

Ce texte est une version provisoire.
La version définitive qui sera publiée sous
www.droitfederal.admin.ch fait foi.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

23.xxx

Stratégie nationale de protection des infrastructures critiques

Approche globale pour garantir l'approvisionnement en biens et prestations essentiels

du ...

Table des matières

1	Introduction	3
2	Contexte	4
2.1	Contexte de la stratégie PIC	4
2.2	Interfaces avec d'autres domaines d'activités	4
2.2.1	Cyberstratégie nationale	5
2.2.2	Approvisionnement économique du pays	5
2.2.3	Politique de gestion des risques menée par la Confédération	5
3	Champ d'application	6
4	Principes	7
4.1	Approche globale	7
4.2	Proportionnalité	9
4.3	Compétences et responsabilités	9
4.4	Collaboration public-privé	9
5	Vision et objectifs de la stratégie nationale PIC	9
5.1	Vision	9
5.2	Objectifs stratégiques	10
5.3	Objectifs de mise en œuvre	10
6	Mesures de la stratégie nationale PIC	12
6.1	Améliorer la résilience dans les secteurs critiques	13
6.2	Améliorer la résilience dans le domaine intersectoriel	14
6.2.1	Champ d'action analyse	14
6.2.2	Champ d'action évaluation	16
6.2.3	Champ d'action mesures (de protection)	17
6.2.4	Champ d'action mise en œuvre et vérification	20
7	Mise en œuvre de la stratégie nationale PIC	21
7.1	Structures et compétences	21
7.2	Calendrier et contrôle	22
7.3	Révision de la stratégie PIC	22
Annexes:		
1.	Description des sous-secteurs et des compétences pour l'amélioration de la résilience dans les secteurs critiques (mesure 1)	23
2.	Aperçu des mesures, des compétences et des interfaces	26
3.	Liste des abréviations	28

Stratégie nationale de protection des infrastructures critiques : approche globale pour garantir l’approvisionnement en biens et prestations essentiels

1 Introduction

On entend par infrastructures critiques les processus, les systèmes et les installations essentiels pour le fonctionnement de l’économie et le maintien des moyens de subsistance de la population. L’approvisionnement en électricité, les organisations d’urgence et les télécommunications en font notamment partie. En effet, des perturbations ou des pannes graves, comme des pannes de courant de longue durée ou des pannes des systèmes de transport et de logistique, entraînent de graves dommages économiques et une perturbation massive de la vie quotidienne. La protection des infrastructures critiques (PIC) a donc pour objectif d’améliorer la résilience de la Suisse en cas de panne ou de perturbation grave de ces systèmes de services et d’approvisionnement, sachant que la résilience décrit la capacité d’un système, d’une organisation ou d’une société à surmonter des perturbations d’origine interne ou externe (capacité de résistance) et à maintenir autant que possible sa fonctionnalité (capacité d’adaptation) ou à la retrouver aussi rapidement et complètement que possible (capacité de régénération). Les ouvrages et les mesures de protection des ouvrages ne représentent ainsi qu’une partie de l’approche globale. Les mesures visant à améliorer la sécurité de l’approvisionnement, la stabilité des systèmes ou la préparation à la gestion des pannes sont tout aussi importantes. La PIC est par conséquent une tâche transversale avec des interfaces vers différents domaines d’activités et différents domaines politiques, tels que l’énergie, les transports, la sécurité ou l’aménagement du territoire. La stratégie nationale PIC vise à améliorer la coordination et à garantir une action concertée entre les différents projets et domaines ainsi qu’entre les différents acteurs (autorités aux niveaux fédéral, cantonal et communal, exploitants, organisations d’intervention, etc.).

La troisième stratégie nationale PIC fait suite aux deux premières que le Conseil fédéral a adoptées respectivement en 2012¹ et en 2017². Elle a été élaborée par l’OFPP en collaboration avec les services fédéraux compétents, les cantons et les exploitants d’infrastructures critiques nationales.

Elle définit des mesures qui sont mises en œuvre en premier lieu par les unités organisationnelles de l’administration fédérale, sous la responsabilité principale des autorités de surveillance et de régulation des différents secteurs. Celles-ci sont tenues d’examiner les conditions générales sous l’angle de la résilience des infrastructures critiques qui relèvent de leur compétence et de prendre des mesures pour les améliorer si nécessaire. Certaines mesures concernent directement les cantons. Ceux-ci s’acquittent de leurs tâches dans le cadre de leurs compétences et de leur mission et selon leurs possibilités et leurs besoins. La stratégie PIC concerne aussi les exploitants, dont la collaboration est indispensable pour atteindre les objectifs. La plupart d’entre eux mettent déjà tout en œuvre afin d’éviter des pannes ou des perturbations. Il est important de pouvoir compter sur leur initiative personnelle pour

¹ FF 2012 7173

² FF 2018 491

améliorer la résilience et sur leur disposition à coopérer avec les organes étatiques et les autres exploitants.

2 Contexte

2.1 Contexte de la stratégie PIC

La répartition des compétences dans le domaine de la PIC est complexe. Selon le secteur, les exigences de résilience sont définies au niveau fédéral (p. ex. approvisionnement en énergie), au niveau cantonal (p. ex. soins médicaux), voire au niveau communal (p. ex. approvisionnement en eau). En conséquence, les approches méthodologiques utilisées pour évaluer les risques et définir un niveau de sécurité d'approvisionnement et de résilience approprié diffèrent d'un domaine à l'autre. De même, l'amélioration de la résilience, souvent considérée comme secondaire dans les domaines politiques, n'est souvent pas prise en compte de manière explicite et globale.

Les infrastructures critiques jouent aussi un rôle important dans la prévention et la gestion de catastrophes ou de situations d'urgence. Les acteurs impliqués ne sont pas les mêmes (service de renseignement, organisations d'urgence, armée, etc.) en fonction du type d'événement (p. ex. cyberattaque ou menace terroriste). La stratégie PIC vise donc avant tout à améliorer la coordination transversale, ou intersectorielle, en ce qui concerne les secteurs, les dangers et les mesures, et à mener une action concertée dans les différents domaines d'activités. Les deux premières stratégies ont permis de réaliser des progrès notables. Ainsi, des analyses de risques et de vulnérabilité ont été réalisées dans la plupart des secteurs critiques. Elles ont permis d'élaborer et de mettre en œuvre des mesures visant à améliorer la résilience. Les exploitants d'importance systémique ont par exemple pu être équipés avec des systèmes de communication résistant en cas de crise et des normes de sécurité spécifiques ont été établies dans certaines branches. L'Inventaire PIC est devenu une base de planification et de décision importante pour la gestion des catastrophes et des situations d'urgence et les plateformes visant à améliorer la collaboration intersectorielle se sont imposées. La garantie d'une démarche concertée pour améliorer la résilience constitue toutefois une tâche permanente qui sera poursuivie dans le cadre la troisième stratégie PIC.

2.2 Interfaces avec d'autres domaines d'activités

La PIC présente des interfaces avec différents domaines d'activités, dont les principaux sont présentés ci-après.

2.2.1 Cyberstratégie nationale

La PIC contre les cyberrisques représente un aspect important de la cyberstratégie nationale (CSN), qui met l'accent sur la création de capacités suffisantes pour analyser les menaces et aider les exploitants dans la gestion des événements. La CSN et la

stratégie PIC sont étroitement coordonnées. Elles poursuivent des buts communs, en particulier concernant les cyberrisques, au moyen notamment de mesures comme l'examen et l'amélioration de la résilience des infrastructures critiques.

