Juin 2015 | www.upic.admin.ch

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

Rapport annuel 2014 du comité de pilotage de la SNPC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Publication: 5 juin 2015

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/themen/01709/01891/index.html?lang=fr

Table des matières

Préambule

Des incidents et des attaques très sophistiquées attribuées à des Etats se sont de nouveau produits en 2014. Les cybercriminels ont eux aussi fait preuve d'ingéniosité. Des failles de sécurité largement répandues ont également joué un rôle notable. Le monde a donc pris davantage conscience non seulement des opportunités de la numérisation croissante, mais aussi de la vulnérabilité d'Internet, des données personnelles et de la sphère privée ainsi que de la confiance fragile dans les technologies du Web. La Suisse continue de suivre sa propre voie pour combattre ces menaces, pour se protéger contre les cyberrisques et pour renforcer les exigences inhérentes à une infrastructure digne de confiance: la mise en œuvre de la «Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)» s'est dès lors poursuivie et les premiers objectifs importants ont été atteints. Ce deuxième rapport annuel sur la mise en œuvre de la SNPC fournit une vue d'ensemble détaillée des menaces ainsi que des mesures adoptées dans le cadre de cette stratégie et de leur avancement.

La Suisse n'est pas la seule à devoir relever les défis de la protection du Web, car les menaces ne connaissent pas de frontières. La coopération internationale est donc plus essentielle que jamais. Des mesures de confiance ont été élaborées lors de la présidence suisse de l'Organisation pour la sécurité et la coopération en Europe (OSCE). Elles sont indispensables à une compréhension commune de la sécurité sur Internet. La conclusion d'accords avec différents Etats concernant l'échange de renseignements relatifs aux failles de sécurité et aux incidents et l'extension des partenariats existants ont permis d'améliorer l'information mutuelle sur les cyberincidents.

En Suisse aussi, ce combat doit être commun et les connaissances doivent être partagées. Le réseau de compétences «Swiss Cyber Experts» a donc été créé dans le cadre d'une collaboration entre la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), le secteur des technologies de l'information et de la communication (TIC) et des partenaires de recherche.

Les réalisations passées sont capitales, mais les travaux de mise en œuvre de la SNPC sont encore loin d'être terminés. En 2015 également, nous mettrons tout en œuvre en Suisse pour qu'Internet demeure un espace sûr et libre de toute censure pour l'économie, les autorités et les citoyens. Cela est et reste notre exigence absolue à l'ère du numérique.

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 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, au cyberespionnage et au cybersabotage.

La mise en œuvre des différentes mesures a été confiée aux offices fédéraux en fonction de leur domaine de compétences. 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). Par ailleurs, le Conseil fédéral a chargé un comité de pilotage de la SNPC (CP SNPC) de suivre cette mise en œuvre grâce à un contrôle de gestion stratégique.

Les seize mesures portent sur quatre domaines: la prévention, la réaction, la continuité et les processus de soutien. Une collaboration étroite et une communication adéquate, notamment, ont permis de réaliser des objectifs importants dans tous ces domaines en 2014.

En matière de prévention, des analyses des vulnérabilités ont été menées ou initiées dans six secteurs partiels critiques (technologies de l'information, trafic routier, approvisionnement en gaz naturel, autorités, organisations de première intervention, protection civile) et un concept de recensement des vulnérabilités des technologies de l'information et de la communication (TIC) a été élaboré au niveau fédéral. Pour identifier les risques, il est indispensable de connaître les menaces existantes et d'avoir un état des lieux complet. Ce dernier repose sur un bilan technique, qui fournit une vue d'ensemble des infrastructures critiques en Suisse et permet aux exploitants de déceler rapidement les appareils infectés sur leur propre réseau. Les principales cybermenaces en 2014 sont répertoriées et exposées dans le rapport semestriel de MELANI et le rapport annuel du Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI).[1]

Concernant la réaction, les centres de compétences destinés à analyser les logiciels malveillants (par ex. GovCERT.ch, CISIRT-OFIT et MilCERT-DDPS) ont été renforcés en 2014 afin d'assurer une disponibilité durable. De plus, il sera possible à l'avenir de faire appel aux connaissances spécialisées de l'association «Swiss Cyber Experts» en cas de cyberincidents complexes et exigeants sur le plan technique, grâce à la convention de coopération conclue en 2014 entre cette association et MELANI.

Dans le domaine de la continuité, l'une des analyses des vulnérabilités effectuées dans les secteurs partiels critiques a permis d'instaurer une gestion de la continuité et des crises. L'objectif visé reste la conclusion d'un accord sectoriel dans lequel les principales entreprises d'approvisionnement s'engagent à se soutenir mutuellement en cas de cyberincidents.

