Stratégie nationale pour la protection des infrastructures critiques

du 27 juin 2012

Condensé

Les infrastructures critiques garantissent la disponibilité de biens et de services d'importance capitale, comme l'énergie, la communication ou les transports. Les défaillances de grande ampleur géographique ont des conséquences graves sur la population et l'économie. Elles compromettent également la sécurité et le bien-être national.

Dans certains domaines, la Suisse dispose aujourd'hui d'un niveau de protection élevé et bénéficie d'un environnement relativement stable, si bien que jusqu'à présent les incidents graves ont été rares et de courte durée. L'importance des infrastructures critiques a néanmoins fortement augmenté avec la mondialisation et l'avènement de l'ère technologique: une panne générale d'électricité à l'échelle du pays pourrait par exemple paralyser l'ensemble de l'économie nationale, entraver le fonctionnement des autres infrastructures critiques (p. ex. les télécommunications, l'approvisionnement en eau ou le trafic ferroviaire) et gêner gravement la population (pannes d'éclairage, d'installations de refroidissement et de congélation, de chauffage, d'ascenseurs, etc.). Ces derniers temps, les risques ont aussi changé de nature, avec l'augmentation du nombre des catastrophes naturelles, des cyberattaques ou le vieillissement rapide des équipements. De plus, les fortes dépendances mutuelles en cas d'incident (interdépendances) exigent une collaboration accrue de tous les acteurs, collaboration transcendant les différents secteurs des infrastructures critiques.

Les raisons qui précèdent rendent nécessaire un renforcement approfondi de la résilience (capacité de résistance) de la Suisse s'agissant des infrastructures critiques. La présente stratégie nationale propose de consolider la protection intégrale dans deux domaines (« champs d'action »): d'une part, l'autoprotection des infrastructures critiques *sera renforcée par l'élaboration et l'application de concepts de protection intégrale par les organes compétents (autorités fédérales, cantonales et communales, exploitants). On veillera à harmoniser cette démarche avec des projets analogues (stratégies en matière de société de l'information, de cyber-risques ou de prévention antisismique). Dans le domaine* transinfrastructures, *la stratégie vise à améliorer la collaboration entre les acteurs (autorités, exploitants) des différents secteurs tout en diminuant la vulnérabilité de la société, de l'économie et des pouvoirs publics en cas de défaillance. Il sera élaboré à cette fin des planifications pour la maîtrise de défaillances graves et pour l'aide subsidiaire apportée aux exploitants lors de tels événements. D'autres mesures concernent l'alerte en cas d'événement, qui doit intervenir au moment opportun, ou le renforcement des capacités de la population et de l'économie à faire face.*

Différents projets ou mesures pertinents sont déjà en cours d'élaboration ou de planification. Par conséquent, la mise en œuvre de la stratégie nationale de protection des infrastructures critiques se fera elle aussi en grande partie dans le cadre des structures et compétences existantes, sous réserve évidemment des attributions des organes fédéraux impliqués.

Stratégie nationale

1 Introduction

La Suisse dépend dans une grande mesure d'un fonctionnement aussi continu que possible des infrastructures critiques (IC). Celles-ci garantissent la disponibilité de biens et services importants comme l'énergie, la communication ou les transports. Les défaillances des infrastructures critiques ont des conséquences graves sur l'économie et la population et compromettent la sécurité et le bien-être national. La protection des infrastructures critiques (PIC) revêt donc une importance capitale pour les pouvoirs publics et les entreprises.

En soi, la protection des infrastructures critiques n'a rien d'une nouveauté. Dans certains domaines, du point de vue des risques spécifiques ou des contre-mesures, les services compétents s'occupent au niveau de la Confédération, des cantons et des exploitants des aspects qui contribuent à atteindre l'objectif premier. Toutefois, une coordination transversale ainsi qu'une procédure globale et harmonisée dans les différents domaines ont longtemps fait défaut.

Le Conseil fédéral a chargé l'Office fédéral de la protection de la population (OFPP) de coordonner les travaux dans le domaine de la PIC et d'élaborer une stratégie nationale en la matière d'ici au printemps 2012.

La stratégie nationale définit les objectifs dans le domaine de la PIC et indique les mesures à prendre pour diminuer les risques. Cette stratégie 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 transcrit le champ d'application, désigne les infrastructures critiques et fixe les principes directeurs de la PIC. Elle fournit en outre une vue d'ensemble de la situation actuelle en Suisse et à l'étranger. Elle définit la vision et les objectifs et propose 15 mesures classées dans deux champs d'action. Enfin, elle détermine les structures et les compétences nécessaires à sa mise en œuvre.

La stratégie nationale PIC s'adresse à tous les services qui ont des responsabilités dans ce domaine, en particulier aux différentes autorités (fédérales, cantonales et communales) concernées, aux responsables politiques et aux exploitants d'infrastructures critiques.

2 Champ d'application et désignation des infrastructures critiques

Le champ d'application de la stratégie de protection des infrastructures critiques est délimité par la définition des concepts pertinents ainsi que par la désignation et la répartition des infrastructures critiques.

Infrastructures

Le terme générique d'infrastructures recouvre les installations et les organisations qui fournissent des services et des produits à la société, à l'économie et aux pouvoirs publics.

