Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Office fédéral de la protection de la population OFPP

Premier rapport sur la protection des infrastructures critiques à l'attention du Conseil fédéral

20.06.2007

Table des matières

1 Contexte

1.1 Les infrastructures critiques

Les infrastructures sont à la base du fonctionnement de nombreux processus sociétaux, économiques et politiques. Elles sont classées en secteurs parmi lesquels figurent entre autres l'approvisionnement en énergie, le transport, les technologies de l'information et de la communication, la finance, l'approvisionnement en eau potable et en denrées alimentaires de même que la santé publique. Le fonctionnement des infrastructures influe sur la qualité de vie d'une société, la valeur ajoutée d'une économie et la sécurité de l'Etat et de sa population.

On décrit en général une infrastructure comme critique lorsqu'elle est essentielle au fonctionnement de l'ensemble du système ou d'autres infrastructures. L'importance d'une infrastructure varie cependant selon le point de vue. C'est ainsi que l'effondrement d'une maison individuelle est en premier lieu une tragédie pour ses habitants. L'incendie d'un bâtiment communal a pour sa part des conséquences pour la commune tout entière. La région environnante, le canton et l'Etat ne sont en revanche pas touchés. Une perturbation du système de gestion centralisé des CFF peut être à l'origine de pannes dans toute la Suisse, qui peuvent même revêtir une dimension transfrontalière. Le présent rapport se réfère aux infrastructures dont les fonctions et prestations ont avant tout une portée nationale.

En soi, la protection des infrastructures critiques (PIC) ne représente pas un thème nouveau. Les Etats ont de tout temps cherché à protéger les infrastructures importantes contre les forces de la nature, les défaillances techniques, les actes de sabotage et de destruction. Lors de conflits armés, les structures essentielles à l'économie de l'adversaire constituent à chaque fois des cibles privilégiées.

La nécessité de disposer d'infrastructures critiques fonctionnant sans faille est aujourd'hui indiscutable pour les nations industrielles occidentales. Les perturbations ou défaillances ont des répercussions directes sur la population et ses bases d'existence. Une infrastructure de haute qualité et stable constitue un des facteurs d'implantation principaux de la Suisse. Le seuil de tolérance face aux perturbations est par conséquent relativement bas.

1.2 Mandat du Conseil fédéral

Au printemps 2004, la Délégation des Commissions de gestion (DélCdG) des Chambres fédérales a sollicité des renseignements sur l'importance accordée aux infrastructures critiques par la Délégation du Conseil fédéral pour la sécurité et l'Organe de direction pour la sécurité. Elle souhaitait notamment savoir si et, le cas échéant, dans quelle mesure les infrastructures indispensables au bon fonctionnement de la société, de l'économie et du système politique avaient été définies et si leur vulnérabilité ainsi que des mesures de protection et de sécurité avaient été évaluées.

L'Office fédéral de la protection de la population (OFPP) a été chargé par le chef du DDPS, le conseiller fédéral Samuel Schmid, qui préside la Délégation du Conseil fédéral pour la sécurité, de lui fournir les informations demandées. L'OFPP s'était déjà penché sur le sujet depuis 2003 et a rédigé, en vue de l'audition de la DélCdG du 5 juillet 2004, un rapport récapitulatif intitulé «Schutz und Sicherheit Kritischer Infrastrukturen in der Schweiz».

Ce rapport identifie les lacunes et les besoins en matière de PIC (notamment à propos d'une compréhension de base commune, des scénarios de danger, des objectifs de protection,

d'une liste des infrastructures critiques et d'un règlement des compétences). Ceux-ci ont été résumés dans la note de discussion du 15 juin 2005 destinée au Conseil fédéral. S'appuyant sur ce document, le Conseil fédéral a chargé le DDPS (OFPP) le 22 juin 2005 de coordonner les travaux liés à la protection des infrastructures critiques et - selon les recommandations formulées à l'alinéa 4 de la note de discussion - de les réaliser avec la collaboration des personnes de contact désignées par les départements ou offices concernés. Le présent rapport expose les premiers résultats des travaux réalisés dans le cadre de ce mandat.

2 Objectifs

2.1 Premier rapport

Les objectifs sur lesquels se fonde ce premier rapport sont fixés dans la note de discussion du 15 juin 2005. Les aspects suivants doivent être traités de manière ciblée et par étapes:

- *Etablissement d'une vue d'ensemble des travaux effectués jusqu'à présent dans le domaine de la protection des infrastructures critiques*
- *Identification des infrastructures critiques déterminantes pour la Suisse*
- *Définition de différents scénarios de base des dangers*
- *Choix d'une infrastructure critique déterminante pour la Suisse et élaboration, à titre de modèle, d'une stratégie et d'un catalogue de mesures*

Résultant d'une large collaboration avec les organes fédéraux représentés dans le groupe de travail PIC, le présent rapport constitue une première étape vers une stratégie nationale pour la protection des infrastructures critiques. Il établit la méthode de travail, les données du problème et les définitions. Il dresse une liste des secteurs d'infrastructures critiques jugés déterminants pour la Suisse. Exposant les bases et conditions-cadres des scénarios de dangers, il en propose ensuite une ébauche. Enfin, il présente les besoins de même que la marche à suivre en ce qui concerne la protection des infrastructures critiques. Quant aux annexes, elles décrivent les travaux effectués jusqu'à maintenant dans le domaine de la protection des infrastructures critiques (activités d'autres Etats et des offices fédéraux concernés et évolution en Suisse).
Dans une première phase, il s'agissait de se mettre d'accord, au sein du groupe de travail qui compte des représentants des sept départements fédéraux, sur des définitions et des conditions-cadres communes et de favoriser une compréhension réciproque entre les intéressés. L'élaboration à titre de modèle d'une stratégie et d'un catalogue de mesures en matière d'infrastructure critique déterminante pour la Suisse n'a ainsi pas été réalisée durant cette étape et fera l'objet de la suite des travaux.

2.2 Stratégie nationale pour la protection des infrastructures critiques

De nombreux organes de la Confédération, des cantons, de l'économie et de la science s'occupent de la protection des infrastructures critiques, à des titres différents et souvent indépendamment les uns des autres. Il s'agit dès lors de définir une stratégie nationale afin de favoriser le dialogue et la collaboration entre ces organes, de créer des synergies et de renforcer, en l'institutionnalisant, l'échange de connaissances et d'expériences.

Le présent rapport servira de base à l'élaboration de cette stratégie nationale qui comprendra des méthodes d'évaluation communes de même que des objectifs de protection uniformes. Celle-ci constituera un cadre cohérent pour des travaux sectoriels et intersectoriels

dans ce domaine. Des organes internes et externes à l'administration fédérale pourront en outre s'y référer pour leurs activités liées à la protection des infrastructures critiques.

La stratégie nationale a pour but de maintenir les bases existentielles de la population. A cette fin, les objectifs suivants devront être atteints:

- Analyse intégrale des risques encourus par les infrastructures critiques, accompagnée de propositions de mesures destinées à réduire ces risques.
- Meilleure compréhension des interactions et des interdépendances entre les différentes infrastructures critiques
- Promotion de la confiance mutuelle, des échanges d'information et de la collaboration entre les autorités, les exploitants d'infrastructures critiques et l'économie privée en vue d'une mise à profit des synergies qui en découlent.
- Recommandations de mesures visant à limiter au maximum la durée et les conséquences d'événements dommageables.

3 Méthode de travail

3.1 Groupe de travail «Protection des infrastructures critiques»

La future stratégie nationale pour la protection des infrastructures critiques doit être réalisée en étroite collaboration avec les offices concernés. Pour l'instant, un groupe de travail (GT PIC) a été constitué sur la base d'une demande officielle. Il comprend des représentants de 18 organes fédéraux (énumérés ci-après selon l'ordre dans lequel ils figurent dans l'annuaire fédéral):

DFAE	SPOL, DDC
DFI	MétéoSuisse, OFSP
DFJP	fedpol
DDPS	PIO, EM cond A, armasuisse immobilier, OFPP
DFF	USIC, OFIT, OFCL
DFE	OFAE
DETEC	OFT, OFEN, OFROU, OFCOM, OFEV

Le GT PIC s'est réuni trois fois entre novembre 2006 et avril 2007 sous la direction de l'OFPP pour l'élaboration du présent rapport. Des versions intermédiaires ont été mises en consultation à plusieurs reprises. Les réunions ont favorisé le développement d'une compréhension commune de la thématique et ont contribué à unifier l'usage des termes les plus importants (voir chap. 5 Définitions). Elles ont aussi permis d'identifier les infrastructures critiques et de déterminer l'éventail des dangers. Ce rapport a été mis en consultation plusieurs fois au sein du GT PIC. Il tient ainsi compte des diverses perspectives des offices qui y sont représentés. Des sous-groupes de travail seront mis en place dans la phase suivante des travaux pour approfondir des thèmes précis. Les résultats seront ensuite intégrés aux travaux du GT PIC.

