Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Unité de pilotage informatique de la Confédération UPIC

Stratégie nationale de protection de la Suisse contre les cyberrisques

Plan de mise en œuvre de la SNPC

15 mai 2013

Table des matières

1 Contexte

Le Conseil fédéral a posé la première pierre d'une approche globale de la cyberproblématique en approuvant, le 27 juin 2012, « la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) ». La SNPC se concentre sur la détection précoce des menaces et des dangers dans le cyberespace, sur l'augmentation de la capacité de résistance (résilience) des infrastructures suisses et sur la réduction des cyberrisques. La stratégie propose 16 mesures concrètes, réparties en 7 champs d'action. Elles devront être mises en œuvre fin 2017 puis devront être intégrées à l'exploitation courante.

Ces champs d'action et ces mesures sont les suivants:

Champ d'action 1	**Mesures**	
Identification des risques par la recherche	1	Recherches nécessaires sur les nouveaux risques en lien avec la problématique de la cybernétique
Champ d'action 2	**Mesures**	
Analyse des risques et vulnérabilités	2	Contrôles indépendants des systèmes Analyses des risques dans le but de les réduire en collaboration avec les autorités, les fournisseurs de prestations TIC et les fournisseurs de systèmes
	3	Analyses de la vulnérabilité des infrastructures TIC sous un angle systémique, organisationnel et technique
Champ d'action 3	**Mesures**	
Analyse de la menace	4	Etablissement de l'image et du développement de la situation
	5	Suivi d'incidents dans le but de poursuivre le développement de mesures
	6	Vue d'ensemble des cas et coordination de cas complexes intercantonaux
Champ d'action 4	**Mesures**	
Formation des compétences	7	Création d'une vue d'ensemble des offres en matière de formation des compétences et identifications des lacunes
	8	Comblement des lacunes par des offres en matière de formation des compétences et recours plus fréquent à des offres qualitativement élevées
Champ d'action 5	**Mesures**	
Relations et initiatives internationales	9	Participation active de la Suisse dans le domaine de la gouvernance d'Internet
	10	Coopération au niveau de la politique internationale de sécurité
	11	Coordination des acteurs lors de leur participation à des initiatives et des bonnes pratiques dans le domaine des processus de sécurité et de sûreté
Champ d'action 6	**Mesures**	
Gestion de la continuité et des crises	12	Renforcement et amélioration de la capacité de résistance (résilience) face aux dérangements et événements imprévus
	13	Coordination des activités en premier lieu avec les acteurs directement concernés et appui des processus décisionnels par l'expertise requise
	14	Mesures actives d'identification des agresseurs et des possibilités de porter atteinte à leurs infrastructures en cas de menace spécifique
	15	Elaboration d'un concept pour des procédures et processus de conduite permettant une résolution des problèmes en temps opportun
Champ d'action 7	**Mesures**	
Bases juridiques	16	Vérification des bases juridiques existantes relativement aux mesures et concepts de mise en œuvre et concrétisation prioritaire des adaptations urgentes

La stratégie part du principe que les cyberrisques ne constituent que l'expression des risques inhérents aux processus et aux structures. Des cyberrisques apparaissent lors de l'utilisation (en réseau) de systèmes TIC, toujours plus présents dans l'exécution et l'exploitation de processus variés. Cela va du simple envoi de courriels au lieu d'un courrier postal, à l'emploi d'installations très complexes de pilotage et de suivi de la production par ordinateur, en lieu et place d'une commande manuelle. L'identification des cyberrisques

requiert par conséquent une appréciation aussi exacte que possible de la menace effective encourue par chaque processus basé sur les TIC et par leur interconnexion. Les mesures requises pour minimiser ces risques ne sauraient toutefois se limiter à la sécurité informatique. De telles mesures devront toujours envisager globalement les questions organisationnelles, avec leurs dimensions physique, humaine et technique. Sur le plan national, ce n'est possible que si chacun assume ses responsabilités et moyennant une bonne intégration des mesures mises en œuvre.

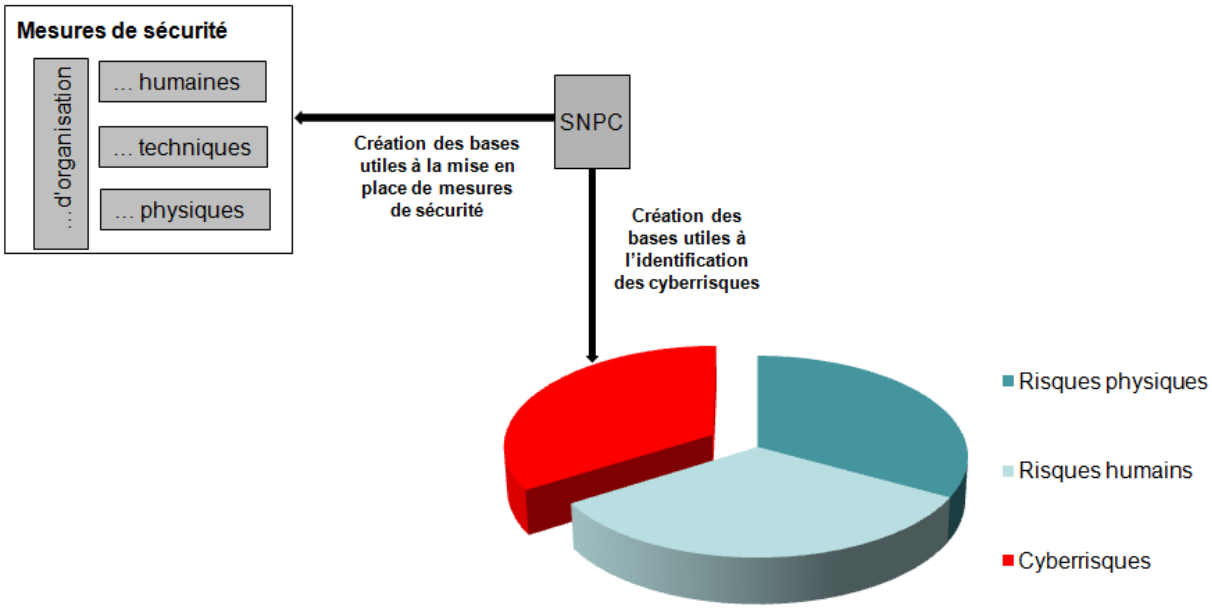

Fig. 1: Cyberrisques et mesure de sécurité

Un organe de coordination (OC) rattaché au Département fédéral des finances (DFF), plus précisément à l'Unité de pilotage informatique de la Confédération (UPIC), veillera à la bonne mise en œuvre de la stratégie. Concrètement, l'OC SNPC est chargé d'élaborer, conjointement avec les services responsables au niveau de la Confédération et avec leurs partenaires au niveau des cantons, un plan de mise en œuvre de la stratégie et d'indiquer, de manière transparente et exhaustive, les éventuels besoins de personnel supplémentaire des départements concernés et de la Chancellerie fédérale à compter de 2014.

