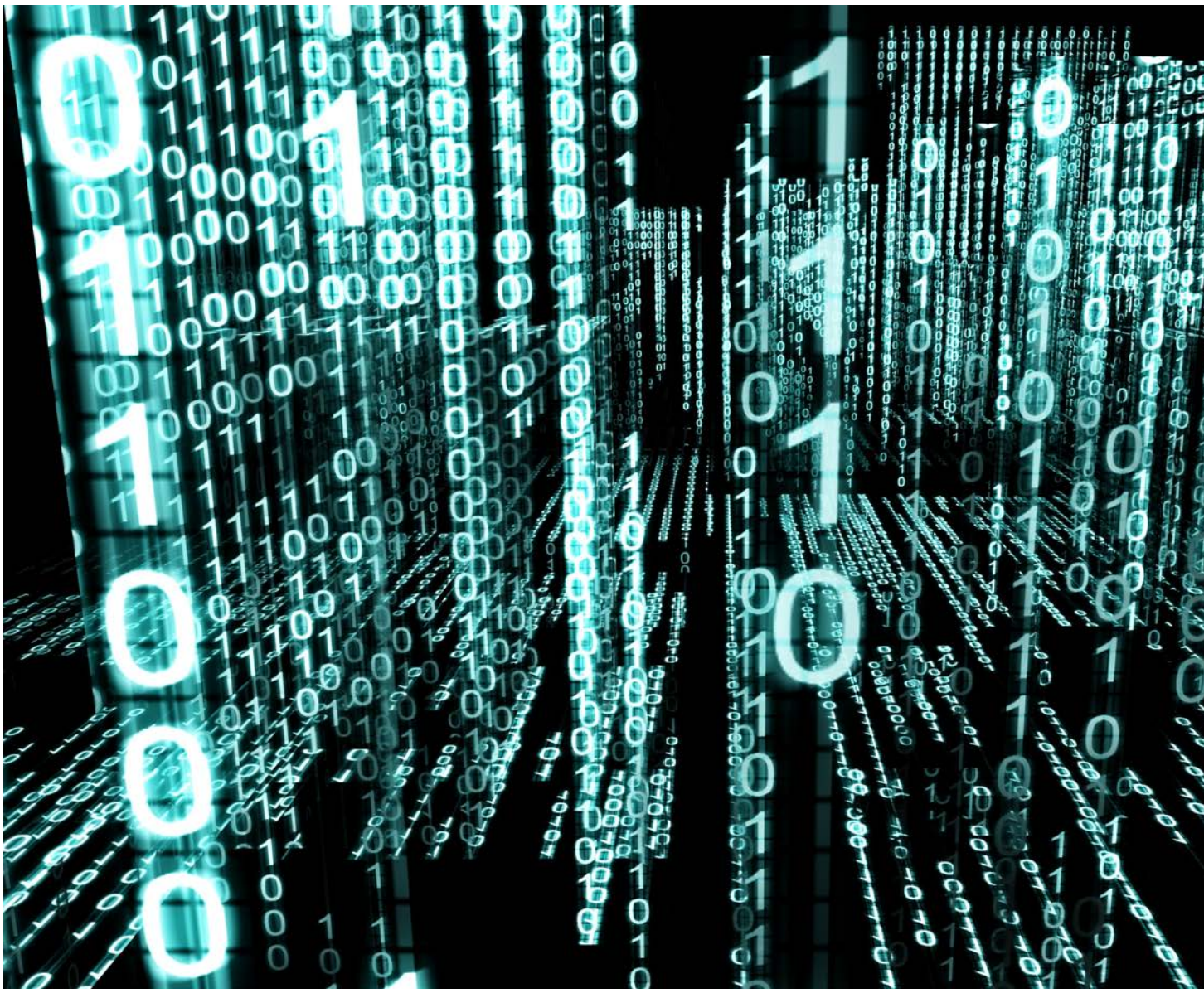
Mai 2014 | www.isb.admin.ch

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

Rapport annuel 2013 du comité de pilotage de la SNPC



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Publication: Mai 2014

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)31 322 45 38
info@isb.admin.ch

Rapport annuel: www.isb.admin.ch/...

Table des matières

Préface

Ces dernières années, Internet s'est mué en un lieu de vie important sur le plan social et économique. Son utilisation constitue un pilier essentiel en matière de liberté, de production, de négoce, d'information et d'auto-détermination. Tout le monde connaît et utilise Internet et souhaite y prendre une part active. Les principales capitalisations boursières concernent d'ailleurs des entreprises du Web. Toutefois, comme dans la vie réelle, cet espace virtuel recèle des dangers: les attaques, la criminalité, ainsi que les intérêts géopolitiques et étatiques y sont devenus réalité. Le Conseil fédéral a identifié ces dangers. En approuvant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et son plan de mise en œuvre, il a posé les bases pour relever le défi de la sécurité du Web. Cette stratégie décrit les mesures et les mécanismes à mettre en place en vue d'une utilisation paisible et libre du Web à tous les niveaux de la société en Suisse. Il s'agit, d'une part, de sensibiliser tous les acteurs concernés dans le pays – et ils sont nombreux compte tenu de la nature même d'Internet – et, d'autre part, de leur permettre d'assumer leurs responsabilités et de réduire les cyberrisques ou leurs effets dans le cadre de la gestion des risques.

La mise en œuvre de la stratégie repose sur seize mesures. Un petit organe de coordination au sein de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) veille à une application harmonisée. On s'assure ainsi de la prise en compte de toutes les parties prenantes et de la réalisation d'un objectif commun: la sécurité sur Internet. Ces mesures visent à établir une cartographie générale des cybermenaces en Suisse et à contrer les cyberattaques critiques. Ces menaces sont variées et les technologies très complexes; les milieux politiques et économiques doivent donc s'adapter à ces nouveaux phénomènes. Le système mondial qu'est Internet continuera de se développer à mesure que la technique et la mise en réseau poursuivront leur progression.

Le premier rapport annuel sur la mise en œuvre de la SNPC fournit une vue d'ensemble des menaces, ainsi que des mesures adoptées et de leur avancement. Il montre les interdépendances qui caractérisent cette problématique et souligne la responsabilité de toutes les parties prenantes. La stratégie a déclenché un vaste mouvement, que ces dernières doivent désormais exploiter dans un but commun. Les bases sont posées, et les attentes en la matière élevées.

1 Résumé

Réelles et variées, les cybermenaces ont fortement augmenté ces dernières années. De nouveaux acteurs, mieux organisés, ont également fait leur apparition. Le rapport semestriel 2013/I de MELANI et le rapport annuel 2013 du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI) présentent brièvement ces nouveaux acteurs et les principales tendances en matière de cybercriminalité en Suisse et sur le plan international. Ils évaluent ces menaces et recommandent des mesures correspondantes.

On parle de cyberrisques lorsque les vulnérabilités ou les points faibles des infrastructures utilisant les technologies de l'information et de la communication sont exposés à des menaces. Pour pallier ce problème, le Conseil fédéral a adopté la «Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)».[1] Le Parlement (sous-commissions de la politique de sécurité du Conseil national et du Conseil des Etats) s'intéresse également de plus en plus à cette problématique et a traité de nombreuses interventions parlementaires à ce sujet ces dernières années, dont les principales sont répertoriées en annexe.

[1] http://www.isb.admin.ch/themen/01709/01710/index.html?lang=fr

En approuvant la SNPC le 27 juin 2012 et son plan de mise en œuvre le 15 mai 2013 (plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques),[2] le Conseil fédéral a jeté les bases pour s'attaquer à cette problématique (cf. annexe 7.1). La SNPC se concentre notamment sur la détection précoce des menaces et des dangers dans le cyberespace et sur l'augmentation de la capacité de résistance des infrastructures critiques. Elle vise également une réduction générale des cyberrisques liés en particulier à la cybercriminalité, aux cyberespionnage et au cybersabotage. La SNPC n'affecte cependant pas les compétences et les tâches des autorités de poursuite pénale de la Confédération et des cantons dans la lutte contre la criminalité sur Internet.

A cet égard, les conditions de base essentielles demeurent l'action dans le cadre des compétences existantes, la collaboration au niveau national entre l'économie et les autorités, ainsi que la coopération internationale. La stratégie adopte une approche décentralisée et considère que les cyberrisques font partie intégrante des processus d'affaires et de gestion. Les milieux politiques, l'Etat, l'économie et les exploitants d'infrastructures critiques analysent les cyberrisques dans leurs domaines de compétences et les réduisent le cas échéant. Cette stratégie garantit par ailleurs la possibilité de soutenir de manière subsidiaire l'économie et les exploitants d'infrastructures critiques.

La stratégie comprend seize mesures, réparties en sept champs d'action, qui doivent être mises en œuvre jusqu'en 2017. Une analyse des résultats sera réalisée à cette date pour évaluer la suite de la procédure et l'état des connaissances sur l'impact financier et personnel de la SNPC. Les services fédéraux responsables ont présenté au printemps 2013 les ressources requises pour l'application de la stratégie. Sur cette base, le Conseil fédéral a approuvé le plan de mise en œuvre et, partant, la création de 28 postes de cyberspécialistes dans les départements concernés. Les ressources nécessaires aux autorités de poursuite pénale de la Confédération et des cantons pour mettre en œuvre le concept découlant de la mesure 6 de la SNPC pourront être définies et demandées uniquement lorsque celui-ci aura été élaboré.

Il est important de préciser que cette stratégie a enclenché un processus de mise en œuvre et constitue elle-même un processus continu, qui doit être contrôlé et actualisé régulièrement. Il serait erroné de croire que l'application débute en 2013 et se termine en 2017. La stratégie commencera, au contraire, à porter ses fruits au niveau opérationnel dès 2014 et 2015 et cela ne s'achèvera pas après 2017. Les activités qui en découlent doivent être vérifiées périodiquement et adaptées aux menaces existantes, qui sont en constante mutation. De même, les mesures de mise en œuvre de la stratégie visent à doter l'économie et l'administration de capacités suffisantes pour pouvoir maîtriser à long terme les cybermenaces.