Pour ce qui est des processus de soutien, la collaboration internationale a été renforcée sur une base bilatérale et multilatérale. Sur ce dernier plan, la Suisse, qui assurait la présidence de l'OSCE en 2014, a participé aux mesures de confiance de cette dernière. De plus, les contacts bilatéraux existants ont été intensifiés et de nouveaux contacts ont été noués.

Un examen de l'efficacité des seize mesures a été prévu à partir de 2015. Ses résultats serviront de base aux décisions du Conseil fédéral concernant la marche à suivre après 2017.

[1] L'année 2014 a été principalement marquée par la détection et l'identification de chevaux de Troie et de failles de sécurité qui ont influé et influeront à l'avenir sur la mise en œuvre de la SNPC: «Heartbleed» (faille de sécurité dans l'une des principales bibliothèques de chiffrement), «Cryptolocker» (progression de ce rançongiciel insidieux) et «Regin» (logiciel d'espionnage très complexe).

2 Collaboration

Ce chapitre présente quelques dates importantes dans la collaboration nationale et internationale.

2.1 Niveau national

Le deuxième cyber-landsgemeinde du Réseau national de sécurité (RNS), qui s'est déroulé le 20 mars 2014, a renforcé la collaboration et le réseautage entre la Confédération et les cantons. Il a réuni quelque 70 participants des autorités correspondantes et portait principalement sur les projets en cours au niveau cantonal et sur l'état actuel de la mise en œuvre de la «Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)».

L'association «Swiss Cyber Experts» a été créée le 26 mars 2014 avec la participation de MELANI et la convention de coopération entre ces deux entités a été signée le 17 décembre. L'accès à des ressources spécialisées supplémentaires sera coordonné sur cette base en cas de cyberincidents graves.

La première conférence sur les cyberrisques en Suisse, qui s'est tenue le 20 novembre 2014, visait à favoriser l'échange d'informations sur les activités de l'administration et de l'économie destinées à réduire les cyberrisques en Suisse, en particulier au niveau des infrastructures critiques, et à présenter l'état actuel de la mise en œuvre de la SNPC. Elle a réuni près de 150 représentants de la Confédération, des cantons et des milieux économiques.

L'exercice du Réseau national de sécurité 2014 (ERNS 14) a été réalisé du 3 au 21 novembre 2014. Il a permis d'examiner la collaboration entre les partenaires au sein du RNS, dans le cadre du scénario «Pandémie et pénurie d'électricité». Y ont participé 26 cantons, les services fédéraux des sept départements, l'armée, les organisations de crise et l'économie privée. L'accent a été mis sur l'échelon politico-stratégique, de la gestion des crises à la prise de décisions politiques. L'ERNS 14 a déjà fourni à tous les participants des enseignements précieux, qui seront évalués de manière plus approfondie.

A l'avenir, les différents acteurs se réuniront régulièrement sous la direction de l'Operation Information Center (OIC) de MELANI (Service de renseignement de la Confédération), afin de garantir une analyse exhaustive des menaces existantes. Celles-ci seront ensuite compilées dans un graphique (radar de situation répertoriant toutes les cybermenaces).

2.2 Niveau international

L'élection de Thomas Schneider (Office fédéral de la communication, OFCOM) à la présidence du Comité consultatif gouvernemental (Governmental Advisory Committee, GAC) de l'Internet Corporation for Assigned Names and Numbers (ICANN) en octobre 2014 permet à la Suisse d'exercer une influence directe sur la gestion d'une ressource centrale du Web. Thomas Schneider représentait jusqu'alors la Suisse au GAC; il était également vice-président de cet organe et responsable de l'application de la mesure 9 de la SNPC.

La deuxième European Cyber Security Alpen Cup s'est déroulée à Linz du 3 au 6 novembre 2014. Il s'agit d'un concours international regroupant des écoliers et des étudiants de Suisse, d'Autriche et d'Allemagne sous la direction de Cyber Security Austria et le patronage de MELANI et de l'association Swiss Police ICT, avec la participation de l'association Swiss Cyber Storm. Ce concours vise à détecter, exploiter et corriger les faiblesses des systèmes informatiques.

Lors de la conférence de l'OSCE du 7 novembre 2014 à Vienne, qui était présidée par la Suisse, des représentants des milieux économiques et scientifiques, de la société civile et des gouvernements ont examiné l'état de la mise en œuvre du premier train de mesures de confiance. Ils ont par ailleurs identifié des besoins supplémentaires et rassemblé des idées en vue d'un deuxième catalogue de mesures. La SNPC a été présentée dans le cadre de la mesure de confiance 7 (stratégies et cyberprogrammes nationaux).

