Rapport annuel 2015

sur la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Publication: 20.04.2016

Rédaction: Organe de coordination de la SNPC

Département fédéral des finances DFF

Unité de pilotage informatique de la Confédération UPIC
Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

Schwarztorstrasse 59
CH-3003 Berne

Tél.: +41 (0)58 462 45 38
Courriel: info@isb.admin.ch

Rapport annuel: www.isb.admin.ch

Table des matières

Préambule

Le numérique gagne du terrain et progresse en rapidité et en complexité. Il s'agit de reconnaître de bonne heure les chances que la numérisation offre à la Suisse et d'en tirer le meilleur parti possible. Il ne faut pas pour autant oublier les risques de ce secteur. Plusieurs événements survenus en 2015 nous ont montré qu'ils doivent être pris très au sérieux. Des activités d'espionnage, des maliciels inédits, des fuites de données ou encore des cas de chantage basés sur des attaques DDos ont rappelé la vulnérabilité des infrastructures numériques de l'économie et de la société. Les exemples les plus spectaculaires ont été les opérations d'espionnage menées contre le Parlement allemand et lors des pourparlers liés à l'accord nucléaire avec l'Iran à Genève.

De tels événements appellent naturellement à se demander si nous en faisons suffisamment en Suisse pour nous protéger des cyberrisques. Or il n'y a pas de réponse simple à cette question. Il va de soi, comme les cyberrisques évoluent très vite, que nous sommes constamment confrontés à de nouveaux scénarios, et qu'il faut constamment revoir et adapter nos mesures de protection. Nous devons aussi renforcer la coopération tant nationale qu'internationale. Mais nous pouvons dire avec certitude que la Suisse n'est pas restée les bras croisés. Le Conseil fédéral a adopté en 2012 la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), et un an plus tard son plan de mise en œuvre. Il a défini comme objectifs stratégiques de la SNPC la détection précoce et précise des cyberrisques, leur réduction concrète et l'augmentation de la capacité de résistance de la Suisse à ces risques.

Le présent rapport 2015 vise à vous donner un aperçu de l'état des travaux, au cours de la troisième année de mise en œuvre de la SNPC. D'importantes avancées ont été réalisées dans tous les domaines. J'aimerais en particulier souligner la coopération accrue entre tous les protagonistes. Seule une collaboration loyale entre la Confédération, les cantons, l'économie et la société permettra de mieux protéger la Suisse face aux cyberrisques. La SNPC a déjà un succès à son actif, avec l'intensification de cette collaboration. Les responsabilités ont été définies grâce à la SNPC, qui garantit désormais que tous les acteurs tirent à la même corde.

Outre un bilan de ce qui a été réalisé, il convient de jeter ici un bref regard aux perspectives d'avenir. Nous poursuivrons à vive allure, en 2016, la mise en œuvre de la stratégie. En outre, il s'agira de mettre sur les rails les travaux de développement de la SNPC. Car l'actuelle stratégie est en vigueur jusqu'à la fin de 2017. Nous allons donc procéder cette année à une évaluation des forces et faiblesses de la SNPC, pour pouvoir soumettre au Conseil fédéral en 2017 une proposition concernant la marche à suivre.

Je vous souhaite une bonne lecture de ce rapport annuel, en me réjouissant de poursuivre une fructueuse collaboration avec tous les partenaires, afin que nous puissions tous, dans la mesure du possible, profiter de la numérisation, sans que la sécurité en pâtisse.

Peter Fischer
Délégué au pilotage informatique de la Confédération (UPIC)

1 Résumé

Le Conseil fédéral a approuvé la «Stratégie nationale de protection de la Suisse contre les cyberrisques» (SNPC) le 27 juin 2012 et son plan de mise en œuvre (plan de mise en œuvre de la SNPC) le 15 mai 2013. La SNPC, qui comprend seize mesures, se concentre sur la détection précoce des menaces et des dangers dans le cyberespace et sur l'augmentation de la capacité de résistance des infrastructures vitales. Elle vise également une réduction générale des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

La mise en œuvre de la SNPC est organisée de manière décentralisée. La responsabilité des travaux a été confiée à un office fédéral pour chacune des seize mesures. Le Conseil fédéral a mis en place un organe de coordination (OC SNPC) pour harmoniser les travaux. Celui-ci est rattaché à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), au sein de l'Unité de pilotage informatique de la Confédération (UPIC). La responsabilité globale incombe au comité de pilotage (CP SNPC), chargé d'accompagner la mise en œuvre lors d'un contrôle de gestion stratégique.

Les seize mesures portent sur quatre domaines: la prévention, la réaction, la continuité et les processus de soutien. D'importants objectifs ont été atteints dans tous les domaines au cours des dernières années, grâce notamment à l'étroite collaboration et à la bonne communication de tous les acteurs.

En matière de prévention, l'Office fédéral de la protection de la population (OFPP) et l'Office fédéral pour l'approvisionnement économique du pays (OFAE) ont procédé jusqu'ici à des analyses des risques et des vulnérabilités dans dix secteurs partiels (approvisionnement en gaz naturel; trafic routier; approvisionnement électrique; trafic aérien; approvisionnement en denrées alimentaires; soins médicaux et hôpitaux; banques; laboratoires; médias; protection civile). Pour identifier les risques, il faut à la fois connaître les vulnérabilités et bien évaluer les menaces actuelles. A cet effet, MELANI a développé un radar de situation interactif, permettant de visualiser les cybermenaces encourues par les infrastructures en Suisse et de juger à chaque fois de leur pertinence. Les rapports semestriels MELANI et le rapport annuel du SCOCI offrent un bon aperçu des principales cybermenaces en 2015.

En ce qui concerne la réaction, les centres de compétences destinés à analyser les logiciels malveillants (par ex. GovCERT.ch, CSIRT-OFIT et milCERT-DDPS) ont continué d'être renforcés, et de nombreux produits ont été mis au point. GovCERT a réalisé et mis en service plusieurs plateformes d'échange d'informations techniques. Elles servent au suivi des maliciels et permettent de les étudier de manière simple et efficace, sur une longue période, lorsqu'il est avéré que des systèmes ou des réseaux ont été manipulés (indicators of compromise, IOC). Les entreprises et organisations concernées peuvent ainsi être rapidement informées et mieux protégées. Les mesures d'identification des agresseurs font également partie de ce domaine. En l'occurrence, l'unité Cyber du Service de renseignement de la Confédération (SRC) a acquis des connaissances spécialisées et des aptitudes lui permettant d'analyser les objectifs, les méthodes et les acteurs d'une cyberattaque, ainsi que d'identifier les agresseurs potentiels.

Dans le domaine de la continuité, un premier projet renfermant les mesures à prendre pour améliorer la résilience, faisant suite à l'analyse des risques et des vulnérabilités, a vu le jour dans deux secteurs partiels, soit l'approvisionnement en gaz naturel et les médias. Dans les autres secteurs partiels, les rapports de mise en œuvre sont en cours d'élaboration selon le calendrier prévu.

Pour ce qui est des processus de soutien, l'accent est mis sur la recherche et la formation, ainsi que sur la collaboration internationale. Le Secrétariat d'Etat à la recherche, à la formation et à l'innovation (SEFRI) a institué un comité de pilotage interdépartemental qui coordonne et promeut au niveau national toutes les activités de recherche et de formation liées aux cyberrisques.

La collaboration internationale a continué d'être renforcée et étendue sur une base bilatérale et multilatérale, sous la conduite de la Division politique de sécurité (DPS) du Département fédéral des affaires étrangères (DFAE) et de l'Office fédéral de la communication (OFCOM). De plus, les contacts bilatéraux existants ont été intensifiés et de nouveaux contacts ont été noués. Au niveau multilatéral, les travaux liés aux mesures de confiance de l'Organisation pour la sécurité et la coopération en Europe (OSCE) ont été poursuivis.

Un examen de l'efficacité des seize mesures, confié à un organe externe et neutre, a débuté en janvier 2016. Ses résultats serviront au Conseil fédéral à se prononcer sur la marche à suivre, au début de 2017.