2.2.2 Approvisionnement économique du pays

La Confédération assure l'approvisionnement du pays en biens et services de première nécessité afin de pouvoir faire face à une grave pénurie à laquelle l'économie n'est pas en mesure de remédier par ses propres moyens. Le Conseil fédéral a confié la préparation de cette tâche à l'approvisionnement économique du pays (AEP). En cas de grave pénurie, l'État intervient de manière ciblée sur le marché afin de rétablir l'offre (notamment en libérant des réserves obligatoires ou en gérant des biens et services de première nécessité). Les mesures sont préparées et mises en œuvre en étroite collaboration avec le secteur économique, les cantons et d'autres acteurs. L'AEP couvre environ la moitié des secteurs et sous-secteurs critiques de la stratégie nationale PIC et contribue ainsi de manière décisive à atteindre ses objectifs. Les autres activités PIC concernent des aspects qui ne relèvent pas de l'AEP, telles que la tenue d'un inventaire des ouvrages d'infrastructures critiques. Ainsi, l'AEP axe son travail avant tout sur les graves pénuries nationales, tandis que la stratégie PIC prend également en considération les perturbations plus courtes ou les pannes qui ne concernent pas toute la Suisse.

2.2.3 Politique de gestion des risques menée par la Confédération

En 2005, la Confédération a mis en place un système structuré de gestion stratégique des risques. L'accent y est mis sur les événements et les développements dont les principaux effets financiers et non financiers peuvent nuire à la poursuite des objectifs et à l'accomplissement des tâches de l'administration fédérale. Son champ d'application matériel est délimité par les compétences que le droit en vigueur confère à la Confédération. Bien que le système présente des liens avec les tâches des organes compétents et des autorités de surveillance et de régulation de la Confédération dans des secteurs critiques (marché de l'électricité, marchés financiers, santé, transports, communication, politique européenne [p. ex. négociations sur un éventuel accord sur l'électricité], politique de la Confédération en tant que propriétaire, etc.), la différence fondamentale avec la PIC réside dans le fait que cette dernière ne prend pas uniquement en considération les risques qui relèvent des compétences et de la responsabilité légales de la Confédération, mais qu'elle se concentre également sur l'ensemble des dommages sociaux et économiques causés par les pannes et les perturbations. Dans le cadre de la mise en œuvre de la stratégie nationale PIC, il convient d'identifier systématiquement les aspects déjà couverts par la gestion des risques menée par la Confédération et de définir les domaines où il y a lieu de prendre des mesures.

3 Champ d'application

Le champ d'application de la stratégie nationale PIC est délimité par la définition du concept d'infrastructure critique (voir chap. 1) et la détermination des secteurs et sous-secteurs critiques (branches).

L'éventail des infrastructures critiques couvre les domaines suivants :

Figure 1

Infrastructures critiques : secteurs et sous-secteurs (branches)

Secteurs	Sous-secteurs (branches)
Autorités	Recherche et enseignement
	Biens culturels
	Parlement, gouvernement, justice, administration
Énergie	Approvisionnement en gaz naturel
	Approvisionnement en pétrole
	Chauffage à distance et chaleur industrielle
	Approvisionnement en électricité
Élimination	Déchets
	Eaux usées
Finances	Services financiers
	Services d'assurance
Santé	Soins médicaux
	Prestations de laboratoire
	Chimie et produits thérapeutiques
Information et communication	Services informatiques
	Télécommunications
	Médias
	Services postaux
Alimentation	Approvisionnement en denrées alimentaires
	Approvisionnement en eau
Sécurité publique	Armée
	Services d'urgence
	Protection civile
Transports	Transport aérien
	Transport ferroviaire
	Transport fluvial
	Transport routier
	Criticité très élevée*
	Criticité élevée*
	Criticité importante*
<p>★ On entend par « criticité » l'importance relative du sous-secteur par rapport aux conséquences possibles d'une défaillance totale de plusieurs jours voire semaines pour la population et l'économie.</p> <p>► L'évaluation ne donne pas d'informations sur la criticité des éléments considérés individuellement.</p> <p>► L'évaluation s'appuie sur une situation de danger normale. En cas de catastrophe ou de situation d'urgence, la criticité des sous-secteurs peut changer.</p>	

Des précisions concernant les prestations d'importance majeure du point de vue de la PIC figurent à l'annexe 1.

On entend par sous-secteur (ou branche) critique tout système de services ou d'approvisionnement qui englobe l'ensemble d'un processus d'approvisionnement (de l'importation, notamment de prestations préalables, à la production ou la fabrication des biens et des services jusqu'à leur consommation) et couvre tous les domaines pertinents pour le fonctionnement du système en question. Ainsi, les infrastructures critiques ne se limitent pas aux ouvrages figurant dans l'Inventaire PIC, mais elles comprennent aussi tous les éléments (exploitant, systèmes informatiques, installations, constructions, etc.) qui fournissent des prestations dans l'un des 27 sous-secteurs mentionnés dans la figure 1, indépendamment de leur criticité. La criticité est une mesure relative de l'importance que revêt une panne de l'infrastructure critique pour la population et ses bases d'existence. Elle dépend de l'angle d'analyse : il existe ainsi des infrastructures d'une criticité nationale, voire internationale (p. ex. système de télécommande central du réseau de transport d'électricité), tandis que d'autres sont critiques pour l'approvisionnement au niveau local ou communal (p. ex. transformateur du réseau de distribution électrique). La criticité dépend également de l'événement qui se produit et de l'état du système : les produits et les services concernés ne sont, par exemple, pas les mêmes en cas de pandémie et en cas de panne de courant à grande échelle.

4 Principes

4.1 Approche globale

La PIC suit une approche globale. Elle tient compte, d'une part, de l'ensemble des vulnérabilités significatives ainsi que des dangers ou menaces qui en résultent et, d'autre part, de l'ensemble des mesures contribuant à améliorer la résilience³.

Les vulnérabilités résultent du fait que le fonctionnement des infrastructures critiques dépend de la disponibilité des ressources et des prestations (préalables) telles que l'énergie, la logistique ou l'informatique. Les différents domaines de ressources sont les suivants :

- le personnel : les personnes dont dépend en grande partie le fonctionnement des infrastructures critiques, comme les spécialistes ou le personnel d'exploitation) ;
- les matériaux et moyens d'exploitation : matières premières, sources d'énergie (carburant et combustible), produits semi-finis et finis ;
- les prestations : services nécessaires pour le fonctionnement, fournis au niveau national ou international, tels que la logistique, l'informatique (p. ex. systèmes de direction et de contrôle, services de navigation ou services en nuage) et l'approvisionnement en énergie.

³ Pour l'explication des notions relatives aux risques, vulnérabilités, etc., voir le glossaire des risques de l'OFPP, 2013, disponible sous www.babs.admin.ch > Autres domaines d'activité > Risques et dangers

Dans de nombreux cas, ces ressources dépendent de chaînes d’approvisionnement mondiales. Dans certains secteurs, il existe en outre une tendance à l’externalisation de processus commerciaux importants.

Les vulnérabilités significatives se trouvent là où une panne ou une perturbation de ces ressources entrave gravement le fonctionnement de l’infrastructure critique. Il faut donc les examiner de manière approfondie sur la base d’une analyse des risques et, si possible, les éliminer. L’analyse des risques a pour but de couvrir l’ensemble des dangers et des menaces, qui peuvent être regroupés dans les domaines suivants :

- dangers naturels : des perturbations graves pouvant être causées, par exemple, par des inondations, des tempêtes, des avalanches ou des séismes ;
- dangers techniques : par exemple, pannes de courant, défaillances de systèmes informatiques ou topologie de réseau lacunaire ;
- menaces et dangers sociétaux : par exemple, en rapport avec la PIC, actes de sabotage, terrorisme, cyberattaques ou pandémie.

Pour déterminer les risques, il est important de connaître la plausibilité d’un danger ainsi que les dommages pour la population et ses bases d’existence pouvant découler de la perturbation ou de la destruction de l’infrastructure critique.