Les Etats de l'Organisation du traité de l'Atlantique Nord (OTAN) ont testé leurs capacités à déjouer des cyberattaques lors d'un exercice d'envergure réalisé entre le 18 et le 20 novembre 2014. La collaboration lors du traitement de ces attaques et la coordination ont été analysées. Sept pays non membres de l'OTAN, dont la Suisse, ont été invités à participer à l'exercice.

En décembre 2014, l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a publié l'étude «Framework for Evaluating National Cyber Security Strategies»[2]. La Suisse participe au «Cyber Expert Working Group» de l'ENISA, qui est chargé de comparer les stratégies nationales de cyberprotection et d'identifier les meilleures pratiques et les principes de base. Outre la Suisse, ce groupe de travail comprend 18 Etats membres de l'Union européenne (UE) et sept pays non membres de l'UE.

Sur le plan multilatéral, la Suisse a co-organisé le Sino-European Cyber-Dialog, qui s'est tenu une fois à Genève et une fois à Pékin. Elle a présenté le processus de l'OCDE et proposé l'élaboration de mesures de confiance entre les pays européens participants et la Chine. Dans le cadre de l'Organisation des Nations Unies (ONU), la Suisse s'est notamment engagée pour la protection des droits de l'homme dans le cyberespace, en particulier en tant que membre du groupe à l'origine de l'initiative «Le droit à la vie privée à l'ère du numérique», qui vise à renforcer la protection de la sphère privée dans le cyberespace.

3 Etat de la mise en œuvre de la SNPC en 2014

La SNPC est une stratégie complète qui poursuit une approche globale à travers ses seize mesures 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 deuxième année de mise en œuvre et la plupart des travaux concernant les mesures sont bien avancés. Ce chapitre propose une vue d'ensemble de la mise en œuvre. Les services responsables et l'OC SNPC ont défini concrètement les objectifs et les étapes des différentes mesures et les ont présentés dans une feuille de route (cf. illustration 1). Chaque service responsable de l'application expose brièvement l'état de cette dernière pour la ou 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».

