Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

[Signature]

[QR Code]

Stratégie nationale pour la protection des infrastructures critiques 2018–2022

du …

Condensé

Par infrastructures critiques (IC) on entend les processus, les systèmes et les installations qui sont essentiels pour le bon fonctionnement de l'économie ou le bien-être de la population. Il s'agit par exemple de l'approvisionnement en énergie, du transport de personnes et de biens ou encore des soins médicaux. En matière de risques courants, la Suisse dispose dans de nombreux domaines d'un niveau de protection élevé, si bien que jusqu'à présent les incidents graves ont été rares et de courte durée. Les événements tels que les brèves pannes de courant à Zurich, le pont endommagé par un camion sur l'autoroute A1 ou la panne générale sur le réseau électrique des CFF de 2005 montrent cependant à quel point la société et l'économie actuelles sont sensibles aux ruptures d'approvisionnement. Une panne de courant générale de longue durée ou une défaillance des réseaux de télécommunications (internet entre autres) à l'échelle nationale pourrait paralyser la quasi-totalité de l'économie, perturber le fonctionnement d'autres IC (p. ex. approvisionnement en denrées alimentaires, finances) et entraver lourdement le quotidien de la population (panne d'éclairage public, d'approvisionnement en eau, d'évacuation des eaux usées, de chauffage, etc.). La tendance actuelle est à l'accroissement de ces risques, par exemple en raison de catastrophes naturelles plus fréquentes, de cyberattaques plus sophistiquées, de la pression exercée sur les coûts dans les entreprises et l'administration ou du vieillissement rapide des constructions.

Le Conseil fédéral a approuvé en juin 2012 une stratégie nationale de protection des infrastructures critiques (PIC) pour améliorer la résilience (capacité de résistance, d'adaptation et de rétablissement) de la Suisse s'agissant des IC. La stratégie PIC actualisée reprend les objectifs et axes prioritaires définis par la stratégie de 2012. Grâce à la stratégie révisée, les principaux travaux, tels que la tenue d'un inventaire PIC régulièrement mis à jour, font l'objet d'un processus continu, sont inscrits dans la législation et complétés de manière ponctuelle.

La stratégie nationale PIC 2018–2022 définit 17 mesures visant à améliorer les résiliences sectorielle et intersectorielle. Pour chaque secteur, la résilience des IC est vérifiée et renforcée si nécessaire. Ces travaux seront en partie pris en charge par les exploitants d'IC, qui disposent généralement d'un système de gestion des risques et de la continuité pour garantir le maintien des activités en cas d'événement. Pour des raisons économiques, cela n'est cependant possible que de manière limitée. C'est pourquoi les exploitants d'IC sont responsables d'évaluer et si possible d'améliorer eux-mêmes la résilience, par exemple en s'appuyant sur le Guide PIC existant. Conformément à l'annexe 1, les autorités compétentes, les organes de surveillance et les organes de régulation au sein des différents secteurs sont priés de vérifier ensemble si les dispositions prises sont suffisantes ou s'il convient de mettre en place des mesures supplémentaires pour renforcer la résilience. À cet effet, ils analyseront les vulnérabilités et les risques pour les différents secteurs. Il convient en outre d'élaborer et de mettre en œuvre si nécessaire des mesures dans les domaines de la prévention et de la préparation afin d'empêcher, si possible, les pannes et de rétablir rapidement le bon fonctionnement des IC. La question du niveau de sécurité et de résilience à atteindre pour chaque IC et celle

des conditions financières et du cadre légal liés aux éventuelles mesures de protection supplémentaires nécessaires doivent être négociées dans les différents domaines politiques (politique énergétique, politique des transports, politique de la santé, etc.).

Il s'agit ensuite d'améliorer la résilience intersectorielle en réduisant la vulnérabilité de la société, de l'économie et de l'État face aux pannes graves et en prenant des mesures pour renforcer l'aide subsidiaire en faveur des exploitants pour la maîtrise des événements en cas de catastrophe et en situation d'urgence. La tenue d'un inventaire PIC régulièrement mis à jour fait partie des mesures prévues à cet effet. Dans la mesure du possible, afin de soutenir les exploitants d'IC dans les domaines de la gestion des situations d'urgence, de la gestion de crise et de la gestion de la continuité des activités, des planifications d'intervention préventives des partenaires de la protection de la population (police, sapeurs-pompiers, protection civile, etc.) et de l'armée ayant pour but la protection d'IC particulièrement importantes sont élaborées et régulièrement mises à jour.

La protection des infrastructures critiques est une tâche transversale avec des interfaces vers différents domaines politiques et différents domaines d'activités (politique énergétique, politique de sécurité, protection contre les dangers naturels, etc.). La mise en œuvre de la stratégie nationale PIC s'effectue par conséquent principalement au niveau de structures et de compétences décentralisées. Les compétences des services fédéraux concernés, des cantons et des communes ainsi que des exploitants d'IC restent inchangées. Dans le cadre de la mise en œuvre de la stratégie nationale PIC, il s'agit toutefois d'étudier notamment la possibilité d'élaborer une base légale contenant des directives intersectorielles destinées aux exploitants d'IC.

La présente stratégie sera examinée en 2022 et mise à jour en cas de besoin.

Table des matières

Stratégie nationale pour la protection des infrastructures critiques 2018–2022

1 Introduction

1.1 Situation initiale

La Suisse dépend d'une disponibilité aussi continue que possible des biens et des services de base tels que l'énergie, les transports ou les télécommunications. Les défaillances dans les domaines de l'approvisionnement en énergie, des transports, de la santé ou de la sécurité publique ont des conséquences graves sur l'économie et la société. La protection des infrastructures critiques (PIC) revêt donc une importance capitale. Elle englobe toutes les mesures nécessaires pour améliorer la résilience des IC, comme les mesures de construction et les mesures techniques, organisationnelles ou administratives dans le domaine de la prévention, de la préparation et de la gestion d'événements. La PIC n'est pas un domaine politique en soi mais une tâche transversale liée à de très nombreux autres domaines d'activités (comme la politique énergétique, la politique des transports, la politique de sécurité ou l'aménagement du territoire). L'objectif de la stratégie nationale PIC est d'améliorer la coordination et l'harmonisation des tâches entre les différents domaines politiques.

En juin 2012, le Conseil fédéral avait approuvé la première stratégie nationale PIC.[1] Il avait chargé l'Office fédéral de la protection de la population (OFPP) de coordonner la mise en œuvre des mesures définies dans ce cadre et de contrôler puis d'actualiser si nécessaire la stratégie PIC. La stratégie nationale PIC de 2012 a permis de prendre d'importantes mesures pour améliorer la résilience des IC. La présente stratégie révisée doit permettre d'inscrire ces travaux dans un processus institutionnel, de les fixer dans la législation et de les compléter de manière ponctuelle. L'orientation stratégique dans le domaine PIC reste toutefois en grande partie inchangée.

1.2 Objectifs et contenu de la stratégie PIC

La stratégie nationale PIC 2018–2022 a pour objectif d'améliorer la résilience de la Suisse (capacité de résistance, d'adaptation et de rétablissement) s'agissant des IC. Elle contribue ainsi de manière décisive à la protection de la population, à la préservation de la prospérité économique et à la sécurité du pays.

La stratégie définit les objectifs de la Suisse dans le domaine de la PIC et indique les mesures à prendre pour améliorer la résilience de la Suisse s'agissant des IC. Elle transcrit le champ d'application, désigne les infrastructures critiques pour la Suisse et fixe les principes supérieurs de la PIC. Elle définit les principaux objectifs dans le domaine PIC et propose 17 mesures fondées sur celles de la stratégie 2012. Enfin,

[1] FF **2012** 7173

elle indique dans quelles structures et avec quelles compétences a lieu la mise en œuvre. La présente stratégie PIC remplace celle de 2012.

1.3 Destinataires de la stratégie PIC

Adoptée par le Conseil fédéral, la stratégie nationale PIC définit des mesures qui sont mises en œuvre principalement par les unités organisationnelles de l'administration fédérale. Certaines mesures concernent également les cantons. Ceux-ci s'acquittent des tâches liées à la PIC dans le cadre de leurs compétences et de leur mission et selon leurs possibilités et besoins. La stratégie PIC concerne aussi les exploitants d'IC, dont la collaboration est indispensable pour atteindre les objectifs. La plupart des exploitants mettent déjà tout en œuvre afin d'éviter des pannes ou des dysfonctionnements. Il est important de pouvoir compter sur leur initiative personnelle pour vérifier et améliorer si nécessaire les dispositions en vigueur ainsi que sur leur disponibilité à coopérer avec les organes étatiques et les autres exploitants d'IC.