En ce qui concerne la protection des infrastructures critiques (IC), la stratégie s'appuie sur la stratégie nationale pour la protection des infrastructures critiques (stratégie PIC) de l'Office fédéral de la protection de la population (OFPP). Les analyses prévues dans le cadre du programme PIC devront également identifier les cyberrisques et créer ainsi la base de la réduction des risques uniforme et spécifique au domaine. Les analyses des risques et de la vulnérabilité faisant partie de la SNPC tiendront compte des secteurs et secteurs partiels définis dans la stratégie PIC. Les régulateurs ainsi que les autorités de surveillance concernés participeront au processus, au même titre que l'Office fédéral pour l'approvisionnement économique du pays (OFAE) et l'Office fédéral de la protection de la population (OFPP). L'AEP[1] et l'OFPP[2] seront chargés de mener, pour les secteurs partiels

[1] L'AEP chapeaute treize secteurs partiels, relevant de l'énergie (approvisionnement en gaz naturel; pétrole; électricité), de l'industrie (chimie et pharma; industrie des machines, des équipements électriques et des métaux), de l'information et de la communication (technologies de l'information; télécommunications), de l'alimentation (approvisionnement en denrées alimentaires; eau potable) et des transports (trafic aérien; trafic ferroviaire; navigation; trafic routier).

[2] L'OFPP est responsable de quinze secteurs partiels, répartis entre les autorités (Parlement, gouvernement, justice, administration; instituts de recherche et de formation; biens culturels; organisations internationales), l'élimination des déchets (eaux usées; déchets), les finances (banques; assurances), la santé publique (soins médicaux et hôpitaux; laboratoires), l'information et la communication (médias; transport postal) et la sécurité

leur ayant été attribués, une analyse des risques et de la vulnérabilité. Ils se concerteront, là où c'est possible et judicieux, sur la façon de procéder et les méthodes à utiliser, pour parvenir à une approche aussi homogène que possible.

La consolidation des résultats, sous forme d'analyse globale de la menace, se fera en collaboration avec la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

Les rapports de dépendance ou interfaces avec la stratégie PIC sont en résumé les suivants:

- La stratégie nationale PIC est la stratégie faîtière dans le domaine des infrastructures critiques suisses. Elle inclut leur protection contre les cyberrisques.
- Les mesures de la SNPC destinées aux infrastructures critiques seront coordonnées avec celles de la stratégie PIC (p. ex. analyses des risques et de la vulnérabilité).
- La mise en œuvre des mesures de la stratégie dans le domaine des infrastructures critiques se fera en étroite coordination entre l'AEP, l'OFPP et l'UPIC.

Pour concrétiser ces mesures, l'OC SNPC a tout d'abord mené des discussions avec les offices fédéraux concernés (voir Annexe), dont les résultats ont été compilés et consolidés. Il a analysé aussi bien la situation actuelle que les autres travaux planifiés en vue de la mise en œuvre de la stratégie. Les résultats suivants ont été obtenus:

a) Le modèle de responsabilité personnelle préconisé dans la stratégie, avec la subsidiarité de la Confédération, est correct.
b) A l'issue des analyses prévues portant sur les risques et la vulnérabilité, il sera possible de déterminer, sur la base des intérêts nationaux supérieurs, le besoin d'agir et les surcoûts qui s'ensuivront pour corriger les risques existants.
c) Certains départements ont déjà procédé aux travaux préparatoires à la mise en œuvre des mesures, dans le cadre de leurs tâches.
d) Tout besoin de ressources devra être dûment justifié.

Le présent plan de mise en œuvre du DFF servira de base aux départements et offices pour concrétiser et mettre en place les mesures utiles. Il ne cherche pas à préciser les tâches et devoirs des services à créer; ce sera aux organisations concernées à le faire, sur la base de leur expérience et de leurs activités courantes. Il a été conçu sur la base des mesures inscrites dans la stratégie, qu'il faudra réaliser et intégrer au cycle régulier d'exploitation d'ici la fin de 2017.

Les cantons seront intégrés au processus de mise en œuvre via le mécanisme de consultation et de coordination du réseau national de sécurité (MCC RNS). En outre l'OC SNPC encadrera, conjointement avec le MCC RNS, un « groupe spécialisé Cyber» composé de représentants de la Confédération, des cantons et des communes.

La SNPC exclut expressément les situations de guerre et de conflit. Il est du devoir de l'armée d'assurer elle-même, en toutes circonstances, la protection et la défense de ses propres infrastructures et systèmes. Il lui incombe par ailleurs d'esquisser, dans les limites de sa mission et de ses responsabilités, des solutions destinées à traiter les cybermenaces et leurs conséquences. Le Chef de l'Armée a désigné à cet effet un délégué à la cyberdéfense de l'armée, qui a pris ses fonctions le 1er janvier 2013.

---

publique (armée; organisations de première intervention, protection civile).

2 Mandat et conditions-cadres

Comme le renforcement visé de la sécurité lié aux cyberisques ne peut aboutir qu'avec le concours de l'administration, des autorités cantonales, des secteurs/secteurs partiels ainsi que des exploitants d'infrastructures critiques (IC), la stratégie fédère tous ces acteurs en vue de la mise en œuvre des mesures.

Le plan de mise en œuvre a été établi avec la participation active de l'Office fédéral de l'approvisionnement économique du pays (OFAE) et de l'Office fédéral de la protection de la population (OFPP. Le Réseau national de sécurité (MCC RNS), par son mécanisme de consultation et de coordination faisant office de charnière entre la Confédération et les cantons, est également un partenaire central dans ce contexte.

3 Leçons à tirer

3.1 Ressources nécessaires

Les estimations des besoins ont été consolidées lors des interviews et se basent sur les besoins aujourd'hui avérés et les notes de synthèse en la matière des offices concernés, ou découlent des mesures figurant dans la présente stratégie. Le besoin de ressources est manifeste, car l'administration fédérale sera confrontée à un surcroît de charges pour assumer la part spécifiquement cybernétique de ses processus existants, dans le but de mettre en œuvre les mesures de la SNPC.

Divers offices doivent acquérir une solide expertise sur des thèmes similaires dans le cyberespace. Aussi a-t-il été question des formes de collaboration qui permettraient de développer en commun et de diffuser un tel savoir. Notamment dans le domaine de la réglementation, offrant des synergies aux autorités spécialisées comme l'Office fédéral de l'aviation civile (OFAC), l'Office fédéral des routes (OFROU), l'Office fédéral de l'énergie (OFEN), etc. Il faut agir ici, p. ex., en examinant ensemble la problématique des cyberrisques liés à l'usage croissant de systèmes de pilotage et de contrôle. Les mêmes personnes pourraient aussi collaborer ponctuellement à des inspections se rapportant au cyberespace. Dans quelle mesure les départements pourraient-ils couvrir ce besoin avec une équipe d'experts concentrant au même endroit des ressources spécialisées se recoupant et tenues à disposition des offices en ayant besoin? La question est en cours d'examen.

La stratégie a élargi le mandat de base de MELANI (DDPS et DFF) qui s'acquittera, dans le cadre des travaux de mise en œuvre, de prestations supplémentaires – états des lieux, appui et suivi lors d'incidents, aide pour les analyses des risques et de la vulnérabilité des exploitants d'IC. En outre, MELANI devra davantage associer à ses travaux les fournisseurs de prestations TIC et les fournisseurs de systèmes. Par conséquent, la centrale jouera un rôle-clé dans la mise en œuvre des mesures de la stratégie, en se chargeant de la coordination, de l'évaluation et de l'acheminement des flux d'information liés à la maîtrise des cyberrisques, ainsi qu'en garantissant les échanges d'informations avec les exploitants d'IC, les fournisseurs de prestations TIC et les fournisseurs de systèmes concernés. Cette plaque tournante de l'information, à élargir, est au cœur de la stratégie. A l'issue des travaux de mise en œuvre à fin 2017, MELANI devra assumer là où c'est nécessaire une fonction de coordination et de conduite, dans le cadre de son mandat. D'où l'indication séparée des tâches de MELANI dans le tableau ci-dessous.