La PIC doit également prendre en compte toutes les mesures qui contribuent à éviter les pannes ou à réduire le temps d’indisponibilité. Il s’agit de mesures préventives, préparatoires et liées à l’engagement qui visent à éviter les pannes ou à garantir le maintien du bon fonctionnement (continuité) en cas d’événement (p. ex. en définissant des processus de substitution ou des processus alternatifs, ou en renonçant à externaliser des processus commerciaux critiques). Les mesures visant à réduire l’ampleur des dommages en cas d’événement, notamment en améliorant le niveau de préparation de la population et de l’économie, jouent également un rôle important (la constitution de réserves domestiques et les groupes électrogènes de secours détenus par les entreprises contribuent entre autres de manière déterminante à réduire les dommages en cas de panne d’électricité). Les mesures à examiner peuvent être les suivantes :

- mesures techniques et mesures de construction : renforcement des bâtiments, acquisition de groupes électrogènes, séparation des systèmes informatiques, etc. ;
- mesures organisationnelles et administratives : contrôles d’accès, définition de postes de travail de remplacement, protection par des organisations de sécurité externes, choix d’un fournisseur particulièrement sûr lors de projets d’acquisition, etc. ;
- mesures concernant le personnel : règlement des suppléances, formation et sensibilisation des collaborateurs, etc. ;
- mesures juridiques et réglementaires : modification de bases légales spéciales (lois, ordonnances, instructions).

Les mesures de protection des informations sont valables pour tous ces domaines.

4.2 Proportionnalité

Les mesures PIC doivent présenter un équilibre optimal entre coûts et bénéfices (réduction des risques). L'objectif n'est pas d'éliminer complètement tous les risques. Un tel objectif n'est pas réalisable techniquement et nécessiterait par ailleurs des investissements trop élevés. Des perturbations et des pannes ne peuvent être entièrement exclues, mais il faut les gérer au mieux. Les mesures retenues ne doivent causer aucune distorsion du marché ou de la concurrence. D'une manière générale, les mesures de résilience doivent être financées par les acteurs qui en profitent (utilisateurs, exploitants, etc.).

4.3 Compétences et responsabilités

Les directives et les obligations applicables aux exploitants d'infrastructures critiques découlent notamment de la législation spéciale de chaque secteur (énergie, transports, finances, etc.). Les autorités de surveillance et de régulation sont chargées de vérifier si la législation est respectée et appropriée ou si elle doit être modifiée. En cas de catastrophe ou de situation d'urgence, les cantons, compétents en matière de sécurité intérieure et de protection de la population, sont tenus d'aider les exploitants dans la maîtrise des événements qui se produisent sur leur territoire en fonction de leurs moyens et de leurs possibilités. Dans le cadre d'engagements subsidiaires, l'armée peut, en cas de besoin, appuyer les autorités dans leurs tâches selon les moyens à disposition.

4.4 Collaboration public-privé

La PIC nécessite une collaboration entre tous les acteurs concernés (autorités fédérales, cantonales et communales, exploitants). La collaboration public-privé est notamment essentielle pour l'analyse et l'évaluation communes des risques et la définition de mesures de protection appropriées. L'échange d'informations est également indispensable.

5 Vision et objectifs de la stratégie nationale PIC

5.1 Vision

La stratégie nationale de PIC poursuit la vision suivante.

La Suisse est résiliente du point de vue de ses infrastructures critiques de sorte à éviter les pannes de grande ampleur et à limiter les dommages suite à un événement.

5.2 Objectifs stratégiques

Sur la base de cette vision, les objectifs suivants peuvent être définis.

-
- Les *infrastructures critiques* sont résilientes, de façon à éviter dans la mesure du possible des pannes graves et de grande ampleur géographique et à garantir rapidement le rétablissement du bon fonctionnement en cas d'événement.
 - Les *autorités* sont résilientes et préparées à aider efficacement (à titre subsidiaire) les exploitants dans la maîtrise des événements et à réagir de manière appropriée aux défaillances des infrastructures critiques.
 - La *population et l'économie* sont résilientes, si bien que les dommages causés par des pannes et des perturbations des infrastructures critiques restent limités.

5.3 Objectifs de mise en œuvre

Les objectifs stratégiques permettent de conclure qu'il faut améliorer non seulement la résilience des infrastructures critiques dans les différents secteurs, mais aussi la résilience intersectorielle, qui touche principalement les autorités, la population et l'économie.

1. Amélioration de la résilience dans les secteurs critiques : les exploitants et les autorités de surveillance et de régulation compétents sont tenus de vérifier la résilience des infrastructures critiques dans chaque secteur et, si possible, de l'améliorer. Le but est de déterminer les vulnérabilités et les risques spécifiques, afin de mettre en œuvre des mesures visant à éviter autant que possible les pannes et les perturbations graves ou de réduire les temps d'indisponibilité.
2. Amélioration de la résilience intersectorielle : l'accent est mis sur la résilience des autorités, de la population et de l'économie. Le but est de faire en sorte que tous les acteurs concernés travaillent ensemble afin de prendre des dispositions pour prévenir ou gérer les pannes qui touchent tous les secteurs. Les préparatifs doivent notamment viser à apporter un appui subsidiaire aussi efficace que possible aux exploitants des différents secteurs lors de la maîtrise des événements.

L'amélioration de la résilience dans chacun de ces deux domaines repose sur un processus en cinq étapes avec des objectifs propres à chacune.

Boucle de régulation pour améliorer la résilience



Analyse

- Les processus, systèmes, objets, etc. critiques sont identifiés.
- Les vulnérabilités et les risques susceptibles d’entraîner des pannes graves sont identifiés et analysés.
- Les modifications significatives des dangers et des menaces concernant les infrastructures critiques sont détectées suffisamment tôt et communiquées aux services pertinents.

Évaluation

- Les écarts avec les directives en vigueur sont connus.
- Le niveau de sécurité visé est fixé.

Mesures (de protection)

Des mesures sont définies pour éviter, dans la mesure du possible, les pannes graves ou pour les maîtriser. Seules les mesures qui permettent d’atteindre un niveau de résilience optimal doivent être adoptées (coûts totaux minimaux, qui se composent des coûts des mesures supplémentaires et des coûts liés aux risques qui subsistent après la mise en œuvre).

Mise en œuvre

- Les mesures définies sont mises en œuvre de manière efficace.

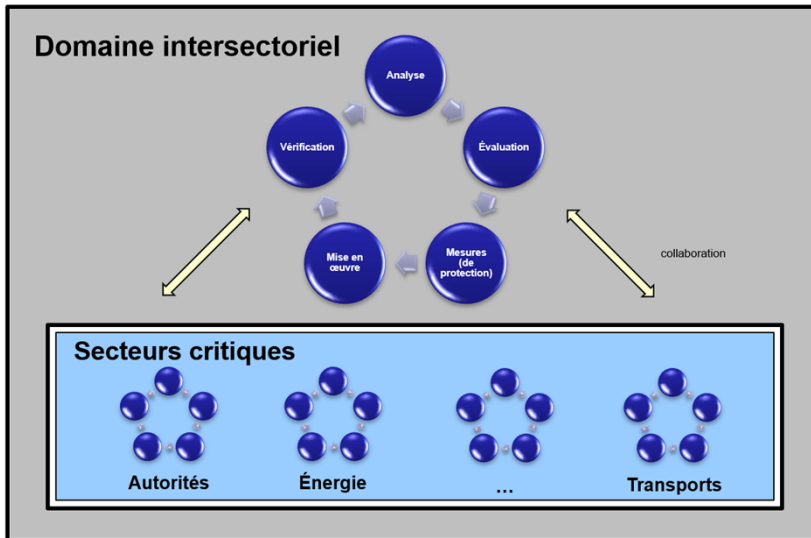
Vérification

- Les mesures sont consolidées dans le cadre d'exercices et de formations.
- L'efficacité des mesures mises en œuvre est contrôlée.