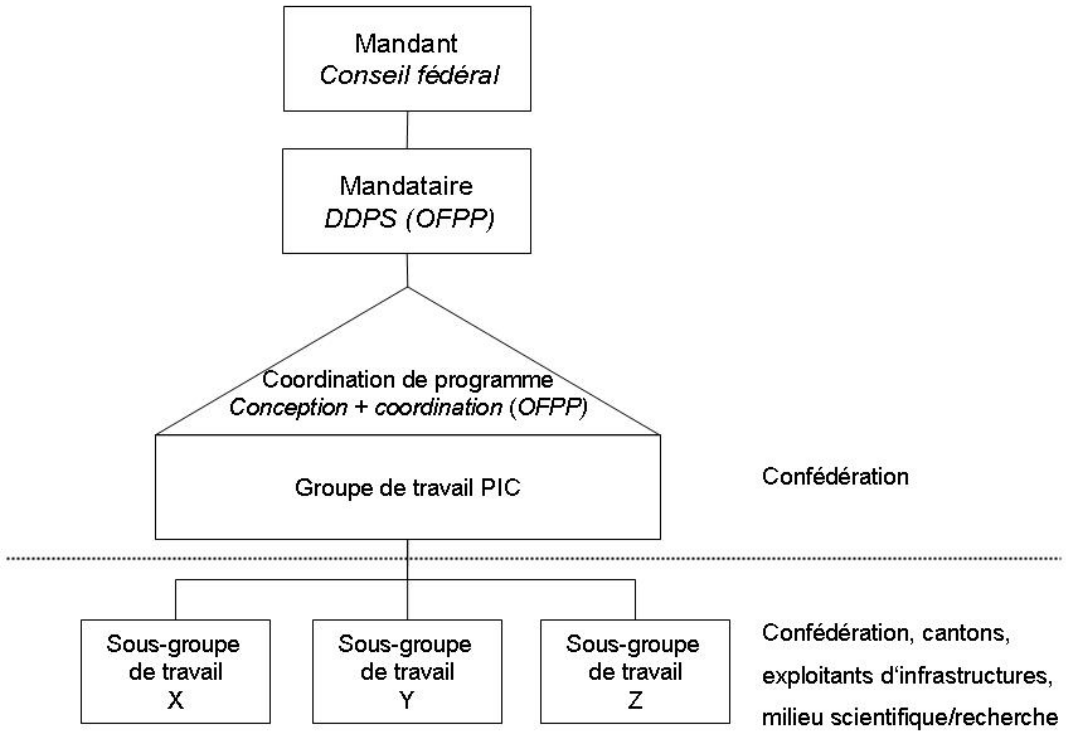

Figure 1: Organisation du programme de protection des infrastructures critiques

3.2 Collaboration

La collaboration de tous les intéressés constitue une condition préalable essentielle au succès de l'élaboration et de la mise en œuvre de la future stratégie nationale pour la protection des infrastructures critiques. L'intégration de tous les organes fédéraux concernés, des milieux économiques (industrie et commerce, fournisseurs de services, etc.) et des autorités cantonales compétentes est ainsi indispensable. Une collaboration a déjà lieu aujourd'hui dans le cadre du groupe de travail PIC entre différents organes fédéraux concernés. De plus il existe déjà des instruments communs dans certains secteurs d'infrastructure (p.ex. MELANI, SONIA, tables rondes d'Infosurance, voir annexes 2 et 3). Ces outils seront étendus à d'autres partenaires dans le cadre de l'élaboration d'une stratégie nationale.

4 Données du problème

4.1 Facteurs d'influence

La protection des infrastructures critiques continuera à gagner en importance au gré des changements de la situation en matière de politique de sécurité et des conditions-cadres politiques, économiques et techniques. Les facteurs suivants sont prépondérants à cet égard:

- Renforcement des interdépendances: les produits et services de la société moderne sont de plus en plus dépendants du bon fonctionnement des infrastructures. L'importance des services d'infrastructure (p.ex. approvisionnement en électricité, transports, technologies de l'information et de la communication) pour la vie sociale, politique et économique s'est

accrue de manière significative par rapport au passé. Le risque d'effets domino en cas d'événements en est augmenté d'autant.

- Intégration croissante de systèmes techniques: les infrastructures sont de plus en plus équipées de composants techniques (p.ex. technologie de l'information, automatisation de la production, etc.). S'ils soutiennent les processus de production et de gestion, ces éléments entraînent cependant une plus grande vulnérabilité des infrastructures en raison de leur complexité accrue.
- Evolution économique: les effets des conditions-cadres économiques actuelles (délocalisation de la production à l'étranger, production en série, raccourcissement des délais de production et réduction des stocks, libéralisation et mondialisation, diminution de la diversité des produits informatiques) contribuent à renforcer la vulnérabilité des infrastructures.
- Diminution des redondances: la pression sur les coûts a conduit à la suppression de nombreuses redondances (p.ex. groupes électrogènes de secours, réserves de secours), ce qui accroît la vulnérabilité et peut prolonger la durée d'indisponibilité en cas de perturbations affectant les infrastructures.
- Concentration des valeurs: la concentration croissante des valeurs (immobilier, mobilier, biens culturels, etc.) dans les centres urbains ainsi que leur utilisation plus intensive que par le passé génèrent de plus grands dommages lors d'événements.
- Attractivité des cibles: les installations civiles représentent des cibles particulièrement attractives lors d'attentats à la bombe et de guerre asymétrique, du fait qu'elles ne sont pas aussi bien sécurisées que les installations militaires, notamment pour des raisons économiques. Les bâtiments gouvernementaux, les centres névralgiques de l'économie, de la finance et des transports ainsi que les infrastructures de l'énergie et de l'information peuvent être spécialement visés.

4.2 Importance des infrastructures critiques

Les exemples suivants mettent en évidence les dommages qui peuvent résulter de défaillances ou de perturbations affectant les infrastructures critiques:

- Catastrophes naturelles: les catastrophes naturelles, dont le degré d'occurrence a augmenté ces dernières années et devrait encore s'amplifier à l'avenir, causent d'importants dégâts aux infrastructures critiques: l'ouragan Katrina, qui a frappé la Nouvelle-Orléans en été 2005, a non seulement causé la mort de nombreuses personnes et occasionné des dommages matériels élevés mais également paralysé pendant plusieurs semaines la production, l'importation et le raffinage de pétrole brut de même que l'approvisionnement en électricité et les installations portuaires (un des ports américains les plus importants pour l'exportation de produits agricoles). En novembre 2005, de violentes chutes de neige et de pluie givrante ont détruit en Allemagne environ 70 mâts à haute tension, privant quelque 250'000 personnes d'électricité pendant plusieurs jours et ce par des températures glaciales. L'approvisionnement général de la population en a été affecté de même que le secteur des transports, un grand nombre de liaisons ferroviaires et aériennes ayant dû être supprimées.
- «Blackout» généralisé: une panne de courant a affecté la quasi-totalité de l'Italie le 28 septembre 2003. Les dommages ont été estimés à quelque 185 millions de CHF (dus surtout aux pertes dans l'industrie alimentaire et aux coûts de remise en état). Il s'agissait de la quatrième panne de courant généralisée en l'espace de sept semaines après celles des USA, de la Suède et du Danemark ainsi que celle de Londres. Ces incidents mettent en évidence la dépendance des infrastructures par rapport à l'approvisionnement en électricité et l'ampleur des dommages consécutifs.
- Panne d'un réseau électrique isolé: une panne de courant survenue le 22 juin 2005 sur l'ensemble du réseau des chemins de fer fédéraux (CFF) a touché 2'000 trains et plus de 200'000 voyageurs. Les CFF, jusqu'alors estimés pour leur fiabilité, ont subi une impor-

tante perte d'image. Les dommages financiers, dus principalement au paiement de dédommagements, se sont élevés à environ 5 millions de CHF.

- Problème de logiciel: L'introduction d'un nouveau logiciel au Japon début mars 2003 a provoqué la défaillance sur tout le territoire du système de gestion de vol. Plusieurs centaines de vols ont été annulés et le système n'a pu être totalement remis en état qu'après plusieurs jours.
- Sabotage: Un homme de 49 ans a pénétré en mars et avril 2000 dans le système informatisé de gestion de l'approvisionnement en eau du Queensland (Australie). Il a pris les commandes de plus de 300 nœuds de contrôle du réseau de distribution d'eau potable et des eaux usées: plusieurs millions de litres d'eaux usées ont ainsi été déversés dans les rivières, les parcs et les hôtels de luxe. La faune marine environnante a subi d'importants dommages et l'économie du tourisme, des pertes financières considérables.
- Attentats terroristes: Des événements tels que les attentats terroristes du 11 septembre 2001 montrent que les attaques sont dirigées de plus en plus contre les points faibles (civils) et les infrastructures critiques. L'effondrement des tours jumelles du World Trade Center a causé la mort de plus de 2'600 personnes. D'importantes infrastructures de communication ont été détruites, ce qui a fortement perturbé le fonctionnement de la Bourse de New York Wall Street et du système financier mondial. Les dommages économiques ont dépassé durant les seuls premiers mois qui ont suivi les attaques le seuil des 100 milliards USD. Les actes terroristes de Madrid en 2004 et de Londres en 2005 ont fait quelques centaines de morts et plusieurs milliers de blessés. Paralysant le trafic ferroviaire complet pendant plusieurs heures, ils ont également provoqué des traumatismes psychologiques douloureux chez les personnes impliquées et nécessité un renforcement des mesures de sécurité.