2 Contexte

2.1 Stratégie nationale PIC 2012

La stratégie nationale PIC de 2012 définissait 15 mesures. Fin 2016, le Conseil fédéral a été informé de la mise en œuvre au moyen d'une note d'information et d'un rapport de situation. Les expériences ont montré que la stratégie a fait ses preuves et que son orientation peut être maintenue. Il convenait par contre de revoir la désignation des secteurs et sous-secteurs critiques ainsi que la définition des mesures. Les adaptations nécessaires sont présentées de manière détaillée dans un rapport de fond concernant la stratégie PIC 2018–2022. S'agissant des mesures, la présente stratégie mentionne les buts à atteindre ainsi que les actions à engager.

2.2 Interfaces avec d'autres domaines d'activités

La PIC est une tâche transversale avec des interfaces vers de nombreux autres domaines d'activités. Beaucoup de projets, tâches, etc., qu'ils soient en cours ou planifiés, contribuent à atteindre les objectifs décrits dans la stratégie PIC. En principe, ils ne couvrent qu'une partie de l'éventail de la PIC, par exemple des secteurs ou des risques particuliers (p. ex. cyberrisques ou dangers naturels). Les travaux réalisés dans le cadre de la stratégie PIC se fondent sur les bases existantes et les complètent si nécessaire en collaboration avec les organes concernés. Les interfaces avec la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), l'approvisionnement économique du pays (AEP) ainsi que la politique de gestion des risques menée par la Confédération sont présentées ci-après à titre d'exemples. Un recensement détaillé des bases importantes disponibles ainsi qu'une analyse

commune des besoins supplémentaires sont effectués lors de la mise en œuvre des différentes mesures.

2.2.1 Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

En juin 2012, le Conseil fédéral a adopté la SNPC conjointement à la stratégie nationale PIC. La SNPC présente de quelle manière la Suisse se protège contre les cyberrisques et par quels moyens elle renforce sa résilience face à ceux-ci. De 2012 à 2017, ce ne sont pas moins de 16 mesures qui ont été mises en œuvre dans les domaines de la prévention, de la réaction et de la gestion de la continuité. La nouvelle SNPC, qui a été élaborée en collaboration avec tous les départements, des représentants de l'économie privée et les cantons, entrera en vigueur en 2018. Elle a pour but de poursuivre et de développer les travaux en cours.

La protection des IC représente un aspect important de la SNPC. Celle-ci couvre les cyberaspects de la stratégie PIC et met en œuvre les mesures y relatives en coordination étroite avec la stratégie PIC.

2.2.2 Approvisionnement économique du pays (AEP)

L'AEP a pour objectif de garantir l'approvisionnement du pays en biens et en services importants. En cas de difficultés d'approvisionnement graves, il intervient en appliquant des mesures ciblées (p. ex. libération de réserves obligatoires, acquisition de biens importants tels que l'électricité). 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 les objectifs de celle-ci. Les autres activités liées à la PIC concernent des sous-secteurs qui ne sont pas couverts par l'AEP (p. ex. autorités ou organisations de secours) ou des aspects thématiques qui ne sont pas traités par l'AEP. Ainsi, l'AEP se concentre avant tout sur des pénuries nationales de longue durée, alors que la stratégie PIC prend également en considération des perturbations de courte durée ou qui ne concernent pas tout le pays (p. ex. pannes et dysfonctionnements régionaux).

2.2.3 Politique de gestion des risques menée par la Confédération

En 2005, la Confédération a mis en place un système de gestion des risques. L'accent y est mis sur des incidents dont les principaux effets financiers et non financiers nuisent à la poursuite des objectifs et à l'accomplissement des tâches de l'administration fédérale. Cette gestion des risques concerne par conséquent principalement le secteur des autorités. Il existe néanmoins un lien avec les tâches des autorités compétentes, des organes de surveillance et des organes de régulation de la Confédération dans les autres secteurs. Les différences fondamentales avec la PIC

sont liées au fait que cette dernière ne prend pas en considération les risques pour la Confédération mais ceux qui concernent la population et l'économie. Ainsi, certains risques sont importants pour la Confédération sans pour autant concerner la société ou l'économie. En outre, les IC ne relèvent souvent pas uniquement de la Confédération mais aussi, voire uniquement, de la compétence des cantons et des communes (approvisionnement en eau, santé publique, etc.). Dans la cadre de la mise en œuvre de la stratégie PIC, il convient d'identifier les aspects déjà couverts par la gestion des risques menée par le 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 des concepts d'IC et de PIC ainsi que par la désignation des IC.

3.1 Infrastructures critiques

Le concept d'IC est défini comme suit: *On entend par infrastructures critiques les processus, systèmes et installations revêtant une importance capitale pour le fonctionnement de l'économie et le bien-être de la population*.

Pour la Suisse, l'éventail des IC couvre les domaines suivants:

Secteurs	Sous-secteurs
Autorités	Recherche et enseignement
	Biens culturels
	Parlement, gouvernement, justice, administration
Énergie	Approvisionnement en gaz naturel
	Approvisionnement en pétrole
	Approvisionnement en électricité
	Chauffage à distance et production de chaleur industrielle
Élimination	Déchets
	Eaux usées
Finances	Services financiers
	Services d'assurance
Santé	Soins médicaux
	Prestations de laboratoires
	Chimie et produits thérapeutiques

Secteurs	Sous-secteurs
Information et communication	Services informatiques
	Télécommunications
	Médias
	Services postaux
Alimentation	Approvisionnement en denrées alimentaires
	Approvisionnement en eau
Sécurité publique	Armée
	Organisations d'urgence (police, sapeurs-pompiers, services sanitaires)
	Protection civile
Transports	Trafic aérien
	Trafic ferroviaire
	Trafic fluvial
	Trafic routier

Tableau 1: Secteurs et sous-secteurs critiques en Suisse

Des précisions concernant les prestations et les fonctions des sous-secteurs d'importance majeure du point de vue de la PIC figurent dans l'annexe 1.

Font partie de l'IC tous les éléments (exploitants, systèmes informatiques, installations, constructions, etc.) qui fournissent des prestations dans l'un des 27 sous-secteurs, conformément au tableau 1, indépendamment de leur criticité. La criticité est une mesure relative de l'importance que revêt une panne de l'IC pour la population et ses bases d'existence. Elle dépend de l'angle d'analyse: il existe ainsi des IC d'une criticité importante à l'échelon local ou communal (p. ex. un transformateur du réseau de distribution électrique) alors que d'autres le sont à l'échelon national et même international (p. ex. système de télécommande central du réseau de transmission).

3.2 Protection des infrastructures critiques

La protection des infrastructures critiques englobe les mesures permettant de réduire la probabilité de survenance et / ou l'ampleur des dommages dus à une défaillance, un arrêt ou une destruction des IC, ou de diminuer la durée du non-fonctionnement. Les mesures doivent toujours être adaptées à l'importance de chaque IC. La PIC intervient à tous les échelons: au niveau fédéral, où l'on retrouve principalement des IC d'importance nationale voire internationale, mais aussi au niveau cantonal ou communal, où l'accent est mis sur les IC des niveaux correspondants.

4 Vulnérabilités, risques et mesures de protection

Les IC sont susceptibles de connaître des pannes causées par d'importants facteurs de vulnérabilité. De telles vulnérabilités engendrent des risques, qui peuvent être réduits grâce à des mesures de protection appropriées.

4.1 Vulnérabilités

Le bon fonctionnement des infrastructures critiques dépend de la disponibilité des ressources telles que le personnel, les matières premières, l'énergie ou encore les technologies de l'information et de la communication (TIC). Les vulnérabilités existent là où une pénurie ou un dysfonctionnement d'une de ces ressources entrave le bon fonctionnement d'une IC. Les différents domaines de ressources sont les suivants:

- Personnel: il s'agit des personnes dont dépend en grande partie le bon fonctionnement des IC, comme les spécialistes et les personnes-clés pour chacun des processus.
- Matériaux et carburants: matières premières, sources d'énergie (carburants et combustibles), produits finis et semi-finis.
- Prestations: ce domaine comprend la logistique (transports, bâtiments) et les prestations du domaine TIC (y compris les données) et de l'approvisionnement énergétique (p. ex. électricité). Il convient de tenir compte du fait que les prestations importantes peuvent être assurées tant en Suisse qu'à l'étranger. De nombreuses IC dépendent par exemple de systèmes de guidage par satellites (p. ex. GPS ou Galileo). Les vulnérabilités peuvent provenir d'une concentration sur un petit nombre de fournisseurs (monopolistes).