Les objectifs de mise en œuvre présentés dans la boucle de régulation concernent à la fois les différents secteurs et le domaine intersectoriel. Ils peuvent être représentés comme suit.

Figure 3

Objectifs de mise en œuvre



6 Mesures de la stratégie nationale PIC

Les mesures présentées permettront d'atteindre les objectifs de mise en œuvre décrits au ch. 5 et dans la figure 3. La mesure 1 (ch. 6.1) montre comment améliorer la résilience dans les secteurs critiques. Les mesures 2 à 8 (ch. 6.2) concernent le domaine intersectoriel.

Le but est de déterminer les actions nécessaires pour atteindre les objectifs, en formulant tout d'abord des mesures, puis en esquissant la manière dont elles seront mises en œuvre.

Les mesures présentées se limitent à des tâches essentielles à long terme. Elles seront concrétisées dans des planifications de mise en œuvre ou des plans d'action distincts et, si nécessaire, complétées par d'autres mesures à plus court terme (voir à ce sujet les explications relatives à la mise en œuvre de la stratégie au ch. 7).

Dans le contexte de la PIC, de nombreux projets, mesures, etc. déjà établis ou planifiés sont pertinents. C'est pourquoi la mise en œuvre de la stratégie nationale PIC consiste souvent à vérifier les processus en place et à les compléter si nécessaire. La stratégie nationale PIC s'appuie autant que faire se peut sur ce qui existe déjà.

6.1 Améliorer la résilience dans les secteurs critiques

Les mesures prises pour améliorer la résilience dans les secteurs critiques visent à faire en sorte que chacun des secteurs (électricité, télécommunications, transport routier, etc.) ait une résilience à la hauteur de son importance. Que ce soit du côté des exploitants ou au sein des différents secteurs, de nombreuses dispositions ont généralement été mises en place pour améliorer la résilience (p. ex. des règlements spécifiques aux secteurs ou des mesures particulières dans le cadre de l'AEP). Il s'agit par conséquent d'appliquer la procédure décrite au ch. 5.3 pour vérifier si les dispositions prises sont suffisantes ou si des modifications sont nécessaires.

Ces travaux doivent en particulier être menés à deux niveaux.

1. Au niveau de chaque exploitant, qui dispose généralement d'un système de gestion des risques, des situations d'urgence, des crises et de la continuité. Des dispositions parfois importantes sont ainsi mises en œuvre afin de maintenir les activités en cas de catastrophe ou de situation d'urgence. Il n'est toutefois pas garanti que les processus essentiels pour la population et l'économie soient considérés comme prioritaires par les entreprises qui exploitent des infrastructures critiques. C'est pourquoi les exploitants sont responsables de vérifier si les dispositions sont suffisantes ou s'il convient de prendre des mesures supplémentaires pour améliorer la résilience. L'OFPP a publié un guide et un manuel d'application sur lesquels les exploitants peuvent s'appuyer pour réaliser ces travaux⁴.
2. Il convient par ailleurs de vérifier et d'améliorer la résilience au niveau de chaque sous-secteur critique (approvisionnement en eau et en électricité, télécommunications, etc.). À cet effet, les autorités responsables des secteurs selon l'annexe 2 et les exploitants vérifient ensemble s'il existe des vulnérabilités et des risques importants, et s'il faut prendre des mesures supplémentaires pour atteindre un niveau de résilience ou de sécurité (de l'approvisionnement) approprié et proportionné (voir à ce sujet les explications concernant les mesures [de protection] au ch. 5.3 et les champs d'action évaluation au ch. 6.2.2). Les dispositions en vigueur (mesures prises par les exploitants ou, p. ex., par l'AEP) doivent être prises en considération. Les risques résiduels peuvent souvent être réduits en recourant à des solutions sectorielles telles qu'une convention réglant la collaboration en cas d'événement. Mais il peut aussi s'avérer nécessaire d'édicter des directives ou des prescriptions supplémentaires pour les exploitants en modifiant les bases légales spéciales. L'élaboration des directives et le financement des éventuelles mesures de protection supplémentaires nécessaires doivent être

⁴ Ce manuel est disponible sous www.infraprotection.ch > Guide PIC.

négociés dans les différents secteurs politiques (politique énergétique, politique des transports, politique de la santé, etc.) sous la responsabilité des organes compétents et des autorités de surveillance et de régulation. Étant donné que les vulnérabilités et les risques dans les différents secteurs évoluent en permanence (p. ex. dans le contexte de la numérisation ou de l'externalisation de processus clés), la résilience doit faire l'objet d'une vérification périodique.

Mesure 1

- Examiner périodiquement les infrastructures critiques afin de vérifier s'il existe des vulnérabilités et des risques susceptibles d'entraîner des perturbations et des pannes graves et si des mesures supplémentaires sont nécessaires pour améliorer la résilience.

Mise en œuvre

- Les exploitants vérifient et améliorent leur résilience, en s'appuyant par exemple sur le guide PIC. Ces travaux relèvent de la responsabilité des exploitants et sont menés en collaboration avec les organes compétents et les autorités de surveillance et de régulation.
- Les organes compétents et les autorités de surveillance et de régulation visés à l'annexe 2 examinent périodiquement, en général tous les quatre ans, s'il existe des vulnérabilités et des risques susceptibles d'entraîner des pannes et des perturbations graves dans les sous-secteurs critiques. Elles déterminent les mesures nécessaires pour améliorer la résilience, en clarifient les coûts et l'utilité, et créent les conditions légales nécessaires à leur mise en œuvre.

6.2 Améliorer la résilience dans le domaine intersectoriel

Les mesures visant à améliorer la résilience dans le domaine intersectoriel s'appuient également sur la boucle de régulation présentée au ch. 5.3 (analyse, évaluation, mesures [de protection], mise en œuvre, contrôle, voir fig. 2).

6.2.1 Champ d'action analyse

Champ d'action analyse – identifier les infrastructures critiques et fixer les priorités

Avant que des mesures puissent être prises et des priorités fixées pour la gestion des risques ou pour la maîtrise des catastrophes et des situations d'urgence, les services compétents doivent connaître les infrastructures particulièrement critiques. Les constructions et les installations sont particulièrement concernées en raison leur nombre et de leur importance. C'est pourquoi l'OFPP tient un inventaire des infrastructures critiques (Inventaire PIC), qui répertorie les ouvrages importants au niveau national ou cantonal. L'Inventaire PIC doit être mis à jour périodiquement. Certains exploitants dont l'activité ne dépend pas ou que partiellement de certains ouvrages (p. ex. entreprises de transport) peuvent néanmoins avoir une grande importance. Il est donc important d'identifier également ces entreprises et organisations et d'identifier les processus critiques, en se fondant sur leur importance pour les bases d'existence de la population et le fonctionnement de l'économie.

Mesure 2

- Tenir un inventaire des infrastructures critiques mis à jour périodiquement, dans lequel figurent les constructions et installations critiques ainsi que les entreprises et organisations critiques et les processus correspondants.

Mise en œuvre

- Le DDPS (OFPP) est responsable d'identifier les infrastructures critiques revêtant une importance majeure d'un point de vue national et de mettre régulièrement à jour les données en collaboration avec les offices compétents et les exploitants. Les données de base (en particulier les interlocuteurs) sont vérifiées tous les deux ans et l'inventaire est entièrement révisé tous les quatre ans. Les cantons identifient les ouvrages d'infrastructures critiques revêtant une importance primordiale d'un point de vue cantonal et mettent à jour les données périodiquement.

Champ d'action analyse – connaître les risques, les vulnérabilités et les mesures de protection

Pour améliorer la résilience des infrastructures critiques, il faut disposer d'analyses intersectorielles sur les risques significatifs. Les analyses provenant des sous-secteurs critiques doivent donc être consolidées et réunies afin d'obtenir une vue d'ensemble des risques.