5 Définitions

Les définitions suivantes ont été élaborées par le GT PIC qui s'est fondé sur les définitions existantes d'autres Etats et de l'Union européenne (voir annexe 1) en les adaptant aux spécificités suisses (notamment sur les plans politique, économique, technologique, culturel, géographique et topographique). Ces ajustements s'avèrent nécessaires d'une part, vu l'absence d'une définition explicite et généralement reconnue et, d'autre part, eu égard à la nécessité de différencier les définitions nationales selon le degré de développement du pays (technologie et politique), la perception de l'importance des infrastructures (culture, sensibilité et histoire) et la situation du pays (géographie et politique de sécurité).

Les définitions fixent le cadre terminologique de la protection des infrastructures critiques et offrent une base pour la suite des travaux. Au besoin, elles devront être adaptées ou élargies à la lumière de la stratégie nationale.

Infrastructures
Le terme générique *infrastructure* recouvre les personnes, organisations, processus, produits, prestations, flux d'information de même que les constructions et les équipements techniques et physiques qui, isolément ou conjointement, permettent le fonctionnement de la société, de l'économie et de l'Etat.
Les infrastructures sont réparties en trois échelons:

- **Secteurs**: p.ex. énergie, finance, santé publique
- **Sous-secteurs**: p.ex. approvisionnement en électricité, approvisionnement en pétrole, approvisionnement en gaz naturel
- **Objets spécifiques/éléments**: p.ex. pompes, conduites, barrages, lignes à haute tension, systèmes de commande

Infrastructures critiques
Les *infrastructures critiques* sont les infrastructures dont la perturbation, la défaillance ou la destruction ont des conséquences graves sur la santé, la vie publique, l'environnement, la politique, la sécurité et le bien-être économique ou social.

Criticité
La *criticité* d'une infrastructure décrit son importance relative par rapport aux conséquences qu'une perturbation, une défaillance ou une destruction aurait pour la population ou ses bases d'existence.

Objectif de la protection des infrastructures critiques
La protection des infrastructures critiques a pour but de réduire la probabilité d'occurrence et l'ampleur des dommages d'une perturbation, d'une défaillance ou d'une destruction des infrastructures critiques et, le cas échéant, de minimiser la durée de non-disponibilité.

Protection des infrastructures critiques et protection des infrastructures d'information critiques
On distingue la protection des infrastructures critiques PIC (Critical Infrastructure Protection, CIP) de la protection des infrastructures d'information critiques PIIC (Critical Information Infrastructure Protection, CIIP). La PIC englobe la protection de toutes les infrastructures critiques, alors que la PIIC se limite à la protection des infrastructures d'information critiques et constitue un des aspects d'une stratégie de protection globale.

6 Identification des infrastructures critiques

Une première identification des infrastructures critiques déterminantes pour la Suisse a été établie par le GT PIC. La liste sera réexaminée au cours des travaux d'élaboration de la stratégie nationale et complétée par des objets spécifiques et éléments d'infrastructure critiques.

La classification d'une infrastructure parmi les infrastructures critiques se réfère au secteur/sous-secteur dans son ensemble et non à des éléments d'infrastructure individuels (p.ex. énergie et non un barrage isolé). L'ordre dans lequel les infrastructures critiques sont énumérées ne donne pas d'indication quant à leur importance. Il est néanmoins prévu de procéder par la suite à une pondération sur la base de l'importance des secteurs (et de leurs sous-secteurs et éléments d'infrastructure).

Secteur	Sous-secteur
Autorités	Parlement, gouvernement, justice, administration
	Instituts de recherche
	Biens culturels d'importance nationale
	Représentations étrangères et sièges d'organisations internationales
Industrie chimique	Production, transport, entreposage et traitement de substances chimiques
Energie	Approvisionnement en électricité
	Approvisionnement en pétrole
	Approvisionnement en gaz naturel
Elimination des déchets	Eaux usées
	Déchets industriels et ménagers
	Déchets soumis à des contrôles
Finance	Banques
	Assurances
Santé publique	Soins médicaux et hôpitaux
	Médicaments
	Laboratoires
Technologie de l'information et de la communication (TIC)	Télécommunications
	Systèmes et réseaux d'information
	Internet
	Systèmes d'instrumentation, d'automatisation et de contrôle
	Radiodiffusion et médias
Alimentation	Approvisionnement en denrées alimentaires et garantie de la sécurité alimentaire
	Approvisionnement en eau potable
Sécurité publique, services de sauvetage et d'urgence	Organisations de première intervention (police, sapeurs-pompiers, service de sauvetage sanitaire)
	Protection civile
	Armée
Transports	Transport routier
	Transport ferroviaire
	Transport aérien
	Transport naval
	Trafic postal et logistique

Tableau 1: Secteurs et sous-secteurs d'infrastructures critiques en Suisse

7 Principes de base et conditions-cadres

7.1 Gestion intégrale des risques

La protection des infrastructures critiques sera conçue selon un système de gestion intégral des risques. Du fait de la complexité et des interdépendances des infrastructures critiques, il est en effet indispensable d'adopter une approche globale pour garantir une protection optimale.

La planification de mesures doit avoir lieu conformément au cycle de gestion des risques. Celui-ci favorise le choix de mesures appropriées et optimise leur mise en œuvre pour toutes les phases de la gestion des risques. Le concept élaboré par l'OFPP dans le cadre de KATARISK (cf. figure 2) sert de base pour les travaux ultérieurs. Dans le domaine de la prévention spécialement, ce concept devra être adapté aux besoins de la protection des infrastruc-

tures critiques par des mesures de construction de même que par des mesures techniques, organisationnelles et juridiques.

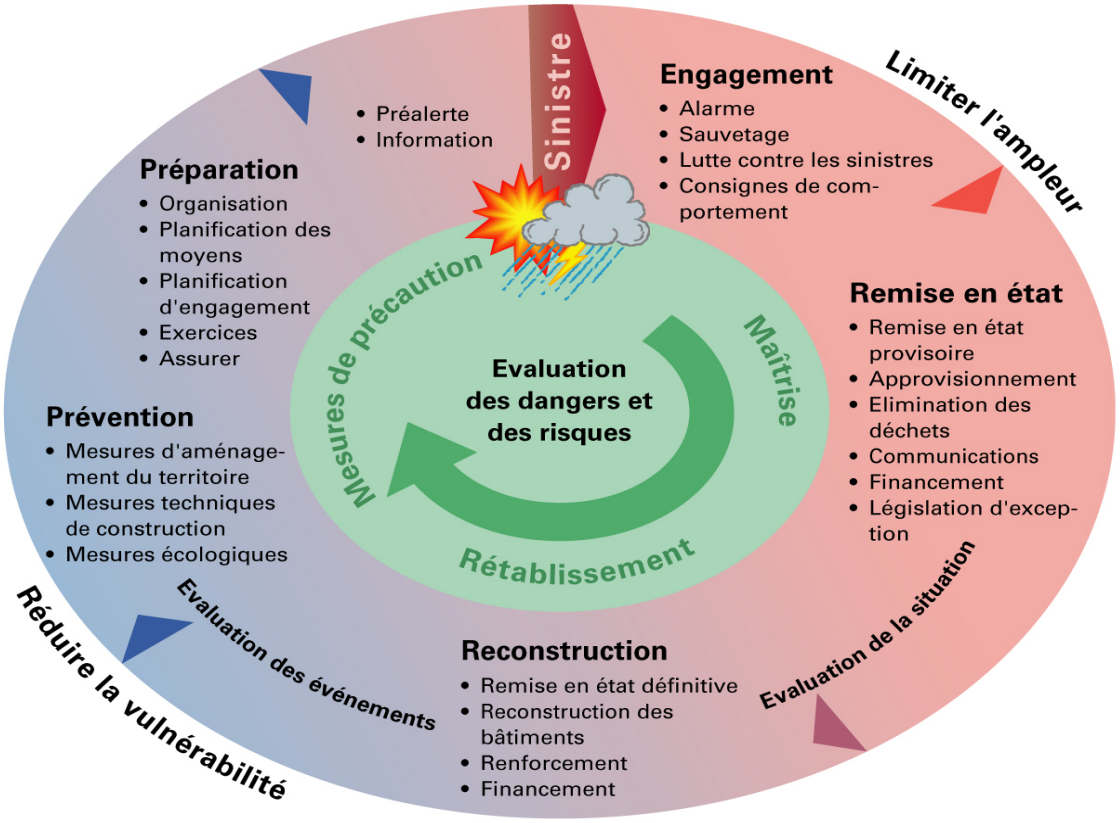

Figure 2: Cycle de gestion des risques (OFPP 2003)

La gestion intégrale des risques peut s'appliquer comme suit à la protection des infrastructures critiques (voir figure 3). A cet égard, il s'agit de prévoir non seulement des mesures de prévention et de préparation mais également des mesures d'intervention.