[2] https://www.enisa.europa.eu/media/enisa-en-francais/

Feuille de route SNPC

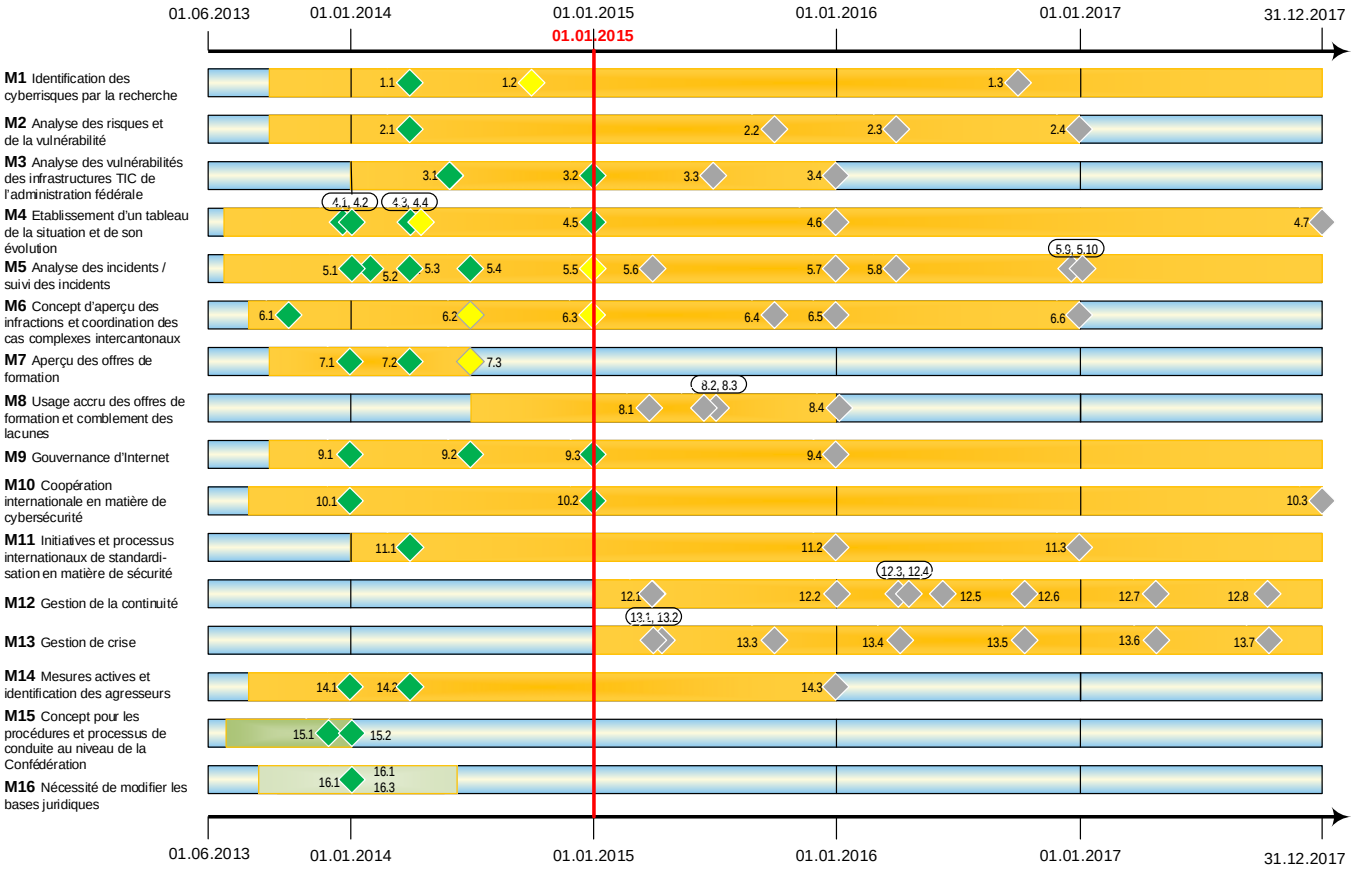

Illustration 1: Feuille de route SNPC

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 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 et M4).

3.1.1 Mesure 2: analyse des risques et vulnérabilités

Compétence: 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.

Etat actuel:

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) et l'Office fédéral de la protection de la population (OFPP) ont réalisé des analyses des vulnérabilités pour le premier groupe de secteurs partiels. L'analyse relative à l'approvisionnement en gaz naturel est achevée (OFAE, octobre 2014). Les travaux concernant les technologies de l'information et le trafic routier (OFAE) sont bien avancés. Les analyses portant sur les secteurs partiels Parlement, Gouvernement, Justice et administration, Protection civile et Organisations de première intervention (OFPP) ont commencé et sont en bonne voie, conformément au plan de mise en œuvre.

Le processus de réalisation des analyses et, partant, la coordination entre les acteurs économiques participants et l'administration ont été harmonisés.

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

Compétence: 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. 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 en matière de TIC de l'administration fédérale au niveau des faiblesses systémiques, organisationnelles et techniques.

Etat actuel:

Dans un premier temps, les tâches ont été analysées et le champ d'application du concept de contrôle M3 a été délimité. Les analyses précédentes des vulnérabilités dans l'administration fédérale, les interfaces avec des projets similaires et les responsabilités ont été identifiées dans un deuxième temps. Une analyse des risques liés à la mise en œuvre de ce concept a ensuite été effectuée et les principales interrogations ont été recensées. Une première ébauche du concept de contrôle a été établie sur cette base.

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 décrive les risques et dommages potentiels de ces attaques dans chaque secteur critique, ainsi que leur pertinence en Suisse.

La SNPC vise à établir un tableau uniforme de la situation en étroite collaboration avec tous les acteurs. Celui-ci intègre toutes les informations pertinentes provenant d'analyses techniques, de sources du service de renseignement et de sources policières.

Etat actuel:

Les travaux destinés à l'élaboration d'un état des lieux ont commencé et un prototype a été développé pour présenter les menaces existantes. Les processus correspondants et leur contrôle, ainsi que les procédures organisationnelles et les responsabilités ont également été

recensés. Cela a permis de déterminer les processus et réglementations nécessaires, tout en tenant compte des priorités.

La rédaction d'un rapport sur la situation technique actuelle a contribué à la réalisation d'une étape importante dans ce domaine. Il est ainsi possible, d'une part, de localiser les appareils infectés et, d'autre part, d'obtenir un aperçu de la situation technique concernant les infections.

Conformément à la mise en œuvre de M4, l'OIC de MELANI assure depuis fin 2014 la coordination des différents acteurs techniques et opérationnels (GovCERT, BAC-COE CNO, Cyber SRC, OFIT-CSIRT, MilCERT et Cyber RM) afin d'analyser de manière approfondie les menaces existantes et d'harmoniser la gestion des incidents.

3.2 Réaction

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

3.2.1 Mesure 5: analyse et suivi des incidents

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

Rattaché à MELANI, le GovCERT œuvre depuis des années dans l'analyse des logiciels malveillants. La SNPC renforce ces capacités techniques et les connaissances spécialisées, notamment en augmentant le temps de disponibilité et la réactivité de tous les CERT et en améliorant leur mise en réseau. L'OIC de MELANI a encore été développé en vue d'améliorer la contextualisation des incidents et l'estimation de leur pertinence. Grâce à la mise en place de Cyber SRC, le Service de renseignement de la Confédération dispose désormais des ressources et des capacités nécessaires pour traiter les incidents relevant de la sûreté de l'Etat.