De plus, une recherche scientifique fondamentale est indispensable pour développer la PIC sur le plan méthodologique, notamment dans le domaine des analyses de résilience, d'interdépendance ou de criticité. Il convient également de suivre les évolutions technologiques, environnementales et contextuelles afin d'identifier les nouveaux risques. Ces travaux sont menés dans le cadre de la recherche de l'administration fédérale et des cantons, de sorte qu'aucune mesure spécifique n'est prévue au niveau de la stratégie PIC.

Champ d'action analyse – améliorer la collaboration et l'échange d'informations entre les secteurs

Les infrastructures critiques dépendent souvent les unes des autres. La collaboration et le dialogue sur les risques et les mesures de protection possibles (*best practices*) entre les représentants des différents secteurs sont par conséquent indispensables. L'OFPP coordonne actuellement deux plateformes de collaboration au sein desquelles les acteurs importants des différents secteurs échangent des informations (plateforme des exploitants d'infrastructures critiques nationales et groupe de travail PIC des autorités). L'expérience montre que la collaboration intersectorielle et intercantonale dans le domaine PIC rencontre un vif intérêt. Les plateformes offrent la possibilité aux différents acteurs (services fédéraux et exploitants) ainsi qu'aux cantons d'échanger leurs expériences et d'envisager ensemble des solutions. Il faut aussi renforcer les échanges entre les différentes plateformes (p. ex. entre les exploitants et les cantons) à titre d'amélioration supplémentaire. Une autre mesure pertinente est de créer une structure pour la formation et la formation continue ciblées des partenaires compétents de la Confédération, des cantons et des exploitants (p. ex. en ce qui concerne la méthode et les bonnes pratiques). Enfin, étant donné que les infrastructures critiques forment souvent des systèmes transfrontaliers, la

collaboration intersectorielle au niveau international peut également être importante. Les thèmes spécifiques aux secteurs sont traités dans le cadre des politiques et des domaines d'activités sectoriels.

Mesure 3

- Maintenir les plateformes qui contribuent à améliorer la collaboration intersectorielle et intensifier les échanges entre et au sein de ces plateformes en cas de besoin. Vérifier périodiquement leur composition.

Mise en œuvre

- Le DDPS (OFPP) coordonne la plateforme des exploitants d'infrastructures critiques nationales et le groupe de travail PIC des autorités (Confédération et cantons). Les cantons gèrent, si nécessaire et selon leurs possibilités, leurs propres plateformes de coopération. Les exploitants gèrent également d'autres plateformes d'échange sous leur propre responsabilité.

Champ d'action analyse – détecter et annoncer à temps les dangers et les menaces

En cas d'événements menaçants (p. ex. graves crues imminentes, cyberattaques ou actes de sabotage), les exploitants doivent être informés à temps du danger ou de la menace afin de pouvoir adapter leur dispositif de sécurité. Dans certains domaines ou pour certains dangers et certaines menaces, des modes de coopération ont été mis en place pour s'assurer que les exploitants soient informés dans les meilleurs délais en cas d'événement (p. ex. cercle fermé des clients du NCSC, suivi coordonné de la situation de la NEOC [ancienne CENAL], collaboration dans le domaine du SRC, etc.). Dans le contexte de la stratégie PIC, le défi consiste à s'assurer périodiquement que tous les exploitants concernés sont impliqués dans les processus pertinents. De leur côté, les exploitants veillent à informer le plus tôt possible les organes de crise de la Confédération et des cantons, qui ont besoin d'être rapidement mis au courant en cas de panne ou de perturbation. La NEOC dispose elle aussi de processus établis. Dès lors, le but est de vérifier périodiquement que les principaux exploitants sont impliqués.

Mesure 4

- Examiner régulièrement, du point de vue de l'implication des exploitants, les processus spécifiques aux dangers qui garantissent la transmission des informations dans les meilleurs délais en cas d'événement et compléter ces processus si nécessaire.

Mise en œuvre

- Le DDPS (OFPP) vérifie, en collaboration avec les organes compétents en fonction des différentes menaces, si les principaux exploitants sont impliqués dans les processus requis et élaborent au besoin des propositions pour compléter les processus concernés.

6.2.2 Champ d'action évaluation

L'évaluation vise à définir les principes, pour le domaine intersectoriel, permettant aux infrastructures critiques des différents secteurs de présenter un niveau de résilience adéquat. En matière de PIC, il ne faut pas fixer de valeurs limites, comme

la durée maximale tolérable d'une panne, car de telles valeurs ne tiennent pas compte du coût des mesures requises pour les atteindre. Il faut plutôt choisir une approche fondée sur les risques et sur une évaluation des coûts marginaux. Cette approche consiste à s'assurer d'atteindre le meilleur rapport possible entre le coût des mesures de protection supplémentaires et les risques résiduels après la mise en œuvre. La démarche est différente pour chaque cas individuel. Le but est de procéder à une pesée des intérêts qui prenne en compte d'autres aspects (p. ex. durabilité, atteintes à la liberté économique) et de les intégrer au processus de décision.

Les explications précédentes montrent clairement que le degré optimal de résilience dépend en grande partie des mesures à prendre (en particulier de leur coût et de la réduction des risques qui en découle). C'est pourquoi il n'est déterminé qu'à l'étape mesures de protection de la boucle de régulation décrite au ch. 5.3.

Dans le domaine intersectoriel, l'étape évaluation vise avant tout à définir les principes relatifs au niveau de sécurité visé. Compte tenu de l'approche fondée sur l'évaluation coûts marginaux qu'il convient d'appliquer dans le cadre de la PIC, il s'agit donc en particulier de déterminer le prix que la société est prête à payer pour éviter des dommages (p. ex. pour éviter la perte d'une vie). Ce niveau de sécurité devrait être identique et comparable dans tous les domaines des infrastructures critiques. Toutefois, le niveau concret de résilience ne sera pas partout le même. La démarche vise en effet à ce que toutes les infrastructures critiques présentent un niveau de résilience en rapport avec leur importance. Comme les infrastructures critiques de très grande importance présentent des risques plus élevés, il est possible de prendre davantage de mesures présentant un rapport coûts-utilité optimal pour atteindre ainsi un niveau de résilience plus élevé.

La démarche ainsi que l'estimation des coûts marginaux et du prix que la société est prête à payer sont décrites en détail dans la documentation méthodologique pour l'examen et l'amélioration de la résilience des infrastructures critiques (en particulier dans le guide PIC).

6.2.3 Champ d'action mesures (de protection)

Champ d'action mesures (de protection) – créer les bases nécessaires pour prévenir les pannes des infrastructures critiques

Dans ce champ d'action, les mesures intersectorielles visant à améliorer la résilience ou à prévenir les perturbations et les pannes graves sont au premier plan. En cas de catastrophe ou de situation d'urgence (p. ex. une pandémie ou une grave pénurie d'électricité), la maîtrise de l'événement doit autant que possible accorder la priorité aux infrastructures critiques afin d'éviter les pannes subséquentes. Des dérogations ou des priorités de ce type sont déjà prévues pour les entreprises d'importance systémique et les entreprises importantes pour l'approvisionnement. La stratégie nationale PIC de 2012 proposait également différentes approches pour définir les priorités en matière d'infrastructures critiques. Celles-ci doivent à présent être mises en œuvre et actualisées périodiquement.

Les travaux menés à ce jour relatifs à la vérification et à l'amélioration de la résilience des infrastructures critiques ont montré que ces infrastructures sont pratiquement toutes dépendantes d'un réseau de télécommunications fiable. Le bon fonctionnement

de la communication entre les exploitants et les services chargés de la maîtrise des événements est également une condition indispensable pour pouvoir maîtriser les catastrophes et les situations d'urgence, en particulier en cas de pénurie d'électricité ou de panne de courant de longue durée. En conséquence, la mise en place, en cours de réalisation, d'un nouveau réseau télématique sûr, autonome et hautement disponible, auquel les exploitants d'infrastructures critiques pourront également être raccordés constitue une mesure intersectorielle importante pour prévenir les pannes.