Principales cybermenaces en 2015

Les principales cybermenaces constatées en 2015 ont été les suivantes:

- **espionnage** (Duqu 2: espionnage des négociations avec l'Iran sur son programme nucléaire; Carbanak: hold-up en ligne; cyberattaque contre le Parlement allemand);
- **fuites d'information** (plus de 21 millions de données copiées sur les fonctionnaires américains [Office of Personnel Management]; Rex Mundi);
- **attaques contre les systèmes de contrôle industriels** (honeypot simulant une centrale hydroélectrique: 31 attaques; piratage de voitures);
- **usage de logiciels criminels** (chevaux de Troie bancaires comme Torpig, Dyre, Tinba, Gozi ou Zeus);
- **attaques DDOS** (TV5 Monde, Charlie Hebdo, vols de Polish Airlines supprimés);
- **chantage** (Cryptolocker: Cryptowall 3.0, Teslascript);
- **defacement** (défiguration de sites Web, après l'attentat contre Charlie Hebdo, par des sympathisants islamistes en France et en Suisse romande);
- **Social Engineering, phishing** (attaques contre des banques cantonales, vol de données de cartes de crédit).

2 Activités

Ce chapitre présente quelques activités ou manifestations importantes, ayant eu lieu au niveau national ou international.

2.1 Niveau national

Le Cyber 9/12 Student Challenge a eu lieu les 22 et 23 avril 2015 à Genève. L'Atlantic Council et le Geneva Centre for Security Policy (GCSP) étaient les hôtes de cette manifestation, où des étudiants d'universités basées aux Etats-Unis, en Grande-Bretagne, France, Pologne, Hongrie, Finlande, Estonie et Suisse devaient se préparer à une vaste cyberattaque et formuler des recommandations adéquates. L'équipe suisse s'est imposée lors de cette épreuve.

La troisième cyber-landsgemeinde s'est déroulée le 23 avril 2015. Quelque 80 responsables de la Confédération et de tous les cantons, et d'étroits partenaires du Réseau national de sécurité (RNS) ont participé à cette manifestation de réseautage. Comme les années précédentes, les discussions ont principalement porté sur l'état d'avancement des projets menés au niveau cantonal ou dans le cadre de la SNPC.

Du 19 au 22 octobre 2015, Lucerne a accueilli le troisième European Cyber Security Challenge. Dans cette compétition internationale, des écoliers ou étudiants venus d'Autriche, d'Allemagne, de Roumanie, de Grande-Bretagne, d'Espagne et de Suisse devaient découvrir, exploiter et corriger les vulnérabilités de systèmes informatiques. Les hôtes de la manifestation étaient l'association Swiss Cyber Storm, le DFAE et le Département fédéral des finances (DFF).

La deuxième conférence sur les cyberrisques en Suisse s'est tenue le 2 novembre 2015. Elle visait à donner aux représentants de l'économie et de la politique un aperçu détaillé de la mise en œuvre des mesures de la SNPC, ainsi qu'à favoriser l'échange d'informations entre les protagonistes de l'administration ou du secteur privé (exploitants d'infrastructures vitales notamment).

2.2 Niveau international

Les 16 et 17 avril 2015, La Haye a accueilli la conférence mondiale sur le cyberespace (Global Conference on Cyberspace, GCCS), qui s'est concentrée sur la création de normes étatiques de bonne conduite. Le conseiller fédéral Didier Burkhalter a inauguré la conférence en plaidant pour la mise en œuvre, dans le cyberespace, d'un système de règles de nature politique et juridique.

Un atelier de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) consacré à la sécurité des infrastructures d'importance vitale dans l'UE et en Suisse a été organisé les 29 et 30 septembre 2015. La Suisse était le seul pays non membre de l'UE représenté dans ce groupe de travail. La manifestation visait à comparer le niveau de protection des infrastructures vitales (processus, organisation, acteurs) en place dans quinze pays de l'UE et en Suisse. Les résultats ont été publiés sur le site de l'ENISA.

En 2015, la Suisse a participé à deux reprises au Sino-European Cyber Dialogue. Il s'agit d'un dialogue multilatéral noué entre des Etats européens et la Chine pour mieux comprendre les perceptions respectives des menaces et identifier les questions dont l'approfondissement présente un intérêt commun.

Une conférence de l'OSCE s'est tenue les 28 et 29 octobre 2015 à Belgrade, sous la présidence de la Serbie et avec la participation de la Suisse. Il y a principalement été question de la poursuite de l'approche multipartite, dans le contexte de la politique de sécurité. La conférence a été d'une grande utilité pour les Etats qui doivent se doter d'une

cyberstratégie nationale. En outre, la DiploFoundation a procédé à un premier exercice réel de grande dimension visant à renforcer la coopération interétatique à un forum multilatéral. La Suisse a activement soutenu cette conférence au niveau conceptuel et financier.

En 2015 également, le groupe spécialisé Cyber International (GS-CI) a veillé à assurer un flux systématique d'informations entre les services fédéraux intéressés, dans le but d'améliorer la cohérence et l'efficacité de la politique extérieure relative au cyberespace.

3 Etat de la mise en œuvre de la SNPC en 2015

La SNPC est une stratégie complète qui poursuit une approche globale à travers ses seize mesures (M1 à M16) et entend ainsi protéger la Suisse des cybermenaces. Ces mesures sont réparties dans quatre domaines, en fonction de leur déploiement dans le temps et de leurs dépendances:

- Prévention (M2, M3, M4)
- Réaction (M5, M6, M14)
- Continuité (M12, M13, M15)
- Processus de soutien (M1, M7, M8, M9, M10, M11, M16)

La SNPC est entrée dans sa troisième année de mise en œuvre, et la plupart des travaux concernant les mesures définies sont déjà bien avancés. Le présent chapitre propose une vue d'ensemble de la mise en œuvre (feuille de route). Les services responsables y exposent brièvement, à chaque fois, l'état actuel de la mise en œuvre des diverses mesures, regroupées par domaine.