Le Conseil fédéral a chargé un organe de coordination (OC SNPC), rattaché à l'Unité de pilotage informatique de la Confédération (UPIC), d'harmoniser les travaux de mise en œuvre. Avec les offices responsables des mesures de la SNPC, cet organe a défini l'état visé, les principales étapes et le calendrier des différentes mesures, puis a rassemblé ces informations dans une feuille de route. Le Conseil fédéral a nommé les membres du comité de pilotage (CP SNPC), qui s'assure en son nom de l'application coordonnée et ciblée de la SNPC. Le CP SNPC vérifie à l'aide d'un contrôle de gestion stratégique que les mesures progressent de façon ciblée et présente des rapports correspondants au Conseil fédéral par l'intermédiaire de la Conférence des secrétaires généraux (CSG). La réunion constituante du comité de pilotage a eu lieu le 30 octobre 2013.

Par ailleurs, deux groupes spécialisés ont été mis en place pour garantir respectivement le flux d'information entre la Confédération et les cantons ainsi que les travaux au niveau international: Cyber (GS-C), du mécanisme de consultation et de coordination du réseau national

[2] http://www.isb.admin.ch/themen/01709/01711/index.html?lang=fr

de sécurité (MCC RNS), et Cyber International (GS-CI), sous la responsabilité du Département fédéral des affaires étrangères (DFAE).

La SNPC est mise en œuvre en collaboration avec les responsables de la stratégie du Conseil fédéral pour une société de l'information en Suisse (OFCOM)[3], de la stratégie nationale pour la protection des infrastructures critiques (OFPP)[4] et de la gestion des risques de la Confédération[5]. Comme prévu, la mise en œuvre de la plupart des mesures de la SNPC a commencé et les premières étapes ont été atteintes fin 2013 pour certaines. Les services responsables présentent l'avancement de la mise en œuvre au chapitre 4 du présent rapport annuel.

[3] http://www.bakom.admin.ch/themen/infosociety/index.html?lang=fr. Le 19 février 2014, le Conseil fédéral a pris acte des progrès de la mise en œuvre de la stratégie pour une société de l'information en Suisse (cf. note d'information du DETEC du 12 février 2014): rapports sur la mise en œuvre de la stratégie Société de l'information

[4] http://www.bevoelkerungsschutz.admin.ch/internet/bs/fr/home/themen/ski.html

[5] http://www.efv.admin.ch/d/downloads/finanzpolitik_grundlagen/risiko_versicherungspolitik/Handbuch_Risikomanagement_Bund.pdf

2 Principales dates

27 juin 2012: le Conseil fédéral adopte la «Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)» (cf. annexe)

- Pose de la première pierre pour une approche globale de la cyberproblématique
- Axes: détection précoce des cyberrisques; augmentation de la capacité de résistance des infrastructures critiques; réduction générale des cyberrisques (cybercriminalité, cyberespionnage et cybersabotage)
- Seize mesures réparties en sept champs d'action

15 mai 2013: le Conseil fédéral adopte le plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (cf. annexe)

- Plan de mise en œuvre détaillé pour les seize mesures de la SNPC à appliquer d'ici fin 2017
- Organe de coordination (OC SNPC) rattaché à l'Unité de pilotage informatique de la Confédération (UPIC) et chargé de coordonner la mise en œuvre de la stratégie
- Ressources nécessaires présentées au printemps 2013 par les services fédéraux responsables
- Déclenchement d'un processus de mise en œuvre qui déploiera ses effets au niveau opérationnel avant 2017
- Processus global de mise en œuvre toujours en cours après 2017

15 mai 2013: le Conseil fédéral adopte le mandat du comité de pilotage de la SNPC (cf. annexe)

- Comité de pilotage de la SNPC chargé par le Conseil fédéral de veiller à la mise en œuvre coordonnée et ciblée de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)
- Contrôle de gestion stratégique du portefeuille de mesures de la stratégie par le comité de pilotage de la SNPC (CP SNPC) pour s'assurer que les travaux progressent de façon ciblée et dans le respect des délais; rapports au Conseil fédéral par l'intermédiaire de la CSG
- Nomination des membres du CP SNPC. Réunion constituante le 30 octobre 2013

25 octobre 2013: création du groupe spécialisé Cyber International (GS-CI), sous la responsabilité du DFAE

- Objectif du GS-CI: obtenir une vue d'ensemble des activités internationales des différents services de la Confédération
- Utilisation du GS-CI par l'organe de coordination de la SNPC comme plate-forme supplémentaire pour présenter l'avancement de la mise en œuvre de la cyberstratégie
- Représentation des services suivants dans le groupe spécialisé interdépartemental: DFAE-DP et DDIP; DETEC-OFCOM et OFEN; DFF-UPIC; DDPS-POLSEC, SRC, état-major de l'armée et BAC; DFJP-fedpol et OFJ.

18 décembre 2013: création du groupe spécialisé Cyber (GS-C) du mécanisme de consultation et de coordination du réseau national de sécurité (MCC RNS)

- Coordination de la mise en œuvre de la SNPC au niveau des cantons
- Interface entre la Confédération et les cantons
- Organe de coordination de la SNPC membre du GS-C; il fait le lien au niveau de la Confédération avec les travaux de projet du GS-C pour exploiter au mieux les synergies
- Tâches: participation des cantons en tant que partenaires centraux à toutes les mesures de mise en œuvre les concernant
- Réunion constituante le 18 décembre 2013

3 Menaces actuelles, objectifs et principaux éléments de la SNPC

3.1 Cybermenaces

Ces dernières années, l'importance et l'utilisation des technologies de l'information et de la communication (TIC) ont fortement progressé, modifiant fondamentalement l'économie, l'Etat et la société. Le nombre de participants à ces processus a, lui aussi, augmenté. L'accès à des informations précieuses a été sensiblement simplifié. L'utilisation des TIC est indispensable au développement de l'économie suisse, tant pour répondre aux besoins croissants d'information que pour la croissance, l'innovation et la prospérité. Malheureusement, le recours au cyberespace ne se traduit pas uniquement par de nombreux avantages et opportunités. Des personnes suspectes, des organisations et des Etats s'en servent également à des fins criminelles ou hégémoniques. Les technologies de l'information peuvent être utilisées abusivement en vue d'espionnage, de chantage ou de sabotage. Il est fréquent que les auteurs ne soient pas des individus, mais des groupes très organisés. On soupçonne que ceux-ci sont parfois financés par des Etats ou que certains pays participent directement à ces agissements. Les cyberattaques sont non seulement plus nombreuses, mais également plus ciblées, mieux organisées et, dans l'ensemble, plus professionnelles.

Les perturbations, les manipulations et les attaques entraînant un dysfonctionnement d'Internet pourraient impacter considérablement notre société. Les cyberattaques contre des infrastructures critiques notamment (énergie, transport, etc.) pourraient avoir de graves conséquences, car elles affecteraient le fonctionnement de ces infrastructures et déclencheraient des réactions en chaîne désastreuses. En Suisse, les infrastructures critiques sont gérées par des acteurs tant privés que de droit public. Elles englobent, entre autres, les autorités et les administrations à tous les échelons (Confédération, cantons, communes), dont le fonctionnement en tant qu'organes législatifs, exécutifs ou judiciaires pourrait être entravé directement par des cyberattaques ou indirectement, en qualité d'utilisateurs d'autres infrastructures critiques. Les cyberrisques concernent cependant tous les utilisateurs de systèmes d'information et de communication privés et professionnels ainsi que d'infrastructures critiques.

Le rapport semestriel 2013/I de MELANI[6] et le rapport annuel 2013 du SCOCI présentent les principales tendances actuelles liées aux dangers et aux risques liés aux TIC en Suisse et à l'étranger.

Les cybermenaces actuelles sont exposées brièvement ci-après:

CYBERMENACES 2013

L'année 2013 a été principalement marquée par les révélations d'Edward Snowden et les intrigues des grands services de renseignement, tels que la National Security Agency (NSA) aux Etats-Unis ou le Government Communications Headquarters (GCHQ) en Angleterre. Ces révélations reflètent la domination de certains Etats et montrent comment ceux-ci peuvent influer sur des entreprises qui développent et commercialisent du matériel informatique et des logiciels. Les exploitants d'infrastructures critiques et les PME doivent dès lors clairement identifier les données et informations confidentielles, voire secrètes, qu'ils détiennent et protéger celles-ci de manière adéquate.

[6] MELANI est chargée par le Conseil fédéral de protéger les infrastructures critiques en Suisse: http://www.melani.admin.ch/.

L'administration, les exploitants d'infrastructures critiques et les PME demeurent exposés aux dangers cybernétiques. Les possibilités d'Internet sont énormes en la matière et des attaques ciblées à des fins d'espionnage font désormais partie du quotidien. Les assaillants s'adaptent très rapidement aux nouvelles technologies. Dans le domaine de l'e-banking par exemple, ils ont développé des chevaux de Troie qui visent spécifiquement les applications mobiles correspondantes sur les téléphones portables et les manipulent en conséquence. Il est ainsi également possible d'intercepter et d'utiliser abusivement les SMS servant à la validation des transactions.

Le rapport semestriel 2013/I de MELANI indique que les attaques visant des infrastructures critiques en Suisse et à l'étranger ont augmenté: les attaques DDoS, les tendances en matière de phishing, les maliciels, les moyens de chantage (*ransomware*), les e-mails munis d'un lien vers des chevaux de Troie et les attaques ciblées d'ingénierie sociale se sont intensifiés ces dernières années. Les plus graves attaques DDoS de l'histoire d'Internet (*amplification attack* contre Spamhaus, opérations d'Anonymous) ont été recensées au premier semestre 2013. Une forte progression des maliciels d'e-banking sur les smartphones (cheval de Troie Gozi, maliciel Citadel et *ransomware* Reveton), des courriels munis de lien vers des sites infectés et des usages abusifs de la VoIP (Voice over IP)[7] a également été observée. Une nouvelle vague d'attaques contre des systèmes suisses d'e-banking utilisant une validation des transactions par SMS a aussi été signalée à la même période; elle a conduit à plusieurs paiements frauduleux.