Etat actuel:

La disponibilité a pu être accrue au sein de GovCERT, de sorte qu'elle est désormais optimale lors d'une exploitation normale. Grâce aux contacts étroits et au réseautage avec des services connexes (autres CERT de l'administration fédérale), il est possible de faire appel à des spécialistes supplémentaires de l'administration fédérale pour surmonter une crise. Les experts de l'association «Swiss Cyber Experts», qui a été créée récemment, sont également disponibles. Concernant le traitement des incidents relevant de la sûreté de l'Etat, le SRC a mis en place une nouvelle unité et lui a alloué les ressources prévues par la SNPC.

La coopération opérationnelle entre la BAC (MilCERT et Computer Network Operations [CNO]), le SRC (Cyber SRC), le RM (Cyber Defence) et l'OFIT (CSIRT) a été davantage systématisée en matière de gestion des cyberincidents dans l'administration fédérale. Par ailleurs, les instruments d'échange d'informations ont été développés, puisqu'une réunion de coordination se tient régulièrement sous l'égide de MELANI. L'armée a renforcé ses propres moyens de détection et d'analyse.

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:

Un questionnaire élaboré par la police et les ministères des affaires publiques de la Confédération et des cantons a permis de dresser, fin juin 2014, un état des lieux de la lutte contre la cybercriminalité en Suisse. Les processus existants, les procédures organisationnelles et les responsabilités des autorités fédérales et cantonales de poursuite pénale ont également été examinés. Certains aspects juridiques ont été clarifiés. Le projet de concept repose donc sur une base solide. Une première version est disponible.

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:

Créée le 1er janvier 2014, la nouvelle unité Cyber du SRC est chargée de traiter les informations pertinentes du Service de renseignement. Elle a commencé son activité, est entièrement opérationnelle et 80 % de ses postes sont déjà pourvus. La mise en œuvre des étapes de la SNPC est donc conforme au calendrier dans ce domaine. Les interfaces avec l'OIC de MELANI ont été mises en place et l'échange d'informations a été initié. La signature d'un accord sur les niveaux de service, qui régit la coopération correspondante, permet de faire appel aux capacités techniques de la BAC pour soutenir Cyber SRC.

3.3 Gestion de la continuité et des crises

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).

3.3.1 Mesure 12: gestion de la continuité

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

En se fondant sur les résultats de l'analyse des risques et vulnérabilités (mesure 2), l'OFAE en sa qualité de chef de file et l'OFPP définissent, dans les entreprises concernées et les services spécialisés compétents, les mesures nécessaires pour assurer la continuité.

Etat actuel:

Les étapes pour poursuivre la mesure 12 ont été fixées jusqu'en 2017 et figurent dans la feuille de route. Les mesures 12 et 13 sont traitées parallèlement. La procédure est tout d'abord testée avec les premiers secteurs partiels, la méthodologie correspondante étant définie et coordonnée par l'OFPP et l'OFAE.

L'OFAE et les représentants de l'industrie du gaz ont obtenu des avancées concrètes pour mettre en place une gestion de la continuité, l'objectif étant la signature d'un accord sectoriel dans lequel les principales entreprises d'approvisionnement s'engagent à se soutenir mutuellement en cas de cyberincidents. Cet accord portera en particulier sur les dépendances inhérentes aux moyens de communication et à la main-d'œuvre qualifiée qui ont été mises en évidence dans l'analyse des vulnérabilités. Un projet d'accord est en consultation auprès de l'industrie du gaz (octobre 2014).

3.3.2 Mesure 13: gestion des crises

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

A travers 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 vulnérabilités (mesure 2). En matière de gestion des crises, il faut faire la distinction 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. De plus, il convient de noter que la mesure 13 complète la mesure 12 et qu'elle doit être considérée au sens d'une gestion de la continuité des affaires et non d'une gestion des crises classique.

Etat actuel:

Les étapes pour poursuivre la mesure 13 ont été fixées jusqu'en 2017 et figurent dans la feuille de route. Les mesures 12 et 13 sont traitées parallèlement. L'OFAE et les représentants des fournisseurs suisses de gaz naturel ont obtenu des avancées concrètes pour mettre en place une gestion de la continuité et des crises (cf. ci-dessus).

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

Compétence: ChF

La mesure 15 vise à inclure les aspects cybernétiques dans la gestion générale des crises.

Etat actuel:

Le concept pour les procédures et processus de conduite permettant de résoudre les problèmes en temps opportun a été établi et mis en œuvre. Le CP SNPC l'a approuvé en février 2014.

Le concept relatif à la mesure 15 a été défini. Il a été étendu par le groupe de travail 3 du mécanisme de consultation et de coordination du Réseau national de sécurité (MCC RNS) *Gestion des crises* et inclut désormais les cantons. Son efficacité doit à présent être évaluée à l'aide d'un scénario approprié; le concept sera adapté le cas échéant (cf. chap. 3.6).