Feuille de route SNPC

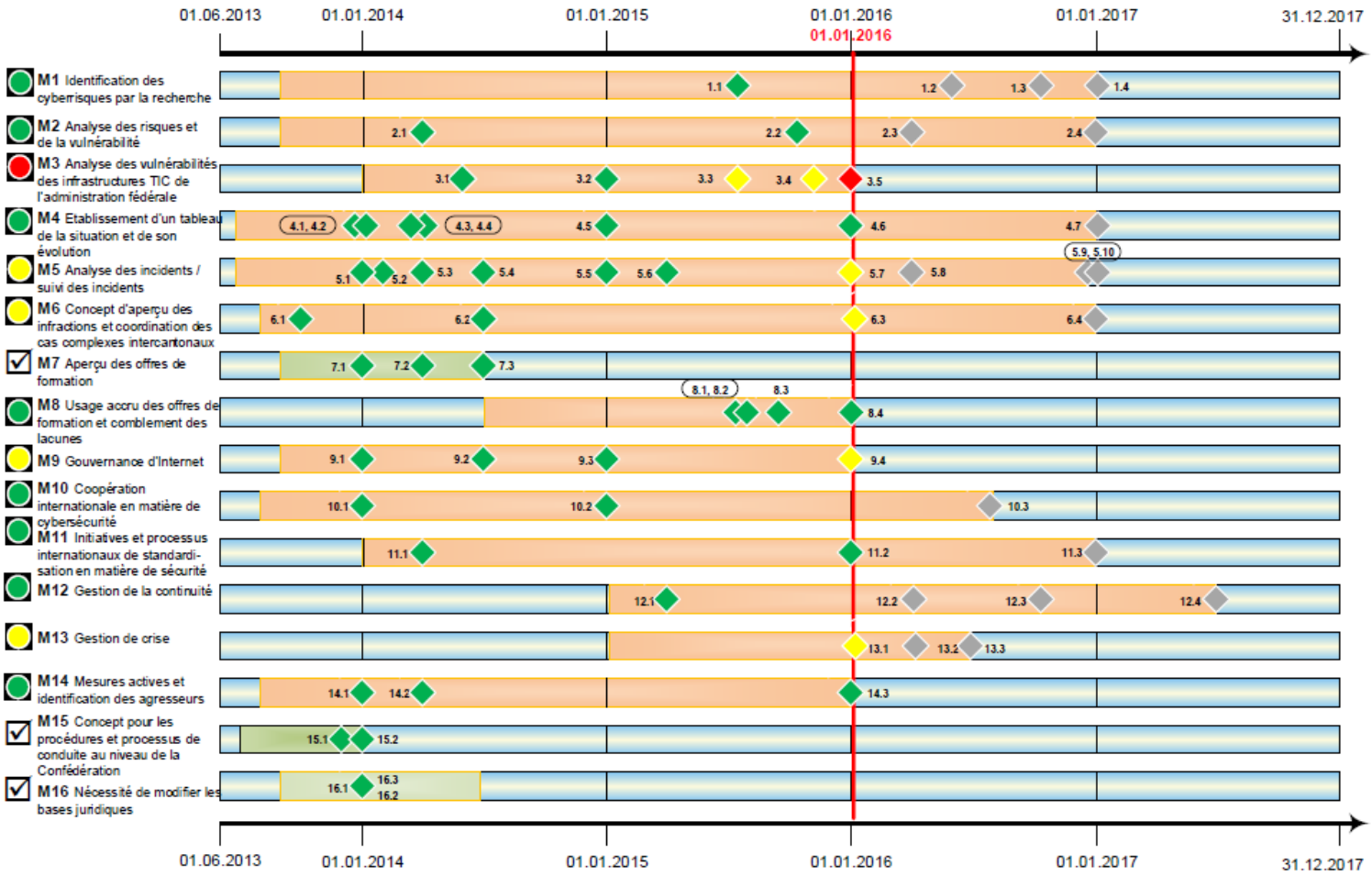

Illustration 1: Feuille de route SNPC

Légende: Etat des étapes

- Étape menacée
- Étape en retard
- Étape mise en œuvre selon le calendrier
- Étape mise en oeuvre pas encore commencer

3.1 Prévention

La prévention englobe les mesures suivantes: analyse des risques et vulnérabilités (M2), contrôle des vulnérabilités informatiques au sein de la Confédération (M3), et exposé de la situation (M4).

3.1.1 Mesure 2: analyse des risques et vulnérabilités

Compétence: DEFR-OFAE, DDPS-OFPP, autorités spécialisées; DFF-MELANI

Une analyse des risques et vulnérabilités vise à déterminer, pour la Suisse, les risques qui découlent des vulnérabilités informatiques des infrastructures d'importance vitale. Il existe des cyberrisques lorsque ces points faibles font l'objet de menaces (par ex. cyberattaques).

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) et l'Office fédéral de la protection de la population (OFPP) se partagent les travaux à réaliser dans les 28 secteurs partiels définis en Suisse et coordonnent leur approche. Les analyses des risques et vulnérabilités ainsi effectuées ont généralement respecté le calendrier. De nombreux experts issus des entreprises, des organisations de branche ou des services fédéraux compétents y ont participé. Les analyses bénéficient ainsi d'un large soutien, et ont confirmé le réel intérêt des services concernés.

Etat actuel:

En janvier 2016, les analyses des risques et de vulnérabilité étaient terminées dans dix secteurs partiels: approvisionnement en gaz naturel; trafic routier; approvisionnement électrique; trafic aérien; approvisionnement en denrées alimentaires; soins médicaux et hôpitaux; banques; laboratoires; médias; protection civile. En outre, les analyses sont en cours dans sept secteurs partiels: Parlement, gouvernement, justice, administration; armée; organisations de première intervention; eau potable; eaux usées; pétrole.

3.1.2 Mesure 3: analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale à l'aide d'un concept de contrôle

Compétence: DFF-UPIC; DFF-MELANI et OFIT, DDPS-BAC

Selon la SNPC, les services de la Confédération doivent examiner les vulnérabilités de leurs infrastructures informatiques en impliquant les fournisseurs de prestations dans ce domaine, ainsi que les fournisseurs de systèmes. L'Unité de pilotage informatique de la Confédération (UPIC) a été chargée d'élaborer d'ici à fin 2015 un concept de contrôle périodique des infrastructures informatiques de l'administration fédérale portant sur leurs faiblesses systémiques, organisationnelles et techniques.

Etat actuel:

Un concept de contrôle a été esquissé en vue de l'analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale. Il a été soumis en août au comité de pilotage (CP SNPC) pour consultation. La principale divergence apparue tenait à ce que le concept propose une méthode d'analyse des risques. La mesure 3 de la stratégie vise pourtant à proposer une méthode d'analyse des vulnérabilités. Divers membres du CP SNPC estiment par ailleurs que les travaux de mise en œuvre seraient trop lourds et doutent de surcroît qu'ils produisent le résultat espéré. Le CP SNPC se prononcera à sa sixième séance, prévue en février 2016, sur la suite des travaux concernant la mesure 3.

3.1.3 Mesure 4: établissement d'un tableau de la situation et de son évolution

Compétence: DFF-MELANI, DDPS-SRC, DFJP-SCOCI; DDPS-BAC et RM, DFF-OFIT

Pour contrer les cyberattaques, il faut un état des lieux qui informe des évolutions dans le cyberespace et qui décrive les risques et dommages potentiels de ces attaques dans chaque secteur d'importance vitale, ainsi que leur pertinence en Suisse.

Toutes les informations pertinentes, qu'elles proviennent d'analyses techniques, de sources des services de renseignement ou encore de sources policières, seront intégrées au tableau de la situation, afin qu'il soit le plus complet possible. D'où la nécessité de définir les processus entre acteurs, avec leur processus internes respectifs, en précisant les responsabilités de chacun. Les acteurs comprennent le Computer Emergency Response Team de MELANI à l'UPIC (GovCERT), l'Operation Information Center de MELANI au SRC (MELANI OIC), l'unité Cyber du SRC et le Service de renseignement militaire (RM). La SNPC vise à établir un tableau uniforme de la situation, en étroite collaboration avec tous les acteurs.

Etat actuel:

Les processus ont été recensés afin d'établir un tableau de la situation et de préciser les procédures organisationnelles, le rythme de conduite ainsi que les responsabilités respectives de MELANI-UPIC/GovCERT, MELANI-OIC et Cyber SRC. En outre l'unité Cyber du SRC, chargée de traiter les informations pertinentes du Service de renseignement, a étendu ses capacités et ses connaissances spécialisées (but et méthode d'une cyberattaque, analyse de la menace, provenance de l'agresseur). De même, les capacités techniques de la Base d'aide au commandement (BAC) de l'Armée suisse ont été mises à contribution pour soutenir le SRC. Un accord sur les niveaux de service (service level agreement, SLA) a été signé à cet effet. Par ailleurs, des processus ont été définis et introduits entre MELANI et les services compétents de l'OFAE et de l'OFPP. Enfin, les adaptations opérationnelles requises pour mettre en œuvre la mesure 15 de gestion des crises sont presque achevées, si bien qu'il sera possible de tester au niveau opérationnel les processus de gestion des crises lors d'exercices internationaux.

3.2 Réaction

Il faut procéder à l'analyse coordonnée et au suivi des incidents, de façon à réagir le plus vite possible le cas échéant. La SNPC prévoit une extension des capacités et une hausse de la réactivité des organisations et acteurs participants. Cela garantit une analyse rapide des incidents, une poursuite pénale efficace et une identification plus diligente des auteurs. Les mesures suivantes sont prévues dans le domaine de la réaction: analyse et suivi des incidents (M5), vue d'ensemble des infractions et coordination des cas intercantonaux complexes (M6), et mesures actives d'identification des agresseurs (M14).

3.2.1 Mesure 5: analyse et suivi des incidents

Compétence: DFF-MELANI, DDPS-SRC; DDPS-BAC et RM, DFF-OFIT

La capacité à se préparer et à réagir aux cyberincidents est une condition essentielle de la réduction des cyberrisques. Le plan de mise en œuvre de la SNPC prévoit, dans le cadre de l'analyse de la menace, l'analyse et le suivi des incidents ainsi que le développement de mesures adéquates. Les divers centres d'alerte et de réaction aux attaques informatiques (GovCERT, CSIRT-OFIT, milCERT-DDPS) doivent renforcer leurs capacités d'analyse des maliciels, afin de pouvoir traiter les données en cas d'incident et adopter les contre-mesures indiquées sur le plan technique. L'accomplissement de ce mandat exige en premier lieu un

renforcement des capacités techniques et des connaissances spécialisées, de même qu'une analyse exhaustive et une évaluation des menaces. S'ajoutent à cela un renforcement de l'endurance et de la capacité de réaction de tous les CERT, de même qu'un réseautage plus marqué de ces derniers.