Infrastructures critiques

Il s'agit d'infrastructures dont le dérangement, la défaillance ou la destruction peut avoir des conséquences graves pour la société, l'économie et les pouvoirs publics. Les infrastructures critiques sont subdivisées en trois niveaux:

- *secteurs:* p. ex. énergie, finances, santé
- *sous-secteurs:* p. ex. approvisionnement en électricité, en pétrole, en gaz naturel
- *objets ou éléments (individuels):* p. ex. centres de coordination, systèmes de commande, centres de recherche, barrages, canalisations, exploitants

L'éventail des infrastructures critiques se présente ainsi:

Tableau 1

Liste des infrastructures critiques

Secteurs	Sous-secteurs
Autorités	Représentations diplomatiques, organisations internationales
	Recherche et enseignement
	Biens culturels
	Parlement, gouvernement, justice, administration
Energie	Approvisionnement en gaz naturel
	Approvisionnement en pétrole
	Approvisionnement en électricité
Elimination	Déchets
	Eaux usées
Finances	Banques
	Assurances
Santé	Soins médicaux et hôpitaux
	Laboratoires
Industrie	Industrie chimique et pharmaceutique
	Industrie mécanique, électrique et métallurgique
Information et communication	Technologies de l'information
	Médias
	Trafic postal
	Télécommunications
Alimentation	Approvisionnement en denrées alimentaires
	Approvisionnement en eau
Sécurité publique	Armée
	Services d'urgence (police, sapeurs-pompiers, sauvetage)
	Protection civile
Transports	Trafic aérien
	Trafic ferroviaire
	Trafic fluvial
	Trafic routier
	Criticité très importante*
	Criticité importante*
	Criticité normale*

* – On entend par «criticité» l'importance relative du sous-secteur par rapport à la dépendance, à la population et à l'économie (≠ importance absolue). Selon la situation, on tiendra également compte de la menace et de la vulnérabilité des infrastructures critiques.
– L'évaluation se réfère à une situation de risque normale.
– L'évaluation ne donne aucune information sur la criticité des éléments considérés individuellement.

Protection des infrastructures critiques

La protection des infrastructures critiques englobe des mesures qui réduisent la probabilité de survenue et/ou l'ampleur des dommages d'un dérangement, d'une défaillance ou d'une destruction d'infrastructures critiques ou qui réduisent le plus possible la durée de non-disponibilité.

3 Principes de la protection des infrastructures critiques

Approche globale fondée sur les risques: la protection des installations critiques est fondée sur les risques. Ceux-ci résultent du danger, de la criticité et de la vulnérabilité. L'analyse des dangers considère par conséquent un éventail complet de ceux-ci. Cela signifie qu'en principe, tous les dangers significatifs (risques naturels, risques techniques, risques sociaux)[1] sont pris en compte. Il faut également considérer un éventail de mesures complet pour évaluer l'ampleur des mesures de protection (aspects architecturaux, techniques, organisationnels et juridiques dans les phases de prévention, de préparation, de maîtrise des situations d'urgence et de crise, remise en état et reconstruction). Ce faisant, il convient également de garantir la protection des informations.

Proportionnalité: les coûts d'application des mesures de protection des infrastructures critiques doivent être mis en rapport avec les bénéfices attendus. De plus, les mesures retenues doivent être conformes à la Constitution et juridiquement légitimées. En outre, elles ne doivent causer aucune distorsion inutile du marché.

Responsabilité: les mesures doivent être prises aussi bien par les pouvoirs publics que par les exploitants des infrastructures critiques. Comme une grande partie de ces dernières sont exploitées par des entreprises privées, celles-ci doivent avoir la responsabilité de l'amélioration des mesures de protection. Les autorités compétentes sont invitées à vérifier si ces mesures sont suffisantes. Le cas échéant, des objectifs de protection et de résultat devront être fixés au niveau politique.

Partenariat public-privé: la protection des infrastructures critiques nécessite une collaboration accrue entre tous les acteurs concernés aux niveaux de la Confédération, des cantons, des communes et des exploitants. Les mesures de protection doivent être si possible élaborées, appliquées et financées en commun. La possibilité de partenariat public-privé doit être étudiée dans tous les domaines de la protection des infrastructures critiques, en particulier pour les projets de construction (p. ex. de nouvelles infrastructures critiques), l'élaboration des directives et des normes ou en ce qui concerne l'échange d'informations.

1 La répartition des risques s'inspire des travaux de «Risques Suisse»

4 Situation actuelle

4.1 Protection des infrastructures critiques en Suisse

En Suisse, la situation est la suivante:

- Il existe déjà un grand nombre d'organisations, de structures, de mesures, de règlements, de projets, etc. qui contribuent à la protection des infrastructures critiques[2]. Ces travaux se font souvent dans le cadre de politiques spécifiques, par exemple de l'énergie, des transports ou de sécurité. Ils se limitent le plus souvent à certains secteurs et/ou à certains risques ou à des contre-mesures spécifiques. De plus, ils donnent lieu en général à différentes approches méthodologiques (par exemple pour l'évaluation des risques et pour en déduire des contre-mesures).
- Les aspects relatifs à la protection ont souvent une importance plutôt secondaire dans les domaines sectoriels spécifiques. Une prise en compte explicite et globale de la thématique fait défaut. Cependant, l'importance des infrastructures critiques augmente constamment, notamment avec la place de plus en plus grande prise par la technologie, et la Suisse dépend toujours plus du fonctionnement sans interruption de ces infrastructures. Des défaillances de grande ampleur, touchant par exemple l'approvisionnement en électricité ou les télécommunications, auraient aujourd'hui des conséquences infiniment plus graves que cela n'aurait été le cas il y a encore quelques années. Des changements sont également intervenus dans l'éventail des risques (p. ex. cyber-menaces ou terrorisme). Un autre élément qui concourt à l'augmentation de la vulnérabilité est le caractère transfrontalier de différents réseaux dans lesquels toute défaillance, même minime, peut avoir des conséquences au plan international. En outre, les processus de production et de distribution sont aujourd'hui en grande partie automatisés alors que des redondances ont été supprimées.
- Le Conseil fédéral a approuvé la stratégie générale en matière de protection des infrastructures critiques en juin 2009[3]. Celle-ci a certes permis d'améliorer la coordination et les principes dans le domaine de la PIC, mais il manque encore une procédure systématique et globale.

[2] Par exemple, dans le sous-secteur de l'énergie, la Confédération a mis au point une stratégie relative aux réseaux énergétiques visant notamment à garantir à terme la sécurité et le fonctionnement du réseau électrique. Par ailleurs, le programme de mesures de la Confédération de mitigation des séismes s'intéresse notamment au renforcement de l'infrastructure électrique contre les effets des tremblements de terre. Pour réduire le plus possible l'ampleur des dégâts en cas d'incident, l'approvisionnement économique du pays élabore pour la gestion de l'électricité en cas de crise des mesures de planification qui seront appliquées par l'organisation pour l'approvisionnement en électricité dans des situations extraordinaires (OSTRAL).