4.2 Risques

Il convient d'analyser les vulnérabilités significatives dans la perspective des risques qui en résultent. Des pannes importantes peuvent être causées par des dangers naturels, techniques ou encore sociétaux:

- Dangers naturels: des défaillances graves peuvent être causées par des dangers naturels tels que les inondations, les tempêtes, les avalanches ou les séismes.
- Dangers techniques: par exemple des défaillances de systèmes, des pannes de courant ou une topologie de réseau lacunaire.
- Dangers sociétaux: dans le domaine PIC, il peut s'agir d'actes de sabotage, de terrorisme ou de pandémie. L'utilisation de plus en plus fréquente de systèmes automatisés et de télécommandes engendre un risque accru de pannes dues à des cyberattaques.

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 panne ou de la destruction de l'IC. Les risques qui en résultent sont amoindris par les mesures de protection déjà mises en place.

4.3 Mesures de protection

Lors de l'évaluation et de la mise en œuvre des mesures, il convient d'opérer une distinction entre les mesures préventives, préparatoires ou liées à l'engagement. Elles visent à éviter les pannes, à garantir le maintien du bon fonctionnement (continuité) en cas d'événement ou encore à réduire l'ampleur des dommages – par exemple par la définition de processus alternatifs ou de substitution. Les mesures visant à améliorer le niveau de préparation de la population et des secteurs de l'économie susceptibles d'être touchés par une panne d'IC jouent également un rôle déterminant.

Les mesures de protection peuvent être classées en différentes catégories:

- Mesures de construction et mesures techniques: renforcement des bâtiments, acquisition de groupes électrogènes de secours, séparation des systèmes informatiques, etc.
- Mesures organisationnelles et administratives: par exemple la mise en place d'un état-major de crise, l'exécution de contrôles d'entrée ou encore la définition de postes de travail alternatifs.
- Mesures juridiques et réglementaires: par exemple l'adaptation d'une base juridique spécifique (loi, ordonnance, directive, etc.).
- Mesures concernant le personnel: il s'agit par exemple de régler la suppléance ou la formation et la sensibilisation des collaborateurs.

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

5 Principes pour la protection des infrastructures critiques

Approche globale basée sur les risques: la protection des IC suit une approche globale basée sur les risques. Il convient de tenir compte de l'ensemble des vulnérabilités significatives ainsi que des risques qui en résultent et de les confronter entre eux. Cette manière de procéder doit également être appliquée lors de l'élaboration et de la mise en œuvre de mesures de protection.

Proportionnalité: les mesures de protection des infrastructures critiques doivent présenter un équilibre optimal entre coût et bénéfice (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. Les mesures retenues doivent être conformes à la Constitution et juridiquement légitimées. En outre, cela ne doit causer aucune distorsion du marché.

Responsabilité commune: la PIC est une tâche transversale avec des interfaces vers différents domaines d'activités et différents domaines politiques. Les responsables de chaque domaine sont priés de porter une attention appropriée à la protection des IC. L'initiative personnelle des exploitants d'IC joue également un rôle important dans la vérification et l'amélioration de la résilience. La population et l'économie, qui sont tous deux dépendantes du bon fonctionnement des IC, sont également priées d'améliorer leur résilience. Une meilleure préparation (p. ex. en constituant des réserves de vivres dans les ménages ou en installant des groupes électrogènes de secours dans les entreprises) contribue pour une part importante à limiter les dommages en cas de pannes d'IC.

Collaboration public-privé: la protection des IC nécessite une collaboration entre tous les acteurs concernés (autorités fédérales, cantonales, communales et exploitants d'IC). Les mesures de protection doivent si possible être élaborées en commun. La collaboration public-privé est importante notamment lors de l'élaboration des directives et des normes ou pour ce qui concerne l'échange d'informations.

Maintien des compétences et des responsabilités: les directives et les obligations des exploitants d'IC découlent en particulier de la législation spécialisée de chaque secteur (dans les secteurs de l'énergie, des transports, des finances, etc.). Les cantons, soutenus par la Confédération (p. ex. Police judiciaire fédérale, Corps des gardes-frontière, Service fédéral de sécurité), sont notamment compétents en matière de protection contre les dangers dans le cadre de leur sécurité interne et de la protection de la population. Dans le cadre d'engagements subsidiaires, l'armée peut, en cas de besoin, appuyer les autorités civiles selon les moyens à disposition.

6 Vision et objectifs de la stratégie nationale PIC

6.1 Vision

La stratégie nationale 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.

La résilience décrit la capacité d'un système, d'une organisation ou d'une société à surmonter des dysfonctionnements 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).

6.2 Objectifs stratégiques

L'objectif prioritaire de la stratégie nationale PIC est l'amélioration de la résilience de la Suisse concernant les IC. À cet effet, elle vise les objectifs sectoriels suivants:

- Les IC 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.
- La population et l'économie sont résilientes, si bien que les dommages causés par des pannes et des dysfonctionnements des IC sont limités.
- Les autorités sont préparées à réagir de manière appropriée aux pannes d'IC.
- Les exploitants d'IC reçoivent un soutien efficace pour maîtriser des incidents.

6.3 Mise en œuvre

La résilience se base sur un processus en cinq étapes, composé des éléments suivants:

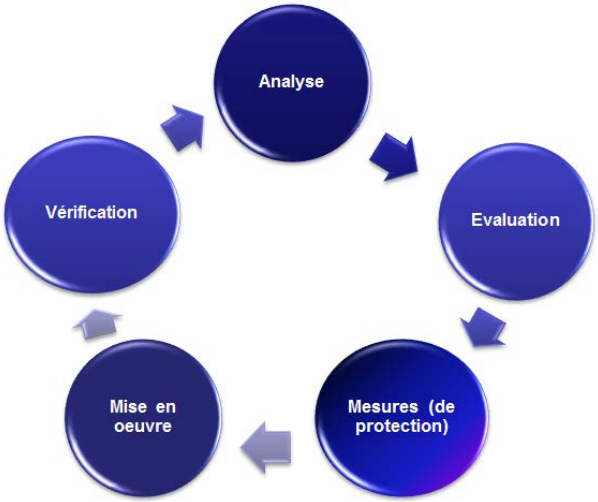

Illustration 1: Boucle de régulation pour la vérification et l'amélioration de la résilience

Analyse

– Les processus, systèmes, objets critiques, etc. sont identifiés.

– Les vulnérabilités et les risques, qui peuvent entraîner des pannes graves, sont identifiés et analysés.

– Les modifications significatives des dangers et des menaces concernant les IC sont détectées suffisamment tôt et communiquées aux principaux organes.

Évaluation

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

Mesures (de protection)

– Les mesures sont définies et approuvées:
  – pour éviter dans la mesure du possible des pannes graves;
  – pour maîtriser les événements;
  – pour permettre un retour rapide au fonctionnement normal, ou
  – pour réduire les effets des pannes.

Les mesures présentent un rapport optimal entre coûts et risques résiduels.

Mise en œuvre

– Les mesures définies sont mises en œuvre dans les délais impartis.

Vérification

– L'efficacité des mesures mises en œuvre est contrôlée.

– Les mesures sont consolidées dans le cadre d'exercices et de formations.

Pour renforcer la résilience de la Suisse s'agissant des IC, il faut améliorer, conformément au processus décrit, la résilience des IC non seulement au sein des différents secteurs mais aussi de façon intersectorielle:

1. Amélioration de la résilience dans les secteurs critiques: la résilience des IC doit être vérifiée et, en cas de besoin, améliorée. Conformément à la procédure décrite précédemment, il convient d'analyser les vulnérabilités et les risques spécifiques et de prendre des mesures afin d'améliorer la résilience des IC.
2. Renforcement de la résilience intersectorielle: il convient d'améliorer la résilience de la population, de l'économie et de l'État s'agissant de pannes d'IC ou de prendre des mesures pour apporter un appui subsidiaire aux exploitants d'IC pour maîtriser les incidents (en complément aux mesures sectorielles d'aide subsidiaire en faveur des exploitants d'IC).

7 Mesures de la stratégie nationale PIC

Sur la base des objectifs stratégiques et de leur réalisation (voir ch. 6), des mesures sectorielles et intersectorielles sont définies et inscrites dans une planification de mise en œuvre. Cette dernière sera complétée par une planification détaillée élaborée séparément après l'approbation de la stratégie nationale PIC. Dans le domaine de la PIC, de nombreux projets, plans ou mesures importants sont planifiés ou déjà en cours. Il s'agira souvent, lors de la mise en œuvre de la stratégie nationale PIC, de contrôler les processus existants et de les compléter le cas échéant. Dans la mesure du possible, la stratégie nationale PIC se base sur ce qui existe déjà. La mise à jour détaillée est garantie dans le cadre de la planification de la mise en œuvre. Les différentes mesures et les principales interfaces avec d'autres travaux sont résumées dans l'aperçu proposé à l'annexe 2 et ne sont par conséquent pas explicitement nommées dans le texte.