Les bases légales intersectorielles et leurs directives destinées aux exploitants d'infrastructures critiques constituent un autre instrument important pour prévenir les pannes. Un premier examen des bases légales existantes a été effectué dans le cadre de la stratégie nationale PIC 2018–2022. Il portait sur les prescriptions relatives à l'annonce de graves incidents de sécurité et de pannes, sur la réalisation de contrôles de sécurité pour les collaborateurs exerçant des fonctions critiques (notamment dans le domaine des centrales de commande et de contrôle) et sur l'édiction de directives contraignantes en matière de résilience. Il s'est avéré que le droit en vigueur ne contient pratiquement pas de prescriptions concrètes et explicites en matière de résilience, auxquelles les exploitants pourraient se référer comme ils peuvent le faire dans d'autres domaines (comme la prévention des accidents majeurs). La motion 23.3001 « Bases légales modernes pour la protection des infrastructures critiques » et un audit du CDF sur la PIC, publié début 2023, réclament également des bases légales plus contraignantes dans ce domaine⁵. Il faut donc élaborer des propositions pour une telle base légale.

Mesure 5

- Examiner une proposition de base légale en vue de l'édiction de directives intersectorielles.

Mise en œuvre

- Le DDPS (OFPP) et les acteurs compétents (en particulier le DEFR, le DETEC, le DFJP et le DFF) étudient ensemble une proposition de base légale intersectorielle. Celle-ci doit se concentrer sur les aspects du contrôle de la sécurité relatif aux personnes exerçant des fonctions critiques, sur l'obligation d'annoncer les incidents de sécurité et les pannes et sur l'édiction de directives contraignantes en matière de résilience.

Champ d'action mesures (de protection) – améliorer l'appui subsidiaire aux exploitants pour la maîtrise des événements

En cas de menaces et de dangers imminents ou de panne grave, les exploitants doivent bénéficier d'un appui subsidiaire efficace des autorités avec des moyens ou des capacités externes afin de maîtriser l'événement. Il peut s'agir de forces d'intervention (police, sapeurs-pompiers, protection civile, armée), de moyens de communication ou de groupes électrogènes de secours. Cela permet d'éviter, par exemple en cas de crue ou d'attaque terroriste, que la population, l'économie ou d'autres infrastructures critiques subissent des dommages supplémentaires en cas de panne d'une infrastructure critique (effets dominos).

⁵ Le rapport est disponible sous www.efk.admin.ch > Publications > Défense & armée.

Pour les risques conventionnels, les exploitants peuvent disposer, de manière parfois limitée, des moyens de la police, des sapeurs-pompiers, des services sanitaires et de la protection civile. En ce qui concerne les substances chimiques, biologiques et radiologiques, des moyens de l'OFPP (groupe d'intervention du DDPS) peuvent constituer une aide subsidiaire pour les équipes d'intervention sur place. Étant donné que la PIC fait partie de la mission générale (de protection) des organisations d'intervention, celles-ci doivent s'assurer que les moyens à disposition sont utilisés de manière optimale en cas d'événement. Lors de l'attribution des moyens dans le cadre de l'appui, les priorités doivent être fixées en tenant compte de l'importance (criticité) des infrastructures critiques, de la situation de la menace et des moyens disponibles. Il faut partir du principe que seul un petit nombre d'infrastructures critiques d'importance majeure peuvent être protégées. Les exploitants doivent par conséquent disposer de mesures de prévention efficaces et d'un système de gestion des risques et de la continuité éprouvé (ce qui correspond à l'objectif de la mesure 1). Les collaborations sectorielle et intersectorielle entre les exploitants d'infrastructures critiques jouent également un rôle capital dans la gestion des incidents.

Concernant la priorisation des organisations d'intervention étatiques, le défi réside dans le fait que les moyens opérationnels dans le domaine de la police et de la protection de la population relèvent des cantons et des communes ; ce sont eux qui établissent souvent l'ordre de priorité pour la répartition des moyens en cas d'événement, alors que de nombreuses infrastructures critiques représentent des systèmes en réseau exploités à un niveau national ou international (p. ex. réseaux de transport d'électricité). Il est par conséquent important de procéder à une évaluation générale à l'échelon national en fonction des événements. Lors de la mise en œuvre de la stratégie nationale PIC 2018-2022, les processus et les compétences dans le domaine de l'appui aux exploitants lors de la gestion d'événements ont été examinés et des propositions d'optimisation ont été élaborées. Un élément important dans ce contexte a été l'établissement d'une pesée globale des intérêts impliquant tous les acteurs concernés, comme cela a été fait lors de la gestion de la pandémie de COVID-19 dans le cadre de la gestion fédérale des ressources. La coordination globale des ressources est préparée dans le cadre de la mise en œuvre des recommandations relatives à l'exercice du Réseau national de sécurité 2019.

Afin d'optimiser la gestion des événements, des planifications préventives des interventions adaptées à la situation actuelle sont nécessaires. L'armée et certains cantons disposent déjà de telles planifications pour des ouvrages d'importance majeure figurant dans l'Inventaire PIC. Il convient de les réviser périodiquement et de les compléter en cas de besoin.

Mesure 6

- Élaborer et mettre à jour périodiquement des planifications des interventions PIC pour les ouvrages particulièrement critiques

Mise en œuvre

- Le DDPS (Groupement Défense) élabore et actualise périodiquement des dossiers d'ouvrages militaires pour les ouvrages de l'Inventaire PIC des classes de rendement 4 et 5. Pour les infrastructures critiques particulièrement importantes, les cantons élaborent et actualisent des planifications civiles dans

le domaine de la protection de la population, par exemple dans le cadre de l'analyse de dangers et des mesures de protection. Les planifications civiles et militaires sont coordonnées.

Champ d'action mesures (de protection) – améliorer la préparation de la population, de l'économie et des pouvoirs publics

Des pannes graves d'infrastructures critiques peuvent affecter considérablement les moyens de subsistance de la population, nuire à l'environnement et compromettre sérieusement le fonctionnement de l'économie et des pouvoirs publics. Il est possible de réduire l'ampleur des dommages par une préparation appropriée de la population, l'économie et l'État. Pour cette raison, une grande importance est accordée aux planifications préventives pour maîtriser les incidents ainsi qu'à la sensibilisation préalable de la population et de l'économie aux risques éventuels et aux mesures préventives autonomes. En raison de l'importance cruciale de l'approvisionnement en électricité, la priorité est accordée aux planifications visant à maîtriser une coupure de courant ou une pénurie d'électricité. Plusieurs travaux sont en cours dans ce cadre, aussi bien au niveau de la Confédération que des cantons. Afin de sensibiliser les entreprises et la population, différents outils ont également été élaborés et font l'objet d'un suivi dans le cadre de l'AEP et d'Alertswiss (p. ex. guide pratique sur les questions liées à l'électricité destiné à l'économie et à la population, modèle pour élaborer un plan d'urgence personnel).

Mesure 7

- La Confédération et les cantons élaborent et actualisent périodiquement des planifications préventives pour la gestion des pannes graves d'infrastructures critiques.

Mise en œuvre

- Dans le cadre des planifications préventives de la Confédération, les autorités fédérales compétentes élaborent, avec les acteurs concernés (cantons, association, etc.), des planifications préventives pour la gestion des pannes d'infrastructures critiques. À l'échelon cantonal, des planifications correspondantes sont réalisées dans le cadre de l'analyse des dangers et de la mise en œuvre de mesures de protection.