[3] La stratégie PIC peut être téléchargée sur le site www.protpop.admin.ch > thèmes > Protection des infrastructures critiques.

4.2 Stratégies PIC à l'étranger

Ces dernières années, différents pays ont adopté des stratégies nationales sur le thème de la protection des infrastructures critiques ou ont mis à jour de telles stratégies. Une comparaison de différentes stratégies démontre que les aspects suivants sont au centre des préoccupations:

- encouragement du dialogue et de la collaboration (intra et intersectoriels) par la création de plates-formes (Allemagne) ou d'agences (Etats-Unis, Australie). Les autorités et les exploitants des IC y sont toujours représentés;
- établissement d'un répertoire des infrastructures critiques, ou identification des différents objets/éléments (notamment en France et en Allemagne). Les infrastructures critiques sont parfois uniquement désignées de façon générique (p. ex. «centrales électriques»), sans qu'il soit précisé de quels objets il s'agit concrètement. En ce moment, l'Union européenne élabore elle aussi une liste des infrastructures critiques dans les secteurs de l'énergie et des transports, l'accent étant mis sur les conséquences transfrontalières des défaillances affectant ces infrastructures;
- élaboration de concepts et de programmes de protection pour les infrastructures identifiées comme critiques, en général selon un processus cadre imposé dans la stratégie (Etats-Unis notamment). Encouragement du dialogue et de la collaboration (spécifique aux secteurs, mais aussi trans-secteurs) par la création de plates-formes (Allemagne) ou d'agences (Etats-Unis, Australie). Les autorités et les exploitants des IC y sont toujours représentés.

Cette comparaison montre en outre qu'aucune des stratégies examinées ne parle de déficits dans certains secteurs des infrastructures critiques, des différentes contre-mesures ou des coûts induits par d'éventuelles contre-mesures. Au lieu de cela, la première préoccupation est toujours de garantir une procédure uniforme et globale.

5 Vision et objectifs de la stratégie nationale PIC

5.1 Vision

La stratégie nationale PIC doit permettre de se conformer à la vision suivante:

«La capacité de fonctionnement de ses infrastructures critiques assure à la Suisse une résilience permettant d'éviter dans la mesure du possible des défaillances graves et de grande ampleur géographique des infrastructures critiques et des biens et services qui en dépendent et de façon qu'en cas d'incident, l'étendue des dommages reste limitée.»

5.2 Objectifs

La stratégie nationale en matière de PIC vise à renforcer la résilience de la Suisse s'agissant des infrastructures critiques. Elle doit de plus garantir une action coordonnée de l'ensemble des acteurs.

On entend par résilience l'aptitude d'un système, d'une organisation ou d'une société à résister aux dérangements d'origine interne ou externe et à préserver le plus possible sa capacité de fonctionnement ou à rétablir celle-ci dans les meilleurs délais. La résilience comporte quatre constituants:

1. la robustesse intrinsèque des systèmes (infrastructures critiques, pouvoirs publics, économie et société);
2. la disponibilité de redondances;
3. la capacité à mobiliser des secours efficaces;
4. la rapidité et l'efficacité des secours.

Sur cette base, les objectifs de la stratégie nationale PIC recouvrent deux domaines et consistent par conséquent à:

– augmenter la robustesse et la souplesse infrastructures critiques;
– améliorer la coopération inter-infrastructures, la capacité de résistance et d'adaptation de la société, de l'économie et des collectivités publiques (Confédération, cantons et communes) et à assurer, en cas d'événement, la disponibilité rapide et efficace de secours et de redondances.

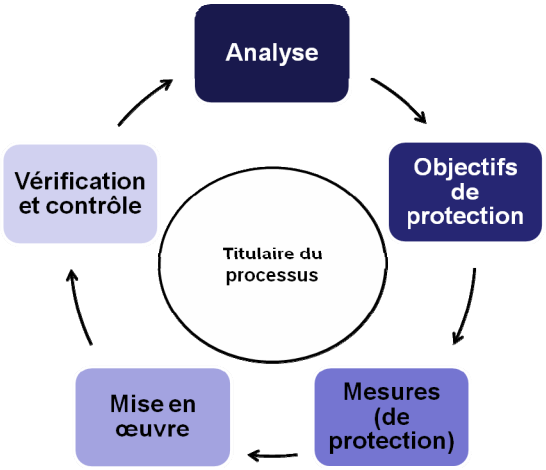
Ces objectifs doivent être atteints par une amélioration de la *protection intégrale* (voir ch. 6) dans ces deux domaines grâce à une procédure harmonisée et coordonnée.

6 Protection intégrale

La protection intégrale repose sur un processus systématique piloté dans chaque cas par un responsable qui en assume la responsabilité (les responsables de processus sont désignés au ch. 8):

Figure 1

Processus de protection intégrale



Les objectifs suivants doivent être atteints dans tous les cas:

Analyse

- Les processus, les systèmes, les objets critiques, etc. sont identifiés et des priorités sont fixées.
- Les risques et les vulnérabilités, qui peuvent entraîner des défaillances graves, sont identifiés et évalués.
- Les modifications significatives de la menace sont détectées suffisamment tôt.

Objectifs de protection

- Les objectifs de protection et de résultats sont fixés au niveau politique et mis en œuvre par les exploitants.

Mesures (de protection)

- En s'appuyant sur les objectifs de protection et de résultats convenus, les différents services compétents indiquent des mesures (incluant concepts, structures, processus et instruments)
  - évitant dans la mesure du possible des défaillances graves et de grande ampleur géographique,
  - permettant de combattre des menaces et de maîtriser des événements, et
  - autorisant un retour rapide au fonctionnement normal.

  Pour mettre au point ces mesures, on tiendra compte du rapport coût-efficacité en se fondant sur les risques.

Mise en œuvre

- Les mesures définies sont mises en œuvre.