7.1 Amélioration de la résilience dans les secteurs critiques

Pour améliorer la résilience du système global des IC, il convient de s'assurer que tous les principaux composants individuels (approvisionnement en électricité, télécommunications, trafic routier, etc.) sont résilients en fonction de leur importance. Que ce soit du côté des exploitants d'IC 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). Concernant la résilience spécifique aux secteurs, il s'agit par conséquent de vérifier si les dispositions en vigueur permettent d'atteindre les objectifs de la stratégie PIC ou si elles doivent être complétées. À cet effet, il convient d'analyser les vulnérabilités et les risques spécifiques à chaque infrastructure conformément à la procédure décrite au chiffre 6.3 puis d'élaborer et de mettre en œuvre des mesures préventives et de précaution pour réduire les risques.

Ces travaux doivent être effectués à deux niveaux: au niveau des exploitants d'IC d'une part, au niveau des différents sous-secteurs critiques de l'autre. Les exploitants d'IC disposent généralement d'un système de gestion des risques, des situations d'urgence, des crises et de la continuité des activités. Dans ce contexte, des dispositions parfois importantes ont été 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 exploitant les IC, qui se préoccupent avant tout de leurs propres intérêts économiques. Les exploitants sont responsables de vérifier, en collaboration avec les autorités compétentes, les organes de surveillance et les organes de régulation, si les dispositions sont suffisantes ou s'il convient de prendre des mesures supplémentaires pour améliorer la résilience. L'OFPP a publié un guide ainsi qu'une aide à la mise en œuvre sur lesquels les exploitants peuvent s'appuyer pour réaliser ces travaux.

Les autorités compétentes ainsi que les organes de surveillance et les organes de régulation spécifiques à chaque secteur sont priés, conformément à l'annexe 1, de

vérifier ensemble si les dispositions mises en place sont suffisantes ou s'il subsiste des risques systémiques liés à des pannes graves et à grande échelle. À cet effet, il convient de vérifier la résilience sectorielle au niveau des sous-secteurs critiques (approvisionnement en électricité, trafic ferroviaire, télécommunications, etc.) en intégrant les dispositions déjà en vigueur, que ce soit du côté des exploitants ou dans le cadre de planifications sectorielles telles que l'AEP. Le but est de déterminer s'il subsiste d'éventuels risques importants qu'il convient de réduire. Cela est souvent possible en recourant à des solutions sectorielles (p. ex une convention réglant la collaboration en cas d'événement). Mais il peut aussi s'avérer nécessaire d'édicter des directives supplémentaires pour les exploitants d'IC. L'élaboration des directives et le financement des éventuelles mesures de protection supplémentaires nécessaires doivent être négociés dans les différents secteurs politiques (politique énergétique, politique des transports, politique de la santé, etc.). Dans le cadre de la stratégie nationale PIC et de la SNPC de 2012, des analyses ont été effectuées pour tous les sous-secteurs critiques, et les premières mesures ont été prises. Pour environ la moitié des sous-secteurs, les travaux traitent avant tout des aspects liés aux TIC (s'agissant des autres sous-secteurs critiques, des vulnérabilités et des risques supplémentaires ont été pris en considération conformément à la stratégie PIC). Il est par conséquent nécessaire de compléter ces travaux. Par ailleurs, il convient de mettre à jour régulièrement ces analyses ainsi que toutes les autres étant donné que les risques évoluent dans le temps.

Vu que la stratégie nationale PIC n'a pas de force légale, les exploitants aussi bien que les autorités compétentes, les organes de surveillance et les organes de régulation des différents secteurs ne sont pas contraints à vérifier et à améliorer la résilience des IC. Conformément à la procédure fixée, ces travaux reposent sur l'initiative et la responsabilité des acteurs compétents. Par ailleurs, certains sous-secteurs ne relevant pas de la Confédération (p. ex. les hôpitaux), il peut s'avérer difficile d'élaborer ou d'adapter des bases légales sectorielles. Une base légale contenant des directives intersectorielles relatives à la résilience des exploitants d'IC permettrait d'atteindre plus facilement les objectifs de la stratégie PIC. Cette base légale devrait couvrir les sous-secteurs pour lesquels les analyses réalisées au niveau des sous-secteurs critiques ont révélé un besoin en la matière ou pour lesquels les mesures nécessaires ne peuvent être prises ailleurs (p. ex. en appliquant une solution spécifique au secteur ou en élaborant voire en adaptant une base légale sectorielle).

Objectif:

– Les IC de tous les secteurs critiques ont le degré de résilience correspondant à leur importance. Les principaux risques sont connus, et les mesures pour atteindre une sécurité optimale sont définies et mises en œuvre en prenant en considération un vaste éventail de dangers et de mesures.

Mesure 1:

– Élaborer des analyses des risques et des vulnérabilités pour les IC où un tel besoin existe en appliquant la procédure décrite au chiffre 6.3 et prendre et mettre en œuvre des mesures pour améliorer leur résilience. Ces travaux doivent être mis à jour régulièrement.

Mise en œuvre:

- Les exploitants d'IC 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 autorités compétentes ainsi que les organes de surveillance et les organes de régulation. Dans la mesure de ses possibilités, l'OFPP apporte un soutien méthodologique.
- Les analyses des vulnérabilités et les planifications de mesures concernant les sous-secteurs critiques qui ont jusque-là pris en considération uniquement les aspects liés aux TIC sont complétés par l'analyse d'autres risques importants. Ces travaux sont réalisés par les autorités compétentes, les organes de surveillance et les organes de régulation, en collaboration avec les exploitants d'IC (voir annexe 1). Les travaux en cours qui couvrent un large éventail de vulnérabilités, de risques et de mesures sont mis à jour tous les quatre ans. Les organes figurant dans l'annexe 1 désignent le service responsable. En cas de besoin, l'OFPP apporte son soutien.

Mesure 2:

- Examiner la possibilité de créer une base légale pour édicter des directives intersectorielles concernant la résilience des exploitants d'IC. Cette base légale couvre les domaines pour lesquels les analyses réalisées au niveau des sous-secteurs critiques ont révélé un besoin en la matière.

Mise en œuvre:

- Le DDPS (OFPP) examine, en collaboration avec les acteurs compétents (en particulier le DEFR, le DETEC et le DFF), l'élaboration d'une proposition de base légale intersectorielle pour édicter les directives nécessaires à l'amélioration de la résilience des IC. Il s'agit en particulier de vérifier si les compétences empiètent sur des directives en vigueur ou des réglementations spécifiques à chaque secteur.

7.2 Amélioration de la résilience dans le domaine intersectoriel

L'amélioration de la résilience dans le domaine intersectoriel comprend l'ensemble des activités nécessaires à la conception, au pilotage et au perfectionnement des mesures pertinentes pour la PIC. Il s'agit notamment d'accroître la résilience de la société, de l'économie et des pouvoirs publics et de prendre les mesures nécessaires pour aider les exploitants d'IC à maîtriser des incidents. Les objectifs et les mesures se fondent pour cela sur le processus présenté au chiffre 6.3.

7.2.1 Analyse

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

Avant que des mesures de protection puissent être prises, les services compétents doivent connaître les infrastructures particulièrement critiques. En cas de catastrophe ou de situation d'urgence, des connaissances relatives aux IC et à leur importance sont indispensables pour pouvoir procéder à des évaluations de la situation et fixer des priorités en matière de mesures de protection. C'est pourquoi un inventaire des infrastructures critiques (Inventaire PIC) a été élaboré dans le cadre de la stratégie PIC 2012. Celui-ci recense les bâtiments et installations revêtant une importance stratégique majeure d'un point de vue national ou cantonal. L'ensemble est classifié «SECRET». Les extraits qui ne contiennent qu'une partie des informations sont généralement classifiés «CONFIDENTIEL». L'Inventaire PIC ainsi que les données qu'il contient doivent être mis à jour périodiquement. Il est prévu de compléter l'inventaire et de recenser également les exploitants d'IC – ou les entreprises – ainsi que les systèmes TI critiques en se basant si possible sur des données inscrites dans d'autres inventaires.

Objectif:

– Les IC suisses sont recensées et enregistrées avec des indications mises à jour dans le respect des prescriptions en matière de protection de l'information et des données. Les bâtiments et installations, les systèmes et les exploitants sont identifiés et priorisés.

Mesure 3:

– Mettre à jour périodiquement l'Inventaire PIC et compléter celui-ci avec des données relatives aux systèmes informatiques critiques et aux exploitants d'IC.

