouveaux canaux de communication au risque de ne pas toutes disposer des mêmes informations au même moment en cas d'intervention commune. Lors des attentats du 11 septembre 2001 contre le World Trade Center de New York, le manque de capacité de communication entre les différentes organisations a été la cause de mauvaises décisions qui ont compliqué les interventions. Une enquête avait été diligentée après les événements. Si l'alarme par sirènes ne fonctionne pas, le temps de réaction de la population en cas de danger imminent va s'allonger car elle ne pourra plus être avertie à temps. Les malentendants demeureraient hors de portée si l'alarme par sirènes combinée avec les messages ICARO diffusés par la radio n'est pas complétée par un canal d'alarme et d'information alternatif, par exemple Alertswiss. La nécessité d'alerter et d'informer rapidement la population a été démontrée lors d'attentats terroristes à l'étranger ces dernières années.

Si de nouveaux projets comme RDS/Polydata ne sont pas réalisés, l'échange de données et d'importantes applications utilisées par la protection de la population resteront à la merci des coupures d'électricité et de défaillances des réseaux d'opérateurs privés. Faute d'un réseau fermé, les systèmes de télécommunication demeureront insuffisamment protégés contre les cyberrisques. Des failles de sécurité connues et pointées du doigt à plusieurs reprises (p. ex. dans les recommandations résultant de l'ERNS 14) ne seront pas comblées. En cas d'événement, le risque persiste que la Confédération, les cantons et les exploitants d'infrastructures critiques ne puissent pas échanger d'informations et de données par large bande au niveau stratégique. Il serait alors impossible d'agir rapidement et de manière coordonnée, en particulier lors d'événements touchant tout le pays. On courrait dès lors le risque de dommages supplémentaires évitables dus à des mauvaises décisions, à un retard dans la prise de mesures ou à un engagement inefficace de ressources.

Sans un réseau national de suivi de la situation en état de marche, couvrant toutes les formes d'événements et diffusant toutes les informations, les organes de conduite de la Confédération et des cantons ainsi que les exploitants d'infrastructures critiques manqueront d'informations consolidées sur la situation à l'échelle du pays. C'est pourtant une condition pour pouvoir prendre des décisions stratégiques harmonisées à l'échelon supérieur, par exemple en cas de menace terroriste imminente dans plusieurs régions ou pour permettre à la Confédération de gérer les ressources en cas de catastrophe nationale.

Faute de communication sans fil à large bande sécurisée, des organisations telles que le Cgfr, la police, les sapeurs-pompiers et les premiers secours ne pourraient pas mener leurs interventions ou ne pourraient pas le faire avec l'efficacité voulue. Les smartphones, les tablettes et les notebooks sont d'ores et déjà des outils indispensables au niveau tactique. Les possibilités sécurisées d'échanger des informations, de transmettre des photos ou des vidéos de la situation ou encore d'accéder à des banques de données (p. ex. pour les personnes recherchées, le contrôle aux frontières) feraient défaut. Il pourrait en découler des dommages aux personnes et aux biens. En outre, les retards pris dans le retour à l'état normal entraineraient des coûts élevés.

L'élimination des failles de sécurité identifiées améliore non seulement la résistance aux défaillances des systèmes de télécommunication et l'échange de données entre les organisations de conduite, d'interventions et de sauvetage mais aussi, d'une manière générale, le niveau de sécurité dont la population peut profiter. En cas de catastrophe ou de situation d'urgence, l'ampleur des dommages pourrait s'en trouver sensiblement réduite. Sans ces nouveaux systèmes, la population de la Suisse resterait exposée à un risque accru.

## 10 Suite des travaux

1. Le présent rapport est remis au Conseil fédéral avec l'évaluation de la consultation et une proposition, en même temps que le projet de révision de la LPPCi destiné à la procédure de consultation.
2. Le Conseil fédéral statue sur l'ordre de priorité et la marche à suivre.