6.2.4 Champ d'action mise en œuvre et vérification

Les services compétents de la Confédération, des cantons et des exploitants mettent en œuvre les mesures de la stratégie nationale PIC. Les deux stratégies précédentes montrent que la répartition des responsabilités entre de nombreux acteurs constitue un défi de taille et que la stratégie, qui fait de la PIC une tâche commune à tous ces acteurs, n'est pas encore devenue une évidence. Jusqu'à présent, la PIC est encore trop souvent perçue comme une tâche exclusive de l'OFPP et l'on oublie parfois qu'elle relève également des autorités sectorielles de surveillance et de régulation. Pour que les politiques et les tâches sectorielles prennent mieux en compte la protection et la résilience des infrastructures critiques, il est donc nécessaire de renforcer l'assise de la stratégie PIC sur le plan politique et stratégique. L'audit du CDF sur la PIC, publié début 2023, est parvenu à la même conclusion en disant que le Conseil fédéral devait suivre de plus près la mise en œuvre de la stratégie nationale.

En conséquence, il est désormais prévu que la délégation du Conseil fédéral pour l'énergie, l'environnement et les infrastructures, comptant des représentants du DETEC, du DFF et du DDPS, examine périodiquement l'avancement des mesures de la stratégie. Cette délégation regroupe des départements dont de nombreux offices s'occupent des infrastructures, des intérêts du propriétaire des entreprises liées à la Confédération et des organes de sécurité de la Confédération.

Dans ce champ d'action, il est aussi important d'organiser des exercices afin de tester la praticabilité des structures et les planifications. Ces exercices pourront être intégrés aux exercices déjà organisés au niveau fédéral et cantonal.

Mesure 8

- Vérifier l'avancement des mesures de la stratégie nationale PIC dans le cadre de la délégation du Conseil fédéral pour l'énergie, l'environnement et les infrastructures

Mise en œuvre

- Le DDPS (OFPP) tient un suivi des mesures de la stratégie nationale PIC et prépare le dossier à l'intention du DETEC, qui assure la présidence de la délégation.

7 Mise en œuvre de la stratégie nationale PIC

7.1 Structures et compétences

La stratégie nationale PIC est mise en œuvre de façon décentralisée dans le cadre des structures et des responsabilités existantes. Les exploitants, les organes compétents et les autorités de surveillance et de régulation sont en particulier responsables de la résilience des infrastructures critiques. Ils assurent l'examen périodique et, si nécessaire, l'amélioration de la résilience conformément à la mesure 1 de la stratégie. À cette fin, ils analysent systématiquement les vulnérabilités et les risques spécifiques susceptibles d'entraîner des pannes et des perturbations graves. Ils se fondent sur les résultats afin de définir les mesures nécessaires pour atteindre un niveau de résilience approprié et créent les conditions requises pour les mettre en œuvre. Les compétences pour la mise en œuvre de ces mesures sont définies dans les annexes 1 et 2. L'annexe 2 donne en outre un aperçu des compétences pour la mise en œuvre des autres mesures de la stratégie PIC.

Le secrétariat PIC de l'OFPP assure la coordination générale des travaux de mise en œuvre, dont font notamment partie les tâches suivantes :

- coordonner les mesures visant à renforcer la résilience dans le domaine intersectoriel (p. ex. tenue de l'Inventaire PIC) ;
- appuyer sur le plan méthodologique et conseiller les autorités compétentes et les exploitants dans la vérification et l'amélioration de la résilience ;
- conseiller les cantons en matière de PIC ;
- coordonner les deux plateformes d'échange nationales ;

-
- servir d’interlocuteur en matière de PIC aux plans national et international ;
 - contrôler l’avancement des différentes mesures de la stratégie ;
 - rendre compte de l’état d’avancement et mettre à jour la stratégie.

La délégation du Conseil fédéral pour l’énergie, l’environnement et les infrastructures surveille la mise en œuvre des mesures de la stratégie nationale PIC (mesure 8). Elle contrôle notamment l’avancement des mesures visant à améliorer la résilience des secteurs critiques (mesure 1) en se concentrant sur les sous-secteurs ou branches présentant une criticité particulièrement élevée (selon la fig. 1).

Il convient par ailleurs d’examiner, par exemple dans le cadre du développement de la gestion de crise de la Confédération, s’il serait possible de confier la fonction de comité de pilotage à un organe existant au niveau de la direction, qui regrouperait notamment des représentants des services de la Confédération concernés, des exploitants d’infrastructures critiques et des cantons.

7.2 Calendrier et contrôle

La mise en œuvre des différentes mesures et des recommandations générales est précisée dans une planification spécifique et vérifiée au moyen d’un système de contrôle. La planification définit notamment les responsabilités concrètes liées aux différentes mesures (en particulier en ce qui concerne la mesure 1 relative à la vérification et à l’amélioration de la résilience au niveau des sous-secteurs critiques). En sa qualité d’organe de pilotage, la délégation du Conseil fédéral pour l’énergie, l’environnement et les infrastructures est chargée, sur le plan stratégique, de contrôler l’efficacité de la mise en œuvre et de mener les discussions sur la planification de cette dernière et sur les plans d’actions, y compris sur les mesures supplémentaires à prendre le cas échéant.

7.3 Révision de la stratégie PIC

La stratégie nationale PIC formule des mesures valables à long terme. Le besoin de mise à jour est examiné tous les quatre ans ou en cas de besoin concret de révision (p. ex. en raison d’une modification fondamentale de la situation en matière de dangers ou de menaces).

Date

Au nom du Conseil fédéral suisse :

Le président de la Confédération, Alain Berset

Le chancelier de la Confédération, Walter Thurnherr

Description des sous-secteurs et des compétences pour l'amélioration de la résilience dans les secteurs critiques (mesure 1)

Secteur	Sous-secteur	Prestations d'importance majeure du point de vue PIC (liste non exhaustive)	Organes fédéraux compétents (liste non exhaustive)*
Autorités	Recherche et enseignement	Prestations basées sur les résultats de recherche en cas de catastrophe et de situation d'urgence (p. ex. service sismologique)	SEFRI
	Biens culturels	Garantie de la sécurité du droit (en particulier archives d'État), création d'une identité culturelle	OFPP, OFC
	Parlement, gouvernement, justice, administration	Législation, conduite et exécution des tâches de l'État, jurisprudence et application de la loi, tâches administratives d'ordre général (p. ex. alerte et alarme en cas de danger, maintien de la sûreté intérieure)	SP, ChF, départements
Énergie	Approvisionnement en gaz naturel	Commerce, transport, stockage et distribution de gaz naturel	OFEN, IFP, OFAE
	Approvisionnement en pétrole	Commerce, transport, stockage et distribution de combustibles et carburants (essence, kérosène, etc.)	OFEN, IFP, OFAE
	Approvisionnement en électricité	Production, stockage, commerce, transport et distribution d'énergie électrique	OFEN, ECom, OFAE, IFSN, ESTI,
	Chauffage à distance et chaleur industrielle	Production et distribution de chaleur à distance et de chaleur industrielle	OFEN
Élimination	Déchets	Collecte, élimination et valorisation des déchets spéciaux, urbains et industriels	OFEV
	Eaux usées	Élimination des eaux usées résidentielles, artisanales et industrielles pour protéger la population (santé) et l'environnement	OFEV
Finances	Services financiers	Exécution des opérations de paiements, approvisionnement de la population en argent liquide, capitalisation de tiers,	FINMA / BNS, SFI, OFAE, OFCOM