Etat actuel:

En 2015 le GovCERT a réalisé et mis en service deux plateformes d'échange d'informations techniques sur les cybermenaces. Toutes deux se basent sur le logiciel libre MISP (Malware Information Sharing Plattform).

Un projet pilote a été réalisé avec des membres spécialement choisis du cercle fermé de MELANI (secteur énergétique et secteur financier). Il permet aux organisations et au GovCERT de rechercher de manière simple et efficace, sur une longue période, les manipulations (indicators of compromise, IOC) des systèmes ou réseaux informatiques.

En outre, diverses plateformes mises en service permettent de procéder au suivi du phishing et des attaques de maliciels, afin d'informer et de protéger les entreprises ou organisations concernées. Il convient notamment de citer antiphishing.ch. Ce nouveau site Web permet aux particuliers et aux entreprises d'annoncer commodément à MELANI les adresses URL utilisées dans un but de phishing. Les informations ainsi collectées sont exploitées statistiquement et servent à établir un bilan technique de la situation.

Le GovCERT a encore accru sa capacité d'analyse et de résistance, grâce à la création d'un poste supplémentaire.

3.2.2 Mesure 6: concept de vue d'ensemble des infractions et de coordination des cas intercantonaux complexes

Compétence: DFJP-SCOCI; DFF-MELANI

Une poursuite pénale nationale et internationale efficace s'impose en matière de lutte contre la cybercriminalité pour réduire durablement les cyberrisques. A cette fin, la SNPC prévoit (M6) que le SCOCI, rattaché au Département fédéral de justice et police (DFJP), présente d'ici à fin 2016, en collaboration avec les cantons, un concept intitulé «Vue d'ensemble des infractions et coordination des cas intercantonaux complexes».

Etat actuel:

Le concept a été élaboré et soumis pour consultation en 2015 aux autorités de poursuite pénale de la Confédération et des cantons. L'actuel projet de concept tient compte des remarques matérielles formulées par les services consultés.

Outre ce concept, fedpol a établi en collaboration avec le Ministère public de la Confédération (MPC) des fiches phénoménologiques portant sur la cybercriminalité (25 phénomènes). Elles décrivent les diverses formes de cybercriminalité, les agresseurs, les moyens ou méthodes d'attaque, les cibles et aussi le degré de complexité technique. Ces fiches sont déterminantes pour la définition concrète de la cybercriminalité en Suisse.

La consultation a notamment confirmé que les autorités de poursuite pénale privilégient un enregistrement centralisé des infractions relevant de la cybercriminalité, afin d'établir un aperçu national des cas découverts. Les phénomènes recensés dans le cadre de la mesure 6 ont été pris en compte dans les travaux actuels de l'organisation Harmonisation de l'informatique policière (HIP). D'où la garantie qu'indépendamment des systèmes utilisés, il sera possible d'enregistrer de manière centrale tous les cas relevant de la cybercriminalité.

En parallèle aux travaux conceptuels liés à la mesure M6 de la SNPC, la Conférence des commandants des polices cantonales de Suisse (CCPCS) et fedpol préparent une stratégie nationale globale couvrant tous les aspects de la répression de la cybercriminalité. Cette stratégie Cybercrime englobera le travail d'enquête proprement dit, ainsi que les questions

d'organisation, d'infrastructure et de formation. Elle devra notamment préciser, le moment venu, les modalités de mise en œuvre des mesures ou estimations des besoins faisant l'objet de la mission du SCOCI ou figurant dans le rapport relatif à la mesure 6.

3.2.3 Mesure 14: mesures actives d'identification des agresseurs

Compétence: DDPS-SRC; DFF-MELANI, DFJP-SCOCI, DDPS-RM

La SNPC entend renforcer les capacités du Service de renseignement de la Confédération (SRC) en matière d'identification des auteurs d'un acte (analyse des acteurs et du contexte, développement de moyens auxiliaires techniques). Une collaboration étroite entre les acteurs concernés (MELANI, SRC, SCOCI, Cyber SRC et, accessoirement, l'armée) est nécessaire à cet égard.

Etat actuel:

Le SRC a créé la division Cyber SRC, ayant pour fournisseurs de prestations la BAC et le Service de renseignement militaire (RM), afin de disposer de connaissances et d'aptitudes spécifiques au cyberespace. Les interfaces entre Cyber SRC et MELANI ont été mises en place, et l'échange d'informations a débuté. Cyber SRC a su élargir ses compétences et son savoir, et tisser un vaste réseau de contacts et de sources d'information. Fort de ce bagage à sa disposition, Cyber SRC parvient à détecter de bonne heure, de lui-même ou avec la BAC et le RM, ses fournisseurs de prestations, les cyberattaques visant les intérêts suisses. Ces découvertes sont ensuite reprises dans l'analyse de l'état actuel de la menace faite par MELANI. La BAC et le RM ont également développé, grâce à la SNPC, leur expertise technique et analytique ainsi que leurs connaissances des enjeux militaro-stratégiques du cyberespace.

3.3 Gestion de la continuité et des crises

La gestion des crises requiert des procédures et des processus de gestion clairement définis pour les cyberincidents. La gestion de la continuité vise quant à elle à garantir le maintien des processus d'affaires même en cas de crise. La continuité englobe les mesures suivantes: gestion de la continuité et amélioration de la résilience des secteurs partiels (M12), coordination des activités avec les acteurs directement concernés et appui des processus décisionnels par l'expertise requise (M13), ainsi que concept pour les procédures et processus de conduite incluant les aspects cybernétiques (M15).

3.3.1 Mesure 12: gestion de la continuité et amélioration de la résilience des secteurs partiels

Compétence: DEFR-OFAE, DDPS-OFPP, autorités spécialisées; DFF-MELANI

En se fondant sur les résultats de l'analyse des risques et vulnérabilités, l'OFAE ou l'OFPP en leur qualité de chefs de file définissent, en collaboration avec les entreprises concernées et les services spécialisés compétents, les mesures nécessaires pour assurer la continuité. Sur la base de l'analyse des risques et des vulnérabilités, un rapport renfermant des mesures concrètes est établi pour chacun des 28 secteurs partiels.

Etat actuel:

Dans le domaine de l'approvisionnement en gaz naturel, un premier projet de catalogue de mesures a été établi et soumis à l'organe de coordination de la SNPC. Les entreprises concernées établiront un service de permanence commun (24 heures sur 24 et 7 jours sur 7), rapidement opérationnel dans toute la Suisse en cas de cyberincident. En outre, elles se procureront le système de communication d'urgence Polycom et adhéreront au cercle fermé

de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

Le trafic routier étant peu vulnérable, aucune mesure n'a été proposée jusqu'ici. Il s'agit plutôt d'observer les développements actuels (par ex. informatique embarquée dans les véhicules), afin de les réévaluer lors des analyses périodiques de la vulnérabilité.

Le domaine des médias aura droit à son propre groupe dans le cercle fermé de MELANI. En outre, certaines entreprises envisagent de créer des sites redondants. Il s'agira encore d'observer l'évolution dynamique du paysage médiatique (par ex. nouvelles technologies de diffusion), et de l'évaluer périodiquement à la lumière des vulnérabilités et risques récents.

Dans les autres secteurs partiels, où les travaux devraient s'achever en janvier 2016, l'analyse des risques et des vulnérabilités a également permis d'identifier de premières mesures possibles. Elles sont en cours d'examen auprès des services compétents et des autorités spécialisées, et seront exposées plus en détail dans le rapport prévu pour chaque secteur partiel.

3.3.2 Mesure 13: coordination des activités avec les acteurs directement concernés et soutien grâce à l'expertise requise

Compétence: DEFR-OFAE, DFF-MELANI, DDPS-OFPP; DFAE-PD, DFJP-SCOCI

MELANI assure en cas de crise son appui subsidiaire aux acteurs concernés, en leur offrant son expertise. MELANI soutient l'échange volontaire d'informations entre les exploitants d'infrastructures vitales, les fournisseurs de prestations informatiques et les fournisseurs de systèmes concernés, afin de renforcer la continuité et la capacité de résistance selon le principe de l'auto-assistance. Pour cela, les prestations actuellement disponibles ne sont pas seulement garanties mais également développées.