Au niveau international, les révélations d'Edward Snowden (programmes de cyberespionnage: Prism, Tempora, XKeyscore) ainsi que d'autres actes politiques d'espionnage et de sabotage (par ex. Flame, Red October, Stuxnet)[8] ont fait la une de l'actualité.[9]

[7] Désignation de la technologie permettant de téléphoner sur des réseaux IP à partir d'un réseau privé contrôlé ou d'Internet.

[8] **Flame** est la plus importante arme cybernétique découverte jusqu'à présent. Ce programme a été conçu pour effectuer du cyberespionnage. Il peut voler des informations précieuses, dont des renseignements sur les systèmes visés, des fichiers sauvegardés, des données de contacts, et faire des copies d'écran ainsi que des enregistrements audio. Sa complexité et ses fonctions dépassent celles de toutes les autres armes cybernétiques connues. L'**opération Red October** est un autre réseau d'espionnage dont la structure équivaut à l'infrastructure très complexe du virus Flame. **Stuxnet** concerne le cybersabotage: ce maliciel a été spécialement développé pour un système précis de surveillance et de gestion des processus industriels (système SCADA). La centrale nucléaire iranienne Busher a ainsi été attaquée. Jusqu'à présent, Stuxnet est unique en son genre, en raison de sa complexité et de son objectif, à savoir saboter les systèmes de surveillance d'installations industrielles.

[9] Pour de plus amples informations sur ces cyberattaques, voir les rapports semestriels 2011, 2012 et 2013 de MELANI à l'adresse www.melani.admin.ch.

3.2 Objectifs de la SNPC

Les cyberrisques doivent être pris au sérieux; leur ampleur et leur dynamique croissent rapidement, comme on l'a observé ces dernières années. Le Conseil fédéral a décidé que la protection des infrastructures d'information et de communication contre les cyberrisques relevait de l'intérêt national de la Suisse et a ordonné l'élaboration d'une «Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)». Celle-ci a été approuvée le 27 juin 2012 et son plan de mise en œuvre, le 15 mai 2013. Le Conseil fédéral poursuit ainsi trois objectifs principaux: la détection précoce des menaces et des dangers dans le cyberespace, l'augmentation de la capacité de résistance des infrastructures critiques et la réduction des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

En adoptant la SNPC et son plan de mise en œuvre, le Conseil fédéral a posé la première pierre pour une approche globale de la cyberproblématique. Par ailleurs, plusieurs interventions parlementaires répertoriées en annexe ont encouragé les mesures contre les cybermenaces.

La SNPC est une stratégie complète qui poursuit une approche globale à travers ses seize mesures (M1 à M16, cf. illustration 1) et entend ainsi protéger la Suisse des cybermenaces. Le Conseil fédéral a décidé de répartir ces seize mesures de la SNPC dans quatre domaines en fonction de leur déploiement dans le temps et de leurs dépendances. Pour obtenir la capacité de résistance requise, il faut savoir prévenir, réagir, assurer la continuité et offrir un processus de soutien.

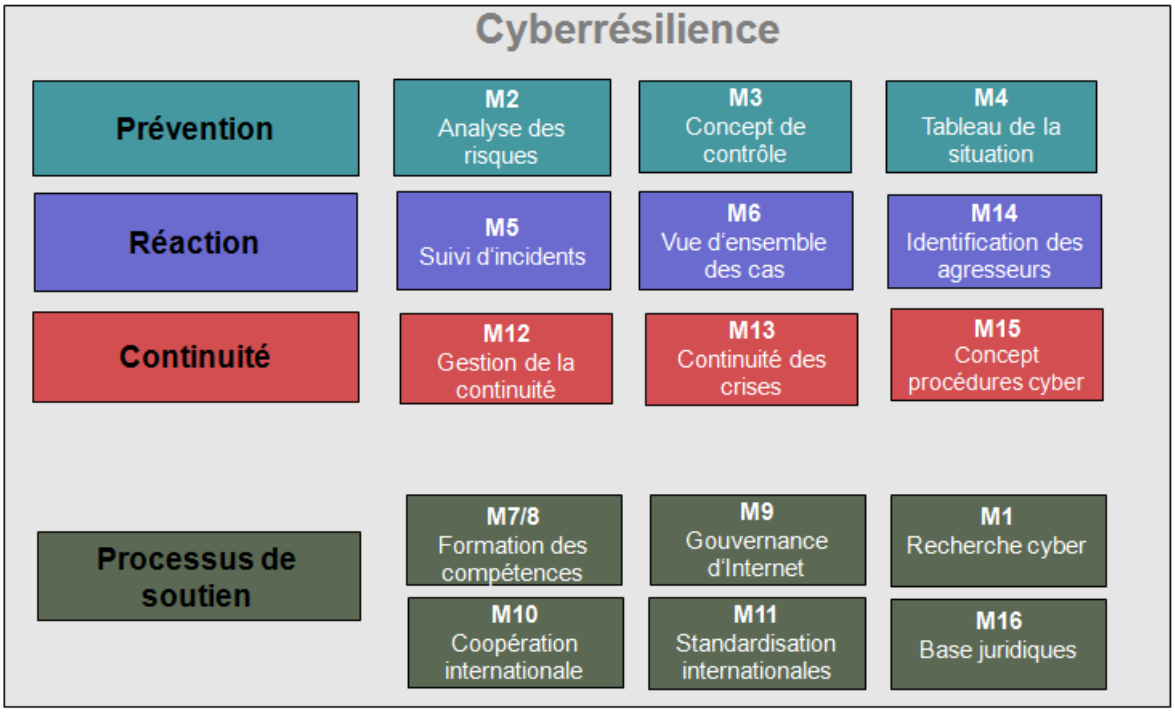


Illustration 1: Les seize mesures de la SNPC

Les quatre domaines sont:

- Prévention: aucune mesure de protection appropriée ne peut être mise en place sans une estimation précise des cybermenaces. La prévention doit dès lors analyser les risques et les vulnérabilités, ainsi que la menace. Même les meilleures mesures préventives ne peuvent cependant pas empêcher tous les incidents. Aussi faut-il développer les capacités de réaction si ces derniers se produisent.
- Réaction: une réaction efficace englobe le traitement de l'incident, l'identification des

auteurs et les interfaces avec la poursuite pénale. Dès que l'incident est maîtrisé, les enseignements acquis sont mises au profit du domaine de la prévention pour que les connaissances correspondantes demeurent à jour.

- Continuité: si un incident se mue en crise, il faut assurer la gestion de la continuité et des crises.
- Processus de soutien: il repose sur de nombreux processus de soutien concernant l'évolution au niveau international, les bases légales et la définition des compétences.

3.3 Principaux éléments de la SNPC

La SNPC met en évidence trois éléments principaux: une approche décentralisée qui conserve les structures et les compétences/responsabilités individuelles existantes, la gestion des risques, ainsi qu'une coopération nationale et internationale. Ces éléments sont exposés ci-dessous:

Approche décentralisée qui conserve les structures et les compétences/responsabilités individuelles existantes:

La SNPC réduit les cyberrisques dans le cadre des structures et des compétences existantes. Elle part du principe qu'ils font partie intégrante des responsabilités et des processus en place. Les différents acteurs de l'Etat, de l'économie et des milieux politiques sont donc incités dans un premier temps à identifier et à diminuer les risques dans leur domaine de compétences. De plus, les autorités spécialisées responsables et les exploitants d'infrastructures critiques analysent les risques pour la Suisse qui découlent des vulnérabilités que présentent ces infrastructures et, le cas échéant, réduisent ces risques. L'Etat assure par ailleurs un soutien subsidiaire efficace. Il fournit déjà des prestations subsidiaires dans la protection contre les cyberrisques, par exemple grâce à l'échange d'informations et aux connaissances des services de renseignement. Si nécessaire, ces capacités seront étendues (par ex. MELANI) et les processus existants seront optimisés pour diminuer efficacement les cyberrisques.

Approche globale:

La SPNC poursuit une approche globale en termes de risques. Sur la base de l'analyse des vulnérabilités et des risques, une gestion de ces derniers sera mise en place dans les sous-secteurs critiques et une gestion de la continuité et des crises sera implémentée. Il existe un risque lorsque des menaces portent sur des vulnérabilités. Il faut donc analyser d'abord celles-ci, puis les risques pour évaluer le risque résiduel. Les résultats de l'analyse des risques sont transposés dans des plans correspondants de gestion des risques, de la continuité et des crises. La SNPC part du principe que les cyberrisques font partie intégrante du risque global. Il faut donc non seulement tenir compte de ces cyberrisques, qui sont principalement d'ordre technique, mais également des risques personnels, physiques et organisationnels. Les mesures requises pour réduire les risques ne doivent pas uniquement se focaliser sur la sécurité des TIC, mais considérer toutes les dimensions. Cela signifie que la compétence incombe chaque fois à l'organe de direction suprême et qu'elle ne peut pas être déléguée à un responsable de la sécurité des TIC.

Coopération nationale:

L'économie et les autorités sont tenues de collaborer étroitement sur le plan national en raison de la SNPC. Celle-ci encourage le renforcement de la collaboration opérationnelle pour soutenir l'échelon stratégique. Pour ce faire, la Suisse doit utiliser à bon escient son modèle de partenariat public-privé (PPP), qui a été instauré depuis 2004. MELANI favorise l'échange de renseignements sur les cyberattaques entre les entreprises et aide subsidiairement les exploitants des infrastructures critiques suisses dans leur processus de protection de l'infor-

mation. Elle collecte des informations techniques ou non, les évalue et transmet les données pertinentes à ces exploitants. MELANI soutient ainsi la gestion des risques au sein des infrastructures critiques, par exemple en proposant des évaluations de la situation et des analyses pour identifier précocement les attaques ou les incidents, en évaluant leur impact et, en cas de besoin, en recherchant des maliciels. La Centrale gère une clientèle précise, qui comprend des entreprises et unités administratives sélectionnées qui exploitent des infrastructures critiques pour la Suisse (environ 100 membres, dont des banques, des entreprises de télécommunication et des fournisseurs d'énergie). MELANI propose son soutien au reste de l'économie et à la population sous forme de listes de contrôle, de guides et des programmes d'apprentissage.