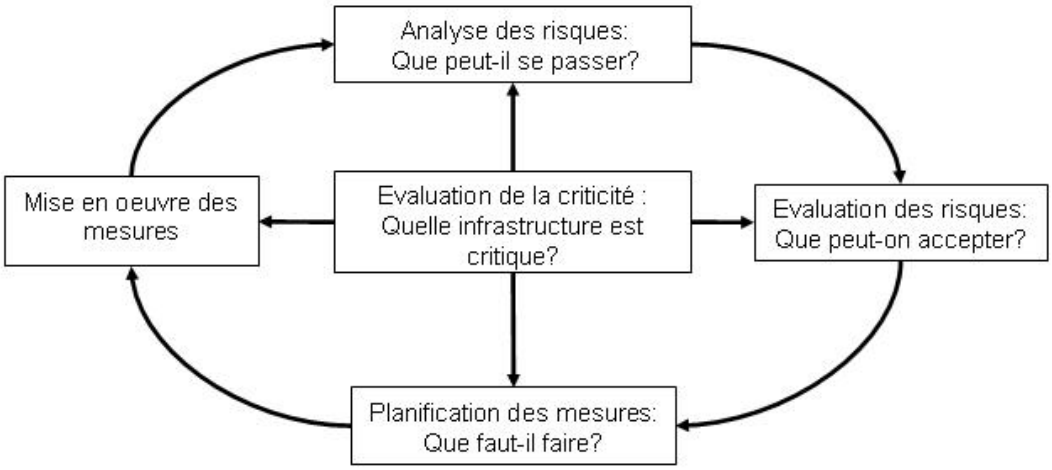

Figure 3: Gestion intégrale des risques appliquée à la protection des infrastructures critiques

La société, les technologies de même que le contexte économique et la situation en matière de politique de sécurité sont en constante mutation. C'est pourquoi il est nécessaire d'actualiser périodiquement l'analyse des risques et d'adapter en conséquence les mesures de protection. Des mesures ponctuelles et de durée limitée sont insuffisantes pour atteindre une protection globale. La protection des infrastructures critiques constitue ainsi une tâche permanente pour la Suisse. C'est le seul moyen de garantir de manière efficace et durable une protection adaptée à la situation de risque du moment.

7.2 Objectifs de protection

Les objectifs de protection définissent le niveau de sécurité à atteindre avec les moyens financiers disponibles et déterminent les mesures de protection qui en résultent. L'objectif de protection lui-même n'est pas absolu et dépend de la situation en matière de politique de sécurité.
Les objectifs de protection généraux découlent de la description de la situation. Des objectifs spécifiques doivent être établis pour chaque secteur d'infrastructure (p.ex. approvisionnement minimal en électricité dans le secteur Energie). Ils dépendent du type et de la criticité de l'infrastructure.

Situation	Description de la situation	Objectif de protection général
Situation normale	Situation dans laquelle les processus ordinaires permettent de faire face aux problèmes et aux défis.	Au quotidien, les infrastructures critiques doivent constamment être en mesure de fournir les prestations habituelles et de maîtriser les éventuelles défaillances sans conséquences perceptibles.
Situation particulière	Situation dans laquelle les processus normaux ne permettent plus d'accomplir certaines tâches. A la différence de la «situation extraordinaire», la situation particulière n'engendre qu'une limitation sectorielle de la capacité de fonctionnement. Le besoin de concentrer rapidement les moyens disponibles et de rationaliser les procédures est typique d'une telle situation.	Le niveau habituel des prestations doit être maintenu autant que faire se peut et le fonctionnement de l'économie doit être aussi peu entravé que possible. Les restrictions doivent être rares et limitées dans l'espace et le temps. De plus, leurs effets doivent pouvoir être gérés et contrôlés à tout moment.
Situation extraordinaire	Situation dans laquelle les procédures normales ne permettent plus, dans de nombreux domaines et secteurs, de faire face aux problèmes et défis, par exemple en cas de catastrophes naturelles ou de faits de guerre affectant sérieusement l'ensemble du pays.	La situation normale doit pouvoir être rétablie après un certain temps et avec certaines restrictions par des moyens et des mesures extraordinaires. Les services nécessaires à la survie (p.ex. eau, subsistance, logement) doivent à nouveau être garantis et doivent par conséquent revêtir une importance prioritaire.

Tableau 2: Objectifs de protection généraux pour les situations normale, particulière et extraordinaire (description reposant sur le rapport sur la politique de sécurité 2000)

7.3 Eventail des dangers

Suivant le système de gestion intégrale des risques (voir figure 3), l'analyse des risques consiste à procéder d'abord à une analyse des dangers qui doit être globale («all hazards approach»). Des priorités portant sur la protection contre des dangers précis ne peuvent être fixées qu'une fois accomplies l'analyse et l'évaluation des risques.

La liste des dangers qui suit n'est pas exhaustive. Elle peut être adaptée en privilégiant d'autres dangers en fonction de l'infrastructure ou de l'élément d'infrastructure concerné et les objectifs de protection correspondants.

Catégories	**Dangers**
Dangers naturels	Tremblement de terre
	Avalanche
	Mouvements de terrain géologiques
	Inondation
	Tempête
	Sécheresse
	Température extrême
	Incendie
Dangers techniques	Défaillance technique d'un système
	Défaillance humaine sur des systèmes techniques
	Accident majeur concernant des ouvrages d'accumulation
	Accident nucléaire
	Accident chimique
	Accident en cas de transport de marchandises dangereuses
Dangers sociétaux	Pandémie
	Migration massive
Violence (infra-guerrière et guerrière)	Criminalité organisée
	Sabotage
	Chantage
	Terrorisme
	Conflit armé

Tableau 3: Liste des dangers

8 Scénarios de dangers

Les scénarios sont indispensables à l'analyse des risques car ils décrivent des événements ou des développements potentiels et constituent ainsi un outil important pour la préparation à ces événements.
Les études et bases de planification établies jusqu'à présent dans le domaine de la protection des infrastructures critiques reposent en partie sur des scénarios de dangers divergents qui ne comprennent souvent pas de données quant à la probabilité d'occurrence et aux effets sur les infrastructures. Il est donc nécessaire de disposer d'une série de scénarios communs dans l'optique d'une stratégie cohérente et de mesures coordonnées.

Les scénarios de référence classiques ne peuvent pas être directement transposés pour l'analyse des risques des infrastructures critiques et doivent être remodelés pour les raisons suivantes:

- Les scénarios classiques se fondent sur des dangers et menaces spécifiques et isolés de même que sur leurs effets généraux. Les conséquences d'un événement sont cependant peu prévisibles dans le cas des infrastructures critiques car elles dépendent fortement des interactions avec d'autres éléments d'infrastructures critiques qui ne sont pas exposés aux dangers de la même façon. Les scénarios de danger spécifiques ne sont par conséquent applicables que si les effets prévus portent sur de vastes régions (p.ex. pandémies) ou englobent un grand nombre d'infrastructures critiques (p.ex. tremblement de terre). Une autre approche consisterait à élaborer des scénarios qui concernent directement la défaillance de certaines infrastructures critiques (p.ex. interruption de l'approvisionnement en électricité).
- Les scénarios classiques considèrent un seul événement à la fois. Il arrive cependant de plus en plus souvent que les perturbations et défaillances soient causées par plusieurs événements concomitants. Les scénarios doivent tenir compte de ces éventualités.
- Les interdépendances entre les infrastructures critiques font que seul un scénario très complexe pourrait représenter de manière réaliste les effets domino. L'un des grands défis consiste à concevoir les scénarios de telle manière qu'ils permettent d'une part de garder la vue d'ensemble et qu'ils tiennent compte, d'autre part, de toutes les interactions déterminantes.

Quatre scénarios de base seront actualisés et remaniés à titre de modèle dans le cadre de la stratégie nationale:

- **Tremblement de terre**: ce danger naturel a des conséquences à grande échelle et peut ainsi être utilisé comme scénario de danger générique pour les infrastructures critiques. Le scénario a été élaboré dans le document «Plan d'intervention en cas de séisme en Suisse» (OFPP, 2004). Les conséquences au niveau des infrastructures critiques pourraient être complétées à la lumière de l'évaluation de l'exercice transfrontalier «RHEINTAL» qui s'est déroulé en octobre 2006.
- **Pandémie**: une pandémie aurait de graves conséquences pour bon nombre d'infrastructures critiques. Le scénario qui a été élaboré dans le cadre du *plan suisse en cas de pandémie 2006* sous la direction de l'Office fédéral de la santé publique (OFSP) pourrait être adapté en ce qui concerne les effets sur les infrastructures critiques.
- **Panne d'électricité:** le scénario de coupure d'électricité a été partiellement élaboré par l'Office fédéral pour l'approvisionnement économique du pays (OFAE). Les effets sur les autres infrastructures critiques devraient être développés au moyen d'une analyse de risques détaillée.
- **Défaillance de l'infrastructure d'information:** ce scénario a été produit en 2004 dans la cadre du projet «Szenarien- und Expertenpool Risikoanalyse Schweiz» de l'EPFZ. Depuis lors l'OFAE établit, en collaboration avec les services fédéraux et les milieux économiques, des analyses de risques de secteurs spécifiques (scénarios, risques, mesures) dans les secteurs des technologies de l'information et de la communication, de la finance, de l'énergie (électricité), du transport et de la santé publique (hôpitaux).

9 Suite des travaux

Les recommandations suivantes ont été formulées pour la suite des travaux en s'appuyant sur les enseignements acquis par le groupe de travail PIC pendant la première étape:

9.1 Groupe de travail Protection des infrastructures critiques

Le DDPS, représenté par l'OFPP, continue d'assurer la coordination des activités dans le cadre du groupe de travail Protection des infrastructures critiques (GT PIC). Le GT PIC a fait ses preuves en permettant d'intégrer les divers intérêts des offices fédéraux représentés et en parvenant à une compréhension de base commune en ce qui concerne la protection des infrastructures critiques. Le GT PIC doit être complété selon les besoins par des représentants de services fédéraux (p.ex. EM DélSéc, DPS, AFF, OFAC) qui n'ont pas encore été associés au projet. D'autres projets menés actuellement par la Confédération seront aussi pris en compte. En particulier, la coordination avec la "gestion des risques au sein de la Confédération" sera assurée pour en tirer des synergies. Pour la suite des travaux, des sous-groupes de travail ad hoc devront être constitués pour traiter plus à fond des thèmes spécifiques (voir ci-dessous).