Département	Postes créés	Postes supprimés jusqu'à fin 2017	Mise en œuvre des mesures suivantes de la SNPC
DFAE	+2	0	7;8;9;10;11;13
DFJP	+1	-1	4;6;13;14
DDPS	+17	0	2;3;4;5;6;11;12;13;14
DFF	+6	-1	2;3;4;5;6;7;8;9;10;11;12;13;14;16
DEFR	+2	0	2;12;13
DETEC	+2	0	2;3;7;8;9;10;11;12
Total	+30	-2	
MELANI (ressources déjà affichées au DFF + DDPS)	+6	0	2;3;4;5;6;10;11;12;13;14

3.2 Rôle des secteurs, secteurs partiels et exploitants d'IC

La Confédération n'a que des possibilités limitées de renforcer la cyberrésilience nationale en prenant elle-même les mesures utiles. Les efforts consentis par la Confédération servent à créer des conditions-cadres optimales en vue d'une cyberrésilience nationale accrue. Quant à la collaboration des secteurs (partiels) critiques de l'économie, avec leurs exploitants d'infrastructures critiques correspondants, elle s'avère cruciale pour la bonne mise en œuvre des mesures de la stratégie. D'où la nécessité que les offices fédéraux réussissent à faire participer ces secteurs aux mesures correspondantes, en prévoyant des processus d'information et de consultation adéquats. La stratégie PIC donne d'utiles indications pour l'attribution des compétences.

3.3 Subsidiarité de l'armée

La SNPC exclut certes expressément les situations de guerre et de conflit, et charge l'armée de se préparer à de telles éventualités. Or l'armée connaît remarquablement bien les cyberrisques, notamment leurs enjeux techniques. Il faudrait donc que les offices responsables incluent ces compétences dans leurs processus de mise en œuvre, et les sollicitent le cas échéant. Ce serait d'ailleurs conforme au modèle de subsidiarité des engagements de l'armée qui a fait ses preuves, p. ex. pour les catastrophes naturelles. Il est dès lors prioritaire, pour les offices ou secteurs administratifs chargés de la mise en œuvre de la SNPC, d'acquérir ou consolider les connaissances et aptitudes qui leur permettront de faire un usage ciblé et orienté solution des ressources de l'armée. Autrement dit, une coordination précoce avec la mise en œuvre de la SNPC implique que les offices responsables identifient et exploitent de bonne heure les synergies possibles dans ce domaine. En outre, cette intégration précoce de l'armée permettra d'ajuster à tout le système suisse le concept de cyberdéfense que l'armée est chargée d'élaborer.

3.4 Risques du projet

Il existe plusieurs risques à prendre en compte dans la mise en œuvre de la stratégie. L'un des principaux risques – et de loin – étant que les mesures de mise en œuvre n'agissent pas en temps voulu. D'autres risques ont:

- Les connaissances lacunaires de certains acteurs constituent un facteur de risque, tout comme il est à craindre que la stratégie paraisse obsolète aux yeux du public si des incidents surviennent avant sa mise en œuvre.
- En prenant en compte trop tard ou insuffisamment les secteurs et secteurs partiels ainsi que les exploitants d'IC, les offices mettraient en péril l'analyse des risques et de la vulnérabilité ainsi que la gestion de la continuité.
- Une communication déficiente et des attentes exagérées de la part des secteurs, des secteurs partiels ou des exploitants d'IC pourraient menacer la coopération.
- L'octroi trop tardif des ressources nécessaires pourrait compromettre la mise en œuvre des mesures dans tous les domaines de la stratégie.
- La mise en œuvre de la stratégie pourrait révéler les défaillances de certaines infrastructures critiques, avec des coûts pour corriger de tels risques.

4 Organisation de mise en œuvre de la SNPC

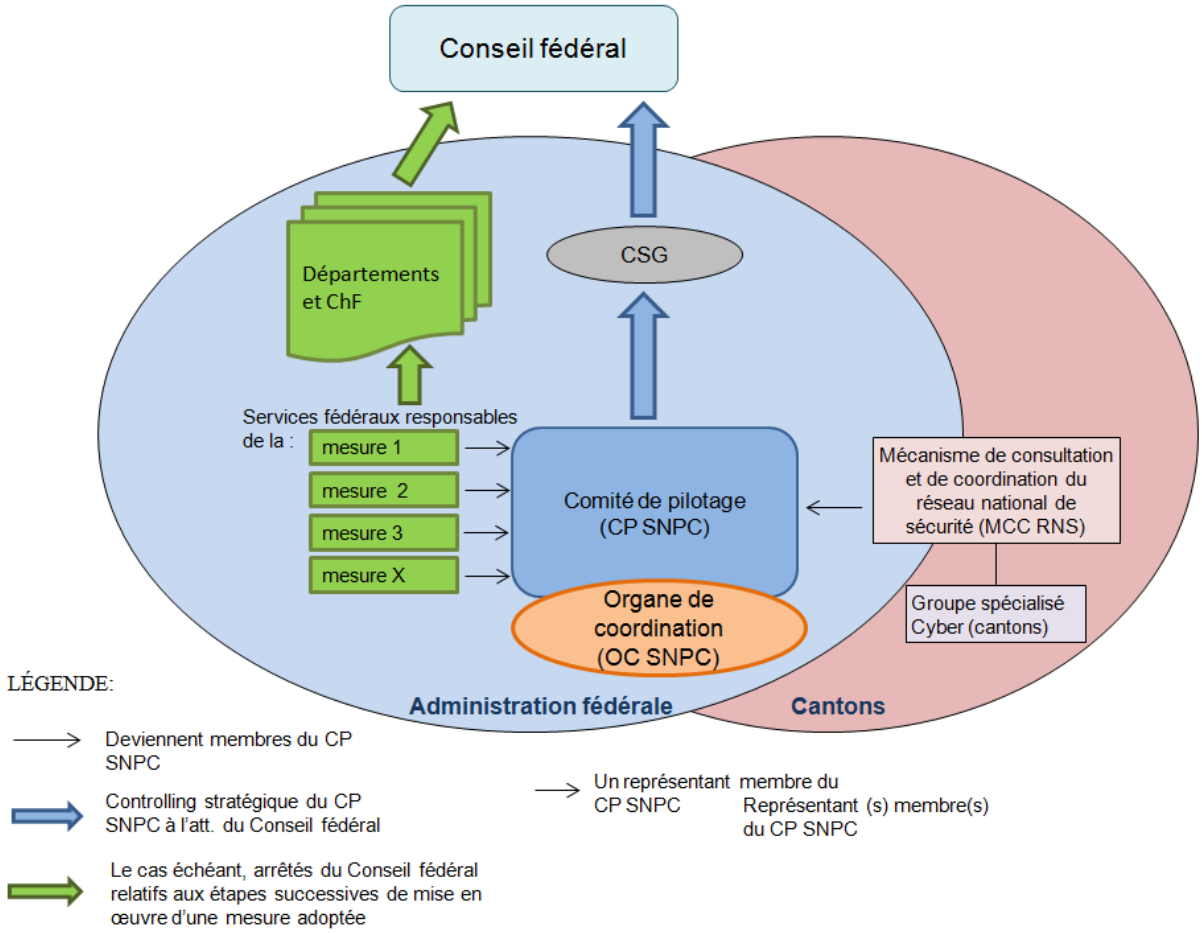

Fig. 2: Organisation de mise en œuvre de la SNPC

4.1 Comité de pilotage de la SNPC

Sur mandat du Conseil fédéral, le comité de pilotage de la SNPC veille à la mise en œuvre coordonnée et ciblée de la stratégie nationale de protection de la Suisse contre les cyberrisques (voir fig. 2).