Coopération internationale:

Dans le domaine de la cybernétique, les intérêts liés à la politique de sécurité doivent être préservés vis-à-vis de la communauté internationale. Le cyberespace, qui ne connaît pas les frontières nationales, constitue davantage une nouvelle dimension de la politique extérieure. Il faut donc également en tenir compte dans les réflexions correspondantes, car la Suisse, son économie et sa société sont très étroitement liées sur le plan numérique. L'importance de la cybersécurité croît régulièrement pour la Suisse et pour sa place économique.

La sécurité des infrastructures nationales ne pourra toutefois s'accroître à long terme que si les Etats coopèrent au niveau international et s'entendent pour limiter le recours au cyberespace dans la propagation violente des conflits. De même, les activités illégales d'acteurs non étatiques ne pourront être évitées que si les pays s'engagent à les combattre sur leur territoire par l'intermédiaire de règles de conduite. De nombreux processus et initiatives sont déjà en cours sur le plan international afin de définir des règles communes en la matière. La Suisse y participe.

3.4 Distinction entre la SNPC et la cyberdéfense

La SNPC se concentre principalement sur les risques dans le domaine civil. De son côté, l'armée élabore une stratégie de cyberdéfense pour protéger ses propres systèmes et développer ses capacités en vue d'apporter un soutien subsidiaire à ses partenaires civils. Elle est responsable de la protection et de la défense de ses propres infrastructures et systèmes contre les dangers, dans toutes les situations. Elle doit donc définir des solutions pour traiter les cybermenaces et leurs conséquences dans son domaine de tâches et de responsabilités et se préparer à faire face aux cas particuliers. Lorsqu'elle développe ses capacités de réduction des cyberrisques, l'armée doit en coordonner la mise en œuvre avec les autres autorités, car elle est étroitement liée au domaine civil. En cas de besoin, les offices responsables peuvent intégrer et utiliser les capacités existantes de l'armée dans leurs processus de mise en œuvre. Le chef de l'armée a nommé un délégué pour élaborer le concept de cyberdéfense de l'armée. Ce délégué est entré en fonction le 2 janvier 2013.

Les cyberrisques peuvent également être réduits en poursuivant efficacement la criminalité sur Internet au niveau pénal. La stratégie doit donc fixer les interfaces concernées et l'échange d'informations pertinentes pour la SNPC. Celle-ci ne porte toutefois pas sur les compétences et les tâches des autorités de poursuite pénale de la Confédération et des cantons pour lutter contre la cybercriminalité. La Suisse ne dispose pas (encore) d'une stratégie nationale de lutte contre la criminalité sur Internet.

4 Etat de la mise en œuvre de la SNPC en 2013

La phase de mise en œuvre a commencé, tout comme les travaux relatifs à la plupart des mesures. Pour certaines d'entre elles, les premières étapes ont été atteintes fin 2013. Ce chapitre propose une vue d'ensemble de la mise en œuvre dans une feuille de route SNPC, chaque service responsable de l'application exposant brièvement l'état de cette dernière pour les mesures concernées. Certaines mesures de la SNPC sont réalisées en collaboration avec les responsables de la stratégie du Conseil fédéral pour une société de l'information en Suisse et de la stratégie nationale pour la protection des infrastructures critiques.

4.1 Vue d'ensemble: feuille de route

L'organe de coordination de la SNPC a défini concrètement les objectifs et les étapes des mesures avec tous les services responsables et les a compilés dans une feuille de route:

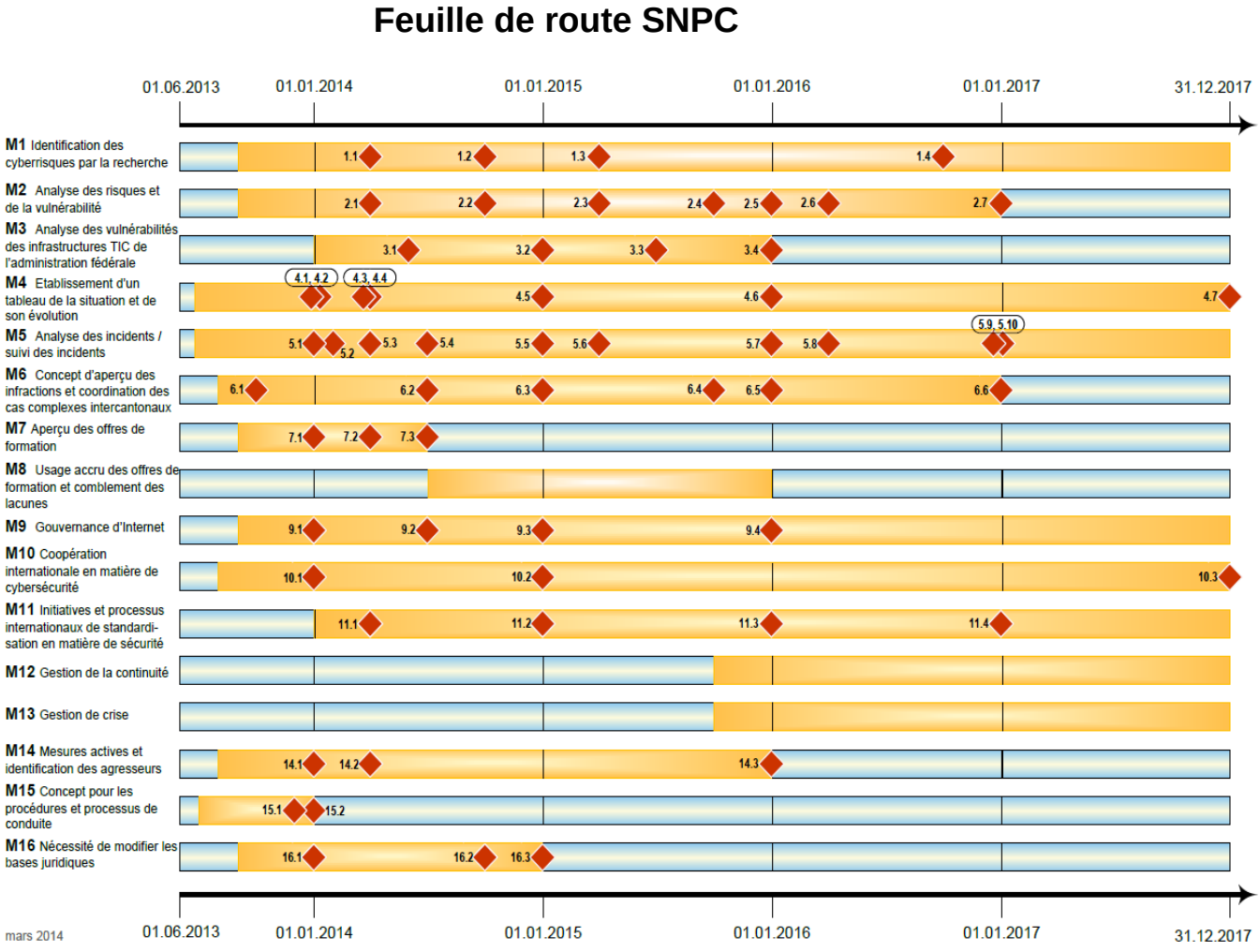


Illustration 2: Feuille de route SNPC

La feuille de route complète, qui comprend des informations détaillées sur les objectifs et les étapes, est disponible sur le site Web de l'UPIC: www.isb.admin.ch -> Thèmes -> Cyberrisques SNPC -> Feuille de route[10].

[10] http://www.isb.admin.ch/themen/01709/01841/index.html?lang=fr

4.2 Prévention

La prévention englobe des mesures sur l'analyse des risques et vulnérabilités, le contrôle des vulnérabilités des TIC au sein de la Confédération et un exposé de la situation (M2, M3, M4).

4.2.1 Analyse des risques et vulnérabilités (M2)

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

L'analyse des risques et vulnérabilités vise à déterminer, pour la Suisse, les risques qui découlent des vulnérabilités des infrastructures critiques au niveau des TIC. Il existe des cyberrisques lorsque des menaces (par ex. cyberattaques) concernent ces points faibles.

Ces dernières années, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a élaboré, en collaboration avec l'économie, des bases méthodologiques concernant l'analyse des vulnérabilités et les a déjà appliquées à différents sous-secteurs (par ex. dans le secteur énergétique).

L'Office fédéral de la protection de la population (OFPP) a identifié avec les partenaires concernés (autorités spécialisées, exploitants, etc.) les processus, systèmes et objets pertinents dans les 28 sous-secteurs critiques (transport routier, télécommunication, approvisionnement en eau, etc.). De plus, une analyse nationale des menaces, qui englobe également les cyberrisques, a été réalisée.

Dans le cadre de la mise en œuvre de M2, les travaux existants de l'OFAE et de l'OFPP doivent être coordonnés sur le plan méthodologique et l'analyse des risques et vulnérabilités doit être menée pour les 28 sous-secteurs critiques.

Etat actuel:

Lors d'une première étape, les approches méthodologiques ont été consolidées et la suite de la procédure a été définie conjointement. On garantit ainsi la cohérence et la comparabilité des résultats dans les 28 sous-secteurs.

4.2.2 Analyse de la vulnérabilité des infrastructures en matière de TIC de l'administration fédérale à l'aide d'un concept de contrôle (M3)

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

D'après la SNPC, les services de la Confédération doivent examiner les vulnérabilités de leurs infrastructures en matière de TIC en impliquant les fournisseurs de prestations dans le domaine des TIC et les fournisseurs de systèmes. Conformément au plan de mise en œuvre de la SNPC, l'Unité de pilotage informatique de la Confédération (UPIC), qui est rattachée au DFF, a été chargée d'élaborer d'ici la fin 2015 un concept de contrôle périodique des infrastructures en matière de TIC de l'administration fédérale au niveau des faiblesses systémiques, organisationnelles et techniques.