Vérification et contrôle

- L'efficacité des mesures prises est vérifiée.
- Les mesures sont consolidées à l'aide d'exercices.

7 Mesures de la stratégie nationale PIC

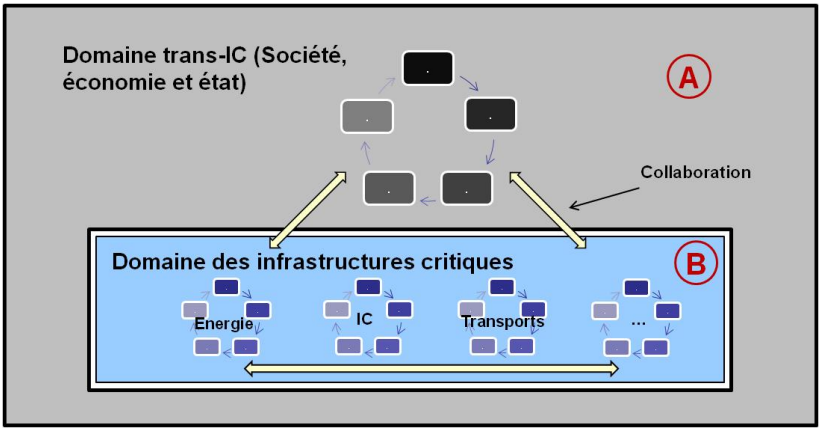
En référence aux objectifs énumérés au ch. 5, la stratégie nationale PIC définit des mesures appelées à renforcer la *protection intégrale* dans deux domaines (champs d'action):

- *dans le domaine transinfrastructures,* elles doivent garantir la coordination de la procédure et améliorer la capacité de résistance de la société, de l'économie et des pouvoir publics en cas de défaillance d'infrastructures critiques *(champ d'action A)*. Des processus touchant plusieurs infrastructures critiques sont mis en place, notamment pour améliorer la coordination et l'assistance des exploitants en cas d'événement. En outre, des mesures sont prises afin de réduire la vulnérabilité de la société, de l'économie et des pouvoirs publics;

– *dans le domaine des infrastructures critiques,* l'autoprotection et la robustesse de celles-ci doivent être améliorées *(champ d'action B)*. Les risques spécifiques aux différentes infrastructures seront identifiés et réduits. En améliorant la protection des différentes infrastructures et en garantissant la compatibilité des mesures par une procédure uniformisée, on réduit également les risques inhérents aux dépendances mutuelles (interdépendances).

Figure 2

Champs d'action de la stratégie nationale PIC



Des mesures qui contribuent à la réalisation des objectifs présentés aux chiffres précédents sont décrites ci-dessous pour les deux champs d'action.

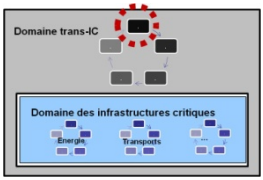
Comme il est dit au ch. 4.1, différents projets, processus ou mesures déjà établis ou programmés en rapport avec la protection des infrastructures critiques sont pertinents. La mise en œuvre de la stratégie PIC consistera souvent à vérifier des processus existants et à les compléter le cas échéant. La stratégie nationale PIC se développera dans la mesure du possible à partir de ce qui existe déjà. Cela se fera en détail au moment de l'application des différentes mesures. Une vue d'ensemble des mesures et des principales interfaces avec les autres travaux figure en annexe. On a renoncé à les citer explicitement dans le présent texte.

7.1 Renforcer la protection intégrale dans le domaine transinfrastructures (champ d'action A)

La protection intégrale dans le domaine transinfrastructures comprend l'ensemble des activités nécessaires à la conception, au pilotage et au perfectionnement des mesures pertinentes pour la PIC. Elle doit accroître la résilience des collectivités publiques, de la société et de l'économie et créer les conditions cadres voulues pour la protection des infrastructures critiques. Les mesures s'inspirent pour cela de la protection intégrale évoquée au ch. 6, les phases de mise en œuvre, de vérification et de contrôle étant traitées au ch. 8 de la stratégie.

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. Des connaissances relatives aux infrastructures critiques et à leur importance sont également nécessaires pour évaluer la situation en cas d'incident.

A ce sujet, l'inventaire des infrastructures critiques (inventaire PIC) est élaboré sur la base de la stratégie générale du Conseil fédéral en matière de PIC. Tous les objets critiques (ouvrages et constructions) sont identifiés, tant au niveau national que cantonal et local. Dans le deuxième cas, la tâche est accomplie par les cantons. On se référera dans la mesure du possible aux données déjà recensées dans le cadre d'autres inventaires.

Objectif:

– Les infrastructures critiques suisses sont identifiées et enregistrées dans le respect des dispositions sur la protection des informations (en cas d'informations classifiées). En particulier, les systèmes et objets critiques sont reconnus et affectés d'une priorité.

Mesure:

– *M1:* Tenir une liste périodiquement mise à jour des infrastructures critiques suisses (inventaire PIC), afin que des extraits puissent être établis en temps voulu, dans le respect de la protection des informations, pour différents services ou autorités en ayant besoin. Il convient de vérifier si la législation donne accès aux listes d'objets existantes. Avant que des mesures de protection puissent être prises, les services compétents doivent savoir quelles sont les infrastructures critiques. Des connaissances relatives aux infrastructures critiques et à leur importance sont également nécessaires pour que des évaluations de la situation puissent être faites en cas d'incidents.

Connaître les risques, les vulnérabilités et les possibilités de protection

L'amélioration de la protection intégrale des infrastructures critiques doit pouvoir se fonder sur des informations intersectorielles concernant les risques significatifs. Pour cela, il faut en particulier établir un catalogue des risques à considérer et évaluer leur probabilité et l'ampleur des dégâts potentiels. Ces hypothèses sont complétées au niveau des infrastructures critiques par des considérations concrètes sur les risques.

De plus, des connaissances scientifiquement fondées, par exemple dans le domaine des analyses d'interdépendance et de la criticité, sont nécessaires pour le perfectionnement méthodologique des infrastructures critiques. De même, doivent être suivies les évolutions technologiques et celles de l'environnement naturel et social susceptibles d'être à l'origine de nouveaux risques.