Ses compétences et fonctions sont les suivantes:

- Il procède à un contrôle de gestion stratégique du portefeuille de mesures de la stratégie, pour s'assurer que les travaux progressent de façon ciblée et dans le respect des délais, et présente à ce sujet des rapports au Conseil fédéral, via la Conférence des secrétaires généraux (CSG).
- Il coordonne l'approche des départements chargés de la mise en œuvre des mesures, notamment si ces mesures concernent la législation.
- Il soutient activement la collaboration des services fédéraux avec les services compétents des cantons, avec les milieux économiques et la société civile.
- Il veille à ce que les activités de mise en œuvre tiennent dûment compte de la politique de gestion des risques menée par la Confédération, de la stratégie nationale pour la

protection des infrastructures critiques, ainsi que de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

- Il étudie avec les services responsables les synergies possibles ainsi qu'une simplification et un allégement des moyens et systèmes d'annonce.
- Il observe l'évolution des cyberrisques et soumet au Conseil fédéral des recommandations visant à adapter la stratégie en conséquence.
- Il informe le Conseil fédéral une fois par an, via le Département fédéral des finances (DFF), de l'état de la mise en œuvre de la stratégie, ainsi qu'à la fin de 2017 sous la forme d'un rapport final complet avec une évaluation de l'efficacité de la stratégie et de son plan de mesures. L'évaluation de l'efficacité sera déjà soumise au Conseil fédéral au début de 2017.

Font partie du comité de pilotage les départements chefs de file pour au moins une des mesures de mise en œuvre. Le mécanisme de consultation et de coordination du réseau national de sécurité (MCC RNS) fait aussi partie du comité de pilotage, dont le DFF assure la présidence.

4.2 Organe de coordination de la SNPC

L'organe de coordination de la SNPC coordonne la mise en œuvre de la stratégie au niveau technico-opérationnel.

Ses tâches sont les suivantes:

- Il observe et évalue systématiquement l'avancement des travaux de mise en œuvre de la stratégie et en informe le comité de pilotage.
- Il coordonne et soutient les activités de mise en œuvre des services compétents et exécute les mesures lui ayant été confiées.
- Il identifie et exploite les synergies entre les mesures de mise en œuvre.
- Il organise la collaboration avec des experts tant internes qu'externes à la Confédération, et avec leurs organisations respectives.
- Il suit de près au niveau national et, d'entente avec le Département fédéral des affaires étrangères (DFAE), au niveau international également, les tendances en matière de cyberstratégies et communique au fur et à mesure ses conclusions aux partenaires concernés.
- Il organise une rencontre annuelle des experts de la SNPC, où les partenaires de sa mise en œuvre peuvent tisser des liens, s'informer et échanges leurs idées sur le plan suisse.

4.3 Groupe spécialisé Cyber (GS-C) et Groupe spécialisé International (GS-CI)

Afin de coordonner les travaux comportant des interfaces avec les cantons, le mécanisme de consultation et de coordination du réseau national de sécurité (MCC RNS) constitue le groupe spécialisé Cyber (GS-C), composé de représentants de la Confédération, des cantons et des communes.

Le GS-C coordonne la mise en œuvre de la SNPC au niveau des cantons. Ses tâches sont les suivantes:

- Il associe les cantons, en tant que partenaires centraux de la Confédération, à toutes les mesures de mise en œuvre les concernant.
- Il dirige des projets partiels, sous la forme de groupes de travail actifs dans trois domaines : le renforcement de la capacité de résistance (résilience), la gestion des incidents et la gestion des crises.
- Il coordonne la mise en œuvre des projets partiels cantonaux et vérifie, au moyen d'un contrôle de gestion stratégique, qu'ils avancent conformément aux objectifs et aux délais.
- Il s'assure qu'il soit dûment informé des activités de mise en œuvre menées par la Confédération dans le cadre de la stratégie et il encourage les échanges d'expériences entre ses membres.

L'organe de coordination de la SNPC est membre du groupe spécialisé Cyber du MCC RNS et, au niveau fédéral, il fait le pont avec les travaux de projet du GS-C, de façon à utiliser les synergies de façon optimale et à éviter les redondances.

En outre, un groupe spécialisé Cyber International (GS-CI) est prévu, sous la responsabilité du DFAE. Il a pour but de garantir le flux d'informations, en étroite coopération/coordination entre tous les protagonistes. Le DFAE invitera à une séance constitutive les parties intéressées par la coopération internationale dans le cyberespace. Cette première rencontre servira à discuter de l'utilité que pourrait avoir, pour ses membres, un groupe de travail interdépartemental s'occupant exclusivement des aspects internationaux de la question.

5 Mesures à prendre et responsabilités

Les sept champs d'action proposés dans la stratégie, avec leurs mesures concrètes (M1 à M16), peuvent être répartis en quatre domaines définis en fonction du moment de leur déploiement et de leurs dépendances:

- **Prévention**
- **Réaction**
- **Gestion de la continuité et des crises**
- **Processus de soutien**