9.2 Prochaines étapes

Compte tenu de la complexité de la thématique ainsi que du nombre d'offices associés, il est nécessaire de continuer à procéder par étapes et de fixer des axes prioritaires pour chaque phase. La deuxième étape, à réaliser jusqu'à fin 2008, sera centrée sur les activités suivantes:

- Choix d'un secteur d'infrastructure critique déterminant pour la Suisse et élaboration, à titre de modèle, d'une stratégie, y compris une analyse de risques ainsi qu'un catalogue de mesures (étude de cas)
- Approfondissement des scénarios de dangers
- Lancement de projets de recherche fondamentale sur des thèmes-clés (p.ex. les interdépendances entre les infrastructures critiques)
- Encouragement de la collaboration (au niveau de secteurs d'infrastructures spécifiques et au niveau intersectoriel) avec les cantons et les exploitants d'infrastructures critiques de même qu'avec les pays voisins et des organisations internationales dans le domaine de la protection des infrastructures critiques

Sur la base de ces travaux, les axes prioritaires suivants seront traités au cours de la période 2009-2011:

- Elargissement de l'étude de cas à d'autres infrastructures critiques
- Elargissement de la recherche fondamentale à d'autres thèmes-clés en collaboration avec les milieux universitaires et le secteur privé
- Elaboration de la stratégie nationale pour la protection des infrastructures critiques avec le concours des cantons et du secteur privé
- Elargissement de la collaboration avec les pays voisins et des organisations internationales dans le domaine de la protection des infrastructures critiques, p.ex. sous forme d'analyses de risques transfrontalières et, éventuellement, d'exercices communs.

La mise en œuvre et l'actualisation de la stratégie nationale pour la protection des infrastructures critiques suivront finalement à partir de 2012.

9.3 Conséquences en matière de personnel

Il n'y a pas de besoin en personnel supplémentaire au niveau fédéral pour la deuxième étape. Il faudra néanmoins compter au courant de la troisième étape prévue (2009-2011) avec un renforcement des ressources humaines pour assurer les activités nécessaires de coordination.

9.4 Conséquences financières

Aucune ressource financière supplémentaire n'est nécessaire pour la deuxième étape au niveau fédéral. Les projets de recherche prévus se dérouleront en effet dans les limites des crédits de recherche existants. A ce propos, il s'agira aussi d'examiner la possibilité d'utiliser des moyens du Fonds national et du 7^{e} programme-cadre de recherche de l'UE (sécurité).

9.5 Information destinée au Conseil fédéral

D'ici au printemps 2009, le DDPS établira un rapport pour informer le Conseil fédéral sur les résultats de la deuxième étape du projet de même que sur la suite des travaux.

Annexe 1 Programmes de protection des infrastructures critiques d'Etats tiers

Depuis le milieu des années 1990, de nombreux Etats accordent une importance croissante à la protection des infrastructures critiques. Ci-dessous, quelques exemples illustrent la façon dont ce sujet est traité ailleurs.

USA
Sous l'angle de la politique de sécurité, le débat sur le rôle des infrastructures critiques civiles est lancé au milieu des années 90. Menée jusqu'alors essentiellement sur les aspects militaires et économiques, la discussion s'élargit alors pour s'inscrire dans le cadre d'une politique de sécurité globale. En 1996, l'entrée en fonction de la *Presidential Commission on Critical Infrastructure Protection* (PCCIP) sous l'égide du président Bill Clinton est l'une des principales étapes de cette ouverture. Pour le gouvernement fédéral, c'est le premier pas fait dans le cadre de la politique de sécurité en direction de la protection des infrastructures critiques. La protection physique n'étant pas nécessairement l'objectif premier des réflexions, l'accent est mis sur les technologies de l'information.
2001 marque un tournant, dans ce domaine comme dans beaucoup d'autres. Les attentats terroristes du 11 septembre 2001 mettent en évidence la vulnérabilité physique des USA face à de tels actes. Désormais, la protection des infrastructures critiques est placée dans la double optique «Sécurité intérieure» et «Protection contre les attentats terroristes». En février 2003, le gouvernement américain publie le document «*The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets»* Cette stratégie vise la protection physique globale des infrastructures critiques aux USA. En septembre 2005, l'ouragan Katrina, qui ravage la région de la Nouvelle-Orléans, démontre la vulnérabilité et l'insuffisance des préparatifs face aux dangers naturels. Le rapport *National Infrastructure Protection Plan*, qui fait état de 17 infrastructures critiques et ressources-clés, est publié en juin 2006.

Canada
Le passage au nouveau millénaire a poussé le Canada à intensifier les activités en matière de protection systématique des infrastructures critiques. Une analyse des risques étendue est effectuée en vue d'évaluer la «criticité» des infrastructures. Le «Department of Public Safety and Emergency Preparedness Canada» (PSEPC) est créé en 2003. Ce département coordonne les activités des ministères et autres autorités coresponsables de la sauvegarde de la sécurité nationale. C'est sous la forme d'un partenariat que le PSEPC collabore étroitement avec d'autres entités publiques (y compris les provinces et les territoires) et le secteur privé.
Dans son premier rapport global sur la sécurité nationale, le gouvernement canadien relève l'importance de la protection des infrastructures critiques. Fin 2006, le PSEPC ébauche une *National Strategy for Critical Infrastructure Protection*. Parallèlement démarrent plusieurs projets de recherche scientifique concernant les interdépendances entre les infrastructures critiques.

Norvège
En septembre 2003, la Norvège crée la Direction de la protection civile et de la gestion des crises (DSB), subordonnée au Ministère de justice et police. Elle coordonne les mesures de protection des infrastructures critiques en collaboration avec d'autres partenaires. En principe, les ministères concernés détiennent la responsabilité de leurs domaines respectifs tant en situation ordinaire qu'extraordinaire. Fin 2004, en vue d'une évaluation complète des infrastructures critiques, le gouvernement norvégien met sur pied une commission constituée de représentants des divers secteurs d'infrastructures. Cette commission livre ses conclusions au Ministère de justice et police en avril 2006.

Allemagne

En Allemagne, l'attention se concentre longtemps sur la protection des infrastructures d'information critiques. Dans le pacte anti-terroriste allemand, l'Office fédéral pour la sécurité en matière de technologies de l'information (BSI) obtient des ressources en personnel et financières. Jusqu'aux attentats du 11 septembre 2001, le BSI analysait les menaces sur les infrastructures d'information (IT) et les menaces physiques sur les infrastructures critiques. En 2004, le « monopole » du BSI s'assouplit. Un Centre pour la protection des infrastructures critiques est créé au sein du nouvel Office fédéral de la protection de la population et de l'aide en cas de catastrophe (BBK). Il traite de la dimension physique de la protection des infrastructures critiques. L'Office fédéral de la police judiciaire (BKA) se consacre à la protection contre la menace terroriste et aux poursuites pénales. Ces trois offices font partie du Ministère fédéral de l'Intérieur (BMI).
Jusqu'en 2005, l'Allemagne n'avait pas de stratégie nationale de protection des infrastructures critiques. Le BMI publie alors un Plan national pour la protection des infrastructures d'information *(NPSI)*. Le document *Schutz Kritischer Infrastrukturen – Basisschutzkonzept* (Protection des infrastructures critiques – Concept de protection de base) contient des directives destinées aux entreprises et visant à protéger les infrastructures non seulement contre les événements naturels mais aussi contre la menace terroriste. Le secteur public renforce sa collaboration avec le secteur privé.

Pays-Bas
La protection des infrastructures critiques revêt une grande importance pour la sécurité nationale des Pays-Bas. Suite aux attentats du 11 septembre 2001 aux USA, le Ministère de l'intérieur est chargé de procéder à une analyse globale, assortie de la planification de mesures, en mettant sur un pied d'égalité les aspects physique et informatique. Pendant la phase dite „Quick Scan Phase" (2002-2003), onze secteurs d'infrastructures et leurs interdépendances respectives sont examinés. Au terme de cette étape, le nombre de secteurs jugés critiques est porté à 12. Lors de la phase suivante, de 2004 à 2005, les points-clés conditionnant le fonctionnement de chaque secteur et leurs emplacements géographiques sont identifiés. Ensuite, quelques mesures destinées à améliorer la protection des infrastructures critiques sont élaborées puis soumises au Parlement en septembre 2005. Depuis 2004, la Direction de la gestion des crises, rattachée au Ministère de l'intérieur, coordonne la mise en œuvre en collaborant étroitement avec l'économie privée.