Dans les cas susceptibles d'avoir des implications de politique étrangère, le DFAE sera informé et associé à l'élaboration d'une planification préventive.

Etat actuel:

MELANI a mené une enquête en ligne dans son cercle fermé, pour mieux cerner les besoins des acteurs concernés. Les résultats en cours d'évaluation serviront de base pour développer ou adapter les produits et services de MELANI. Le concept visant à renforcer MELANI comme plateforme d'échange d'information a été consolidé et ajusté, et son extension est prévue, en réponse aux besoins de gestion de la continuité des secteurs partiels.

3.3.3 Mesure 15: concept pour les procédures et processus de conduite incluant les aspects cybernétiques

Compétence: ChF

La mesure15 vise à inclure les aspects cybernétiques dans la gestion générale des crises déjà en place.

Etat actuel:

Cette mesure a pris fin en 2014.

La mesure 15 s'est terminée au niveau de la Confédération avec l'adoption d'un concept pour les procédures et processus de conduite incluant les aspects cybernétiques. Mais la

collaboration avec les cantons et les exploitants d'infrastructures vitales s'est poursuivie, dans le cadre de la mise en œuvre de la SNPC incombant au Réseau national de sécurité, au sein du groupe de travail 3 Gestion des crises. Les activités de ce groupe de travail ont également leur place dans le rapport annuel sur la SNPC. Les détails sont résumés au chapitre 3.6.

3.4 Processus de soutien

Les coopérations internationales, le développement des compétences par la formation et la recherche et, le cas échéant, l'adaptation des dispositions légales constituent les bases et processus nécessaires pour aborder la problématique de la cybernétique. Les trains de mesures suivants ont été définis à cet effet:

- Recherche et formation des compétences: (M1, M7, M8)
- Coopérations internationales: (M9, M10, M11)
- Bases légales: (M16)

3.4.1 Mesure 1: identification des cyberrisques par la recherche

Compétence: SEFRI; OC SNPC

La recherche doit permettre d'identifier les cyberrisques pertinents à venir, de même que les changements de la configuration des menaces, afin que les décisions politiques et économiques puissent être prises à temps dans une perspective d'avenir. A cet effet, la recherche (tant fondamentale qu'appliquée) est encouragée dans le domaine de la protection contre les cyberrisques. Le Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI) est responsable de la mise en œuvre, en collaboration avec l'organe de coordination de la SNPC (OC SNPC).

Etat actuel:

En janvier 2015, le SEFRI a mis en place le Comité de pilotage Recherche et Formation Cyber (CoPiRFCyber). Ce comité interdépartemental est formé de représentants de tous les organes de l'administration fédérale intéressés par les questions de recherche et de formation dans le domaine des cyberrisques. Il vise à définir la direction à suivre pour les travaux de recherche et les principaux thèmes dans un horizon de 5, 10 ou 20 ans (recherche fondamentale et recherche appliquée).

Le CoPiRFCyber a nommé, pour le soutenir dans sa tâche, un groupe d'experts formé de quatorze spécialistes de l'enseignement, de la recherche ou de la pratique actifs dans le domaine des cyberrisque. Ce groupe d'experts s'est mis au travail en janvier 2016.
En outre, le SEFRI organise une conférence pour le lancement de la recherche sur les cyberrisques en Suisses, qui permettra d'associer d'autres spécialistes aux travaux du groupe d'experts. La Swiss Cyber Risk Research Conference (SCRRC) aura lieu le 20 mai 2016 au Swiss Tech Convention Center de l'Ecole polytechnique fédérale de Lausanne.[1]

3.4.2 Mesure 7: aperçu des offres de formation

Compétence: OC SNPC; DETEC-OFCOM, DFAE-PD, DFI-OFAS

Le renforcement de la cyberrésilience en Suisse exige que l'on consolide ou crée des compétences spécifiques ciblées. D'après la SNPC, il faut élaborer une vue d'ensemble des

[1]Pour en savoir plus sur cette manifestation, voir le site www.scrrc.ch (dès février 2016).

offres existantes en matière de formation des compétences afin d'identifier les lacunes et de les combler. La mesure est étroitement coordonnée avec la mise en œuvre de la «Stratégie du Conseil fédéral pour une société de l'information en Suisse» et avec le Département fédéral des affaires étrangères (DFAE).

Etat actuel:
La mesure s'est achevée en 2015, avec la publication du rapport «Offres de formation dans le domaine des cyber-risques»[2]. Ce rapport se fonde sur des interviews de 40 experts. Il indique quelles offres sont prises en compte par quels groupes d'utilisateurs, et où l'offre reste lacunaire. Les experts ont notamment relevé des déficiences en matière de culture de la sécurité, ainsi que l'absence de passerelle entre les spécialistes de l'informatique et les décideurs. Ils ont également mentionné, pour des domaines spécifiques, qu'il n'existait pas d'offre de formation sur la sécurité technique (par ex. pour l'exploitation d'un CERT). Dans le domaine de la justice et de la police, plusieurs experts ont déploré l'absence de formation combinée en droit et en forensique, et plus généralement de sensibilisation aux cyberrisques.

La mesure 8 servira à combler les lacunes constatées au niveau de l'offre.

3.4.3 Mesure 8: usage accru des offres de formation et comblement des lacunes

Compétence: OC SNPC; SEFRI, DFAE-PD

La mesure 8 entend, d'une part, développer les offres existantes en matière de formation des compétences à la gestion des cyberrisques et, d'autre part, combler les lacunes identifiées dans ce domaine. La promotion de la formation est étroitement coordonnée avec celle de l'éducation en matière de cyberrisques, et se fonde sur les résultats de la mesure 7.

Etat actuel:

Le DFAE a donné en 2015 un mandat de recherche de l'administration portant sur la cybersécurité à l'étranger (publication sous http://www.diplomacy.edu/cybersecurity). L'étude examine de près les différentes mesures prises par dix Etats choisis de l'Organisation de coopération et de développement économiques (OCDE) pour renforcer la formation en matière de cybersécurité (par ex. dans les hautes écoles, au moyen de programmes de perfectionnement professionnel, etc.). Les approches ainsi identifiées pourront inspirer des activités potentielles lancées en Suisse dans le cadre de la mesure 8.

En raison des liens étroits existant entre les thèmes de la recherche et de la formation, le SEFRI a décidé avec l'OC SNPC d'aborder également la formation dans le cadre du Comité de Pilotage Recherche et Formation Cyber (CoPiRF Cyber, voir mesure 1). Le but tant de promouvoir la formation dans les hautes écoles, en parallèle à la recherche.

En outre, des travaux visant à encourager la formation professionnelle sont menés avec l'association ICT-Formation professionnelle Suisse. L'idée est ici de créer un diplôme fédéral d'expert en sécurité informatique. Les entretiens sont en cours avec les parties intéressées, et l'association ICT-Formation professionnelle Suisse se prononcera au printemps 2016 sur la faisabilité d'un tel diplôme.

3.4.4 Mesure 9: gouvernance d'Internet

Compétence: DETEC-OFCOM; DFAE-PD, DDPS-POLSEC, DFF-MELANI, autorités

[2] Le rapport est téléchargeable sur la page consacrée à la Société de l'information en Suisse: http://www.bakom.admin.ch/themen/infosociety/04837/index.html?lang=fr

spécialisées

La mesure 9 de la SNPC prévoit que la Suisse (économie, société et autorités) s'engage activement, et de la manière la plus coordonnée possible, en faveur d'une gouvernance d'Internet compatible 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. L'OFCOM est chef de file et participe aux processus internationaux et régionaux concernés tels que l'ICANN (Internet Cooperation for Assigned Names and Numbers, ou Société pour l'attribution des noms de domaine et des numéros sur Internet), le SMSI (Sommet mondial sur la société de l'information), la Commission (de l'ONU) de la science et de la technique au service du développement (CSTD), le FGI (Forum [de l'ONU] de la gouvernance de l'Internet) et le Conseil de l'Europe.