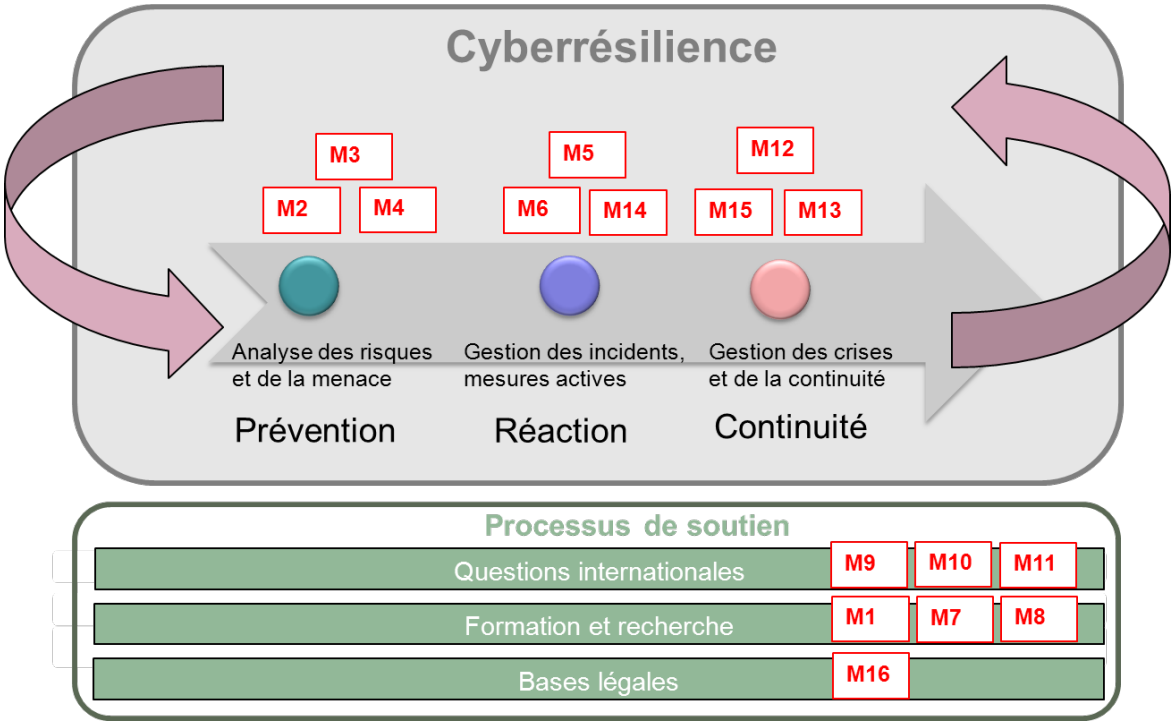

Fig. 3: Aperçu de la stratégie

La cyber-résilience repose sur un enchaînement de processus de prévention, de réaction et de continuité. À l'issue de la gestion de crise liée à un incident, le processus repart cependant depuis le début.

Les sous-chapitres suivants présentent les conclusions des entretiens menés avec les partenaires consultés. Les mesures y sont regroupées par domaine et précisent à chaque fois les responsabilités, les compétences, les objectifs de mise en œuvre et les délais.

5.1 Prévention

Dans le domaine de la prévention, il est prévu d'étendre aux cyberrisques au sens de la présente stratégie le modèle de gestion globale des risques figurant dans la stratégie PIC. Les offices responsables de la mise en œuvre feront une analyse des risques et de la vulnérabilité. L'OFAE en premier lieu, ainsi que les autorités ou régulateurs compétents (OFPP notamment), prendront la direction des opérations.

Il est nécessaire de compiler, dans la présentation de la menace globale, les informations tant techniques que non techniques pour analyser et évaluer de façon complète les cyberrisques. MELANI fournira les informations correspondantes. D'où la nécessité de développer MELANI comme plaque tournante de l'information au service des cantons et des exploitants d'IC.

On peut supposer que la plupart des secteurs critiques, avec leurs exploitants d'IC, ont institutionnalisé une analyse des risques et de la vulnérabilité. Face à la menace grandissante, la stratégie doit aboutir à la prise en compte explicite de l'aspect cybernétique dans l'analyse globale des risques. A cet effet, elle recommande de suivre une approche standardisée et de résumer les résultats consolidés sous forme de tableau complet de la situation, avec les scénarios d'évolution possible.

Une telle approche vise également à garantir que les cyberrisques soient explicités, tout particulièrement dans le cas des exploitants d'IC. Il sera ainsi possible d'identifier les risques résiduels inacceptables et de présenter de manière compréhensible les coûts afférents au besoin d'agir identifié, sur la base d'une réflexion globale menée au niveau national.

Champ d'action 2	**Compétence: OFAE, OFPP, autorités/régulateurs;** MELANI	**Mesure 2**
Analyse des risques et vulnérabilités	L'OFAE procède aux analyses des risques et de la vulnérabilité avec les secteurs, les secteurs partiels et les exploitants d'IC. Les secteurs et secteurs partiels ne relevant pas de l'OFAE seront traités par l'OFPP, avec la participation des autorités compétentes. Une répartition claire des compétences est en place entre l'OFAE et l'OFPP pour les secteurs partiels.	Contrôles indépendants des systèmes. Analyses des risques dans le but de les réduire en collaboration avec les autorités, les fournisseurs de prestations TIC et les fournisseurs de systèmes.

Application:

L'OFAE[3] et l'OFPP[4] sont chargés de mener une analyse des risques et de la vulnérabilité dans les secteurs partiels relevant de leur compétence. Là où c'est possible et judicieux, l'OFAE et l'OFPP se concerteront sur la procédure et les méthodes. Les secteurs et secteurs partiels ne relevant pas de l'OFAE seront traités par l'OFPP, avec la participation des autorités compétentes (régulateurs responsables). Il importe de suivre ici une approche aussi standardisée que possible. Les travaux devront être terminés d'ici la fin de2017.

Les résultats étayant l'analyse globale de la menace sont consolidés en collaboration avec MELANI.

[3] Voir note 1.
[4] Voir note 2.

Champ d'action 2	**Compétence: UPIC;** OFIT, BAC, MELANI	**Mesure 3**
Analyse des risques et de la vulnérabilité	L'UPIC élabore avec les fournisseurs de prestations TIC un concept de contrôle. Ce concept complétera l'aide-mémoire PIC pour le cyberespace. MELANI garantit les échanges avec les exploitants d'IC, les fournisseurs de prestations TIC et les fournisseurs de systèmes.	Analyses de la vulnérabilité des infrastructures TIC sous un angle systémique, organisationnel et technique: Les autorités, les exploitants d'IC et les instituts de recherche examinent leurs infrastructures TIC en impliquant les fournisseurs de prestations TIC et les fournisseurs de systèmes.

Application:

La section Sécurité en matière de TIC de l'UPIC (UPIC-SEC) élabore d'ici la fin 2015 un concept de contrôle qui sera appliqué par les fournisseurs de prestations et les responsables concernés des secrétariats généraux des départements. L'Office fédéral de l'informatique et de la télécommunication (OFIT) et la Base d'aide au commandement (BAC) soutiennent ce concept en tant que fournisseurs de prestations TIC. Il sera diffusé à titre de recommandation au secteur privé et aux exploitants d'IC. Il aura également une valeur de recommandation et d'appui pour les propres analyses des cantons, auxquels le groupe spécialisé Cyber du MCC RNS pourra le soumettre.

Le concept de contrôle sera coordonné avec les projets en cours, à l'instar du système de gestion de la sécurité de l'information (Information Security Management Systems, ISMS) de la Division de la protection des informations et des objets (DPIO).

Les résultats étayant l'analyse globale de la menace sont consolidés en collaboration avec MELANI.

Champ d'action 3	**Compétence: MELANI, SRC, SCOCI;** BAC, RM, OFIT	**Mesure 4**
Analyse de la menace	Des informations en matière de renseignement, policières, médico-légales ou techniques, provenant de sources publiques ou non, sur les menaces et risques dans le cyberespace, sont acquises, évaluées et analysées. Cette mesure sera concrétisée dans divers projets placés sous la responsabilité de différents services. MELANI établit un état des lieux de la menace, en étroite collaboration avec le Service de renseignement de la Confédération (SRC) et fedpol/SCOCI. Le SRC assume les aspects cybernétiques de son mandat. CERT: mise en place des capacités techniques permettant de surveiller constamment (24h/7) = CSIRT-OFIT, CSIRT-SRC, GovCERT.	Établissement d'un tableau de la situation et de son développement.

Application:

MELANI: élaboration (jusqu'à fin 2013) et mise en œuvre (dès 2014) d'un concept de renforcement de MELANI comme plateforme d'échange d'informations. MELANI développe la collaboration systématique avec les fournisseurs de prestations TIC et les fournisseurs de systèmes. L'échange d'informations avec les exploitants d'IC et l'économie est également intensifié.

SRC: acquisition de connaissances spéciales et aptitudes dans le cyberespace, avec le BAC-COE et le Renseignement militaire (RM) comme fournisseurs de prestations du SRC (2014-2015).