Mise en œuvre:

– L'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 spécialisés et les exploitants. Afin que la collaboration puisse s'appuyer sur des bases juridiques, l'OFPP examine la possibilité d'élaborer une base légale dans ce sens et de l'inscrire dans la LPPCi. 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 IC, 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, des connaissances scientifiquement fondées, par exemple dans le domaine des analyses d'interdépendance et de criticité, sont nécessaires pour le développement de la PIC. Il convient également de suivre l'évolution des technologies, du milieu et de l'environnement afin d'identifier les nouveaux risques. Ces travaux sont menés dans le cadre de la recherche de l'administration fédérale et des cantons.

Objectifs:

– Disposer d'une vue d'ensemble consolidée des vulnérabilités et des risques liés aux IC et savoir quelles sont les mesures à prendre.
– Disposer de bases scientifiquement fondées contribuant au développement de la PIC sur le plan méthodologique et les porter à la connaissance des acteurs principaux.

Mesure 4:

– Consolider les conclusions de l'évaluation et de l'amélioration de la résilience des sous-secteurs critiques pour aboutir à une vue d'ensemble complète des risques.

Mise en œuvre:

– En collaboration avec le DFF (UPIC et AFF) et le DEFR (OFAE), le DDPS (OFPP) consolide les résultats des analyses spécifiques aux sous-secteurs.

Mesure 5:

– Approfondir la recherche fondamentale sur les thèmes intersectoriels (p. ex. interdépendances, évolution des technologies, de l'environnement naturel et social).

Mise en œuvre:

– Les organes fédéraux, les cantons et les exploitants sont responsables de la recherche sectorielle au sein de leur domaine de compétence. La recherche fondamentale intersectorielle dans le domaine de la PIC relève quant à elle du DDPS (OFPP).

Champ d'action analyse: renforcer la collaboration et l'échange d'informations

Les IC sont fortement (inter)dépendantes. Une collaboration et un dialogue sur les risques et les mesures de protection possibles (best practices) entre les représentants des différents secteurs critiques sont par conséquent indispensables. Dans le cadre de la stratégie nationale PIC de 2012, trois plates-formes importantes ont été constituées (plate-forme des exploitants d'infrastructures critiques nationales, groupe de travail PIC mis en place par les organes de la Confédération, interlocuteurs cantonaux en matière de PIC). Ces plates-formes offrent la possibilité aux différents acteurs (organes fédéraux et exploitants d'IC) ainsi qu'aux cantons d'échanger leurs expériences et d'envisager ensemble des solutions. L'expérience montre que la collaboration intercantonale et intersectorielle dans le domaine de la PIC rencontre un vif intérêt. Étant donné que les IC forment souvent des systèmes transfrontaliers, la collaboration internationale joue également un rôle important. L'échange

d'informations relatives aux cyberrisques a lieu par l'intermédiaire de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

Objectif:

– Disposer de plates-formes intersectorielles qui contribuent à l'amélioration de la collaboration et au développement de l'échange d'informations sur les risques, les vulnérabilités et les mesures de protection possibles (best practices).

Mesure 6:

– Maintenir les plates-formes mises en place et y renforcer la collaboration en cas de besoin. Vérifier périodiquement leur composition.

Mise en œuvre:

– Le DDPS (OFPP) coordonne la plate-forme des exploitants d'IC nationales, les interlocuteurs cantonaux pour la PIC ainsi que le groupe de travail PIC des autorités (Confédération et cantons). Le DDPS (OFPP) est l'interlocuteur en matière de PIC au niveau international. La collaboration internationale concernant les cyberrisques se fait par l'intermédiaire de MELANI.

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

En cas de menace ou de danger imminent, les exploitants d'IC doivent être informés à temps afin qu'ils puissent adapter leur dispositif de sécurité. Par ailleurs, en cas de défaillance d'IC, il est important que les organisations de crise compétentes aux niveaux fédéral et cantonal ainsi que celles des autres exploitants d'IC soient informées dans les meilleurs délais. La loi fédérale sur le renseignement (LRens) a permis de poser des bases solides en vue d'une détection des menaces, notamment en rapport avec les IC. S'agissant d'autres menaces et dangers (p. ex. cyberrisques ou dangers naturels), des modes de coopération ont été mis en place pour s'assurer que les exploitants d'IC seront informés dans les meilleurs délais en cas d'événement (p. ex. cercle fermé des clients MELANI). Pour le bon fonctionnement de ce système, il convient de vérifier régulièrement si les principaux exploitants d'IC sont impliqués dans les processus requis. En outre, les autorités doivent être informées à temps en cas de panne ou de problème de sécurité affectant une IC afin qu'elles puissent prendre les mesures nécessaires et obtenir un tableau de la situation complet. Dans le cadre de la protection de la population, le système d'annonces Netalert permet, sur une base volontaire, de signaler de telles défaillances. L'obligation d'annoncer les dérangements aux autorités compétentes n'existe que pour quelques sous-secteurs.

Objectif:

– Les principaux exploitants d'IC sont informés en fonction de leur importance. L'information leur parvient suffisamment tôt et elle est complète. De leur côté, les exploitants d'IC informent les organes compétents aux niveaux

fédéral et cantonal au sujet de défaillances et de pannes importantes tout en assurant la protection des informations et des données.

Mesure 7:

– Examiner régulièrement, du point de vue de l'implication des exploitants d'IC, les processus spécifiques aux dangers assurant 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 (notamment MELANI), si les principaux exploitants d'IC sont impliqués dans les processus requis et élaborent au besoin des propositions pour compléter les processus concernés.

Mesure 8:

– Examiner la possibilité d'élaborer un projet de base visant à inscrire dans la loi l'obligation pour les exploitants d'IC d'informer les autorités compétentes en cas de défaillance ou de problème de sécurité important.

Mise en œuvre:

– Le DDPS (OFPP) examine, en collaboration avec le DFF (UPIC) et le DETEC, la possibilité de créer des bases légales visant à inscrire dans la loi l'obligation d'annoncer les défaillances et les problèmes de sécurité importants touchant les IC. Cette obligation concernerait les domaines pour lesquels il n'existe pas de possibilité de créer des bases légales sectorielles. Dans ce contexte, il convient notamment de définir des critères pour décider à partir de quel niveau de gravité un incident doit être signalé.

7.2.2 Évaluation

S'agissant de l'évaluation, il convient d'une part de vérifier si d'éventuelles dispositions sectorielles concernant la résilience sont appliquées. D'autre part, dans le domaine intersectoriel, il s'agit de s'assurer que le niveau de sécurité visé est le même pour tous les secteurs. Les objectifs stratégiques prioritaires sont définis au chiffre 6. En matière de protection d'IC, il est primordial que les IC soient résilientes en fonction de leur importance et de la situation spécifique. Par conséquent, concernant le niveau de sécurité pour les IC, il faut renoncer à définir des objectifs de sécurité dans le sens de valeurs limites (p. ex. une durée maximale de la panne tolérée). Le but est plutôt de fixer pour chaque IC le niveau de sécurité recherché en se fondant sur l'analyse des risques tout en cherchant à obtenir un rapport optimal entre les coûts des mesures de protection et les risques résiduels liés aux pannes des

IC. La définition du niveau de sécurité dépend principalement du montant que la société est disposée à payer pour accroître le niveau de sécurité, pour éviter par exemple le décès d'une personne en cas d'événement ou pour limiter le dommage économique. Plus ce montant est élevé, plus on dispose de ressources pour les mesures de protection, ce qui augmente le niveau de sécurité. Il est par conséquent essentiel de s'assurer que la volonté financière pour éviter des dommages suite à des pannes d'IC est la même dans tous les secteurs. Le guide PIC présente des propositions concernant la volonté financière qui peuvent être appliquées au niveau des sous-secteurs critiques ou des exploitants d'IC. Il faut alors tenir compte du fait que le degré concret de sécurité qui est visé ne sera fixé que lors de la planification des mesures. Le niveau de sécurité visé correspond toujours au rapport optimal entre les coûts engendrés par les différentes mesures et les coûts liés aux risques résiduels. La décision finale concernant la réalisation des mesures et donc le niveau de sécurité optimal à atteindre est d'ordre socio-politique. Il s'agit à chaque fois d'opérer une pesée d'intérêts en tenant compte d'autres impératifs (p. ex. protection de l'environnement, durabilité, préservation de la liberté économique, etc.).

Objectif:

– Disposer dans tous les secteurs d'un niveau de sécurité comparable tout en tenant compte en particulier de l'importance des IC (criticité).

Mesure 9:

– Examiner si nécessaire les bases disponibles concernant le niveau de sécurité.