Objectifs:

- Vue d'ensemble périodiquement mise à jour des risques significatifs avec une estimation de leur probabilité de survenue et de l'ampleur de leurs dégâts potentiels.
- Des bases scientifiquement fondées, contribuant au perfectionnement méthodologique de la protection intégrale, sont disponibles.

Mesure:

- *M2:* lancer des programmes de recherche (p. ex. un programme national de recherche) en tenant compte de bases méthodologiques et de thèmes intersectoriels, comme des analyses d'interdépendance et de criticité, une mesure de la résilience ou des évolutions technologiques.

Améliorer la collaboration et l'échange d'informations

Les infrastructures critiques sont fortement interdépendantes. Une collaboration et un dialogue sur les risques et les mesures de protection possibles (*best practice*) transcendant les limites des différentes infrastructures critiques est donc d'une importance capitale. La collaboration doit pour cela être améliorée, aussi bien entre les exploitants d'infrastructures critiques qu'entre les autorités et les services spécialisés compétents. La coopération internationale revêt une grande importance au vu du caractère transfrontalier de nombreuses infrastructures critiques.

Objectif:

- Un échange d'informations intersectoriel et institutionnalisé sur les risques, les vulnérabilités et les mesures de protection possibles (*best practice*) dans le respect de la protection des informations (pour les informations classifiées).

Mesure:

- *M3:* créer des plates-formes afin de favoriser la collaboration entre les services spécialisés/autorités concernés par les différents domaines de la protection des infrastructures critiques (GT PIC), entre les exploitants (GT Exploitants) et avec les partenaires étrangers.

Garantir l'alerte en cas d'incident

En cas de menace sévère, une alerte donnée en temps voulu est d'une importance capitale pour pouvoir prendre des contre-mesures appropriées. Pour cela, il faut, d'une part, détecter les modifications significatives de la menace, notamment à court terme. Pour différents risques, il existe des procédures bien établies permettant de détecter de telles modifications en temps voulu. Cela n'est toutefois pas garanti de la même manière pour tous les dangers significatifs (en particulier pour les risques techniques). D'autre part, il convient de s'assurer que l'alerte est donnée suffisamment tôt et via des interfaces bien définies. A ce sujet aussi, il existe déjà différents mécanismes bien établis. Cependant, ceux-ci ne disposent quelquefois pas de ressources, notamment humaines, suffisantes, ou alors tous les exploitants ne sont pas intégrés en fonction de leur importance. De plus, certains processus ne sont pas canalisés et prennent en compte des interlocuteurs différents à chaque fois.

Objectifs:

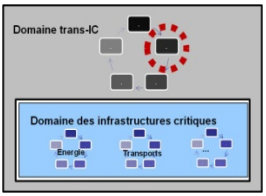
- Les modifications significatives de la menace, notamment à court terme, sont détectées en temps voulu sur tout l'éventail des risques.
- Les exploitants des infrastructures critiques sont prévenus efficacement des menaces sévères, suffisamment tôt et également en situation exceptionnelle, en fonction de leur importance. Cela permet de garantir qu'un éventail de risques complet est couvert, que le processus d'alerte se déroule via des contacts bien définis et des liaisons sécurisées et enfin que la protection des informations est assurée.

Mesures:

- *M4:* vérifier les pouvoirs et capacités nécessaires à la détection et à la surveillance des menaces et des dangers dans toutes les situations.
- *M5:* créer, sur la base des processus et des structures existantes, un mécanisme garantissant que les exploitants d'infrastructures critiques concernés sont prévenus en temps voulu des changements importants de la menace.

Objectifs de protection

Fixer des objectifs prioritaires de protection



Les objectifs de protection fournissent des renseignements sur les niveaux de protection et de résultats visés. Ils sont fixés au niveau politico-social. En fonction des possibilités, des objectifs de protection conçus les uns en fonction des autres et impératifs sont fixés pour les différentes infrastructures critiques dans le cadre d'un processus politique. Compte tenu de l'hétérogénéité des infrastructures critiques et de l'importance politique de cette thématique, l'entreprise est extrêmement difficile. Pour cette raison, la vision décrite dans la stratégie est considérée comme un objectif de protection intersectoriel. L'élaboration de concepts de protection intégrale au niveau des infrastructures critiques (voir mesure M15) précise les objectifs de protection. La législation actuelle sera si possible révisée en tenant compte des objectifs de protection déjà définis.

Objectif:

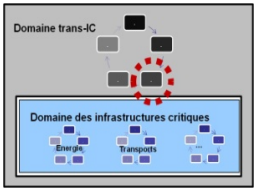
- Des objectifs de protection déterminés les uns en fonction des autres sont imposés pour les infrastructures critiques.

Mesure:

- *M6:* définir des objectifs de protection interdépendants qui seront adoptés par les responsables politiques.

Mesures (de de protection)

Eviter les défaillances des infrastructures critiques



Dans le domaine transinfrastructures, différentes mesures peuvent être prises afin d'éviter les risques significatifs pour toutes les infrastructures critiques et les défaillances graves. De tels risques génériques concernent notamment les personnels responsables de l'exé-

cution des processus centraux. Ces personnels doivent pouvoir être soumis à des contrôles de sécurité afin de respecter les normes de sécurité et de permettre l'échange d'informations classifiées. L'approvisionnement des infrastructures critiques en énergie et leur connexion aux réseaux de télécommunications constituent un autre risque générique. De ce point de vue, d'une part les infrastructures critiques renforcent leur autoprotection dans le cadre du champ d'action B (voir ch. 7.2). D'autre part, les infrastructures critiques nationales doivent, en fonction des possibilités techniques, être traitées en priorité dans le cadre des projets prioritaires et des plans d'exploitation.

Objectifs:

– Les personnes qui ont accès aux processus centraux[4] dans le domaine des infrastructures critiques sont soumises à des contrôles de sécurité.