Secteur	Sous-secteur	Prestations d'importance majeure du point de vue PIC (liste non exhaustive)	Organes fédéraux compétents (liste non exhaustive)*
		rémunération de dépôts et maintien de la stabilité des prix	
	Services d'assurance	Garantie de la couverture d'assurance, de l'aide financière en cas de dommages et prestations dans le cadre de la prévention des dommages (y c. assurances maladie et sociales)	FINMA, SFI, OFAS, OFSP
Santé	Soins médicaux	Traitement et prise en charge de patients (médecine de premier recours, médecine spécialisée ou hospitalière), soins vétérinaires de base	OFSP, OFPP
	Prestations de laboratoire	Analyses de diagnostic de laboratoire pour la protection de l'être humain, de l'animal et de l'environnement	OFSP, OSAV, OFPP
	Chimie et produits thérapeutiques	Approvisionnement en produits thérapeutiques (médicaments et produits médicaux), y c. vaccins	OFAE, Swissmedic, Pharmacie de l'armée
Information et communication	Services informatiques	Services informatiques pour l'économie (en particulier traitement et stockage des données ou services infonuagiques)	OFAE
	Télécommunications	Services accessibles au public (appels d'urgence, internet, etc.), transmission de signaux de radio et de télévision	OFCOM, OFAE
	Médias	Information de la population en cas de catastrophe et de situation d'urgence, formation de l'opinion politique	OFCOM
	Services postaux	Services postaux relevant du service universel, en particulier dans les domaines de la correspondance officielle et de la correspondance commerciale	OFCOM, OFAE
Alimentation	Approvisionnement en denrées alimentaires	Approvisionnement de la population en denrées alimentaires	OFAE, OFAG
	Approvisionnement en eau	Approvisionnement de la population et de l'économie en eau potable et en eau non potable	OFEV, OFAE
Sécurité publique	Armée	Aide militaire en cas de catastrophe, engagements subsidiaires de sûreté, aide à la conduite pour la population civile, défense du pays	Groupement Défense

Secteur	Sous-secteur	Prestations d'importance majeure du point de vue PIC (liste non exhaustive)	Organes fédéraux compétents (liste non exhaustive)*
	Services d'urgence	Garantie de la sécurité publique, interventions de secours et de sauvetage, interventions de la police, des sapeurs-pompiers et des services sanitaires pour maîtriser les catastrophes et les situations d'urgence	fedpol, OFPP
	Protection civile	Soutien pour la maîtrise de catastrophes et de situations d'urgence	OFPP
Transports	Transport aérien	Transport aérien de personnes et de marchandises	OFAC, OFAE
	Transport ferroviaire	Transport ferroviaire de personnes et de marchandises	OFT, OFAE
	Transport nautiquefluvial	Transport fluvial de marchandises (en particulier accès aux ports maritimes)	BAV, BWL
	Transport routier	Transport routier de personnes et de marchandises (trafic motorisé individuel et transports publics)	OFROU, OFAE

* Les services mentionnés, en collaboration avec le secrétariat PIC, désignent le service qui assume la responsabilité principale et indique les autres acteurs (Confédération, cantons, associations, etc.) doivent être impliqués. Les compétences en vigueur restent inchangées.

Aperçu des mesures, des compétences et des interfaces

Mesure	Organes compétents (liste non exhaustive)*	Interfaces (liste non exhaustive)
M1 : Vérifier et améliorer la résilience des infrastructures critiques		
<i>Résilience exploitants</i>	Exploitants	Gestion des risques, BCM
<i>Résilience sous-secteurs / des branches critiques</i>		Projets sectoriels, CSN
<i>Résilience recherche et enseignement</i>	SEFRI	
<i>Résilience biens culturels</i>	OFPP, OFC	
<i>Résilience parlement, gouvernement, justice, administration</i>	SP, ChF, départements	
<i>Résilience approvisionnement en gaz naturel</i>	OFEN, IFP, OFAE	
<i>Résilience approvisionnement en pétrole</i>	OFEN, IFP, OFAE	
<i>Résilience chauffage à distance et chaleur industrielle</i>	OFEN	
<i>Résilience approvisionnement en électricité</i>	OFEN, ElCom, OFAE, IFSN, ESTI	
<i>Résilience déchets</i>	OFEV	
<i>Résilience eaux usées</i>	OFEV	
<i>Résilience services financiers</i>	FINMA, SFI, OFAE, OFCOM	
<i>Résilience services d'assurance</i>	FINMA, SFI, OFAS, OFSP	
<i>Résilience soins médicaux</i>	OFSP, OFPP	
<i>Résilience prestations de laboratoire</i>	OFSP, OSAV, OFPP	
<i>Résilience chimie et produits thérapeutiques</i>	OFAE, Swissmedic, PharmaA	
<i>Résilience services informatiques</i>	OFAE, ChF	
<i>Résilience télécommunications</i>	OFCOM, OFAE	
<i>Résilience médias</i>	OFCOM	
<i>Résilience services postaux</i>	OFCOM, OFAE	
<i>Résilience approvisionnement en denrées alimentaires</i>	OFAE, OFAG	
<i>Résilience approvisionnement en eau</i>	OFEV, OFAE	

Mesure	Organes compétents (liste non exhaustive)*	Interfaces (liste non exhaustive)
<i>Résilience armée</i>	Groupement Défense	
<i>Résilience services d'urgence</i>	fedpol, OFPP	
<i>Résilience protection civile</i>	OFPP	
<i>Résilience trafic aérien</i>	OFAC, OFAE	
<i>Résilience trafic ferroviaire</i>	OFT, OFAE	
<i>Résilience transport fluvial</i>	OFT, OFAE	
<i>Résilience transport routier</i>	OFROU, OFAE	
M2 - Tenir un inventaire PIC mis à jour périodiquement	OFPP	KATAPLAN, protection contre les dangers naturels
M3 - Coordonner les plateformes intersectorielles et régionales	OFPP, cantons	AEP, CSN
M4 - Examiner et mettre à jour régulièrement les processus d'information en cas d'événement	OFPP	CSN, SRC, réseau d'annonce et de suivi de la situation NEOC
M5 - Examiner une proposition de base légale intersectorielle	OFPP et services fédéraux compétents	Autorités sectorielles de surveillance et de régulation
M6 - Élaborer et mettre à jour des planifications d'intervention préventives	Cantons, armée	KATAPLAN
M7 - Élaborer et mettre à jour des planifications préventives pour la gestion des pannes d'infrastructures critiques	Cantons, offices spécialisés	KATAPLAN, planifications préventives de la Confédération, EMFP
M8 - Vérifier l'avancement des mesures dans le cadre de la délégation du Conseil fédéral	OFPP, DETEC	

* Les services mentionnés, en collaboration avec le secrétariat PIC, désignent le service qui assume la responsabilité principale et indique les autres acteurs (Confédération, cantons, associations, etc.) doivent être impliqués. Les compétences en vigueur restent inchangées.

Liste des abréviations

AEP	Approvisionnement économique du pays
BCM	Business continuity management
CDF	Contrôle fédéral des finances
CENAL	Centrale nationale d'alarme (nouvelle NEOC)
ChF	Chancellerie fédérale
CSN	Cyberstratégie nationale
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFF	Département fédéral des finances
DFJP	Département fédéral de justice et police
EICom	Commission fédérale de l'électricité
EMFP	État-major fédéral Protection de la population
ESTI	Inspection fédérale des installations à courant fort
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
IFP	Inspection fédérale des pipelines
IFSN	Inspection fédérale de la sécurité nucléaire
KATAPLAN	Analyse cantonale des dangers et préparation aux situations d'urgence
NCSC	Centre national pour la cybersécurité
NEOC	National Emergency Operation Center
OFAC	Office fédéral de l'aviation civile
OFAG	Office fédéral de l'agriculture
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFC	Office fédéral de la culture
OFCOM	Office fédéral de la communication
OFEN	Office fédéral de l'énergie
OFEV	Office fédéral de l'environnement

OFPP	Office fédéral de la protection de la population
OFROU	Office fédéral des routes
OFSP	Office fédéral de la santé publique
OFT	Office fédéral des transports
PharmA	Pharmacie de l'armée
PIC	Protection des infrastructures critiques
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
SFI	Secrétariat d'État aux questions financières internationales
SP	Services du Parlement
SRC	Service de renseignement de la Confédération