Les capacités techniques permettant de surveiller constamment (24/7) les réseaux de la Confédération doivent être créées avant la fin de 2015.

CERT: MELANI: développement du GovCERT afin d'accroître la capacité de résistance (2014-2016)

OFIT: développement du CSIRT afin d'accroître la capacité de détection.

5.2 Réaction

Les mesures de réaction pertinentes pour la SNPC, *incident handling*, *incident response*, servent à la consolidation des tâches et capacités en place qui contribuent à la cyberrésilience et dont les acteurs ne peuvent se charger isolément. Durant ce processus de *incident handling*, *incident response,* il peut s'avérer nécessaire de prévoir des contre-mesures actives ciblées. En définitive, il appartient aux acteurs politiques de déterminer jusqu'à quel point la Suisse doit pouvoir prendre à l'étranger des mesures actives en dessous du seuil des actes de guerre.

Champ d'action 3	**Compétence: MELANI, SRC;** BAC, RM, OFIT	**Mesure 5**
Analyse de la menace	La Confédération, les cantons et les exploitants d'IC doivent assurer un suivi des incidents importants et étudier les possibilités de développer leurs propres mesures face aux incidents ayant un rapport avec les cyberrisques. MELANI collecte les données, évalue les résultats, les analyse et les met à disposition des acteurs concernés (modèle PPP). Mandat du SRC, voir M4.	Suivi d'incidents dans le but de poursuivre le développement de mesures.
Application: Voir M4 OFIT: création des capacités techniques (accroissement des possibilités de réaction à un incident) en vue d'une surveillance 24/7. Le développement du CSIRT-OFIT permettant de renforcer les capacités techniques et d'accroître la capacité de résistance (résilience) se fera jusqu'en 2014. Cet accroissement permet le soutient de la M4.		

Champ d'action 3	**Compétence: SCOCI;** MELANI	**Mesure 6**
Analyse de la menace	En cas de cyberincident, les cantons portent la responsabilité directe des poursuites pénales requises.	Vue d'ensemble des cas et coordination de cas intercantonaux complexes.

Application:

Fedpol élabore, en collaboration avec les cantons, un concept de gestion offrant une vue d'ensemble globale des cas (infractions), qui se prêtera à la coordination des cas complexes intercantonaux. Ce concept fera l'objet de deux consultations dans les cantons et sera soumis à l'approbation de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP). Au sein de fedpol, le SCOCI assure la coordination. Le concept tiendra dûment compte des projets existants entre les cantons et la Confédération (p. ex. harmonisation de l'informatique de la police HPI; plateforme PICAR dédiée à l'analyse de la délinquance sérielle dans les cantons romands). Un comité restreint de l'organisation de projet sera défini au deuxième trimestre 2013. Y seront représentés:

fedpol, la CCDJP, la Conférence des autorités de poursuite pénale de Suisse (CAPS), la Conférence des commandants des polices cantonales de Suisse (CCPCS), le responsable du groupe de travail informatique de la CCPCS, un représentant de Swiss Police ICT, un représentant du Ministère public de la Confédération (MPC) ainsi que de l'Office fédéral de la justice (OFJ).

La première consultation aura lieu au deuxième trimestre 2014, la seconde au deuxième trimestre 2014. Le concept sera élaboré jusqu'au troisième trimestre 2015 et soumis pour approbation à la CCDJP. La consultation des offices est prévue au quatrième trimestre 2015. Les préparatifs en vue de la réalisation suivront en 2016.

Au niveau international, Europol ainsi qu'Interpol constituent des acteurs-clés, avec lesquels il faudra coordonner le concept.

Les informations ainsi générées (vue d'ensemble des infractions) et les résultats sur les cas complexes obtenus par l'analyse technico-opérationnelle dans le cadre d'une procédure pénale seront intégrés par MELANI dans l'analyse globale de la menace.

Champ d'action 6	**Compétence SRC, MELANI;** SCOCI, RM	**Mesure 14**
Gestion de la continuité et des crises	Le SRC est responsable de chercher et collecter des informations avec les moyens du renseignement, de les analyser et de diffuser les résultats. Il met en place avec la participation de la BAC, son fournisseur technique de prestations et en liaison avec le Renseignement militaire (RM), les capacités nécessaires à l'identification des agresseurs et prépare des mesures actives, si c'est politiquement opportun. Et comme le SCOCI (fedpol) joue un rôle important dans les poursuites pénales et l'identification des agresseurs, il sera dûment intégré.	Mesures actives d'identification des agresseurs. Quand le SRC parvient à identifier les auteurs il transmet, dans la mesure où la loi le permet, les informations correspondantes au Ministère public de la Confédération. Celui-ci décide s'il y a lieu d'ouvrir une procédure pénale. Au cas où des poursuites pénales ne seraient pas indiquées ou impossibles, des contre-mesures actives seront préparées. La base juridique correspondante doit être prévue dans la LSRe.

Application:

Adaptation de l'accord de niveau de service (*service level agreement, SLA*) avec le BAC-COE jusqu'à fin 2013. Acquisition par le SRC de connaissances spéciales, avec le BAC-COE et le RM comme fournisseurs de prestations (2014-2015).

Les résultats enregistrés par MELANI dans l'analyse de la menace ainsi que, dans les limites du mandat légal de poursuite pénale, les possibilités d'investigation et de transfert des auteurs seront intégrés aux mesures à prendre.

5.3 Gestion de la continuité et des crises

On attend de l'Etat qu'il dispose de moyens lui permettant d'appuyer subsidiairement des entités responsables, lorsque celles-ci ne sont plus capables de prendre elles-mêmes les mesures leur permettant de venir à bout de la situation. MELANI apporte, avec ses fournisseurs (SRC notamment), un tel appui dans le cadre de son cercle fermé de clientèle. De telles prestations doivent être mises en place dans les secteurs partiels de tous les secteurs, ainsi qu'au sein des exploitants d'IC.

Les processus d'analyse des incidents ainsi que de gestion de la continuité et des crises doivent être étroitement coordonnés. Une crise est généralement déclenchée par un incident. A contrario, tout incident n'entraîne pas une crise. D'où la nécessité de processus d'escalade – de la gestion des incidents jusqu'à la gestion des crises. Les plans de gestion des crises font partie intégrante de la gestion de la continuité. Il appartient par conséquent aux offices de tutelle, aux autorités spécialisées et aux régulateurs de veiller, dans leurs domaines de compétence respectifs, à ce que chaque secteur (partiel) et les exploitants d'IC disposent d'une gestion des incidents et d'une gestion des crises performantes.

Champ d'action 6	**Compétence: OFAE, OFPP, autorités/régulateurs;** MELANI	**Mesure 12**
Gestion de la continuité et des crises	Les compétences en matière de gestion de la continuité sont identiques à M2.	Renforcement et amélioration de la capacité de résistance (résilience) face aux perturbations et événements imprévus.

Application:

La mise en œuvre de la gestion de la continuité est identique à M2. Le DEFR adapte ses compétences dans le cadre de la révision de la LAP. La gestion de la continuité est un processus permanent. Comme elle s'appuie sur les analyses préalables des risques et de la vulnérabilité, elle ne peut intervenir qu'à l'issue de la M2.