– En cas de mesures d'exploitation ou de coupures dans les domaines de l'énergie et des télécommunications, les infrastructures critiques nationales sont traitées en priorité en fonction des possibilités techniques et des besoins.

Mesures:

– *M7:* créer une base légale permettant de soumettre certaines catégories de personnels des exploitants d'infrastructures techniques à un contrôle de sécurité.

– *M8:* compléter les plans de coupure et/ou d'exploitation existants avec les infrastructures critiques nationales, en fonction des possibilités.

Améliorer la préparation des pouvoirs publics, de l'économie et de la population

Les défaillances graves d'infrastructures critiques peuvent compromettre sérieusement le fonctionnement des pouvoirs publics et de l'économie et gêner gravement la population. Il est possible de réduire l'ampleur des dégâts si les pouvoirs publics, l'économie et la population sont convenablement préparés. Pour cette raison, une grande importance est accordée aux planifications préventives afin de maîtriser les incidents et à une sensibilisation préalable de la population et de l'économie aux risques éventuels ainsi qu'aux mesures préventives personnelles.

Objectif:

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

Mesures:

– *M9:* élaborer des planifications préventives au niveau fédéral et cantonal afin de maîtriser des défaillances graves des infrastructures critiques.

– *M10:* informer et sensibiliser la population et l'économie aux possibilités de protection relevant de la prévention personnelle en cas de défaillance des infrastructures critiques.

4 Ces processus seront définis lors de l'élaboration de l'inventaire PIC.

Aider les exploitants d'infrastructures critiques à maîtriser des incidents

En cas de menace sévère ou de défaillance grave, les exploitants doivent être soutenus subsidiairement avec des moyens ou des capacités extérieurs aux établissements afin de combattre la menace ou de permettre un fonctionnement minimum et le retour rapide à l'exploitation normale.[5] Premièrement, les moyens ou capacités correspondants doivent être disponibles. Alors qu'il est possible de faire appel aux forces d'intervention pour combattre les menaces physiques, les moyens dont disposent les pouvoirs publics pour lutter contre les cyber-menaces d'ampleur stratégique restent insuffisants, notamment en termes de ressources humaines. Deuxièmement, il faut recenser les moyens disponibles et les besoins en situation extraordinaire, notamment en termes de générateurs de secours ou de moyens de communication. Troisièmement, il convient de s'assurer que la répartition des moyens au niveau stratégique est décidée en tenant compte de l'importance (criticité) des infrastructures critiques, de la menace et des moyens à disposition. Quatrièmement, une planification préalable doit être établie afin de garantir l'utilisation efficace des moyens.

Objectif:

– Pour parer aux menaces et permettre un fonctionnement minimum ainsi qu'un retour rapide à la normale, les exploitants d'infrastructures critiques sont efficacement aidés par des moyens extérieurs en tenant compte de leur importance.

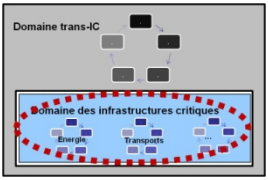
Mesures:

– *M11:* créer des moyens publics suffisants afin d'apporter une aide subsidiaire aux exploitants d'infrastructures critiques pour faire face aux cyberrisques d'importance stratégique.
– *M12:* recenser les ressources disponibles afin d'assurer une exploitation minimale et le retour à la normale dans la perspective d'une situation extraordinaire.
– *M13:* définir les processus concernant la répartition des moyens externes pour aider les exploitants à maîtriser des incidents, en collaboration avec les services concernés.
– *M14:* renforcer la collaboration des organes de crise et de conduite au niveau de la Confédération, des cantons et des communes avec les exploitants d'infrastructures critiques et planifier la protection des éléments d'infrastructures critiques nationales.

7.2 Améliorer la protection intégrale dans le domaine des infrastructures critiques (champ d'action B)

La stratégie nationale PIC vise à renforcer la protection intégrale non seulement dans le domaine transinfrastructures mais aussi dans celui des infrastructures critiques.

[5] Ce sont, par exemple, les forces d'interventon (police, pompiers, protection civile, militaires), les moyens de communication ou les groupes électrogènes de secours.



Comme des défaillances graves peuvent être causées par des risques spécifiques qui concernent soit un élément isolé (p. ex. un poste de commande), un sous-secteur (p. ex. à cause d'un réseau de transport vieillissant) ou un secteur (p. ex. les transports), la protection intégrale telle qu'elle est décrite au ch. 6 doit être renforcée à tous les niveaux correspondants des infrastructures critiques. Dans ce but, des concepts de protection intégrale devront être élaborés et mis en œuvre. La procédure pourra être décrite dans un guide s'appuyant sur la stratégie générale du Conseil fédéral en matière de PIC. Les travaux en cours ou prévus, les bases légales en vigueur, les objectifs de protection, etc. seront réunis et intégrés aux concepts de protection intégrale. Par la suite, on déterminera les risques résiduels spécifiques aux infrastructures, on fixera des objectifs de protection et, le cas échéant, on définira des mesures afin de réduire les risques. Il conviendra également d'examiner le financement des éventuelles mesures de protection et les bases légales nécessaires à la mise en œuvre des concepts de protection intégrale.

Les concepts de protection intégrale doivent être élaborés et mis en œuvre en collaboration avec les principaux acteurs (autorités compétentes au niveau fédéral, cantonal ou communal, services spécialisés en fonction de la menace ou des mesures, associations, etc.). La responsabilité (notamment de la définition des objectifs de protection) incombe aux organes compétents conformément à la législation en vigueur. La définition des objectifs de protection et le financement d'éventuelles mesures de suivi sont convenus dans le cadre des politiques spécifiques. Les travaux se feront selon une approche fondée sur le risque et tenant compte du rapport coût-efficacité: autrement dit, seules seront prises des mesures nécessaires à la réalisation des objectifs de protection et dont le coût est proportionnel au bénéfice que l'on peut en retirer. Les concepts de protection intégrale doivent avant tout donner une vue complète des risques et des vulnérabilités significatifs, à vérifier le niveau de protection existant ainsi qu'à identifier et combler les lacunes éventuelles.