Suède
Au milieu des années 1990, la Suède procède à une analyse de la menace dans le contexte d'un réexamen du système de défense générale. L'identification des risques liés à la conduite de la guerre de l'information établit un premier lien avec les infrastructures critiques. A la fin de cette décennie, une commission composée de membres de haut rang est chargée de se pencher sur les vulnérabilités et la protection de la Suède. Dans son rapport final de 2001, cette commission propose diverses mesures de protection des infrastructures critiques. La PIC y est conçue comme une tâche globale pour garantir la sécurité nationale. En Suède, l'Etat est à l'origine de la majeure partie des initiatives concernant la protection des infrastructures critiques. Le premier rôle est tenu par la Swedish Emergency Management Agency (SEMA), l'office suédois pour la planification des mesures d'urgence, fondé en 2002. Dans les directives 2006 et 2007 pour la gestion des crises, l'importance de la protection des infrastructures critiques est particulièrement soulignée et la priorité est donnée aux mesures préventives.

Union européenne
En matière de protection des infrastructures critiques, l'Union européenne (ÙE) a longtemps été en retard sur les Etats considérés isolément. Après une première série d'initiatives, telles que l'*Information Infrastructure Dependability Support Initiative (DDSI)* en 2002, l'UE se met à accorder une importance accrue à ce thème. Il s'agit aussi d'une conséquence des enseignements tirés des attentats aux USA. En octobre 2004, l'UE annonce le lancement du Programme européen de protection des infrastructures critiques *(PEPIC)*. Ce programme comprend notamment la mise en place d'un *Critical Infrastructure Warning Information Network*

(CIWIN), dont le rôle est de soutenir les Etats membres dans la gestion de leurs infrastructures critiques ainsi que de promouvoir l'établissement de normes spécifiques par le Comité européen de normalisation (CEN). Selon le principe de subsidiarité, l'UE doit se concentrer sur la protection des infrastructures critiques à dimension transfrontalière, laissant les autres infrastructures sous la seule responsabilité des Etats membres. Ce programme de la Commission européenne a pour but de renforcer le potentiel de protection des infrastructures critiques en Europe. Tous les dangers sont pris en considération («all hazards approach»), bien que l'accent soit mis sur la protection contre les effets du terrorisme. Pour la promotion de son programme, l'UE publie un livre vert du PEPIC en novembre 2005, qui vise à intégrer un maximum de participants dans le débat sur le programme européen de protection des infrastructures critiques. Le Livre vert présente des options quant à la façon dont la Commission peut remplir le mandat donné par le Conseil en vue de l'élaboration d'un programme européen détaillé de protection des infrastructures critiques. C'est en décembre 2006, après diverses consultations (incluant aussi la Suisse) que la Commission publie une communication et une directive. La communication définit le cadre de la protection des infrastructures critiques dans l'UE, tandis que la directive règle l'identification des infrastructures critiques en Europe ainsi que leur analyse sous l'angle des risques. Au terme de diverses consultations officielles auprès des Etats membres, le Conseil de l'Europe devrait entériner ces deux documents à la mi-2007.

Infrastructure	**USA**	**CDN**	**N**	**D**	**NL**	**EU**	**CH**
Energie	X	X	X	X	X	X	X
Finance	X	X	X	X	X	X	X
Santé publique	X	X	X	X	X	X	X
Technologies de l'information et de la communication	X	X	X	X	X	X	X
Denrées alimentaires	X	X	X	X	X	X	X
Transports	X	X	X	X	X	X	X
Eau	X	X	X	X	X	X	x
Gouvernement et administration	X	X	X	X	X		X
Industrie chimique	X	X		X	X	X	X
Organisations de sauvetage	X	X	X	X			X
Biens culturels	X	X		X			x
Poste	X				X		x
Agriculture	X	X					
Défense			X		X		x
Armement	X	X					
Recherche				X		X	x

Tableau A1.1: Comparaison des secteurs d'infrastructures critiques dans quelques pays (″X″ désigne la prise en compte d'un secteur d'infrastructures; ″x″ désigne un sous-secteur en Suisse (voir le tableau 1 dans le corps du document))

Le tableau qui précède met en lumière les différentes approches nationales des infrastructures considérées comme critiques. Ces divergences s'expliquent notamment par la géographie, les conditions économiques et politiques ainsi que par le passé historique et culturel. Toutefois, les Etats s'accordent à inclure les sept secteurs suivants parmi les infrastructures critiques: énergie, finance, santé publique, technologies de l'information et de la communication, denrées alimentaires, transports et eau (que la Suisse intègre dans les secteurs alimentation et épuration/élimination des déchets).

Depuis les attentats du 11 septembre 2001, on constate une nette tendance à l'accroissement du nombre des infrastructures considérées comme critiques. Ainsi, en 1998, les USA qualifiaient cinq secteurs d'infrastructures de critiques, alors qu'en 2006, on y dénombrait 17 secteurs d'infrastructures critiques et de ressources-clés essentielles.

Annexe 2 Protection des infrastructures critiques en Suisse – Services fédéraux concernés

Sous ce point sont présentées les tâches fondamentales et activités de quelques services fédéraux concernant la protection des infrastructures critiques. Servant uniquement à des fins d'illustration, cette liste n'est pas exhaustive. Les offices représentés dans le GT PIC y figurent selon l'ordre dans lequel ils apparaissent dans l'annuaire fédéral.

Secrétariat politique
C'est dans le cadre du mandat général portant sur la politique de sécurité extérieure que le Secrétariat politique (SPOL, précédemment Centre de politique de sécurité internationale CPSI) traite de la protection des infrastructures critiques. Sous l'égide du Conseil de partenariat euro-atlantique (CPEA), il organise depuis 2003 des séminaires internationaux consacrés à la PIC et à la gestion civile des crises. Organisés sous forme d'ateliers et suivis par des experts suisses et étrangers délégués par l'administration, le secteur privé et les milieux scientifiques, ils constituent une importante plate-forme pour l'échange d'informations. Le SPOL est représenté dans le groupe de travail spécifique PIC du Comité de protection civile du CPEA, ainsi qu'auprès de l'UE en tant que point de contact PIC (avec l'OFPP).

Direction du développement et de la coopération
La Direction du développement et de la coopération (DDC) n'exploite aucune infrastructure critique. L'aide humanitaire a pour tâche de contribuer de manière globale, par des mesures préventives et d'intervention urgente, à la survie d'êtres humains en danger et à l'allègement de souffrances. En ce qui concerne les infrastructures critiques à l'étranger, la DDC peut faire valoir une longue expérience en matière d'aide d'urgence et de reconstruction après des catastrophes naturelles (séismes, inondations, sécheresse) et anthropiques (événements nucléaires, biologiques et chimiques), mais aussi des ruptures de barrage et d'importantes destructions lors de crises et conflits.

Office fédéral de météorologie et de climatologie (MétéoSuisse)
En plus des prestations générales destinées au public, l'Office fédéral de météorologie et de climatologie (MétéoSuisse) fournit diverses prestations pour l'appréciation de la situation en faveur d'organisations d'intervention civiles et militaires. Il diffuse notamment des alertes d'intempéries, surveille le taux de radioactivité dans l'atmosphère et calcule, en cas d'accident, la propagation de substances nocives (polluantes). En situation particulière et extraordinaire, MétéoSuisse collabore avec les services météo des Forces aériennes et de l'artillerie au sein du domaine coordonné Météo afin de fournir les prestations requises. MétéoSuisse développe actuellement sa capacité de remplir sa mission en toute circonstance. C'est pourquoi une étude préliminaire a été publiée sous le titre *Business Continuity Management (BCM).* Les premières mesures seront rapidement mises en application, d'autres seront intégrées dans un projet qui démarrera dès 2009.

Office fédéral de la santé publique
Au sein de l'Office fédéral de la santé publique (OFSP), le groupe de travail Influenza a établi un plan de pandémie pour la Suisse. En cas de pandémie, ce plan a pour but de garantir le fonctionnement des services indispensables à la vie de la collectivité (transports, communications, information, approvisionnement énergétique, eau potable et alimentation) et, par un programme de vaccinations ciblées, d'assurer les fonctions-clés de la police, des sapeurs-pompiers et de la santé publique. Ultérieurement, une liste des personnes à vacciner en priorité sera établie, qui prendra en compte l'aspect médical, social et politique. Cette liste s'appliquera aussi aux exploitants d'infrastructures critiques. En 2006, le Conseil fédéral a décidé l'acquisition de huit millions de doses d'un vaccin prépandémique. Un concept de vaccination à grande échelle est en cours d'élaboration.

Office fédéral de la police

La protection préventive de l'Etat et les mesures de protection des personnes et ouvrages exposés à des risques font partie des tâches de l'Office fédéral de la police (fedpol). Cet office assume aussi des tâches de poursuite pénale. Fedpol contribue à la protection des infrastructures d'information critiques par les tâches accomplies dans le cadre de MELANI, la centrale d'enregistrement et d'analyse pour la sûreté de l'information. MELANI collabore étroitement avec quelques exploitants d'infrastructures critiques nationales. Fedpol coordonne la poursuite pénale liée à la criminalité sur internet au sein du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), dont le rôle est essentiel.

Protection des informations et des objets, Etat-major du chef de l'armée
Au DDPS, la Division de la protection des informations et des objets (DPIO), rattachée à l'EM CdA, est en charge de divers sujets liés à la ″sécurité intégrale″. Elle contribue ainsi à la sécurité militaire et à la sécurité de l'administration en Suisse et, dans certains cas, à l'étranger. S'appuyant sur des analyses des dangers à court, moyen et long terme, elle élabore des directives, des prescriptions et des mesures pour tous les domaines à protéger (personnes, informations, valeurs matérielles et environnement) et en contrôle l'application. Pour le DDPS, son apport à la mise en œuvre systématique d'une stratégie de sécurité optimale est essentiel par sa prise en compte de tous les aspects de la sécurité (de la sécurité à la protection armée) et en toute situation. La DPIO accomplit sa tâche en étroite collaboration avec ses divers partenaires des administrations fédérale, cantonales et communales de même qu'avec les organes spécialisés de l'étranger.