3.4 Processus de soutien

Les coopérations internationales, l'échange d'expériences en matière de formation et de recherche et, le cas échéant, l'adaptation des dispositions légales constituent les bases et processus nécessaires pour aborder la problématique de la cybernétique (M1, M7, M8, M9, M10, M11, M16). Les trains de mesures suivants ont été définis à cet effet:

- recherche et formation des compétences (M1, M7, M8);
- coopérations internationales (M9, M10, M11).

De plus, le groupe spécialisé Cyber International, qui a été créé récemment, permet d'obtenir une vue d'ensemble des activités, des processus et des initiatives qui déploient leurs effets au niveau international et d'encourager l'échange d'informations entre départements.

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'OC SNPC.

Etat actuel:

Le SEFRI a mis en place le comité de pilotage «Identification des cyberrisques par la recherche», qui prescrit l'orientation générale de la recherche, définit les critères d'attribution des projets de recherche et gère une base de données des chercheurs dans le domaine des cyberrisques.

Le comité de pilotage nommera un pool d'experts en cybernétique (constitué de représentants sélectionnés de la recherche et de l'économie) pour acquérir les connaissances spécialisées requises en matière de recherche sur les cyberrisques. Le pool d'experts conseillera le comité de pilotage sur les questions techniques et contribuera notamment à identifier les sujets de recherche et à fixer les priorités dans ce domaine.

3.4.2 Mesure 7: aperçu des offres de formation

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

Dans un premier temps, une vue d'ensemble des offres existantes en matière de formation des compétences dans la protection contre les cyberrisques a été établie. Elle doit servir de base pour identifier les meilleures pratiques dans les groupes cibles définis au sein de l'économie, de l'administration et de la population. De plus, un bref rapport a été rédigé grâce à des recommandations d'experts pour déterminer les offres correspondantes de grande qualité. La publication des offres identifiées (éventuellement en collaboration avec des tiers) est

à l'étude. Sur mandat de la Confédération, l'International Institute for Management Technology (iimt) de l'Université de Fribourg a recensé les lacunes dans l'offre de formation à la gestion des cyberrisques. Le rapport sera publié en 2015.

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

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

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. L'accent est mis sur les offres de formation des compétences qui sont pertinentes pour les exploitants des infrastructures critiques. La mesure est étroitement coordonnée avec la mise en œuvre de la «Stratégie du Conseil fédéral pour une société de l'information en Suisse». L'OC SNPC est chargé de son application, en collaboration avec le SEFRI, l'OFCOM, le DFAE et l'Office fédéral des assurances sociales (OFAS).

Etat actuel:

La mesure 8 se fonde sur les résultats de la mesure 7. Celle-ci étant achevée, les étapes du comblement des lacunes répertoriées dans l'offre de formation ont été définies jusqu'en décembre 2015 et intégrées à la feuille de route. Les travaux ont commencé le 1er janvier 2015. Le comité de pilotage du SEFRI «Identification des cyberrisques par la recherche» (cf. ch. 3.4.1) et son pool d'experts participent à l'identification d'autres lacunes et à la mise en place d'offres remédiant aux déficiences constatées.

3.4.4 Mesure 9: gouvernance d'Internet

Compétence: DETEC-OFCOM; DFAE-PD, DDPS-POLSEC, DFF-MELANI, autorités 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 nationaux et internationaux concernés.

Etat actuel:

L'OFCOM a dressé un inventaire des manifestations, initiatives et organes internationaux en rapport avec la gouvernance d'Internet[3] et rédigé un rapport sur les priorités de la Suisse en la matière et la participation des acteurs concernés.

La Suisse prend une part active aux travaux de l'Internet Cooperation for Assigned Names and Numbers (ICANN), dont le Comité consultatif gouvernemental est présidé par un Suisse[4] depuis fin octobre.

L'OFCOM participe également à la préparation et à l'organisation du «Forum sur la gouvernance de l'Internet» (FGI); il est l'un des initiateurs et des coorganisateurs du forum de dialogue européen du FGI «EuroDIG (European Dialog on Internet Governance)» et il apporte une contribution active aux groupes d'experts du Conseil de l'Europe et à la «Commission de la science et de la technique au service du développement (CSTD)».

Sur le plan national, l'OFCOM organise régulièrement la plateforme de discussion intitulée «Plateforme tripartite suisse pour le SMSI[5]», qui permet à tous les groupes intéressés (administration fédérale, société civile, universitaires) d'échanger des informations sur des sujets

[3] Cet inventaire régulièrement mis à jour a été publié sur CH@World.

[4] Thomas Schneider, OFCOM

[5] Sommet mondial sur la société de l'information

d'actualité et des évolutions concernant Internet. De plus, la Geneva Internet Platform (GIP)[6] a été mise en place en collaboration avec le DFAE et la DiploFoundation.