Objectif:

– La protection intégrale des infrastructures critiques est garantie à tous les niveaux concernés (secteurs, sous-secteurs et éléments isolés). Tous les risques importants sont identifiés et réduits, après une évaluation du rapport coût-efficacité, conformément aux objectifs de protection et de résultat convenus au niveau politique et compte tenu d'un éventail complet des dangers et des mesures.

Mesure:

– *M15:* élaborer des concepts de protection intégrale pour les infrastructures critiques, en s'appuyant sur le guide PIC, et les mettre en œuvre sur la base de fondements juridiques appropriés. Les concepts de protection intégrale doivent être élaborés et mis en œuvre en collaboration avec les principaux acteurs (autorités compétentes aux niveaux fédéral, cantonal ou communal, exploitants, associations, etc.). Les organes cités au tableau 2 désignent les services responsables et ceux qui doivent être impliqués.

8 Mise en œuvre de la stratégie nationale PIC

8.1 Structures et compétences

La stratégie nationale PIC est mise en œuvre essentiellement dans le cadre des procédures définies ainsi que des structures et compétences existantes. La coordination est garantie par l'implication dès le début du projet de représentants des autorités (Confédération et cantons) et des milieux économiques (en particulier les exploitants d'infrastructures critiques) et scientifiques. La collaboration avec le Mécanisme de consultation et de coordination du Réseau national de sécurité (MCC RNS) est ainsi assurée.

L'organe de coordination PIC aide les services compétents à mettre les mesures en œuvre. Il est notamment chargé des tâches suivantes:

- coordonner les mesures au niveau supérieur conformément au processus de protection intégrale (tenue de l'inventaire PIC, etc.);
- appuyer les autorités responsables et les exploitants dans l'élaboration de concepts de protection intégrale;
- conseiller les cantons en matière de PIC;
- préparer les dossiers de l'organe de pilotage et de la plate-forme de coordination;
- servir d'interlocuteur en matière de PIC au plan international;
- rendre compte de la mise en œuvre de la stratégie nationale PIC.

La coordination de la PIC avec d'autres chantiers similaires dans le domaine transinfrastructures (stratégie nationale en matière de cyber-risques, stratégie pour l'avenir des réseaux nationaux d'infrastructures, gestion des risques au niveau fédéral, programme de prévention antisismique ou approvisionnement économique du pays) reste une tâche importante. Elle est assurée d'une part par l'harmonisation des procédures et l'échange systématique d'expériences dans le domaine transinfrastructures et, d'autre part, par le fait que les résultats de ces travaux sont également pris en considération dans l'élaboration des concepts de protection intégrale des différentes infrastructures critiques.

Les organes désignés en annexe sont responsables de la mise en œuvre des mesures dans le domaine transinfrastructures (M1 à M14). L'organe de coordination PIC assume une fonction de coordination dans le domaine transinfrastructures dans le cadre de la responsabilité de ses processus. En collaboration avec les organes susnommés, il désigne les projets, processus, etc. importants dans le contexte des différentes mesures, évalue la réalisation des objectifs formulés dans le cadre de la stratégie et estime s'il y a lieu de corriger le tir. Les mesures seront mises en œuvre si possible dans le cadre des projets ou activités en cours.

Il sera procédé d'une manière analogue dans le domaine des infrastructures critiques (M15), selon l'échelon responsable du processus (Confédération, cantons ou communes) conformément aux bases légales en vigueur. Les organes énumérés au tableau 2 sont invités à désigner ceux auxquels la responsabilité doit être confiée et qui doivent être impliqués, le cas échéant en collaboration avec l'organe de coordination PIC. Tous les acteurs importants (exploitants, associations, organes spécialisés en fonction des dangers et des mesures, etc.) participent à l'élaboration des

concepts de protection intégrale. L'organe de coordination PIC supervisera les travaux au besoin et selon les possibilités.

Tableau 2

Répartition des compétences par sous-secteur

Secteur	Sous-secteur (SSC)	Services fédéraux assurant la coordination *(non exhaustif)**
Autorités	Représentations diplomatiques, organisations internationales	DFAE, fedpol
	Recherche et enseignement	SER
	Biens culturels	OFPP, OFC
	Parlement, gouvernement, justice, administration	ChF, Services du Parlement, fedpol, OFCL, UPIC et FP
Energie	Approvisionnement en gaz naturel	OFEN, OFAE
	Approvisionnement en pétrole	OFEN, OFAE
	Approvisionnement en électricité	OFEN, OFAE, ElCom, IFSN, ESTI
Elimination	Déchets	OFEV
	Eaux usées	OFEV
Finances	Banques	FINMA, BNS, AFF, SFI
	Assurances	FINMA, OFAS
Santé	Soins médicaux et hôpitaux	SSC
	Laboratoires	OFSP
Industrie	Industrie chimique et pharmaceutique	OFAE
	Industrie MEM	OFAE
Information et communication	Technologies de l'information	OFAE, UPIC
	Médias	OFCOM
	Trafic postal	SG DETEC, OFCOM
	Télécommunication	OFCOM, OFAE
Alimentation	Denrées alimentaires	OFAE, OFAG
	Eau	OFEN, OFAE
Sécurité publique	Armée	PIO
	Organisations d'urgence	OFPP, fedpol, SRC
	Protection civile	OFPP
Transports	Trafic aérien	OFAC, OFAE
	Trafic ferroviaire	OFT, OFAE
	Trafic fluvial	OFT, OFAE
	Trafic routier	OFROU, OFAE

* Les organes énumérés jouent un rôle de coordination: au besoin, ils désignent, en collaboration avec l'organe de coordination PIC, les organes (Confédération, cantons, associations, etc.) dirigeant et participant à l'élaboration des concepts de sécurité intégrale, sous réserve des compétences en vigueur.