Etat-major de conduite de l'armée
C'est en collaboration avec les états-majors cantonaux civils de conduite et divers offices fédéraux que le Service territorial inventorie depuis près de 15 ans les infrastructures d'importance nationale et régionale et dresse le catalogue des ouvrages civils destinés à garantir les besoins existentiels (ouvrages GBE). Ce catalogue contient des listes d'environ 700 ouvrages, qui servent de bases de conduite et de décision aux partenaires civils lorsque ceux-ci adressent au Conseil fédéral des demandes d'aide subsidiaire de l'armée pour la protection d'ouvrages. Ces objets sont répertoriés uniquement sous l'aspect de dangers actifs, soit les actes de violence et l'occupation consécutive à une action terrestre, ainsi que les actes de sabotage. Les dangers passifs ont été exclus de l'inventaire. Les opérations d'information prennent elles aussi en compte la sécurité des infrastructures critiques car celles-ci sont essentielles pour garantir le processus décisionnel de l'armée et des organes qui en dépendent. Ce service ne traite donc pas que de la dimension physique du problème, mais aussi de ses aspects psychologiques et cybernétiques. Un document «Konzeptionsstudie Information Operations», de diffusion restreinte, a été élaboré à ce sujet.

armasuisse Immobilier
En sa qualité de centre de compétence de l'immobilier du DDPS, armasuisse Immobilier gère le parc immobilier du DDPS. Il assume le rôle de gérant et exploite le parc de manière moderne, en assurant une forte valeur ajoutée. Dans la mesure où son portefeuille englobe aussi l'infrastructure militaire, armasuisse Immobilier veille, en collaboration avec le groupe d'étude «Protection de l'infrastructure militaire» (SG SIM), à garantir les bases nécessaires pour les ouvrages de protection et les constructions protégées de l'armée conformément au mandat du Chef de l'armée et du Chef de l'armement.

Office fédéral de la protection de la population
Pour ce qui est des infrastructures critiques, les bases légales de la protection de la population sont déterminantes, en particulier la formulation explicite de l'objectif de «protection de la population et de ses bases d'existence». En automne 2003, l'Office fédéral de la protection de la population (OFPP) a élaboré l'étude «Schutz und Sicherheit von Kritischen Infrastrukturen» à titre de base de travail. L'OFPP coordonne les activités du groupe interdépartemental Protection des infrastructures critiques (GT PIC). Il est, avec le secrétariat politique, l'interlocuteur («Contact Point ») de l'UE pour la PIC et représente la Suisse au sein du Civil Protection Committee du CPEA, qui traite aussi de la question.

La Centrale nationale d'alarme (CENAL), qui fait partie de l'OFPP, joue un rôle essentiel dans la maîtrise d'événements majeurs pouvant produire des effets sur les infrastructures critiques. La capacité de faire face aux catastrophes touchant des infrastructures critiques (télécommunications, approvisionnement en gaz, électricité, denrées alimentaires) a été testée lors de l'exercice «RHEINTAL 06», développé selon le scénario d'un séisme.

Unité de stratégie informatique de la Confédération
L'Unité de stratégie informatique de la Confédération (USIC) est rattachée au Secrétariat général du Département fédéral des finances en tant qu'organe d'état-major, de planification et de coordination du Conseil de l'informatique de la Confédération. Elle émet des prescriptions et des directives pour la sécurité de l'information à l'échelon fédéral. L'USIC remplit une fonction essentielle en matière de protection des infrastructures d'information critiques. Elle a aussi pris une part prépondérante dans l'élaboration du concept d'engagement Information Assurance Schweiz. L'USIC répond de la conduite stratégique de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et de l'Etat-major spécial «Sécurité de l'information» (SONIA).

Office fédéral de l'informatique et de la télécommunication
Les infrastructures des technologies de l'information et de la communication (TIC), placées sous la responsabilité de l'Office fédéral de l'informatique et de la télécommunication (OFIT), sont largement protégées sur les plans de la disponibilité, de la confidentialité et de l'intégrité physique. La protection de base à assurer en permanence est définie dans la directive sur la sécurité informatique dans l'administration fédérale. En outre, en cas de besoin de protection accrue, des mesures spécifiques sont fixées en accord avec certains clients, notamment pour la prévention des catastrophes. Un concept d'accès et de verrouillage à plusieurs niveaux de sécurité est appliqué pour garantir la sécurité physique. L'alimentation continue est assurée par des liaisons redondantes et des groupes électrogènes de secours. Quant à la sécurité des réseaux, elle est obtenue par une infrastructure pare-feu («firewall») et une configuration proxy, par un système de protection efficace contre les virus et les pourriels ainsi que par une segmentation du réseau améliorée en permanence. Pour ce qui est des systèmes et des banques de données, il existe des normes spéciales visant à les sécuriser. De plus, le degré d'application de ces exigences est périodiquement contrôlé par la recherche des points faibles. En cas de défaillance totale, le concept éprouvé de sauvegarde (backup) garantit la sécurité des données. Un emplacement entièrement équipé destiné au le centre de calcul de l'OFIT de même qu'aux autres fournisseurs de prestations TIC de l'administration fédérale est en cours de construction.

Office fédéral des constructions et de la logistique
L'Office fédéral des constructions et de la logistique (OFCL) est responsable de la mise à disposition de locaux pour les éléments civils de l'administration fédérale. L'OFCL tient compte des exigences en matière de PIC en faisant appliquer les normes antisismiques en vigueur lors de la construction de nouveaux immeubles. Lors de rénovations ou de transformations de bâtiments, des mesures de protection en rapport avec la résistance à la sismicité sont prises en tenant compte de la proportionnalité des coûts. Les projets de construction sont réalisés selon les impératifs de sécurité (Security) dans le cadre d'un concept de sécurité et de mesures détaillées. Ces dernières reposent sur l'analyse des risques établie par le Service fédéral de sécurité ainsi que sur les objectifs de protection qui en découlent.

Office fédéral pour l'approvisionnement économique du pays
L'Office fédéral pour l'approvisionnement économique du pays (OFAE) met l'accent sur la maîtrise des difficultés sectorielles, à court et moyen terme, dans l'approvisionnement de base en denrées alimentaires, énergie et produits pharmaceutiques mais aussi au niveau de l'infrastructure des transports, de l'industrie et des TIC. Pour les biens vitaux, l'objectif primaire est de maintenir pendant six mois l'approvisionnement du marché à un niveau de 100%, notamment par des mesures agissant sur l'offre, c'est-à-dire la libération de réserves obligatoires, la stimulation des importations et la canalisation de la production. Au terme de

cette période, cette offre ne pourra plus être assurée systématiquement à 100%. Le cas échéant, les quantités commercialisées et consommées doivent pouvoir être limitées par des mesures destinées à canaliser la demande (contingentement, rationnement ou mesures analogues).

Office fédéral des transports
L'Office fédéral des transports (OFT) garantit la sécurité des transports des chemins de fer, trams, remontées mécaniques, bateaux et automobiles, notamment au moyen de la surveillance de l'exploitation, des équipements et des véhicules des entreprises de transports publics. En outre, dans le cadre de la collaboration internationale, l'OFT est chargé d'assurer l'unité du régime rhénan dans le domaine des prescriptions techniques et de politique de sécurité. Il prépare et applique les décisions en faveur d'une politique cohérente des transports publics, à l'exception de l'aviation civile et de la construction des routes, mais aussi pour les voies de navigation intérieure et la navigation en haute mer.
L'OFT coordonne les transports en cas d'événement (CTE). Cette tâche consiste à harmoniser l'utilisation des infrastructures et des moyens de transport afin d'assurer le bon déroulement des transports.
Le directeur de l'OFT préside le Comité mixte de l'accord sur les transports terrestres entre la Suisse et l'UE. En tant que membre hôte, l'OFT représente les intérêts suisses liés aux infrastructures critiques des transports terrestres au sein d'un groupe d'experts de l'UE.

Office fédéral de l'énergie
L'Office fédéral de l'énergie (OFEN) répond notamment de la législation sur l'énergie et des procédures d'autorisation pour les installations nucléaires, lignes à haute tension, gazoducs et oléoducs. La section «Energie nucléaire» surveille l'application des engagements de la Suisse pour le cycle du combustible nucléaire, ainsi qu'à la protection des installations et des matières nucléaires contre les actes de sabotage. La Division «Force hydraulique et barrages» de l'OFT veille à ce que les forces hydrauliques soient exploitées de manière appropriée et réglemente leur utilisation dans les eaux frontalières. Elle traite également de la sécurité technique et opérationnelle des ouvrages d'accumulation en Suisse. En mars 2003, un groupe de travail institué par le DETEC a présenté un train de mesures visant à améliorer le réseau des lignes à très haute tension afin de parer au mieux à de futures pannes générales d'électricité en Suisse.