Etat actuel:

Le poste de responsable de la sécurité informatique SNPC, qui est chargé de la mise en œuvre de M3, a été pourvu. La personne concernée a pu commencer les travaux relatifs au projet M3 le 1er février 2014. L'OFIT soumet les systèmes à une analyse des vulnérabilités avant leur mise en service. Des analyses régulières sont en préparation. Elles sont déjà réalisées pour les applications Web.

4.2.3 Etablissement de l'image et du développement de la situation (M4)

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

Aucune mesure de sécurité appropriée ne peut être identifiée sans une évaluation claire des cybermenaces actuelles. Pour développer la capacité de résistance cybernétique (résilience) et parvenir à une prévention efficace, il faut donc non seulement une analyse des risques et vulnérabilités, mais également une analyse de la situation actuelle en matière de menaces. Différents acteurs sont aujourd'hui actifs pour évaluer la situation.

MELANI collecte, évalue, analyse et compile les principales informations issues de différentes sources afin de présenter la situation en matière de menaces. Ces indications sont utilisées dans des rapports sur la situation, des rapports spécialisés, des fiches d'information, des rapports semestriels, etc.

Le Service de renseignement de la Confédération (SRC) a la capacité d'obtenir des informations qui permettent de préciser les menaces existantes, tandis que le SCOCI fournit les connaissances de la police et des autorités de poursuite pénale de la Confédération et des cantons.

La SNPC vise à éviter les doublons et à établir un aperçu uniforme de la situation en étroite collaboration avec tous les acteurs. Pour ce faire, MELANI met en place sa propre plate-forme d'échange de renseignements. Le SRC accroît ses capacités dans la cybernétique et le SCOCI crée une vue d'ensemble des cas au niveau national (M6). De plus, les capacités techniques des Computer Emergency Response Teams (CERT) ont été développées en vue d'une surveillance constante des réseaux de la Confédération.

Etat actuel:

Le concept de renforcement de MELANI en tant que plate-forme d'échange de renseignements a été élaboré. MELANI et le Service de renseignement de la Confédération ont défini avec GovCERT les processus nécessaires pour déterminer la situation en matière de menaces. Le SRC a finalisé le concept interne de développement des capacités cybernétiques, qui prévoit la création d'une unité Cyber SRC. Les travaux organisationnels et administratifs correspondants sont déjà achevés et les postes ont été pourvus. Cette unité sera chargée de collecter les informations du service de renseignement concernant les menaces informatiques et la situation en la matière. La BAC (milCERT et Computer Network Operations, CNO) et l'OFIT (CSIRT) ont instauré un échange régulier de renseignements sur les menaces et les stratégies d'identification des cibles pour la surveillance du réseau.

Le renseignement miliaire (RM) a mis au concours le poste prévu par la SNPC afin que l'analyse de la situation cybernétique par l'armée puisse progressivement être intégrée dans la cartographie générale du SRC à partir du 1er avril.

4.3 Réaction

En matière de réaction, une analyse coordonnée et un suivi des incidents s'imposent en vue d'en pallier le plus rapidement possible les effets et de revenir aux affaires courantes (M5, M6, M14).

4.3.1 Analyse et suivi des incidents (M5)

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. Conformément au plan de mise en œuvre de la SNPC, il s'agit d'analyser les incidents, d'en assurer le suivi et de développer les mesures permettant de les contrer. Les enseignements tirés d'incidents importants sont communiqués à MELANI. Les leçons tirées d'incidents en lien avec la protection de l'Etat sont portées par le SRC à la connaissance du SCOCI (aux fins de poursuite pénale) par l'intermédiaire de MELANI. L'analyse des incidents incombe aux *Computer Emergency Response Teams* (CERT) de la Confédération, de l'armée et des exploitants d'infrastructures critiques.

Rattaché à MELANI, le GovCERT œuvre depuis des années dans le domaine de l'analyse des logiciels malveillants. ''En cas d'incident, il peut aujourd'hui déjà analyser et traiter les données de manière à ce que l'organisation visée puisse prendre des contre-mesures techniques. Par ailleurs, depuis 2013, MELANI met à la disposition des exploitants d'infrastructures critiques des informations techniques relatives à la protection de leurs infrastructures.

Par l'approbation de la SNPC, le mandat d'analyse et de suivi des incidents a été élargi. 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':

Le GovCERT a renforcé ses capacités. Sur le plan technique, la structure organisationnelle du GovCERT a été définie (www.GovCERT.ch)[11] et la première phase visant une augmentation de l'endurance (24 heures sur 24 et 7 jours sur 7) est achevée. Pour ce faire, deux postes supplémentaires ont été créés. En matière de renseignement, les travaux de conception relatifs à la structuration des cybercapacités du SRC sont terminés et les profils de postes sont définis. La coopération opérationnelle entre la BAC (MilCERT et Computer Network Operations [CNO]) et l'OFIT (CSIRT) en matière de gestion des cyberincidents a été systématisée. Par ailleurs, les instruments d'échange d'informations se développent et sont implantés en permanence. Simultanément, la BAC a mis au concours deux postes octroyés au titre de la SNPC, qui pourront être opérationnels en 2014 déjà. Enfin, l'armée a décidé (cf. ch.4.7) de renforcer progressivement ses propres moyens de détection et d'analyse.

4.3.2 Concept de vue d'ensemble des infractions et de coordination des cas intercantonaux complexes (M6)

Compétence: DFJP-SCOCI; DFF-MELANI

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

Dans ce cadre, on examinera les diverses tâches en rapport avec le développement et l'organisation de la surveillance des cas. En collaboration avec les cantons, il s'agira d'élaborer un concept de mise en place d'une vue d'ensemble des infractions et de coordination des cas intercantonaux complexes. Pour ce faire, il conviendra en particulier de préciser les as-

[11] http://www.melani.admin.ch/org/00101/01098/index.html?lang=fr

pects organisationnels, techniques, juridiques et professionnels de la problématique, de même que les ressources nécessaires (personnel, infrastructures, informatique, etc.).

Etat 'actuel:

Un mandat d'analyse détaillé a été établi, et l'on a défini l'organisation de projet et les parties prenantes. Sont impliqués des représentants de fedpol, du Ministère public de la Confédération (MPC), de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), de la Conférence des commandants des polices cantonales de Suisse (CCPCS) et de la cps (Conférence des procureurs de Suisse, anciennement Conférence des autorités de poursuite pénale de Suisse [CAPS]), de même qu'un représentant de Swiss Police ICT (Congrès informatique de la police suisse [SPIK]) et de l'Office fédéral de la justice (OFJ).

4.3.3 Mesures actives d'identification des agresseurs (M14)

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

L'important en matière de réaction est non seulement la capacité de se préparer et de réagir à des cyberincidents, mais encore d'identifier les agresseurs. En principe, il incombe au SRC de se procurer des informations par les moyens de renseignement dont il dispose, puis d'analyser et d'exploiter ces données. Le SRC est aujourd'hui déjà en mesure de rechercher les auteurs d'un acte, mais la mesure 14 doit permettre de renforcer ses capacités à cet égard (analyse des acteurs et du contexte, développement des moyens auxiliaires techniques). Pour ce faire, le SRC bénéficie de l'appui de MELANI et du SCOCI.

En matière d'analyse des acteurs et du contexte, les travaux de MELANI/SRC ont déjà produit de nombreux résultats spécifiques, et ils seront poursuivis et approfondis. Les résultats serviront de base à l'identification des agresseurs.

Dans le cadre d'enquêtes pénales, les autorités de poursuite pénale peuvent prendre diverses mesures visant l'identification des agresseurs. Le SCOCI joue un rôle important dans la poursuite pénale et l'identification des auteurs d'infractions. Lorsque l'on constate une infraction en lien avec la SNPC, elle est portée à la connaissance des autorités de poursuite pénale par l'intermédiaire du SCOCI.

Les développements décidés par la direction de l'armée (cf. ch. 4.7) sont également pertinents pour la mise en œuvre de cette mesure.

Etat 'actuel:

La structure organisationnelle du Cyber-SRC est définie, et les postes ont été octroyés pour l'analyse des acteurs et les développements techniques.

4.4 Continuité

Une gestion ciblée des crises exige des procédures et des processus de gestion clairement définis pour les cyberincidents. La gestion de la continuité vise à garantir le maintien des processus d'affaires même en cas de crise (M12, M13, M15).

4.4.1 Gestion de la continuité (M12)

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

En se fondant sur les résultats de l'analyse des risques et de la vulnérabilité (M 2), l'OFAE en sa qualité de chef de file et l'OFPP définissent, avec les entreprises concernées et les services spécialisés compétents, les mesures nécessaires pour assurer la continuité. A cet égard, ils adoptent une démarche globale devant permettre de maintenir ou de réactiver sans délai des fonctions critiques en cas d'indicent interne ou externe, le but étant de limiter autant que possible la défaillance de la prestation concernée.

Etat 'actuel:

Dépendant de la mesure 2, la mesure 12 sera mise en œuvre en œuvre dès l'été 2015.

4.4.2 Gestion des crises (M13)

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

Par la mesure 13, les infrastructures critiques et la Confédération doivent définir les processus permettant de gérer une situation extraordinaire provoquée par un cyberrisque. Les travaux se fondent sur les résultats de l'analyse des risques et de la vulnérabilité (mesure 2). En matière de gestion des crises, on peut distinguer entre les niveaux stratégique et opérationnel. La définition des processus au niveau stratégique relève de l'OFAE et de l'OFPP, celle des processus de nature opérationnelle de MELANI.

Etat 'actuel:

Les travaux relatifs à la gestion stratégique des crises débuteront en été 2015, car ils sont tributaires de la mesure 2.

4.4.3 Concept pour les procédures et processus de conduite incluant les aspects cybernétiques (M15)

Compétence: ChF

Contrairement à la gestion des risques, la gestion des situations d'urgence et des crises est indépendante de scénarios. Les procédures de conduite et de décision sont axées sur les processus et doivent rester constantes quel que soit l'événement qui peut se produire ou s'est déjà produit. Au sein d'une organisation, la gestion des crises définit la structure, les principes, les obligations, l'infrastructure et les processus permettant de maîtriser efficacement une situation extraordinaire.