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 soit utilisé de manière abusive à des fins criminelles, politiques, terroristes ou de renseignement.

Etat actuel:

En 2014, les activités ont principalement porté sur la promotion des mesures de confiance dans le cyberespace, qui visent à accroître la sécurité, la transparence et la prévisibilité des cybermenaces. En tant que présidente de l'OSCE, la Suisse a favorisé l'implémentation du premier train de mesures et sa présentation sur d'autres forums. Elle a notamment exposé sa propre stratégie nationale et commandé une analyse des cyberterminologies existantes. Le développement du catalogue de mesures s'est poursuivi et de nouvelles propositions destinées à renforcer la coopération ont été élaborées avec l'Allemagne.

Dans le cadre de l'ONU, la Suisse a, en particulier, défendu la protection de la sphère privée dans le cyberespace. En ce qui concerne le développement des capacités, elle estime par ailleurs que les pays en développement devraient pouvoir participer aux processus internationaux relatifs à la cybersécurité.

Enfin, les échanges se poursuivent dans le cadre de consultations bilatérales pour défendre les intérêts de la Suisse.

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:

Lors de la mise en œuvre de la mesure 11 de la SNPC, l'OFCOM a réalisé deux tableaux récapitulatifs: le premier répertorie les acteurs de la mesure 11 qui suivent les activités des organisations internationales et les initiatives en matière de cybersécurité et exercent une influence dans ce domaine. Le second tableau comprend les organisations internationales et les initiatives que ces acteurs considèrent comme importantes. Trente-quatre autorités, offices spécialisés et régulateurs ont été invités à participer au premier processus d'élaboration et, sur la base de leurs réponses, 90 autres entreprises privées, associations et instituts de formation. La liste n'est toutefois pas exhaustive. Tous les participants sont dès lors incités à désigner à tout moment d'autres experts nationaux et organisations internationales qui semblent pertinents au sens de la mesure 11.

[6] http://www.giplatform.org/about-gip

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 bases légales pertinentes ont été recensées et la mesure a été approuvée par le CP SNPC en août 2014. L'organe de coordination de la SNPC a établi avec tous les services fédéraux concernés une vue d'ensemble de ces bases légales dans le domaine de la cybernétique et déterminé s'il existait un besoin urgent de révision ou de nouvelle législation. Le besoin législatif constaté sera traité dans le cadre des procédures ordinaires. Il n'existe aucun autre besoin urgent. Il convient cependant de souligner qu'il s'agit uniquement d'un instantané de la situation actuelle et que l'évolution des risques pourrait entraîner à l'avenir de nouveaux besoins sur le plan juridique.

3.5 Mise en œuvre par l'armée

L'armée fait partie des infrastructures critiques du pays pour lesquelles le cyberespace et les cybermenaces sont devenus des sujets importants. Le développement rapide et l'importance croissante du cyberespace offrent de nouvelles options opérationnelles qu'il convient de prendre en considération dans les opérations militaires. Les principales tâches immédiates de l'armée englobent cependant la protection de ses systèmes et infrastructures TIC dans toutes les situations afin de garantir sa capacité et sa liberté d'action.

Compte tenu des besoins susmentionnés, 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. Il est crucial pour celle-ci que les cas de guerre et de conflit soient exclus du champ d'application de la SNPC (cf. chap. 3.4) et qu'elle puisse se préparer à ces situations particulières.

Etat actuel:

Une doctrine a été établie sur la base de l'étude conceptuelle de 2013 sur la cyberdéfense (*Konzeptionsstudie Cyber-Defense,* KS CYD). Elle permet une compréhension commune des tâches de l'armée et de ses partenaires dans le cyberespace. Les principes méthodologiques d'une gestion moderne des cyberrisques et d'une gestion efficace des crises ont été mis en place et sont développés régulièrement. La collaboration de l'armée avec ses partenaires et fournisseurs de prestations critiques a été renforcée, ce qui a permis de réaliser des étapes importantes concernant l'anticipation et l'état de la situation cybernétique.

Le développement des ressources dédiées et la concrétisation du plan de mise en œuvre de la SNPC devraient intervenir en 2015. Les prestations que l'armée doit fournir aux autorités civiles et aux exploitants des infrastructures critiques n'ont pas encore pu être définies précisément dans la politique de sécurité, tout comme leurs responsabilités en cas de conflit ou de guerre.

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:

Un questionnaire concernant l'examen autonome des cyberrisques a été élaboré sur la base de la mesure 3 de la SNPC.