Etat actuel:

L'OFCOM a pris une part active aux travaux du comité consultatif gouvernemental de l'ICANN (Government Advisory Committee, GAC), dont la Suisse assure la présidence. Les activités déployées dans ce contexte, auxquelles le DFAE participait également, se sont concentrées sur le transfert de la surveillance exercée sur les fonctions de l'IANA, ainsi que sur le renforcement de la responsabilisation (accountability). En outre, la Suisse s'est engagée pour l'adoption de mesures propres à renforcer la sécurité et la fiabilité des nouveaux domaines de premier niveau (TLD). Dans le cadre des contrôles de la mise en œuvre des résultats du SMSI, la Suisse a participé avec une délégation de l'OFCOM et du DFAE aux préparatifs de la réunion de haut niveau de l'Assemblée générale des Nations Unies, organisée en décembre 2015 à New York, qui a marqué la fin des travaux.

L'OFCOM a également participé à la préparation et à l'organisation du Forum sur la gouvernance d'Internet (FGI), en tant que cofondateur et coorganisateur du forum de dialogue européen du FGI EuroDIG (European Dialogue on Internet Governance). L'OFCOM siège encore avec le DFAE au groupe de pilotage de la Geneva Internet Platform, dont il soutient les travaux.

Sur le plan national, l'OFCOM organise régulièrement la «Plateforme tripartite suisse pour le SMSI», qui permet à tous les groupes intéressés (administration fédérale, société civile, universitaires) d'échanger des informations sur des sujets d'actualité et des évolutions concernant Internet. Il a ainsi organisé, en mai 2015, le premier Swiss IGF (Swiss Internet Governance Forum), où un dialogue interactif entre les groupes d'intérêt a porté sur les questions de gouvernance Internet.

3.4.5 Mesure 10: coopération internationale en matière de cybersécurité

Compétence: DFAE-PD; DDPS-POLSEC, DFF-MELANI, DETEC-OFCOM

La mesure 10 concerne la défense des intérêts sécuritaires en matière de cyberespace vis-à-vis de l'étranger. Par l'intermédiaire d'initiatives et de ses relations internationales, la Suisse participe aux efforts visant à éviter que le cyberespace ne soit utilisé de manière abusive à des fins criminelles, politiques, terroristes ou de renseignement.

Etat actuel:

En 2015, la Suisse a poursuivi son engagement pour la création d'un dispositif normatif destiné à régler, à l'aide d'instruments politiques et juridiques, l'utilisation et les frontières du cyberespace, ainsi qu'à concrétiser sa vision d'un cyberespace ouvert, libre et sûr.

Parmi les instruments politiques à disposition figure l'instauration d'une confiance mutuelle, gage de transparence, de coopération interétatique et de stabilité dans le cyberespace. La Suisse a pris une part active au processus de l'OSCE visant à créer un climat de confiance. En outre, elle a soutenu la présidence serbe de l'OSCE en vue de l'organisation d'une conférence ministérielle.

Quant à la création de normes étatiques de bonne conduite, la conférence mondiale sur le cyberespace organisée les 16 et 17 avril 2015 à La Haye a constitué le point fort des activités helvétiques. Le conseiller fédéral Didier Burkhalter a inauguré la conférence en plaidant pour la reprise, dans le cyberespace, des règles interétatiques du droit international en vigueur.

Une manifestation organisée par la Suisse à Genève en amont de la Conférence mondiale 2015 sur le cyberespace a servi à comparer les approches régionales et à promouvoir la coopération transrégionale.

Soucieuse de permettre ou faciliter la participation des pays en développement aux processus internationaux, la Suisse a financé des projets concrets de création ou renforcement des capacités dans le cyberespace. Elle est également membre fondateur du Forum mondial sur la Cyber Expertise (Global Forum on Cyber Expertise, GFCE), créé durant l'année sous revue et qui vise à promouvoir le développement des cybercapacités au niveau mondial.

Cette année aussi, la Suisse a participé activement au dialogue multilatéral noué entre des Etats européens et la Chine pour mieux comprendre les perceptions respectives des menaces et identifier les questions dont l'approfondissement présente un intérêt commun.

3.4.6 Mesure 11: initiatives et processus internationaux de standardisation en matière de sécurité

Compétence: DETEC-OFCOM; OC SNPC, autorités spécialisées, DFAE-PD, DFF-MELANI

La mesure 11 vise à renforcer la coordination et la coopération des experts en cybersécurité en Suisse pour optimiser l'engagement international de celle-ci auprès des organismes de normalisation et d'autres initiatives correspondantes.

Etat actuel:

En 2015, des échanges avec les acteurs concernés ont servi à fixer les domaines d'activité prioritaires, de façon à coordonner la standardisation et les initiatives internationales en matière de cybersécurité, ainsi qu'à ajuster les processus nécessaires à cette mesure. Les participants à la mise en œuvre de la M11 envisagent d'organiser à l'avenir un atelier public annuel, et en cas de besoin des projets de coordination seront organisés au sein de groupes spécialisés. Les processus et les domaines d'activité prioritaires ont été documentés et signalés à l'organe de coordination de la SNPC.

3.4.7 Mesure 16: nécessité de modifier les bases juridiques

Compétence: OC SNPC

La mesure 16 prévoit un réexamen du droit en vigueur afin de déterminer s'il comprend les bases nécessaires à la protection contre les cyberrisques et de procéder aux éventuelles adaptations requises. Les unités administratives doivent recenser les bases légales pertinentes dans leur domaine de tâches et évaluer les besoins en matière d'adaptations ou de compléments.

Etat actuel:

Les premières analyses ont pris fin en 2014. Les dernières évolutions n'ont fait naître aucun besoin de coordination en matière de réglementation. La situation continuera toutefois de faire l'objet d'une évaluation régulière.

3.5 Mise en œuvre par l'armée

L'armée fait partie des infrastructures vitales les plus exposées aux cybermenaces. Le développement rapide et l'importance croissante du cyberespace offrent de nouvelles options pour des opérations militaires, qu'il convient de ne pas négliger. Les principales tâches immédiates de l'armée englobent cependant la protection de ses systèmes et infrastructures informatiques dans toutes les situations, afin de garantir sa capacité et sa liberté d'action.

L'armée dispose de connaissances et d'aptitudes étendues auxquelles les offices responsables peuvent recourir de manière subsidiaire en cas de nécessité, pour autant que l'armée n'en ait pas elle-même besoin.

A cet effet, l'armée développe constamment ses connaissances et aptitudes. Ses prestations cybernétiques subsidiaires sont en cours de clarification, de même que son rôle en cas de guerre ou conflit. L'armée n'a pas pu se procurer les ressources humaines prévues pour l'année 2015, mais ce retard devrait être comblé en 2016.

Etat actuel:

Les repères doctrinaux pour les actions militaires dans le cyberespace ont été définis, ainsi que les principes méthodologiques de la gestion des cyberrisques. De même, d'importantes étapes ont été réalisées en ce qui concerne l'anticipation (à commencer par une cartographie des acteurs du secteur académique) et l'état de la situation cybernétique, et un Conseil consultatif a été désigné pour l'accompagnement des travaux. L'exercice «CYBER-PAKT 15», réalisé en 2015, constitue une étape importante dans le domaine de la gestion de crise et de la collaboration de l'armée avec ses partenaires. Les processus de traitement des cyberincidents ont par ailleurs été établis et vérifiés. D'où la disponibilité de base, dans l'armée de milice, d'un état-major apte à assurer la cyberdéfense du pays. Plusieurs actions de sensibilisation ont également été réalisées au profit des unités administratives et des formations de milice. Le concept d'instruction établi sera systématiquement déployé à partir de 2016, dès que les ressources le permettront.

3.6 Mise en œuvre par les cantons

Le MCC RNS est l'interface entre la SNPC et les cantons. Le groupe spécialisé Cyber du MCC RNS assure la coordination entre la Confédération et les cantons dans la mise en œuvre de la SNPC, en collaboration avec ceux-ci, les communes et les services fédéraux concernés. Il pilote quatre sous-projets ou groupes de travail. L'OC SNPC est membre du groupe spécialisé Cyber et joue, au niveau de la Confédération, le rôle de passerelle avec les cantons pour les travaux de projet.