Etat 'actuel:

Le concept pour les procédures et processus de conduite incluant les aspects cybernétiques a vu le jour et a été accepté par le comité de pilotage de la SNPC. Il précise les éléments stratégiques pertinents en cas de crise liée au cyberespace. Le concept se focalise sur l'échelon décisionnel politico-stratégique de la Confédération et non sur le niveau opérationnel. Les aspects opérationnels de la gestion des crises relèvent de la mesure 13.

4.5 Processus de soutien

Il convient encore de concevoir et de définir les bases et processus permettant d'aborder la

problématique de la cybernétique, qui concernent notamment les coopérations internationales, l'échange d'expériences en matière de formation et de recherche, et le cas échéant l'adaptation des bases légales (M1, M7, M8, M9, M10, M11, M16).

4.5.1 Identification des cyberrisques par la recherche (M1)

Compétence: offices fédéraux responsables; OC SNPC

La recherche doit permettre d'identifier les cyberrisques pertinents à venir, de même que les changements de la configuration des menaces, de sorte que les décisions politiques et économiques puissent être prises à temps dans une perspective d'avenir. Les mesures sont mises en œuvre en collaboration étroite avec les responsables de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

L'organe de coordination de la SNPC a pour mission d'identifier avec ses partenaires les aspects pertinents de la cybermenace.

Etat 'actuel:

En collaboration avec la Commission pour la technologie et l'innovation (CTI) et le Secrétariat d'Etat à la formation, à la recherche et à l'innovation (SEFRI), l'organe de coordination de la SNPC a identifié quatre ou cinq des principaux axes de recherche sur le cyberespace.

4.5.2 Aperçu des offres de formation (M7)

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

Le renforcement de la cyberrésilience en Suisse exige que l'on prenne conscience de la nécessité de se prémunir contre les cyberrisques et que l'on acquière les connaissances indispensables. Il convient ainsi de renforcer ou de créer des compétences spécifiques ciblées (par ex. formation de spécialistes de la sécurité des TIC, perfectionnement continu en matière de sécurité de tous les spécialistes des TIC, acquisition de connaissances juridiques et techniques par les autorités de poursuite pénale en rapport avec les cyberdélits, etc.).

L'objectif de la SNPC est d'élaborer une vue d'ensemble des offres existantes en matière de formation des compétences, dans le but d'identifier les lacunes et de faire connaître l'offre liée aux cyberrisques. La mesure est étroitement coordonnée avec la mise en œuvre de la stratégie du Conseil fédéral pour une société de l'information en Suisse.

Le DFAE a remis à l'organe responsable une liste d'organisations internationales et de centres de compétences offrant des formations spécifiques. Le DFAE est associé à la mise en œuvre de la mesure 7 comme en témoigne le rapport de gestion 2013.

Etat 'actuel:

Les groupes concernés de l'administration, des milieux économiques et de la société civile ont été définis. Par ailleurs, des experts ont été consultés pour chacun des groupes à propos des cyberrisques principaux, des compétences nécessaires et des offres de qualité.

4.5.3 Usage accru des offres de formation et comblement des lacunes (M8)

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

La mesure 8 consiste en l'élaboration d'un concept visant le recours plus fréquent à l'offre existante en matière de formation des compétences à la gestion des cyberrisques, et en la

création de nouvelles offres permettant de combler les lacunes dans ce domaine.

Etat 'actuel:

M8 se fonde sur les résultats de M7 et ne sera par conséquent mise en œuvre qu'à l'issue de la seconde, en été 2014.

4.5.4 Gouvernance d'Internet (M9)

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

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.

Le DFAE œuvre également dans le domaine de la gouvernance d'Internet: il a ainsi identifié les processus et initiatives liés aux problèmes de sécurité en la matière, en se fondant sur plusieurs études consacrées à ces processus et initiatives. Simultanément, le DFAE soutient les efforts consentis sur le plan international en faveur du renforcement de la protection des données et de la sphère privée. On peut citer à ce propos la résolution adoptée par l'Assemblée générale de l'ONU sur «Le droit à la vie privée à l'ère numérique», qui stipule notamment que les droits de l'homme valent aussi dans le contexte de la communication numérique.

L'OFCOM et le DFAE collaborent étroitement dans le domaine de la gouvernance d'Internet en vue de défendre une position cohérente et étayée de la Suisse. De plus, l'OFCOM consulte régulièrement tous les représentants concernés de l'administration, des milieux économiques et de la société civile dans le cadre de la plate-forme tripartite.

Etat 'actuel:

L'OFCOM a dressé un inventaire des manifestations, initiatives et organes internationaux en rapport avec la gouvernance d'Internet, appelé à être mis à jour régulièrement. Par ailleurs, la décision a été prise d'associer à la mesure 9 le «Groupe spécialisé Cyber International (GS-CI)» nouvellement créé au Département fédéral des affaires étrangères (DFAE).

Au nom de la Suisse, l'OFCOM assume la vice-présidence du Comité consultatif gouvernemental de l'ICANN (Internet Cooperation for Assigned Names and Numbers) et représente la Suisse au sein des institutions intergouvernementales traitant des questions essentielles de la gouvernance d'Internet, par ex. la CSTD responsable à l'ONU du SMSI et de la gouvernance d'Internet, l'UIT, l'UNESCO et le Conseil de l'Europe. Au nom de la Suisse, l'OFCOM participe également à la préparation et à l'organisation du Forum (de l'ONU) de la gouvernance de l'Internet (FGI), et il est l'un des initiateurs et des coorganisateurs du forum de dialogue européen du FGI «EuroDIG».

4.5.5 Coopération internationale en matière de cybersécurité (M10)

Compétence: DFAE-DP; 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 le biais d'initiatives et de ses relations internationales, la Suisse participe aux efforts visant à éviter que le cyberespace soit utilisé de manière abusive à des fins criminelles, politiques, terroristes ou de renseignement.

Etat 'actuel:

A la faveur de l'approbation de la stratégie nationale de protection de la Suisse contre les cyberrisques, la division Politique de sécurité (DPS) a été chargée de mettre en œuvre la cyberstratégie au sein du département, raison pour laquelle elle a élaboré un concept exposant les divers champs d'activités et structures organisationnelles des unités administratives, de même que les objectifs visés. Les premiers jalons ont été posés comme prévu en 2013.

La DPS a déjà entamé des actions ciblées dans le cadre de la coopération internationale en vue de réduire la cybermenace. On citera à ce propos, dans le cadre de la coopération multilatérale, la participation de la Suisse au processus de l'Organisation pour la sécurité et la coopération en Europe (OSCE) visant l'élaboration de mesures de confiance. La Suisse participe depuis le début et de manière soutenue à ce processus. Sa proposition d'y associer davantage de représentants du secteur privé a été reprise dans une mesure de confiance (mesure de confiance 7 sur le partenariat public-privé).

La Suisse participe également au processus de Londres qui vise l'établissement de règles de conduite internationales. La Suisse était représentée à la conférence de Séoul sur le cyberespace par une délégation interdépartementale conduite par le secrétaire général suppléant du DFAE.

L'échange d'informations sur le cyberespace est devenu partie intégrante et permanente des consultations bilatérales et multilatérales que mène la Suisse en matière de sécurité avec des Etats et des organisations internationales (notamment l'UE, l'OTAN et la Finlande). Simultanément, des consultations spécifiques sur le cyberespace sont menées (Royaume-Uni) ou prévues (Allemagne) avec des Etats choisis.

On étudie depuis 2013 une coopération structurée et approfondie avec l'OTAN et le Centre de compétences de Tallinn. Le conseil de coordination interdépartemental pour le Conseil de partenariat euro-atlantique (CPEA) et le Partenariat pour la paix (PPP) a décidé de renforcer la coopération bilatérale entre l'OTAN et ses partenaires extérieurs dans le domaine de la cybersécurité. A ce propos, une délégation interdépartementale conduite par le DFAE a entamé une consultation avec le Centre de compétences en vue d'étudier les possibilités d'une collaboration dans le domaine civil.

4.5.6 Initiatives et processus internationaux de standardisation en matière de sécurité (M11)

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

En vue d'assurer la protection contre les cyberrisques, des normes de sécurité s'imposent pour les produits et processus. Le réseautage global exige que ces normes soient élaborées au niveau international et que les réglementations qui en résultent soient décidées et appliquées multilatéralement. Par la mesure 11, la SNPC veut garantir que les intérêts de la place économique suisse soient pris en compte de manière coordonnée par les organes internationaux privés et publics dans le domaine de la sécurité, de la protection et de la normalisation. Il faut pour ce faire un processus qui renforce les échanges d'informations entre les exploitants d'infrastructures critiques, les fournisseurs de services TIC, les fournisseurs de systèmes, les associations, les organisations nationales de normalisation, les autorités et les ré-

gulateurs.

Etat 'actuel:

Lors de la première réunion du comité de pilotage de la SNPC du 30 octobre 2013, la responsabilité de cette mesure a été transférée à l'OFCOM, sur proposition de ce dernier.

4.5.7 Nécessité de modifier les bases juridiques (M16)

Compétence: OC SNPC

Le réseautage croissant et le recours accru aux moyens de communication renforcent l'influence du cyberespace sur les tâches et responsabilités existantes et ont des conséquences pour les lois et ordonnances en vigueur. Toutefois, ces réglementations sont souvent peu coordonnées et pour partie lacunaires. Bien que la Confédération et les cantons soient compétents pour imposer des charges en matière de sécurité, les dispositions relatives à la cybersécurité sont encore fréquemment formulées de façon insuffisamment explicite.

La mesure 16 prévoit un réexamen des bases légales et leur adaptation au cyberespace. Dans le cadre de la SNPC, il s'agit pour les unités administratives de recenser, dans leur domaine de tâches, les bases légales pertinentes au regard des cyberrisques, et d'évaluer les besoins en matière d'adaptations ou de compléments.