Le processus de traitement des cyberincidents a fait l'objet d'une description et l'un des cinq processus partiels a été réalisé. Un pool d'experts a participé aux descriptions des processus sous la forme d'un partenariat public-privé (Swiss Cyber Experts, cf. ch. 2.1). De plus, le groupe de travail a élaboré une définition d'un incident de cybersécurité.

Le *concept pour les procédures et processus de conduite incluant les aspects cybernétiques* (mesure 15 de la SNPC) a été étendu aux cantons. Il sera examiné dans le cadre d'une série de formations et d'exercices. Plusieurs scénarios possibles de crise liée à la cybernétique ont été établis; ils seront traités lors d'un séminaire stratégique.

Par ailleurs, on a élaboré un projet de concept de gestion nationale des cas (infractions pénales) et de coordination des cas intercantonaux complexes ainsi qu'un concept de formation des forces de police dans le domaine de la cybercriminalité.

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. Celui-ci examinera chaque semestre l'avancement des mesures de la «Stratégie nationale de protection de la Suisse contre les cyberrisques». Les progrès réalisés au niveau des objectifs et des délais seront rapportés au Conseil fédéral par l'intermédiaire de la Conférence des secrétaires généraux (CSG). L'OC SNPC et les offices fédéraux responsables ont fixé les objectifs, les étapes et le calendrier des seize mesures de la SNPC.

5 Evaluation de l'efficacité

Le Conseil fédéral a chargé le CP SNPC de lui soumettre une évaluation de l'efficacité au plus tard au printemps 2017 (p. 10 du plan de mise en œuvre). Une entreprise externe a été mandatée pour effectuer cette évaluation. Celle-ci doit indiquer:

- le degré de réalisation des mesures de la stratégie en termes de contenu et d'organisation et leur contribution probable à la réalisation des objectifs de la SNPC;
- si l'administration fédérale a utilisé les moyens personnels et financiers alloués pour la mise en œuvre de la stratégie et, en particulier, si des ressources supplémentaires seront nécessaires à l'avenir;
- si la SNPC doit être adaptée en fonction des résultats de l'évaluation.

L'évaluation de l'efficacité est prévue en deux étapes, avec les contenus suivants: lors du concept préliminaire, les principaux éléments de l'évaluation (par ex. priorités au niveau du contenu, ampleur, organisation, etc.) ont été définis en concertation avec les acteurs concernés. La concrétisation relève du concept détaillé, dont l'élaboration a commencé.

6 Considérations finales

Près de deux ans se sont écoulés depuis l'approbation du plan de mise en œuvre de la SNPC en mai 2013. L'application de certaines mesures est un processus long et complexe. La consolidation des projets et l'état des lieux effectué avec les acteurs concernés ont parfois demandé énormément de temps. Les ressources limitées et leur priorisation par les services compétents ainsi que les vérifications approfondies des bases légales ont partiellement retardé les travaux de mise en œuvre. De plus, certaines tâches ne peuvent pas être exécutées en parallèle, car elles dépendent d'autres réalisations. La mise en œuvre respecte néanmoins le calendrier à quelques exceptions près, de sorte que le bilan établi fin 2014 est globalement positif.

Grâce à la SNPC, la collaboration avec les cantons est tournée vers l'avenir et repose sur la confiance. Les échanges réguliers de connaissances et d'expériences entre la Confédération et les cantons sont ainsi encouragés et la coopération avec d'autres services s'est améliorée, ce qui correspond à la philosophie de l'approche décentralisée qui a été retenue pour la mise en œuvre de la SNPC. Cette coopération a également conduit à un partage des meilleures pratiques, qui a réduit la charge des cantons concernés tout en augmentant l'efficacité de leurs mesures. La collaboration avec l'armée a pu être organisée en vue de son soutien subsidiaire. En outre, l'échange d'informations entre les exploitants des infrastructures critiques, les prestataires TIC, les fournisseurs de systèmes, les associations, les organismes nationaux de normalisation, les autorités spécialisées et les régulateurs a été renforcé. Les intérêts de la place économique suisse ont également été exposés et représentés de manière coordonnée dans les instances publiques et privées internationales chargées de la sécurité, de la sûreté et de la normalisation.

La SNPC a initié un processus et doit s'adapter régulièrement aux nouvelles menaces. Il est donc important de maintenir à l'avenir la collaboration, la coopération et la communication entre les acteurs concernés et de faire appel à des acteurs supplémentaires si nécessaire.

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

7.2 Récapitulation des interventions parlementaires relatives aux cyberrisques

Intervention Ip. = Interpellation; Mo. = Motion; Po. = Postulat; Qu. = Question	Déposée le:	Etat au 31.12.2014:
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 délibérations du Conseil des Etats du 15 mars 2011 (BO CE 15.03.2011)	29.06.2010	liquidé
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
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	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 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	liquidé
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
14.1105 Qu. Buttet. Moyens dédiés à la cyber-défense 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

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