MELANI soutient et intensifie l'échange volontaire d'informations entre les exploitants d'IC, les fournisseurs de prestations TIC et les fournisseurs de systèmes, pour soutenir la continuité et la capacité de résistance selon le principe de l'auto-assistance. D'où un besoin accru en capacités médico-légales, et une augmentation des échanges d'informations.

Champ d'action 6	**Compétence: OFAE, MELANI, OFPP;** SCOCI, DFAE, autorités/régulateurs	**Mesure 13**
Gestion de la continuité et des crises	Les compétences en matière de gestion des crises sont identiques à M2 et M12. MELANI assume la partie opérationnelle et garantit, lors des crises, un appui subsidiaire aux acteurs concernés, en leur offrant son expertise. Fedpol / SCOCI est étroitement associé en vue des poursuites pénales. Dans les cas susceptibles d'avoir des implications de politique étrangère, le DFAE sera informé au plus vite et associé à l'élaboration d'une planification préventive. Les offices responsables se coordonnent et se mettent d'accord.	Coordination des activités en premier lieu avec les acteurs directement concernés et appui des processus décisionnels par l'expertise requise.

Application:

La mise en œuvre de la gestion de crise est identique à M12. Le DEFR propose d'adapter ses compétences, dans le cadre de la révision de la LAP. La gestion des crises est un processus permanent. Comme elle s'appuie sur les analyses préalables des risques et de la vulnérabilité, elle ne peut intervenir qu'une fois celle-ci terminée.

Des processus fonctionnels sont en place avec MELANI et ses partenaires du cercle restreint, afin de traiter les incidents selon leur degré de gravité dans les organisations de crise de l'administration ainsi que du secteur privé.

Il est important que l'OFAE et l'OFPP coordonnent leurs activités, afin de garantir une procédure uniforme et cohérente et de tirer le meilleur parti possible des contacts établis.

Champ d'action 6	Compétence: ChF	Mesure 15
Gestion de la continuité et des crises	Sous la conduite de la Chancellerie fédérale (ChF), un concept sera élaboré pour des procédures et processus de conduite permettant de résoudre en temps adéquat les problèmes, compte tenu des aspects cybernétiques.	Elaboration d'un concept pour des procédures et processus de conduite permettant une résolution des problèmes en temps opportun.

Application:

La gestion (globale) des crises doit être adaptée et inclure les aspects cybernétiques. Les procédures et processus de conduite de la Confédération tiendront compte des aspects cybernétiques des processus en place.

Sous la conduite de la ChF un concept sera établi pour les procédures et processus de conduite afin de résoudre en temps opportun les problèmes, compte tenu des aspects cybernétiques.

5.4 Processus de soutien

Comme la protection des infrastructures d'information et de communication contre les cyberrisques revêt un intérêt national en Suisse, il faut créer les bases nécessaires. En font notamment partie:

- un réexamen des bases juridiques existantes quant à leur conformité aux mesures de protection qui s'imposent;
- des coopérations et efforts internationaux visant à préserver le cyberespace de tout abus, sur la base de règles et normes supranationales;
- des échanges d'expériences, travaux de recherche et développement, informations sur certains incidents, ainsi qu'activités en rapport avec l'instruction et les exercices,
- la collaboration de la Suisse au sein d'organisations internationales, étatiques ou non, cherchant à réduire les cyberrisques.

Pour accroître la cyberrésilience, il est indispensable que chaque secteur de responsabilité ait les capacités d'identifier, d'évaluer et d'analyser les risques en lien avec les problèmes du cyberespace. A cet effet, la stratégie a chargé les offices fédéraux compétents de mettre en œuvre des mesures suivantes, avec la collaboration ponctuelle de leurs homologues cantonaux. Les cantons et les exploitants d'IC doivent pouvoir se soutenir afin d'accroître la cyberrésilience sur ces bases, car il s'agit de tâches étatiques susceptibles d'être assumées par les divers acteurs.

Champ d'action 1	**Compétence:** offices fédéraux responsables	**Mesure 1**
Identification des risques par la recherche	Concrétisation au cours de la mise en œuvre.	Recherches nécessaires sur les nouveaux risques en lien avec la problématique de la cybernétique.

Application:

Les groupes-cibles ci-après sont habilités à identifier les lacunes de connaissances et de savoir-faire dans le cyberespace:

- CERT
- exploitants d'IC
- fournisseurs TIC

Les services suivants mènent des projets ou programmes de recherche sur le cyberespace:

- UE
- départements des EPF
- universités et hautes écoles spécialisées
- laboratoires de recherche (p. ex. IBM)

Champ d'action 4	**Compétence: OC SNPC;** OFCOM, DFAE, OFAS	**Mesure 7**
Formation des compétences	L'organe de coordination de la SNPC établit, en collaboration avec l'OFAS (programme Jeunes et médias)[5], le DFAE et l'OFCOM, un aperçu des offres existantes en matière de formation des compétences. L'établissement de cet aperçu sera étroitement coordonné avec les travaux de concrétisation de la stratégie du Conseil fédéral pour une société de l'information en Suisse et avec les cantons. Le DFAE transmet des informations sur les offres faites dans le cadre d'organisations ou institutions internationales.	Création d'une vue d'ensemble des offres en matière de formation des compétences.

Application:

L'aperçu des offres existantes en matière de formation des compétences sera établi jusqu'à fin 2013 et les offres de formation des compétences seront publiées jusqu'à la mi-2014.

[5] ACF du 11.06.2010, Programme national Protection de la jeunesse face aux médias et compétences médiatiques.

Champ d'action 4	**Compétence: OC SNPC;** OFCOM, DFAE, OFAS	**Mesure 8**
Formation des compétences	L'organe de coordination de la SNPC coordonne avec les travaux de la stratégie du Conseil fédéral pour une société de l'information en Suisse, avec les cantons et l'économie et en collaboration avec l'OFAS, le DFAE, l'OFCOM, de même que les autorités compétentes et les régulateurs, l'élaboration d'un concept de concrétisation visant un recours accru aux offres existantes de qualité élevée en rapport avec le traitement des cyberrisques et la création de nouvelles offres formelles et informelles de formation. Le DFAE transmet des informations sur les offres faites dans le cadre d'organisations ou institutions internationales.	Comblement des lacunes par des offres en matière de formation des compétences et recours plus fréquent à de telles offres.
Application: Un concept de concrétisation visant un recours accru aux offres existantes en rapport avec le traitement des cyberisques sera élaboré et de nouvelles offres de formation créées d'ici la fin 2015.		

Champ d'action 5	**Compétence: OFCOM;** autorités/régulateurs, DFAE, POLSEC, MELANI	**Mesure 9**
Relations et initiatives internationales	Soutien du DETEC, DFAE, DDPS et du DFF. L'OFCOM joue un rôle actif dans les processus et institutions internationaux pertinants dans le domaine de la gouvernance d'Internet (ICANN, UIT, CSTD et FGI notamment), identifie en permanence les aspects déterminants pour la stabilité, la disponibilité et la sécurité d'Internet, coordonne les intérêts de la Suisse avec les représentants de l'administration, de l'économie et de la société civile, et représente lesdits intérêts dans les processus et institutions susmentionnés.	Gouvernance d'Internet: la Suisse s'engage activement, et de manière coordonnée, en faveur d'une gouvernance d'Internet qui s'accorde avec sa conception de la liberté et de la responsabilité (individuelle), du service universel, de l'égalité des chances, des droits de l'homme et de l'Etat de droit.
Application: L'OFCOM et le DFAE, secondés du DDPS pour les questions de politique de sécurité (SG-DDPS/POLSEC), établissent pour la fin de 2013, en collaboration avec les départements participants, un aperçu des manifestations, des initiatives prioritaires et des comités internationaux qui ont un lien avec la gouvernance d'Internet.		