Etat 'actuel:

En collaboration avec tous les départements, l'organe de coordination de la SNPC a dressé un inventaire des bases légales pertinentes pour le cyberespace et déterminé les besoins de révision.

On retiendra à cet égard les projets législatifs concernant notamment la loi sur la sécurité des informations (LSI), la loi sur le service de renseignement (LRens), la loi sur l'approvisionnement économique du pays (LAP) et la loi sur l'approvisionnement en électricité (LApEl).

La LSI réglera de manière uniforme et exhaustive la sécurité des informations pour l'ensemble de la Confédération (et non seulement pour l'administration fédérale) et regroupera d'importantes bases légales relatives à la sécurité des informations. Elle remplacera l'ordonnance concernant la protection des informations (OPrI), l'ordonnance du DDPS concernant la sauvegarde du secret et l'ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP), et couvrira les aspects de la sécurité informatique (par ex. le devoir de communication au sein de l'administration fédérale) de l'ordonnance sur l'informatique dans l'administration fédérale (OIAF, art. 11).

De plus, la LSI définira le mandat de MELANI (soutien de la Confédération aux exploitants d'infrastructures critiques dans le domaine de la sécurité des informations) et créera une base légale formelle pour le traitement des données y afférentes. La procédure de consultation sur le projet de LSI est ouverte depuis la fin du mois de mars 2014.

4.6 Mise en œuvre par les cantons

Le mécanisme de consultation et de coordination du Réseau national de sécurité (MCC RNS) est l'interface entre la SNPC et les cantons. L'organe de coordination de la SNPC est membre du groupe spécialisé Cyber du MCC RNS et joue au niveau de la Confédération le rôle de passerelle avec les travaux de projet menés par le groupe Cyber, dans le but d'exploiter au mieux les synergies et d'éviter les redondances. Le 20 août 2013, la plateforme po-

litique du RNS a chargé le groupe spécialisé Cyber de piloter des sous-projets répartis entre quatre groupes de travail (GT).

Etat 'actuel:

Quatre groupes de travail ont été créés dans les domaines de l'analyse des risques et de la prévention (M2 de la SNPC), gestion des incidents (M4 et M5 de la SNPC), de la gestion des crises (M15 de la SNPC) et de la vue d'ensemble des infractions (M6 de la SNPC). Les réunions constitutives des quatre groupes de travail se tiendront très prochainement, alors que celle du groupe spécialisé Cyber a déjà eu lieu. La Confédération et les cantons sont représentés paritairement au sein du groupe Cyber, qui accueille en outre un représentant de chacune des organisations des communes et des villes.

La première cyber-landsgemeinde, à laquelle ont pu participer les représentants des cantons compétents en matière d'informatique et de sécurité des informations, s'est tenue en mars 2013, et la deuxième a eu lieu le 20 mars 2014.

4.7 Mise en œuvre par l'armée

L'armée constitue l'une des infrastructures critiques du pays. A ce titre, elle doit également tenir compte de la nouvelle dimension de la cybermenace si elle entend assumer en toutes circonstances son rôle de réserve stratégique de sécurité de la Confédération. Parallèlement, le cyberespace offre de nouvelles options opérationnelles qu'il convient de prendre en considération dans les opérations militaires. L'armée a pour tâche première de renforcer les capacités dans son domaine de compétence.

Bien que la SNPC (cf. ch. 3.4) exclue de son champ d'application les cas de guerre et de conflit et qu'elle confie à l'armée le soin de se préparer à des situations particulières, l'armée dispose, en raison des besoins mentionnés plus haut, de connaissance et d'aptitudes étendues auxquelles les offices responsables peuvent recourir en cas de nécessité dans leurs processus de mise en œuvre, pour autant que l'armée n'en ait pas elle-même besoin. Cette possibilité obéit au principe éprouvé de la subsidiarité de l'engagement de l'armée.

Etat 'actuel:

La direction de l'armée a approuvé le 3 avril 2013 les principes proposés dans l'étude conceptuelle sur la cyberdéfense (*Konzeptionsstudie Cyber-Defense*, KS CYD) commanditée par le chef de l'armée. L'étude, qui se trouve en phase de mise en œuvre, rend principalement compte de la capacité de défense et du développement des capacités cyber-opérationnelles de l'armée et de ses ressources, de même que des rôles et des compétences. Ses objectifs stratégiques premiers concernent la liberté d'action et les capacités d'intervention de l'armée, de même que son aptitude à collaborer avec ses partenaires et à leur apporter son soutien si nécessaire.

Ultérieurement, on prévoit d'assurer la collaboration avec l'organe de coordination de la SNPC et de concrétiser les éléments du plan de mise en œuvre de la SNPC du Conseil fédéral (cf. ch. 3.3 du plan de mise en œuvre: Subsidiarité de l'armée). Il s'agit particulièrement de faire bénéficier des compétences spécifiques de l'armée les autorités civiles et les exploitants d'infrastructures critiques, et de préciser leurs responsabilités en cas de conflit ou de guerre.

5 Organisation de la mise en œuvre

Le Conseil fédéral a institué un comité de pilotage de la SNPC chargé de veiller à la mise en œuvre coordonnée de la SNPC, conformément aux objectifs. La réunion constitutive du comité de pilotage de la SNPC s'est tenue le 30 octobre 2013.

Le comité de pilotage regroupe des représentants de tous les services de la Confédération portant la responsabilité de l'une au moins des mesures de mise en œuvre. L'organe de coordination de la SNPC, chargée de coordonner la mise en œuvre de la stratégie aux niveaux opérationnel et technique, de même que le mécanisme de consultation et de coordination du Réseau national de sécurité (MCC RNS)[12] qui coordonne les travaux avec les interfaces cantonales, y sont également représentés. Le comité de pilotage de la SNPC est présidé par le DFF.

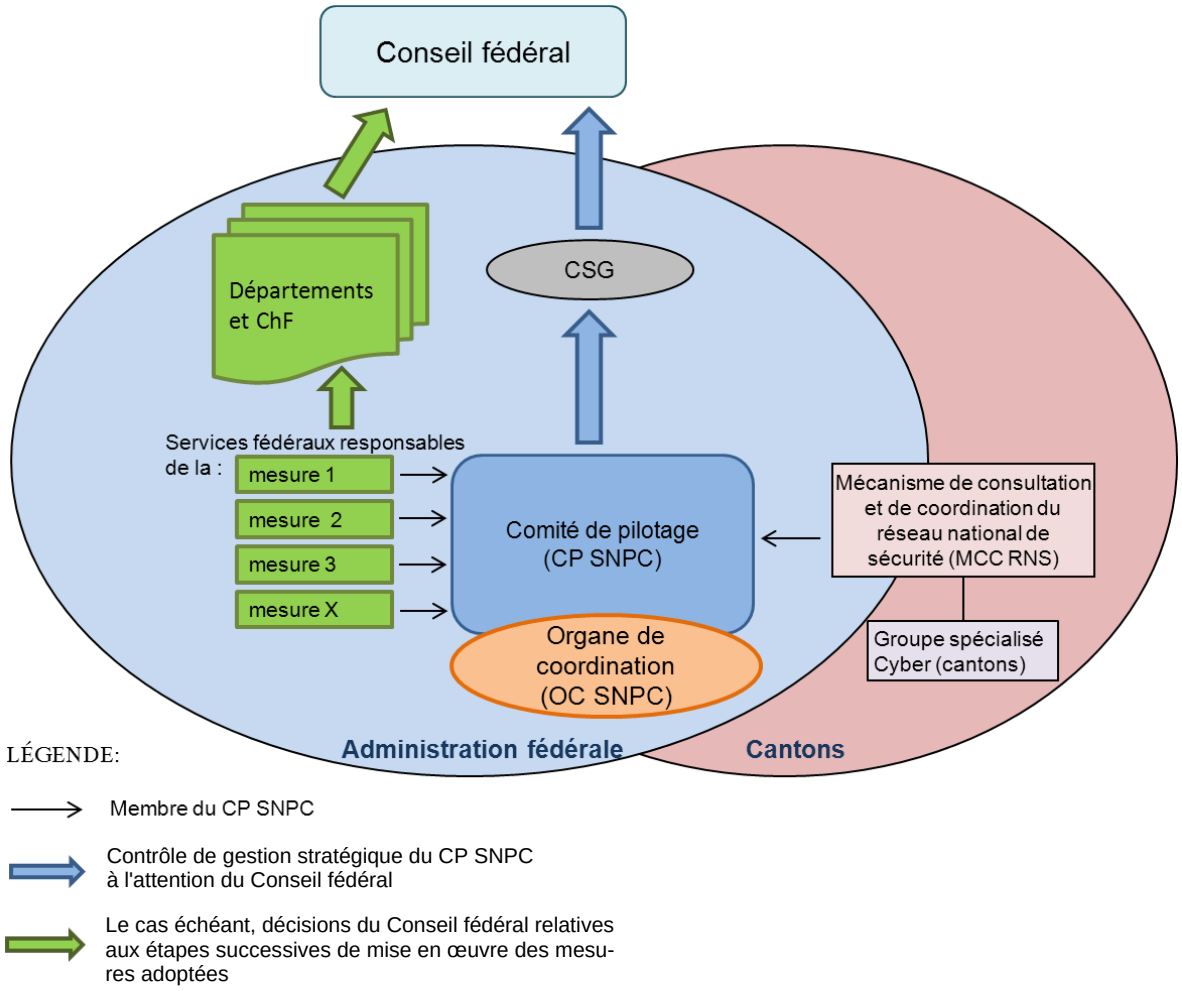


Illustration 3: organisation de la mise en œuvre de la SNPC

Par ailleurs, un groupe spécialisé interdépartemental Cyber International (GS-CI) présidé par la division Politique de sécurité du DFAE a été créé le 25 octobre 2013. Il a pour mission d'assurer la circulation des informations en coopération étroite entre tous les participants. Les travaux de la Confédération liés au cyberespace présentant souvent des interfaces communes et une dimension internationale, le groupe spécialisé est plus particulièrement chargé de fournir une vue d'ensemble des diverses activités concernées.