Office fédéral des routes
L'Office fédéral des routes (OFROU) est l'autorité suisse compétente pour l'infrastructure routière et le trafic individuel. Il élabore les bases d'une politique fédérale durable des transports, conçoit et coordonne les mesures qui en découlent, au niveau national et international. De plus, il veille à la construction, à l'exploitation et à l'entretien d'un réseau routier national sûr et performant. Les risques sont recensés puis évalués dans le cadre d'une gestion globale des risques. L'ordre de priorité des mesures de réduction est déterminé par une analyse du rapport coût / efficacité.

Office fédéral de la communication
C'est en sa qualité d'autorité de surveillance et de régulation que l'Office fédéral de la communication (OFCOM) traite notamment de la sécurité de l'information et de l'infrastructure de communication, ainsi que de la protection des infrastructures critiques. A ce titre, on peut mentionner en particulier:

- la publication du rapport «Sécurité des infrastructures de radiodiffusion et de télécommunication en Suisse lors de situations extraordinaires;
- son rôle de co-initiateur de la «Table ronde» organisée par la Fondation InfoSurance en vue d'analyser les risques spécifiques au secteur de la télécommunication.

En janvier 2006, le Comité interdépartemental pour la société de l'information (CI SI), présidé par l'OFCOM, a publié la nouvelle stratégie du Conseil fédéral pour une société de l'information en Suisse, après l'avoir remaniée entre 2004 et 2006. Cette stratégie actualisée est axée tout spécialement sur les mesures de sécurité et de confiance.

Office fédéral de l'environnement
L'Office fédéral de l'environnement (OFEV) a pour tâches de protéger la population et les biens matériels d'importance contre les dangers naturels, de garantir l'approvisionnement en eau potable ainsi que la protection de l'environnement (loi sur l'aménagement des cours d'eau, loi sur les forêts, loi sur la protection des eaux, législation sur la protection de l'environnement). En outre, il exerce la haute surveillance sur la prévention des accidents majeurs en vertu de l'ordonnance ad hoc, de même que la conduite stratégique en matière de protection contre les dangers naturels. Parallèlement, il favorise des mesures de protection et fournit des documents de base d'intérêt national. A cette fin, l'OFEV élabore et met à jour la législation fédérale correspondante. Il garantit que la protection contre les dangers naturels soit équilibrée sur le plan national. Les séismes de forte amplitude représentent un risque non négligeable, tout comme les inondations, les avalanches, les chutes de pierres et éboulements. La sécheresse, une vague de chaleur ou de froid peuvent avoir un effet sur l'environnement et sur les infrastructures. Il n'existe aucune protection contre les événements extrêmes. La réduction de la vulnérabilité des ouvrages et équipements revêt une grande importance dans une gestion globale des risques (protection d'ouvrages). Lors de la différenciation des objectifs de protection, il importe de tenir compte des risques majeurs, qui peuvent causer de grands dommages, et de la protection des infrastructures critiques.

Annexe 3 Chronologie de la PIC en Suisse

En Suisse, jusque vers 2002, la notion de protection des infrastructures critiques n'avait pas été employée au sens large. Pourtant, dans certains secteurs, divers projets et mesures PIC avaient déjà été lancés, il est vrai souvent sous d'autres désignations et de manière peu coordonnée.

C'est notamment à l'initiative de l'armée et de la protection civile (p. ex. la protection des ouvrages militaires et des abris contre les effets des armes), mais aussi des exploitants de centrales nucléaires (mesures de construction et d'organisation), des exploitants de barrages (contrôle de la sécurité), de la police (sécurité des bâtiments) et d'autres organisations que le thème de la protection des infrastructures critiques s'est développé en Suisse.

Voici une énumération chronologique des principales étapes:

1997: Exercice de conduite stratégique préparé par la Formation à la conduite stratégique (FCS) de la Chancellerie fédérale, centré sur les activités en Suisse. L'exercice a notamment mis en évidence que la société et les infrastructures dépendent de la sécurité de l'infrastructure de l'information.

1998: Stratégie pour une société de l'information en Suisse. Dans un document portant sur la société de l'information en Suisse, le Conseil fédéral préconise que l'accès à l'information et son utilisation doivent être garantis également en situation extraordinaire.

1998 – 1999: Information Assurance. Sur mandat du Conseil fédéral, le Groupe de coordination pour la société de l'information (GCSI) développe le concept Information Assurance (IA), approuvé en juin 2000. Celui-ci établit que 1° la Fondation InfoSurance d'alors soit financée essentiellement par la Confédération (voir plus bas), 2° que l'Office fédéral pour l'approvisionnement économique mette en place une unité Infrastructures de l'information et de la communication (ICT-I) et 3° qu'un état-major spécial pour la sécurité de l'information soit constitué (voir ci-dessous, SONIA).

2000: Rapolsec 2000. Le rapport du Conseil fédéral à l'Assemblée fédérale sur la politique de sécurité de la Suisse (Rapolsec 2000) mentionne explicitement des dangers potentiels pour l'infrastructure informatique et de communication de la Suisse.

2001: Exercice Informo. Sous la conduite de la FCS, le fonctionnement des processus de gestion d'une crise est testé dans les secteurs transports/logistique, énergie, télécommunications, défense, finance, assurances et médias. L'état-major spécial Sécurité de l'information (SONIA) est mis à l'épreuve. L'exercice démontre la pertinence d'un partenariat entre secteurs public et privé.

2001: Rapport du Conseil fédéral du 30 novembre 2001 concernant la sécurité des infrastructures de radiodiffusion et de télécommunication en Suisse lors de situations extraordinaires, adressé aux commissions de la politique de sécurité des Chambres fédérales. Elaboré par un groupe de travail interdépartemental sous la direction de l'OFCOM, ce rapport contient entre autres une analyse des risques pour les TIC. Celle-ci débouche sur des mesures concrètes (p. ex. modification de la législation sur les télécommunications) et influera sur les futurs travaux dans ce domaine (p. ex. l'analyse des risques pour le secteur Télécoms effectuée par InfoSurance).

2002: InfoSurance entreprend une analyse spécifique des infrastructures critiques. Elle met l'accent sur la dépendance par rapport aux TIC et sur les relations entre les diverses infrastructures.

2003: MELANI. En octobre, le Conseil fédéral charge l'Unité de stratégie informatique de la Confédération (USIC) de créer en collaboration avec ses co-exploitants (fedpol – service d'analyse et de prévention et la Fondation Switch – Switch-CERT), une centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Cette centrale est en service depuis le 1er octobre 2004.

2003: Au cours du second semestre, l'Office fédéral de la protection de la population (OFPP) procède à une analyse sommaire de la protection et de la sécurité des infrastructures critiques. Elle sert de base de travail à l'étude conceptuelle «Schutz und Sicherheit von kritischen Infrastrukturen» et donne naissance à une nouvelle méthode pour l'identification et l'évaluation de ces infrastructures. Une analyse sommaire est ensuite réalisée en collaboration avec des experts de divers départements et offices fédéraux. Elle permet de dégager six secteurs d'infrastructures critiques (gouvernement et administration, électricité, communications, protection de la population, santé publique, transports et logistique) et de mettre en évidence cinq scénarios déterminants en matière de menaces (séisme, augmentation de la radioactivité, épidémie et pandémie, défaillance massive de l'infrastructure de l'information et extrémisme / terrorisme).

2004: Le rapport (uniquement en allemand) de l'Office fédéral de l'environnement (OFEV) sur la mitigation des séismes et les ouvrages d'intérêt majeur («lifelines») identifie les ouvrages nécessaires à la survie, leur fonction lors de la maîtrise d'un violent séisme, lors de la phase de sauvetage et d'intervention. Il propose également des objectifs de protection et des mesures correspondantes.

Début 2005: Gestion des risques au sein de la Confédération: le Conseil fédéral a décidé l'introduction d'une gestion systématique des risques au sein de la Confédération. L'accent est mis sur les conséquences des risques sur les finances de la Confédération. Les départements et la Chancellerie fédérale sont chargés de la mise en œuvre de la politique de gestion des risques. Le DFF (AFF) assume diverses tâches d'administration et de coordination et est responsable de la formulation et de la mise en œuvre de la politique en matière d'assurance de la Confédération.

2005: Après les intempéries du mois d'août, le Conseil fédéral charge l'OFPP d'évaluer, en collaboration avec la Plate-forme nationale «dangers naturels» (PLANAT), des mesures de planification et d'organisation et des mesures techniques qui permettraient d'optimiser l'alerte et l'alarme (OWARNA). Quelques faiblesses ont été constatées au niveau des redondances des moyens de transmission de l'alarme et de l'alimentation en électricité des infrastructures critiques. Une analyse approfondie des mesures s'impose.

2005: Coordination des activités PIC. En juin 2005, le Conseil fédéral confie à l'OFPP le mandat de coordonner les activités nationales liées à la protection des infrastructures critiques. Dans une première phase, il s'agit d'établir l'inventaire des travaux accomplis, ainsi que la liste des secteurs d'infrastructures déterminants et de définir des scénarios de base des dangers. Depuis 2006, un groupe d'étude interdépartemental apporte son soutien à ces travaux.

2007: Evaluation de MELANI. Se fondant sur une évaluation effectuée par le «Center for Security Studies» de l'EPFZ, le Conseil fédéral confirme le 24 janvier le maintien définitif de la centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) en tant qu'organe de l'administration fédérale et décide de lui attribuer les ressources en personnel et financières nécessaires.