8.2 Calendrier et controlling

La mise en œuvre des différentes mesures est précisée à l'aide d'un programme d'application et de controlling détaillé qui sera élaboré après l'adoption de la stratégie nationale PIC. La mise en œuvre doit, en gros, se faire selon le calendrier suivant:

Phase 1 (jusqu'à fin 2012)

- La mise en œuvre est planifiée.
- Les objets des infrastructures critiques au niveau national sont identifiés et recensés. (M1)
- Les plates-formes intersectorielles (GT PIC et GT Exploitants) sont en place. (M3)

Phase 2 (jusqu'à fin 2013)

- Le concept de garantie d'alerte en cas d'incident est terminé. (M5)
- Les objectifs de protection harmonisés sont définis et proposés. (M6)
- Un projet de base juridique permettant de soumettre le personnel des exploitants d'infrastructures critiques au contrôle de sécurité est rédigé. (M7)
- Les plans de coupure et d'exploitation existants sont complétés avec les infrastructures critiques nationales. (M8)
- Un mécanisme permettant le recensement des ressources existantes est développé et les processus pour aider les exploitants avec des moyens extérieurs sont définis. (M12, M13)

Phase 3 (jusqu'à fin 2014)

- Une proposition actualisée de programme de national de recherche est déposée. Des examens complémentaires ont été faits au niveau de la recherche sectorielle. (M2)
- Les résultats de la vérification des pouvoirs et capacités nécessaires à la détection et à la surveillance des menaces et des dangers sont disponibles. (M4)
- Les produits d'information pour renforcer l'autoprévention de l'économie et de la population sont élaborés. (M10)
- Les interventions pour la protection des infrastructures critiques sont planifiées. (M14)

Phase 4 (à partir de 2015)

- Les planifications préventives pour la maîtrise des défaillances des infrastructures critiques sont établies. (M9)
- Les ressources humaines et les capacités d'aide subsidiaire nécessaires afin de maîtriser les cyber-risques sont créées par étapes en fonction des bases légales correspondantes. (M11)
- Les concepts de protection intégrale pour les infrastructures critiques sont élaborés et mis en œuvre. (M15)

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

8.3 Révision de la stratégie

La stratégie nationale de protection des infrastructures critiques est périodiquement mise à jour. La présente stratégie est passée en revue et adaptée le cas échéant d'ici à la fin de 2016.

Mesures et interfaces avec les travaux en cours ou prévus

Mesure	Organes compétents (*liste non exhaustive*)*	Interfaces avec d'autres projets/services/organisations (*liste non exhaustive*)
M1: Etablissement de l'inventaire PIC	OFPP, organes fédéraux selon tableau 2, cantons (points de contact cantonaux PIC)	Inventaires existants (cadastre des défaillances, ouvrages d'accumulation, biens culturels, etc.)
M2: lancer des programmes de recherche (y c. programme national de recherche)	OFPP	Fonds national de la recherche scientifique (FNRS), programmes de recherche des organes fédéraux
M3: Création de plates-formes autorités/services spécialisés et exploitants	OFPP	Approvisionnement économique du pays (AEP), Service de renseignement de la Confédération (SRC), Stratégie nationale de protection contre les cyber-risques
M4: Vérification des pouvoirs et les capacités pour la surveillance des menaces	OFEV, OFAE, MétéoSuisse, SRC	Plate-forme commune d'information sur les dangers naturels (GIN), élaboration d'une loi sur le service de renseignement, Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), AEP, Cyber Defense
M5: Etablissement du mécanisme d'alerte précoce	OFPP, OFEV, OFAE, MétéoSuisse, SRC	Projet Netalert (OFPP), Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), AEP
M6: Définition d'objectifs supérieurs de protection	OFPP	Plate-forme interdépartementale «Dangers naturels» PLANAT, AEP

Mesure	Organes compétents (*liste non exhaustive*)*	Interfaces avec d'autres projets/services/organisations (*liste non exhaustive*)
M7: Création d'une base légale permettant de soumettre au contrôle de sécurité les exploitants d'infrastructures critiques	PIO	Projet de base légale-formelle pour la protection des informations (FOGIS), protection des informations et des objets PIO
M8: Reprise des plans de coupure et d'exploitation existants	OFAE	OFEN, ELCOM
M9: Elaboration de planifications préventives pour les défaillances d'infrastructures critiques	OFPP, cantons (organes de conduite cantonaux OCC), OFAE, OFEN	Etat-major fédéral ABCN (EMF ABCN), analyses et prévention des dangers à l'échelon cantonal (KATAPLAN), AEP, IDA Nomex
M10: Amélioration de l'auto-prévention de l'économie et de la population	OFPP, OFAE, ChF	Projet de mesures de protection individuelles (OFPP), ChF
M11: Garantie de l'aide subsidiaire pour la maîtrise de cyber-risques	ChF, UPIC, OFAE, DDPS	Stratégie nationale en matière de cyber-risques, EMF ABCN
M12: Recensement des ressources pour l'exploitation des infrastructures critiques en cas de d'urgence	OFPP	Gestion des ressources au niveau fédéral (ResMaB), AEP
M13: Définition des processus d'attribution de moyens extérieurs aux exploitants d'infrastructures critiques	OFPP	Réseau national de sécurité (RNS), EMF ABCN, ResMaB, AEP, IDA Nomex
M14: Renforcement de la collaboration organes de conduite – exploitants d'infrastructures critiques et élaboration de planifications de protection	EMF ABCN, cantons, communes (organes de conduite, police, sapeurs-pompiers), EM cond A	RNS, développement de la protection de la population/ protection civile, KATAPLAN, IDA Nomex

Mesure	Organes compétents (*liste non exhaustive*)*	Interfaces avec d'autres projets/services/organisations (*liste non exhaustive*)
M15: Elaboration et mise en œuvre de concepts de protection intégrale pour les infrastructures critiques	En accord avec les organes de coordination selon tableau 2	Divers travaux en fonction des secteurs et des menaces (notamment stratégie pour la société de l'information en Suisse, stratégie cyber-risques, prévention antisismique, gestion fédérale des risques, bâtiments fédéraux prioritaires en cas de pénurie d'électricité)

* L'organe de coordination PIC assume une fonction de coordination et veille à ce que tous les organes compétents et importants soient associés au processus, en collaboration avec l'organe mentionné.