Champ d'action 5	**Compétence: DFAE;** POLSEC, MELANI, OFCOM	**Mesure 10**
Relations et initiatives internationales	Le DFAE lancera des activités ciblées avec la communauté internationale. Une option consisterait à établir un «code de conduite» propre au cyberespace, l'objectif à long terme étant de fixer des directives contraignantes de droit international public. Une autre piste consisterait à établir/renforcer Genève comme centre de compétences dans le domaine d'Internet. Le DFAE bénéficiera du soutien de la POLSEC pour la mise en œuvre de ces mesures.	Coopération au niveau de la politique de sécurité internationale, pour faire face avec d'autres Etats et des organisations internationales aux menaces émanant du cyberespace. Des activités ciblées seront lancées ou poursuivies sur la scène internationale, pour permettre à la Suisse de défendre ses intérêts dans les sphères internationales.
Application: Le DFAE élaborera d'ici la fin de 2013 un concept de mise en œuvre à moyen terme de la SNPC avec la coopération internationale. MELANI et l'OFCOM soutiennent ce processus.		

Champ d'action 5	**Compétence: OC SNPC;** autorités/régulateurs, DFAE, MELANI	**Mesure 11**
Relations et initiatives internationales	MELANI et les autorités ou régulateurs compétents intensifient l'échange d'information entre les exploitants d'IC, les fournisseurs de prestations TIC et les fournisseurs de systèmes au sujet des démarches et initiatives internationales. MELANI et le DETEC soutiennent ainsi l'implication coordonnée de la place économique suisse dans ces sphères internationales. Pour autant que cela soit souhaité, MELANI, le DETEC et le DFF veilleront à ce que la représentation soit assurée en accord avec les départements, le DFAE en particulier.	Coordination des acteurs lors de leur participation à des initiatives et des bonnes pratiques dans le domaine des processus de sécurité et de sûreté. Les opérateurs, associations et autorités s'organisent dans le cadre d'initiatives, de conférences et de processus de standardisation privés ou étatiques dans les domaines de la sûreté et de la sécurité pour s'impliquer dans ces organes.
Application: Dans un premier temps, les partenaires concernés (autorités et régulateurs) feront un bilan pour déterminer qui devrait participer aux initiatives et enceintes internationales. Une consolidation suivra dans un second temps. Les autorités spécialisées, les milieux de l'industrie et, le cas échéant, le DFAE seront mis à contribution ici. L'OC SNPC coordonnera le processus.		

Champ d'action 7	Compétence: OC SNPC	Mesure 16
Bases juridiques	L'organe de coordination de l'UPIC coordonne les travaux de la mesure 16, aux fins de la mise en œuvre de la stratégie avec les départements concernés. Les départements compétents élaborent au niveau normatif adéquat les propositions nécessaires concernant les lacunes législatives identifiées comme prioritaires et pour les adaptations juridiques requises.	Examen des bases juridiques en vigueur.
Application: L'organe de coordination de la SNPC élabore d'ici la fin de 2013, avec le concours des départements, un premier aperçu de la nécessité urgente de légiférer et de procéder à des révisions dans le domaine de la cybersécurité. Un concept destiné à combler les lacunes législatives identifiées comme prioritaires, avec un calendrier, sera soumis au Conseil fédéral au plus tard à la fin de 2014.		

6 Annexe

Documents référencés

Titre	Auteur/éditeur	Date
[1] Stratégie nationale de protection de la Suisse contre les cyberrisques	DDPS	19.06.2012
[2] Stratégie nationale pour la protection des infrastructures critiques	DDPS – OFPP	27.06.2012
[3] Aide-mémoire concernant la protection des infrastructures critiques (aide-mémoire PIC)	DDPS – OFPP	projet du 23.07.2012
[4] Handbuch Risikomanagement Bund (manuel de gestion des risques, non traduit)	DFF	version 1.0

Liste des partenaires consultés

Services fédéraux	Participants	Date
OFAE-OFPP-UPIC (séance de coordination)	Ruedi Rytz (OFAE), Toni Lauber (OFAE), Stefan Brem (OFPP), Nick Wenger (OFPP), Pascal Lamia (UPIC), Stefanie Frey (UPIC), Franz Zingg (UPIC), Marc Henauer (NDB)	07.01.2013
OFCOM	Armin Blum	17.01.2013
OFT	Petra Breuer, Ulrich Schär, Heinz Geiser	14.01.2013
OFAC	Urs Haldimann	11.01.2013
OFEN	Christian Holzner, Hans-Peter Binder	17.01.2013
OFIT	Heino Kronenberg	17.01.2013
OFAS	Thomas Vollmer	27.02.1013
DFAE	Michele Coduri, Christoph Bühler	21.01.2013
fedpol-SCOCI	Roland Becker, Thomas Walther, Tobias Bolliger	11.01.2013
FINMA	Marc Sander	04.01.2013
BAC	Riccardo Sibilia, Gérald Vernez	11.01.2013
SG-DDPS	Jürg Treichler	14.01.2013
UPIC-MELANI	Pascal Lamia, Stefanie Frey	18.01.2013
UPIC-SEC	Marcel Frauenknecht, Franz Zingg, Daniel Graf	11.01.2013
MCC RNS	Bernhard Wigger, Dario Walder	14.01.2013
SRC	Philipp Kronig, Reto Camenisch	17.01.2013

Table des acronymes

Acronyme	Signification
BAC	Base d'aide au commandement (DDPS)
BAC-COE	Centre des opérations électroniques de la Base d'aide au commandement du DDPS
CAPS	Conférence des autorités de poursuite pénale de Suisse
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandants des polices cantonales de Suisse
CERT	Computer Emergency Response Team
CP SNPC	Comité de pilotage de la stratégie nationale de protection de la Suisse contre les cyberrisques
CSG	Conférence des secrétaires généraux
CSIRT	Computer Security Incident Response Team
CUG	Closed User Group (groupe restreint d'usagers, défini par MELANI)
Exploitant d'IC	exploitant d'infrastructures critiques
FRT	Formation, recherche et technologie
GS-C	Groupes spécialisés Cyber
LAP	Loi fédérale du 8 octobre 1982 sur l'approvisionnement économique du pays (loi sur l'approvisionnement du pays)
MCC RNS	mécanisme de consultation et de coordination du réseau national de sécurité
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
OC SNPC	Organe de coordination de la mise en œuvre de la stratégie
OFAS	Office fédéral des assurances sociales
OFIT	Office fédéral de l'informatique et de la télécommunication (DFF)
RM	Renseignement militaire (DDPS)
POLSEC	Politique de sécurité (unité du SG-DDPS)
SCOCI	Service de coordination de la lutte contre la criminalité sur Internet (DFJP)
SiLAN SRC	Système de communication chiffré du SRC
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SONIA	Etat-major pour la sûreté de l'information
Stratégie PIC	Stratégie nationale pour la protection des infrastructures critiques
UPIC-SEC	Section Sécurité en matière de TIC de l'Unité de pilotage informatique de la Confédération