Mise en œuvre:

– Si nécessaire, le DDPS (OFPP) examine les propositions concernant le niveau de sécurité en collaboration avec le DETEC (notamment OFEV) et les offices compétents. Une directive légale portant sur la résilience des IC (mesure M2) valable pour tous les secteurs permettrait de s'assurer que le niveau de sécurité visé est comparable dans tous les secteurs critiques.

7.2.3 Mesures (de protection)

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

Dans le domaine intersectoriel, différentes mesures peuvent être prises afin de réduire les risques significatifs pour de nombreux secteurs et d'éviter les pannes graves touchant les IC. De tels risques génériques concernent notamment le personnel responsable de l'exécution des processus centraux. Afin de répondre aux normes de sécurité élevées et de permettre un échange d'informations sur la base de documents classifiés, il devrait être possible de soumettre ce personnel à un contrôle de sécurité selon leur fonction. D'après la législation actuelle, cela n'est prévu que dans des situations exceptionnelles ou en cas de modification des bases légales d'un secteur spécifique. Le contrôle de sécurité relatif aux personnes n'est cependant pas

la seule mesure visant à assurer la sécurité. Il est tout aussi important de former et de sensibiliser le personnel dans le domaine de la sécurité intégrale.

Pour empêcher les arrêts d'IC, les ressources nécessaires à leur exploitation doivent si possible être disponibles sans interruption. À cet effet, des recommandations concernant la priorisation des IC en cas de pénurie de biens et de services importants (p. ex. en cas de pénurie d'électricité) ont été élaborées dans le cadre de la stratégie PIC 2012. Celles-ci doivent être appliquées et mises à jour périodiquement.

Les travaux menés à ce jour relatifs à la vérification et à l'amélioration de la résilience des IC ont montré, d'une part, que celles-ci sont pratiquement toutes dépendantes d'une alimentation en énergie électrique et d'un réseau de télécommunications fiables et, d'autre part, que les risques majeurs sont liés à des pannes de grande envergure sur les réseaux d'électricité et de télécommunications. Alors que la mise en place d'un réseau électrique alternatif est impossible ou inadaptée pour des raisons économiques et techniques, la solution retenue pour le domaine des télécommunications consiste à ériger un réseau de transmission de données fiable, sécurisé et indépendant destiné aux organes de conduite de la Confédération et des cantons ainsi qu'aux exploitants d'IC. La réalisation d'un tel réseau constitue une priorité notamment pour la PIC.

Objectifs:

- Les personnes qui ont accès aux processus centraux liés au domaine des IC doivent pouvoir être soumises à un contrôle de sécurité selon leur fonction.
- En cas de panne ou de pénurie de biens et de services importants, les IC sont approvisionnées en priorité, en fonction des possibilités.
- En cas de panne du réseau public de télécommunications, les exploitants peuvent maintenir les processus nécessaires à l'exploitation des IC et garantir la communication entre les exploitants d'IC et les organisations de gestion des crises aux échelons fédéral et cantonal grâce à un réseau de transmission de données et de communication hautement sécurisé auquel ils peuvent être raccordés.

Mesure 10:

- Élaborer un projet de base légale pour régler le contrôle de sécurité du personnel des exploitants d'IC et des autres titulaires d'une autorisation d'accès.

Mise en œuvre:

- Le DDPS (OFPP, en collaboration avec la SIO) examine la possibilité de créer une base légale pour régler le contrôle de sécurité du personnel-clé engagé par les exploitants d'IC et des autres titulaires d'une autorisation d'accès.

Mesure 11:

- Revoir les bases relatives à la priorisation des IC en cas de panne ou de pénurie conformément aux recommandations.

Mise en œuvre:

– Les organes compétents (notamment le DEFR [OFAE]), en collaboration avec le DDPS [OFPP]), appliquent les recommandations concernant la priorisation des IC en cas de panne ou de pénurie.

Mesure 12:

– Créer un réseau de transmission des données alternatif et sécurisé et élaborer les bases nécessaires au raccordement des exploitants d'IC. Afin d'assurer la communication vocale, un certain nombre d'exploitants d'IC seront sélectionnés et raccordés au réseau Polycom.

Mise en œuvre:

– Sur la base du réseau national de conduite de l'armée, le DDPS (OFPP) réalise le réseau de données sécurisé en collaboration avec d'autres offices fédéraux et les cantons. Il précise également les bases nécessaires pour le raccordement des exploitants d'IC. Pour cela, il convient de décider quels exploitants peuvent profiter de cette possibilité et quelles sont les conditions économiques et techniques qu'ils doivent remplir. Si nécessaire, certains exploitants d'IC peuvent être raccordés au réseau radio de sécurité Polycom dans le cadre de la communication d'urgence de l'OFAE.

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

Les pannes graves d'IC peuvent gêner considérablement la population 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, de l'économie et de 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 ou une pénurie. Aussi bien au niveau de la Confédération que des cantons, plusieurs travaux sont en cours dans ce cadre et seront mis à jour périodiquement. Afin de sensibiliser les entreprises et la population, différents outils ont également été élaborés 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).

Objectif:

– La population, l'économie et les pouvoirs publics sont préparés dans la perspective de pannes graves d'IC, si bien que les effets de telles défaillances peuvent être réduits et les incidents maîtrisés.

Mesure 13:

– La Confédération et les cantons élaborent des planifications préventives pour la gestion des pannes graves d'IC – en particulier celles liées à l'approvisionnement en électricité – et les mettent à jour périodiquement.

Mise en œuvre:

– Dans le cadre des planifications préventives de la Confédération, les autorités fédérales compétentes élaborent des planifications préventives pour la gestion des pannes d'IC. 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. Le DDPS (OFPP) établit une vue d'ensemble des planifications préventives disponibles et les met à jour périodiquement.

Mesure 14:

– Informer et sensibiliser la population et les entreprises au sujet des possibilités de protection relevant de la prévention autonome dans la perspective de pannes d'IC, en particulier du système d'approvisionnement en électricité.

Mise en œuvre:

– Le DEFR (OFAE) met à jour et complète si nécessaire les dispositifs visant à informer et à sensibiliser la population et les entreprises concernant les pannes liées à l'approvisionnement en électricité et aux télécommunications. Dans le cadre d'Alertswiss, le DDPS (OFPP) élabore en collaboration avec d'autres organes (p. ex. OFAE et cantons) des outils de sensibilisation pour renforcer la préparation personnelle de la population.

Champ d'action mesures (de protection): aider les exploitants d'IC à maîtriser des incidents

En cas de menaces et de dangers imminents ou de panne grave, les exploitants d'IC doivent être soutenus par les autorités de manière subsidiaire et efficace avec des moyens ou des capacités externes[2] afin de maîtriser l'événement. Cela permet d'éviter – par exemple en cas de crue – que la population, l'économie ou d'autres IC (effets dominos) subissent des dommages supplémentaires en cas de panne d'IC.

Pour les risques conventionnels, ils peuvent disposer, de manière parfois limitée, des moyens de la police, des sapeurs-pompiers, des services sanitaires et de la protection civile. Concernant les substances chimiques, biologiques ou radiologiques, les moyens de l'OFPP (groupe d'intervention du DDPS) peuvent apporter une aide subsidiaire aux équipes d'intervention sur place. Étant donné que la protection des IC correspond toujours à une mission partielle, elle ne peut à elle seule servir de base pour fixer les valeurs de référence. Par ailleurs, comme la liste des IC menacées dépend du type d'événement, il est impossible de définir à l'avance un ordre de

2 En l'occurrence, il s'agit par exemple de forces d'intervention (police, sapeurs-pompiers, protection civile, armée), de moyens de communication ou de groupes électrogènes de secours.

priorité définitif ou un nombre minimal d'ouvrages à protéger absolument. Il convient donc plutôt de s'assurer que les moyens à disposition sont utilisés de manière optimale en cas d'événement. Dans ce contexte, la gestion fédérale des ressources (ResMaB) et la gestion des ressources par les cantons (ResMaK) peuvent apporter une contribution importante. Sur le plan stratégique, l'ordre de priorité pour la répartition des moyens dans le cadre de l'aide subsidiaire doit être défini en tenant compte de l'importance des IC (criticité), des menaces et des moyens disponibles. Il faut par ailleurs partir du principe que seul un petit nombre d'IC 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'IC jouent également un rôle capital dans la gestion des incidents.