Etat actuel:

Sur la base de la mesure 3 de la SNPC (concept de contrôle des vulnérabilités informatiques), les organisations participantes ont procédé à un examen autonome des cyberrisques. Suite à son évaluation, des mesures de réduction des risques ont été proposées. Conformément aux mesures 4 et 5 de la SNPC, le processus d'ensemble de traitement des cyberincidents a été établi et subdivisé en cinq processus partiels. Tant les processus partiels que la définition d'un incident de cybersécurité ont été mis à la disposition des cantons.
Le *concept pour les procédures et processus de conduite incluant les aspects cybernétiques* (mesure 15 de la SNPC) a été étendu aux cantons et aux infrastructures vitales. Un séminaire stratégique, organisé avec des représentants de la Confédération et de la plupart des cantons, ainsi qu'avec les exploitants d'infrastructures vitales, a servi à sa validation. Un scénario sur mesure de cyberattaque lancée contre le système de rentes suisse avait été mis au point. Les principaux thèmes abordés ont été l'appréhension des problèmes, les processus, les structures, les interfaces et les besoins.

4 Contrôle de gestion stratégique

Le Conseil fédéral a chargé le CP SNPC de suivre la mise en œuvre de la stratégie, grâce à un contrôle de gestion stratégique. Ledit contrôle vise à s'assurer tous les six mois, pour chaque mesure de la stratégie nationale de protection de la Suisse contre les cyberrisques, que les progrès sont conformes aux objectifs et aux délais fixés. Le Conseil fédéral reçoit des rapports à ce sujet par l'intermédiaire de la Conférence des secrétaires généraux (CSG), en vertu du plan de mise en œuvre de la SNPC du 15 mai 2013. La 5e séance de l'OC SNPC a eu lieu le 20 août 2015.

5 Evaluation de l'efficacité

Les travaux préparatoires en vue de l'évaluation de la SNPC ont débuté en 2015. L'évaluation aura lieu en 2016, afin que ses résultats puissent être soumis en avril 2017 au Conseil fédéral, qui décidera sur cette base de la poursuite de la SNPC.

Au printemps 2015, l'OC SNCP a élaboré avec une aide externe un concept détaillé pour l'évaluation de l'efficacité. Il s'agissait d'indiquer une méthode cohérente, de définir les questions concrètes et d'identifier les acteurs chargés d'y répondre. A sa séance du 20 août 2015, le CP SNCP a adopté le concept détaillé. Puis l'OC a confié le mandat à une entreprise qualifiée, lors d'une procédure invitant à soumissionner. La première séance de projet avec les fournisseurs a eu lieu en décembre.

L'évaluation de l'efficacité pourra ainsi débuter dans les délais, sur la base d'un concept bien étudié. Le défi reste néanmoins d'évaluer l'efficacité de la SNPC à un moment où beaucoup de mesures sont encore en phase de réalisation.

6 Considérations finales

La troisième année de travaux a confirmé à quel point la mise en œuvre de la SNPC est une entreprise vaste et complexe. Sachant que les menaces d'aujourd'hui ne correspondent pas à celles de demain, la SNPC doit être suffisamment flexible et constamment adaptée aux nouvelles menaces. En 2015, il a fallu remanier le calendrier et redéfinir certaines tâches. De tels changements visent toujours à garantir la qualité des travaux et des produits de la SNPC. Aujourd'hui déjà, les résultats sont censés déployer leurs effets au-delà de 2017. Les nouveaux processus définis font que la collaboration, les coopérations et les flux de communication entre acteurs se poursuivront à l'avenir et que d'autres acteurs peuvent être impliqués en cas de besoin. Ces facteurs ont occasionné de légers retards pour certaines mesures. Mais comme pour la plupart des mesures les travaux respectent le calendrier, le bilan établi à la fin de 2015 est lui aussi positif.

Face à l'augmentation du nombre de cyber-délits durant l'année sous revue, la coopération tant nationale qu'internationale est plus que jamais d'actualité. Au niveau national, l'accent est mis sur une collaboration empreinte de confiance avec les exploitants d'infrastructures vitales, l'économie et les cantons. De fructueux liens ont également été établis avec l'armée. Afin d'endurcir la Suisse, il faut intensifier encore les échanges d'informations avec les organisations policières et les parquets, ainsi qu'avec les exploitants d'infrastructures vitales, les fournisseurs informatiques et les producteurs de systèmes, les autorités spécialisées et les régulateurs.

La collaboration et les échanges d'informations pertinentes avec les Etats et les

organisations internationales s'avèrent eux aussi centraux. Il faut encourager et encadrer par des instruments tant politiques que juridiques la confiance mutuelle, prérequis à la transparence, à la coopération interétatique et à la stabilité dans le cyberespace. Ainsi seulement, on parviendra à une meilleure compréhension commune de la cybersécurité, et la confiance envers Internet progressera.

L'année 2016 amènera de nouveaux défis, nous obligeant à intensifier encore les collaborations ou coopérations d'aujourd'hui, de façon à intégrer tous les acteurs importants ou appelés à le devenir.

7 Annexes

7.1 Documents de base relatifs à la SNPC

«Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)»:
http://www.isb.admin.ch/themen/01709/01710/index.html?lang=fr

«Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques»:
http://www.isb.admin.ch/themen/01709/01711/index.html?lang=fr

«Rapport annuel 2013 du comité de pilotage de la SNPC»:
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=fr

«Rapport annuel 2014 du comité de pilotage de la SNPC»:
https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

7.2 Récapitulation des interventions parlementaires relatives aux cyberrisques

Intervention Ip. = Interpellation; Mo. = Motion; Po. = Postulat; Qu. = Question	Déposée le:	Etat au 31.12.2015:
08.3050 Po Schmid-Federer. Protection contre la cyberintimidation	11.03.2008	liquidé
08.3100 Mo. Burkhalter. Stratégie nationale de lutte contre la criminalité par Internet; délibérations du Conseil des Etats du 2 juin 2008 (BO CE 2.06.2008), rapport de la CPS-CN du 11 novembre 2008 et délibérations du Conseil national du 3 juin 2009 (BO CN 3.06.2009)	18.03.2008	liquidé
08.3101 Po. Frick. Criminalité informatique. Mieux protéger la Suisse	18.03.2008	liquidé
08.3924 Ip. Graber. Mesures contre la guerre électronique	18.12.2008	liquidé
09.3114 Ip. Schlüer. Sécurité Internet	17.03.2009	liquidé
09.3266 Mo. Büchler. Sécuriser la place économique suisse	20.03.2009	liquidé
09.3628 Po. Fehr HJ. Rapport sur Internet en Suisse	12.06.2009	liquidé
09.3630 Ip. Fehr HJ. Questions relatives à Internet	12.06.2009	liquidé
09.3642 Mo. Fehr HJ. Observatoire de l'Internet	12.06.2009	liquidé
10.3136 Po. Recordon. Evaluation de la menace de cyberguerre	16.03.2010	liquidé
10.3541 Mo. Büchler. Protection contre les cyberattaques	18.06.2010	liquidé
10.3625 Mo. CPS-CN. Mesures contre la cyberguerre; délibérations du Conseil national du 2 décembre 2010 (BO CN 2.12.2010), rapport de la CPS-CN du 11 janvier 2011 et	29.06.2010	liquidé