[12] Cf. Ch. 4.6

5.1 Mandat du comité de pilotage de la SNPC

Le 15 mai 2013, le Conseil fédéral a approuvé le mandat du comité de pilotage de la SNPC (CP SNPC) et lui a confié la tâche de veiller à la mise en œuvre coordonnée de la SNPC, conformément aux objectifs. A cette fin, le CP SNPC examine périodiquement les progrès de la mise en œuvre de la stratégie au moyen d'un contrôle de gestion, et fait rapport au Conseil fédéral par l'intermédiaire de la Conférence des secrétaires généraux (CSG).

En outre, le CP SNPC s'assure d'une démarche coordonnée des départements dans la mise en œuvre des mesures, notamment lorsque ces dernières touchent des aspects législatifs. Il soutient activement la collaboration des services de la Confédération avec les services compétents des cantons, des milieux économiques et de la société civile. Il rend compte annuellement au Conseil fédéral, par l'intermédiaire du Département fédéral des finances (DFF), de l'état d'avancement de la mise en œuvre de la SNPC, et présentera un rapport final à la fin de 2017. Au printemps de 2017, il soumettra au Conseil fédéral un rapport sur l'efficacité de la stratégie et du plan de mise œuvre.

L'organe de coordination de la SNPC coordonne la mise en œuvre de la stratégie sur les plans opérationnel et technique, en tenant compte de la politique des risques de la Confédérations, de la stratégie nationale de protection des infrastructures critiques, de la stratégie de gestion des risques de la Confédération et de la stratégie du Conseil fédéral pour une société de l'information en Suisse. En accord avec le Département fédéral des affaires étrangères (DFAE), il suit les évolutions internationales en matière de cyberstratégies. Lors d'une rencontre annuelle d'experts de la SNPC, les partenaires de la mise en œuvre sont mis en relation, informés et invités à échanger leurs expériences.

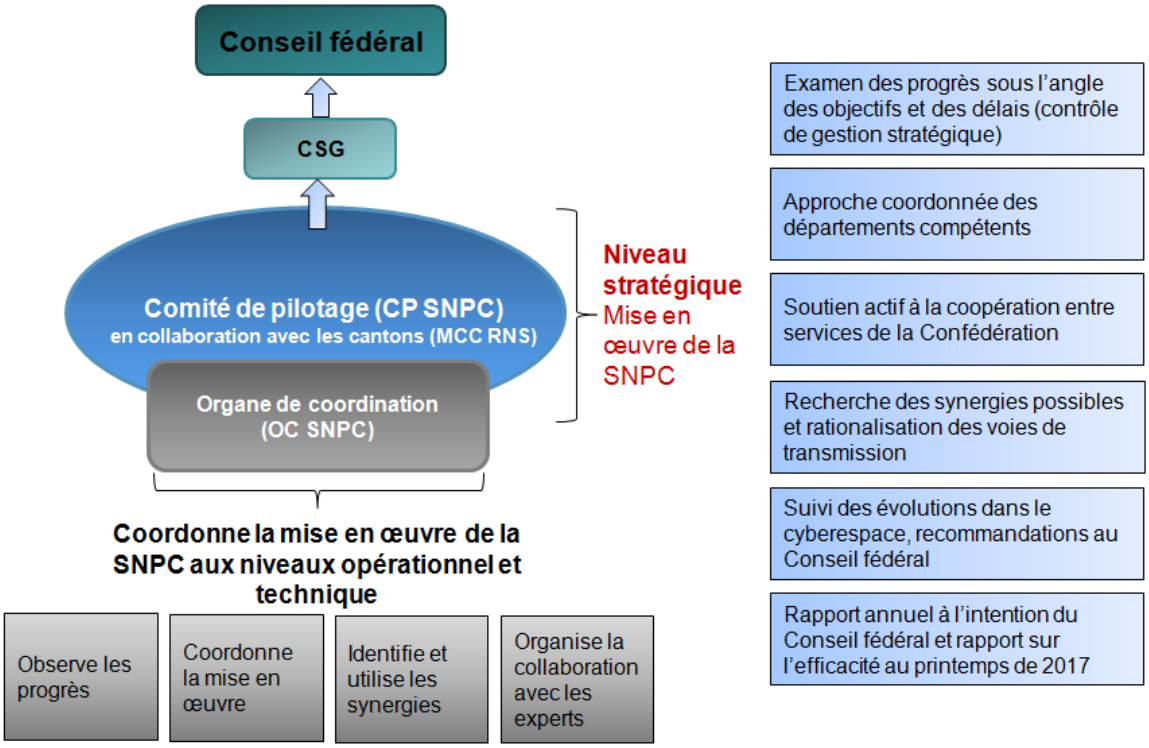


Illustration 4: tâches du comité de pilotage et de l'organe de coordination de la SNPC

5.2 Association des milieux économiques

L'approche décentralisée de la mise en œuvre et la coopération étroite entre la Confédération, les cantons et les milieux économiques sont des éléments clés de la SNPC. Bien que les milieux économiques soient déjà associés à la SNPC sur le plan technique, et que les 28

sous-secteurs et les exploitants d'infrastructures critiques aient été approchés directement par l'OFPP et l'OFAE, le niveau politique des milieux économiques n'a pas encore été associé à la mise en œuvre de la SNPC. C'est pourquoi le CP SNPC a cherché en 2013 les formes appropriées d'une telle participation. La situation s'améliorera en 2014 par la présence de l'association faîtière economiesuisse au sein du CP SNPC à titre d'observateur; elle y jouera également un rôle d'intermédiaire avec les diverses branches.

6 Considérations finales

Le temps qui s'est écoulé depuis l'approbation du plan 2013 de mise en œuvre de la SNPC a été mis à profit pour concrétiser les tâches des services responsables. Le CP SNPC a défini les objectifs et les étapes avec eux et les a consignés dans un document de base. Conformément à la planification, tous les services responsables ont entamé les travaux de mise en œuvre. Quelques étapes ont même été franchies en 2013 déjà et selon les prévisions, de nombreuses autres devraient l'être en 2014. La plupart des mesures ne sont pas mises en œuvre par un seul service fédéral, mais en collaboration entre plusieurs partenaires. En 2013, les offices responsables se sont concertés et ont entamé leur collaboration, créant de la sorte des bases stables de mise en œuvre.

La création du groupe spécialisé Cyber de la DPS (GS-C) et du groupe spécialisé Cyber International du DFAE (GS-CI) garantit également une bonne collaboration avec les cantons et au niveau international. Les travaux ont déjà débuté: le GS-C coordonne la mise en œuvre de la SNPC au niveau cantonal et sert 'd'intermédiaire entre la Confédération et les cantons. L'organe interdépartemental du groupe spécialisé Cyber International a par ailleurs permis d'encourager et de systématiser la circulation des informations et d'aborder au sein de la Confédération, de points de vue différenciés et par divers services, la problématique de la cybersécurité internationale.

Il est important de noter que pour nombre de mesures, les travaux et processus avaient débuté avant même l'approbation de la SNPC. Cette dernière a élargi ou rééquilibré les mandats de services concernés, par exemple ceux de MELANI ou du SRC. A cet égard, une démarche globale et coordonnée s'impose dans le cadre de la SNPC, en collaboration étroite avec les services impliqués.

La stratégie a déclenché un processus de mise en œuvre qui, sur le plan opérationnel, déploiera ses premiers effets en 2014 et 2015 déjà, mais qui ne se terminera pas en 2017. En effet, les activités au titre de la SNPC qui visent la protection contre les cyberrisques doivent être réexaminées périodiquement et être adaptées à l'évolution de la menace.

Au printemps de 2017, un rapport final exhaustif sera soumis au Conseil fédéral, accompagné d'une étude de l'efficacité de la stratégie et du plan de mise en œuvre. Une information suivra quant à la suite des opérations.

7 Annexes

7.1 Documents de base relatifs à la SNPC

«Stratégie nationale de protection de la Suisse contre les cyberrisques»:
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

«Mandat du comité de pilotage de la SNPC et de l'organe de coordination de la SNPC»:
http://www.isb.admin.ch/themen/01709/01712/index.html?lang=fr

«Feuille de route de la SNPC»:
http://www.isb.admin.ch/themen/01709/01841/index.html?lang=fr

7.2 Récapitulation des interventions parlementaires relatives aux cyberrisques

Intervention Ip. = Interpellation; Mo. = Motion; Po. = Postulat	Déposé le:	Etat au 31.12.2013:
08.3050 Po. Schmid-Federer. Protection contre la cyberintimidation	11.03.2008	transmis
08.3100 Mo. Burkhalter. Stratégie nationale de lutte contre la criminalité par Internet avec les discussions au 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	transmis
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 délibérations du Conseil des Etats du 15 mars 2011 (BO CE 15.03.2011)	29.06.2010	transmis
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	transmis
12.3417 Mo. Hodgers. Marchés ouverts de la télécommunication. Stratégies pour la sécurité numérique nationale	30.05.2012	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
13.3692 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	traité par les deux conseils
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 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».)	05.11.2013	non encore traité au conseil
13.4077 Ip. Clottu. Espionnage de données et sécurité sur Internet	05.12.2013	non encore traité au conseil
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

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
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 Indicent Response Team
CTI	Commission pour la technologie et l'innovation
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 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
DFF	Département fédéral des finances
DFI	Département fédéral de l'intérieur
DFJP	Office fédéral de justice et police
DPS	Division politique de sécurité
Fedpol	Office fédéral de la police
FGI	Forum sur la gouvernance de l'Internet
GCHQ	Government Communications Headquarters
GS-C	Groupe spécialisé Cyber
GS-CI	Groupe spécialisé Cyber International
ICANN	Internet Cooperation for Assigned Names and Numbers ou Société pour l'attribution des noms de domaine et des numéros sur Internet
KS CYD	Konzeptionsstudie Cyber-Defense ou étude 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
OSCE	Organisation pour la sécurité et la coopération en Europe
RM	Service de renseignement militaire
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
SMSI	Sommet mondial sur la société de l'information
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