Concernant la priorisation des organisations d'intervention étatiques, la situation peut s'avérer plus difficile. Les moyens opérationnels dans le domaine de la police et de la protection de la population relevant 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 IC représentent des systèmes en réseau qui sont exploités à un niveau national ou international (p. ex. les réseaux de transport d'électricité). Il faut par conséquent procéder à une évaluation générale à l'échelon national en fonction des événements. Dans ce contexte, les organisations sectorielles (p. ex. dans le cadre de l'AEP) mais aussi l'État-major fédéral Protection de la population (EMF PP) peuvent jouer un rôle central. Les travaux sont en cours pour régler et intensifier cette collaboration avec les exploitants d'IC par le biais d'une ordonnance. La coopération avec les organes de conduite aux échelons local, régional et cantonal est indispensable aussi. Dans de nombreux cas, celle-ci est déjà implantée à ces niveaux.

Alors que des moyens subsidiaires existent pour les risques conventionnels, la situation est plus difficile concernant les cyberrisques, pour lesquels les moyens civils ou militaires pour aider les exploitants à maîtriser un incident sont limités. Dans ce domaine également, la protection des infrastructures critiques représente une mission partielle, de sorte qu'il faut mettre en place les capacités requises dans les différents domaines (politique de sécurité, SNPC, réforme de l'armée, etc.). Par conséquent, il convient de s'assurer, dans le cadre des moyens disponibles, que l'importance des IC est prise en considération au moment de fixer l'ordre de priorité.

Afin de gérer des événements de la manière la plus optimale possible, il est finalement nécessaire de disposer de planifications préventives des interventions adaptées à la situation actuelle. Une telle planification existe déjà pour des ouvrages d'importance majeure figurant à l'Inventaire PIC. S'agissant de l'aide apportée par l'armée, les planifications ne concernent que la protection des bâtiments et des installations face à des attaques commises par des tiers. Des planifications concernant d'autres moyens sont également nécessaires (p. ex. la mise en place d'éventuels cybermoyens).

Objectif:

– Pour parer les menaces et permettre un fonctionnement minimum ainsi qu'un retour rapide à la normale, les exploitants d'IC peuvent compter sur des moyens extérieurs en fonction de leur importance.

Mesure 15:

– Analyser et optimiser le cas échéant les processus concernant la répartition des moyens externes pour aider les exploitants d'IC à maîtriser des incidents, en collaboration avec les services concernés.

Mise en œuvre:

– Le DDPS (OFPP), en collaboration avec d'autres services du DDPS (SG, Groupement Défense), le DFJP et le DFF, examine les processus actuels et élabore le cas échéant, en accord avec les offices concernés, des propositions en vue de les optimiser.

Mesure 16:

– Élaborer et mettre à jour périodiquement des planifications préventives des interventions pour la protection des IC.

Mise en œuvre:

– Pour certaines IC, les cantons élaborent des planifications civiles dans le domaine de la protection de la population, par exemple dans le cadre de l'analyse cantonale des dangers et de la préparation aux situations d'urgence. Le DFF (UPIC) examine, en collaboration avec le DDPS (SG), l'élaboration de planifications militaires et civiles des interventions par rapport aux cyber-risques. Les planifications militaires et civiles sont régulièrement mises à jour.

7.2.4 Mise en œuvre et vérification

La mise en œuvre des mesures définies dans la présente stratégie doit être contrôlée et pilotée. Il convient également de s'assurer de l'efficacité de ces mesures. Les tâches correspondantes seront précisées séparément après l'adoption de la présente stratégie. Il est en outre important de tester les aspects PIC dans le cadre d'exercices.

Objectif:

– L'efficacité des mesures visant la protection des infrastructures critiques est testée dans le cadre d'exercices.

Mesure 17:

– Tester de manière ciblée les aspects PIC dans le cadre d'exercices déjà planifiés (exercices du Réseau national de sécurité, exercices fédéraux de conduite stratégique, exercices cantonaux, exercices de simulation, etc.).

Mise en œuvre:

– Les organes de la Confédération, des cantons et des exploitants d'IC qui sont responsables de l'exécution des exercices respectent les aspects PIC lors de la planification et de la réalisation des exercices. Les enseignements tirés de ces derniers sont pris en considération dans le cadre des autres travaux PIC. Ces organes peuvent, en cas de besoin, bénéficier des conseils du DDPS (OFPP).

8 Mise en œuvre de la stratégie nationale PIC

8.1 Structures et compétences

La stratégie nationale PIC 2018–2022 est mise en œuvre dans le cadre des structures et des responsabilités existantes. Sa mise en œuvre est coordonnée par le Secrétariat PIC (OFPP) et garantie par l'implication, dès le début du projet, de représentants des autorités (Confédération et cantons) ainsi que des milieux économiques (en particulier les exploitants d'IC) et scientifiques.

Le Secrétariat PIC aide les organes compétents dans la mise en œuvre des mesures. Il est notamment chargé des tâches suivantes:

– coordonner les mesures visant à renforcer la résilience dans le domaine intersectoriel (p. ex. tenue de l'Inventaire PIC);
– appuyer les autorités compétentes, les organes de surveillance, les organes de régulation et les exploitants dans la vérification et l'amélioration de la résilience des IC des différents secteurs;
– conseiller les cantons en matière de PIC;
– préparer les dossiers pour les plates-formes de coordination;
– servir d'interlocuteur en matière de PIC aux plans national et international;
– rendre compte de l'état d'avancement de la mise en œuvre de la stratégie nationale PIC.

Les organes responsables de la mise en œuvre des mesures sont désignés dans la stratégie et à l'annexe 2. La vérification et l'amélioration de la résilience spécifique aux secteurs sont effectuées en collaboration avec les autorités compétentes, les organes de surveillance, les organes de régulation et les exploitants d'IC (voir annexe 1).

Il convient d'examiner si l'État-major fédéral Protection de la population (ancienne dénomination: État-major fédéral ABCN), dans lequel sont représentés la plupart des directeurs des offices concernés, peut diriger les travaux en tant que comité interdépartemental. Il devrait notamment avoir pour tâche de soutenir, par un controlling stratégique, la mise en œuvre appropriée de la stratégie PIC dans les délais impartis.

Il convient par ailleurs d'examiner la possibilité de confier les demandes en matière de PIC à une commission extraparlementaire existante. Sur le plan stratégique, la commission aurait pour tâche d'impliquer aussi tôt que possible les exploitants d'IC,

souvent des entreprises privées, ainsi que les cantons, l'économie et la société en tant qu'utilisateurs d'IC. Elle doit en outre faire en sorte que les connaissances techniques nécessaires résultant des différents domaines soient prises en compte dans le pilotage stratégique.

8.2 Calendrier et controlling

La mise en œuvre des différentes mesures est précisée à l'aide d'un plan de mise en œuvre et de controlling séparé qui sera élaboré après l'adoption de la stratégie nationale PIC. La mise en œuvre des mesures à durée déterminée doit se faire dans les grandes lignes selon le calendrier suivant[3]:

Phase 1 (jusqu'à fin 2018)

- Élaboration du plan de mise en œuvre.
- Révision de l'Inventaire PIC et intégration des exploitants d'IC (entreprises). (M3)
- Contrôle des processus concernant l'aide subsidiaire apportée aux exploitants d'IC pour maîtriser les incidents. En cas de besoin, élaboration de propositions en vue de les optimiser. (M15)

Phase 2 (jusqu'à fin 2020)

- Examen d'une base légale pour l'obligation d'annoncer les pannes et les défaillances. (M2)
- Projet de base légale pour régler le contrôle de sécurité de certaines catégories de personnel des exploitants d'IC ainsi que d'autres titulaires d'une autorisation d'accès. (M10)
- Constitution des bases nécessaires au raccordement des exploitants d'IC au RDS. (M12)

Phase 3 (jusqu'à fin 2022)

- Vérification de la résilience des sous-secteurs critiques et élaboration de mesures permettant de l'améliorer. (M1)
- Examen d'une base légale contenant des prescriptions intersectorielles. (M2)
- Consolidation des enseignements tirés des analyses réalisées au niveau des sous-secteurs critiques. (M4)

[3] Les tâches permanentes telles que l'exploitation de plates-formes intersectorielles (M6) ou la prise en compte de la PIC lors des exercices (M17), qui ne sont pas mentionnées séparément, sont toutefois prises en considération dans le plan de mise en œuvre.

Tous les deux ans, un rapport sur l'état d'avancement de la mise en œuvre est adressé au Conseil fédéral.

8.3 Révision de la stratégie PIC

La stratégie nationale PIC tient compte des modifications des conditions-cadres et des évolutions du contexte et est mise à jour si nécessaire. La présente stratégie fera l'objet d'un réexamen complet en 2022 et sera modifiée le cas échéant.