délibérations du Conseil des Etats du 15 mars 2011 (BO CE 15.03.2011)		
10.3872 Ip. Recordon. Risque de panne de grande ampleur du réseau électrique en Suisse	01.10.2010	liquidé
10.3910 Po. Groupe libéral-radical. Organe de direction et de coordination pour contrer les cybermenaces	02.12.2010	liquidé
10.4020 Mo. Glanzmann. MELANI pour tous	16.12.2010	liquidé
10.4028 Ip. Malama. Risque d'une cyberattaque contre les centrales nucléaires suisses	16.12.2010	liquidé
10.4038 Po. Büchler. Compléter le rapport sur la politique de sécurité en y ajoutant un chapitre sur la cyberguerre	16.12.2010	liquidé
10.4102 Po. Darbellay. Elaboration d'une stratégie visant à protéger l'infrastructure numérique de la Suisse	17.12.2010	liquidé
11.3906 Po. Schmid-Federer. Loi-cadre sur les TIC	29.09.2011	liquidé
12.3417 Mo. Hodgers. Marchés ouverts de la télécommunication. Stratégies pour la sécurité numérique nationale	30.05.2012	liquidé
12.4161 Mo. Schmid-Federer. Pour une stratégie nationale contre le cyberharcèlement	13.12.2012	liquidé
13.3228 Ip. Recordon. Système d'écoutes téléphoniques fédéral et carences générales de la Confédération en informatique et en télécommunication	22.03.2013	liquidé
13.3229 Ip Recordon. Ampleur de la menace et mesures de lutte contre la cyberguerre et la cybercriminalité	22.03.2013	liquidé
13.3558 Ip. Eichenberger. Cyberespionnage. Evaluation et stratégie	20.06.2013	liquidé
13.3677 Ip. Groupe socialiste. Certains services de renseignement étrangers, tels que la NSA, furètent-ils également en Suisse?	11.09.2013	
13.3692 Ip. Hurter. Marché des télécommunications. La législation et les mesures de régulation en vigueur font-elles encore sens?	12.09.2013	non encore traité au conseil
13.3696 Mo. Müller-Altermatt. Protection des données contre protection des fraudeurs	12.09.2013	non encore traité au conseil
13.3707 Po. Groupe BD. Stratégie cybernétique globale et adaptée aux exigences futures	17.09.2013	non encore traité au conseil
13.3773 Ip. Groupe libéral-radical. Pour une loi sur les télécommunications nous permettant d'affronter l'avenir. Elaborer une stratégie globale consacrée au cyberespace	24.09.2013	non encore traité au conseil
13.3841 Mo. Rechsteiner. Commission d'experts pour l'avenir du traitement et de la sécurité des données	26.09.2013	adopté
13.3927 Ip. Reimann. Protection des données en Suisse	27.09.2013	non encore traité au conseil
13.4009 Mo. CPS-CN. Mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques («Le Conseil fédéral est chargé d'accélérer la	05.11.2013	liquidé

mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques et de mettre en œuvre les seize mesures concrètes d'ici à la fin 2016.»)		
13.4077 Ip. Clottu. Espionnage de données et sécurité sur Internet	05.12.2013	liquidé
13.4086 Mo. Glättli. Programme national de recherche portant sur un système de protection des données applicable au quotidien dans la société de l'information	05.12.2013	non encore traité au conseil
13.4308 Po. Graf-Litscher. Améliorer la sécurité et l'indépendance de l'informatique suisse	13.12.2013	non encore traité au conseil
13.5224 Qu. Reimann. Cyberactivités des services secrets américains en Suisse	10.06.2013	liquidé
13.5325 Qu. Sommaruga. Le Service de renseignement de la Confédération utilise-t-il des données collectées illégalement par la NSA?	11.09.2013	liquidé
14.1105 Qu. Buttet. Moyens dédiés à la cyberdéfense dans la politique de sécurité de la Suisse	10.12.2014	liquidé
14.3654 Ip. Derder. Sécurité numérique. Faisons-nous fausse route?	20.06.2014	non encore traité au conseil
14.4138 Ip. Noser. Procédure d'adjudication pour les infrastructures TIC critiques de l'administration fédérale	10.12.2014	non encore traité au conseil
14.4299 Ip. Derder. Veille transversale de la révolution numérique. Faut-il créer un secrétariat d'Etat de la société numérique?	12.12.2014	non encore traité au conseil
14.5569 Qu. Leutenegger. Affaire Snowden. Ampleur des agissements des Etats-Unis	26.11.2014	liquidé
15.1059 Qu. Berberat. Aide financière d'urgence de la Confédération suite à la cyberattaque contre TV5 Monde	10.09.2015	liquidé
15.3359 Po. Derder. Pour une armée innovante	20.03.2015	non encore traité au conseil
15.3375 Ip. Subtilisation de codes SIM par la NSA et le GCHQ auprès de la société Gemalto	20.03.2015	liquidé
15.3656 Ip. Munz. La télémaintenance des systèmes informatiques représente un danger pour la centrale nucléaire de Mühleberg. Surveillance de l'IFSN remise en cause	18.06.2015	non encore traité au conseil
15.4073 Ip. Derder. L'armée est-elle réellement capable de protéger l'espace cybernétique helvétique?	25.09.2015	non encore traité au conseil
15.5299 Qu. Leutenegger. Protection contre l'espionnage de la NSA	09.06.2015	liquidé

7.3 Liste des abréviations

AE	Approvisionnement économique du pays
BAC	Base d'aide au commandement
BAC COE	Base d'aide au commandement – centre des opérations électroniques
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandants des polices cantonales de Suisse

CdA	Chef de l'armée
CERT	Computer Emergency Response Team
ChF	Chancellerie fédérale
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CP SNPC	Comité de pilotage de la Stratégie nationale de protection de la Suisse contre les cyberrisques
CPEA	Conseil de partenariat euro-atlantique
CSG	Conférence des secrétaires généraux
CSIRT	Computer Security Incident Response Team
CSTD	Commission de la science et de la technique au service du développement
CTI	Commission pour la technologie et l'innovation
Cyber SRC	Unité Cyber du Service de renseignement de la Confédération
D	Défense
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DDPS-POLSEC	Département fédéral de la défense, de la protection de la population et des sports – domaine Politique de sécurité
DEFR	Département fédéral de l'économie, de la formation et de la recherche
DETEC	Département fédéral de l'environnement, des transports, de l'énergie et de la communication
DFAE	Département fédéral des affaires étrangères
DFAE-DOI	Département fédéral des affaires étrangères – division Organisations internationales
DFAE-PD	Département fédéral des affaires étrangères – direction politique
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Département fédéral de justice et police
DPS	Division Politique de sécurité
ENISA	European Network and Information Security Agency Agence européenne chargée de la sécurité des réseaux et de l'information
ERNS	Exercice du Réseau national de sécurité
Fedpol	Office fédéral de la police
FGI	Forum sur la gouvernance de l'Internet
GAC	Government Advisory Committee Comité consultatif gouvernemental
GCHQ	Government Communications Headquarters
GI	Gouvernance d'Internet
GIP	Geneva Internet Platform
GovCERT	Swiss Governmental Computer Emergency Response Team
GS-C	Groupe spécialisé Cyber
GS-CI	Groupe spécialisé Cyber International
ICANN	Internet Cooperation for Assigned Names and Numbers
KS CYD	Konzeptionsstudie Cyber Defence Etude conceptuelle sur la cyberdéfense
LR	Loi sur le renseignement
MCC RNS	Mécanisme de consultation et de coordination du Réseau national de sécurité
MDC	Mesures de confiance
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MilCERT	Computer Emergency Response Team militaire
NSA	National Security Agency
OC SNPC	Organe de coordination de la Stratégie nationale de protection de la Suisse contre les cyberrisques
OFAE	Office fédéral pour l'approvisionnement économique du pays

OFAS	Office fédéral des assurances sociales
OFCOM	Office fédéral de la communication
OFCOM-IR	Office fédéral de la communication – service des Affaires internationales
OFEN	Office fédéral de l'énergie
OFIT	Office fédéral de l'informatique et de la télécommunication
OFPP	Office fédéral de la protection de la population
OIC de MELANI	Operation Information Center de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information
ONU	Organisation des Nations Unies
OSCE	Organisation pour la sécurité et la coopération en Europe
OTAN	Organisation du traité de l'Atlantique Nord
Plan de mise en œuvre de la SNPC	Plan de mise en œuvre de la Stratégie nationale de protection de la Suisse contre les cyberrisques
RM	Service de renseignement militaire
RNS	Réseau national de sécurité
SCOCI	Service de coordination de la lutte contre la criminalité sur Internet
SEFRI	Secrétariat d'Etat à la formation, à la recherche et à l'innovation
SG DDPS	Secrétariat général du Département fédéral de la défense, de la protection de la population et des sports
SLA	Service Level Agreement Accord sur les niveaux de service
SMSI	Sommet mondial sur la société de l'information
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération
Stratégie PIC	Stratégie pour la protection des infrastructures critiques
TIC	Technologies de l'information et de la communication
UPIC	Unité de pilotage informatique de la Confédération
UPIC-SEC	Unité de pilotage informatique de la Confédération – division Sécurité