Annexe 1

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 de la PIC*	Organes fédéraux compétents (liste non exhaustive)**
Autorités	Recherche et enseignement	Prestations basées sur les résultats de recherches en cas de catastrophe et de situation d'urgence (p. ex. service sismologique)	SEFRI
	Biens culturels	Garantie de la sécurité du droit (en particulier les 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, DFAE, MétéoSuisse, fedpol, SIO, SRC, AFF, UPIC et FP, OFEV
Énergie	Approvisionnement en gaz naturel	Commerce, transports, stockage et distribution de gaz naturel	OFEN, IFP, OFAE
	Approvisionnement en pétrole	Commerce, transport, stockage et distribution de combustibles et de carburants (essence, kérosène, etc.)	OFEN, IFP, OFAE
	Approvisionnement en électricité	Production, stockage, commerce, transport et distribution d'énergie électrique (trafic ferroviaire non compris)	OFEN, ElCom, ESTI, IFSN, OFAE
	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

Secteur	Sous-secteur	Prestations d'importance majeure du point de vue de la PIC*	Organes fédéraux compétents (liste non exhaustive)**
	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 paiement, approvisionnement de la population en argent liquide, capitalisation de tiers, rémunération de dépôts et maintien de la stabilité des prix	FINMA, AFF, SFI, OFAE, OFCOM
	Assurances	Garantie de la couverture d'assurance, de l'aide financière en cas de dommages ainsi que des prestations dans le cadre de la prévention des dommages (y c. assurances maladie et sociales)	FINMA, AFF, SFI, OFAS
Santé	Soins médicaux	Traitement et prise en charge de patients (médecine de premier recours, médecine spécialisée ou hospitalière) soins vétérinaires de base	SSC, OFSP
	Services de laboratoires	Analyses de laboratoires dans le cadre de la protection des êtres humains, des animaux et de l'environnement	OFSP, OSAV, OFPP
	Produits chimiques et thérapeutiques	Approvisionnement en produits thérapeutiques (médicaments et dispositifs médicaux), y c. vaccins	OFAE, Swissmedic, Pharmacie de l'armée
Information et communication	services informatiques	Services informatiques à l'intention de l'économie (en particulier traitement et stockage de données)	OFAE, UPIC
	Télécommunications	Appels d'urgence, internet, transmission de signaux de radio et de télévision	OFCOM, OFAE
	Médias	Information de la population en cas de catastrophe ou de situation d'urgence,	OFCOM

Secteur	Sous-secteur	Prestations d'importance majeure du point de vue de la PIC*	Organes fédéraux compétents (liste non exhaustive)**
		formation de l'opinion politique	
	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	Soutien militaire en cas de catastrophe, engagements subsidiaires de sûreté, aide à la conduite pour la population civile, défense du pays	Groupement Défense
	Organisations d'urgence (police, sapeurs-pompiers, services sanitaires)	Garantie de la sécurité publique, interventions de secours et de sauvetage, maîtrise de catastrophes et de situations d'urgence	fedpol, OFPP
	Protection civile	Soutien des organisations partenaires dans la maîtrise de catastrophes et de situations d'urgence	OFPP
Transports	Trafic aérien	Transport aérien de personnes et de marchandises	OFAC, OFAE
	Trafic ferroviaire	Transport ferroviaire de personnes et de marchandises	OFT, OFAE
	Trafic fluvial	Transport fluvial de marchandises (en particulier accès aux ports maritimes)	OFT, OFAE
	Trafic routier	Transport routier de personnes et de marchandises (trafic motorisé individuel et transports publics)	OFROU, OFAE

Tableau 2: Description des sous-secteurs et des compétences spécifiques, mesure 1

* La liste n'est pas exhaustive: les objectifs en matière d'approvisionnement sont fixés par les services compétents (notamment par l'AEP).

** Les organes mentionnés, en collaboration avec le secrétariat PIC, désignent les autres organes responsables en matière de vérification et d'amélioration de la résilience qu'il convient d'impliquer (Confédération, cantons, organisations, etc.). Les compétences en vigueur restent inchangées.

Annexe 2

Aperçu des mesures, des compétences et des interfaces

Mesures	Organes compétents (liste non exhaustive)*	Interfaces avec d'autres projets / tâches / organes (liste non exhaustive)
M1: Vérification et amélioration de la résilience des IC	Conformément à l'annexe 1	SNPC, AEP, différents projets et tâches sectoriels
M2: Examen d'une base légale contenant des prescriptions pour les exploitants d'IC	OFPP, autorités compétentes, organes de surveillance et organes de régulation	SNPC
M3: Tenue de l'Inventaire PIC périodiquement mis à jour	OFPP	KATAPLAN, protection contre les dangers naturels
M4: Établissement d'un aperçu des risques pour les sous-secteurs critiques	OFPP, UPIC, AFF	SNPC, gestion des risques de la Confédération, AEP
M5: Approfondissement de la recherche fondamentale dans le domaine de la PIC	OFPP	Recherche de l'administration fédérale
M6: Exploitation de plates-formes intersectorielles	OFPP	MELANI, AEP
M7: Contrôle et mise à jour périodique des processus spécifiques à l'information en cas d'événement	OFPP	MELANI
M8: Examen de l'obligation d'informer en cas de panne ou d'incident affectant la sécurité	OFPP, UPIC	SNPC
M9: Contrôle et mise à jour périodiques des tâches concernant le niveau de sécurité	OFPP, autorités compétentes, organes de surveillance, organes de régulation et OFEV	Protection contre les dangers naturels
M10: Projet de base légale pour le contrôle de sécuritédu personnel des exploitants d'IC et d'autres titulaires d'une autorisation d'accès	OFPP, SIO	LSI
M11: Mise en œuvre et mise à jour périodique des recommandations concernant la priorisation des IC en cas de pénurie ou de panne	OFAE, OFPP	AEP
M12: Création d'un réseau sécurisé de transmission des données et élaboration des bases nécessaires pour raccorder les exploitants d'IC à ce réseau	OFPP, Groupement Défense, cantons	RDS

Mesures	Organes compétents (liste non exhaustive)*	Interfaces avec d'autres projets / tâches / organes (liste non exhaustive)
M13: Élaboration et mise à jour de planifications préventives pour la gestion des pannes graves d'IC	Cantons, offices spécialisés, OFPP	KATAPLAN, planifications préventives de la Confédération, EMF PP
M14: Amélioration de la préparation autonome de l'économie et de la population	OFPP, OFAE, ChF	Alertswiss, AEP
M15: Analyse et optimisation des processus concernant l'aide subsidiaire accordée aux exploitants d'IC	OFPP, SG DDPS, fedpol	ResMaB, EM cond P, EMF PP
M16: Élaboration et mise à jour des planifications d'intervention préventives	Cantons, UPIC, SG DDPS, OFPP	SNPC, KATAPLAN, PACD
M17: Prise en compte des aspects PIC lors des exercices	OFPP, cantons, ChF, RNS	ECS, ERNS

Tableau 3: Mesures, compétences et interfaces

* Le secrétariat PIC joue un rôle de coordination et garantit l'implication des organes compétents importants.

Annexe 3

Liste des abréviations

AEP	Approvisionnement économique du pays
AFF	Administration fédérale des finances
Ch.	chiffre
ChF	Chancellerie fédérale
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
ECS	Exercice de conduite stratégique
ElCom	Commission fédérale de l'électricité
EM cond P	État-major de conduite Police
EMF ABCN	Etat-major fédéral compétent en matière de dangers atomiques, biologiques, chimiques et naturels (nouvelle désignation EMF PP)
EMF PP	État-major fédéral Protection de la population
ERNS	Exercice du Réseau national de sécurité
ESTI	Inspection fédérale des installations à courant fort
fedpol	Office fédéral de la police
FINMA	Autorité fédérale de surveillance des marchés financiers
FP	Fournisseur de prestations
GPS	Global Positioning System
IC	Infrastructure(s) critique(s)
IFP	Inspection fédérale des pipelines
IFSN	Inspection fédérale de la sécurité nucléaire
LPPCi	Loi fédérale du 4 octobre 2002 sur la protection de la population et sur la protection civile (RS *520.1*)
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement (RS *121*)
LSI	Loi sur la sécurité de l'information (projet du Conseil fédéral du 22 février 2017, FF *2017* 2907)
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
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
PACD	Plan d'action pour la cyberdéfense
PIC	Protection des infrastructures critiques
ResMaB	Gestion fédérale des ressources
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
SFI	Secrétariat d'État aux questions financières internationales
SG	Secrétariat général
SIO	Sécurité des informations et des objets
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SP	Services du Parlement
SRC	Service de renseignement de la Confédération
SSC	Service sanitaire coordonné
TI	Technologies de l'information
UPIC	Unité de pilotage informatique de la Confédération