Rapport annuel 2016

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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

Publication: Mai 2017

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
info@isb.admin.ch

Rapport annuel: www.isb.admin.ch

Table des matières

Préambule

L'année 2016 a elle aussi rappelé à quel point la numérisation et l'automatisation sont devenues des enjeux importants et complexes dans tous les domaines de la vie. La démonstration en a notamment été faite au salon CeBIT, dont la Suisse était le pays partenaire en 2016. Il était placé sous le signe de la numérisation et de l'automatisation croissantes de nouveaux secteurs. Les progrès réalisés sur le terrain de la mobilité autonome, ou le développement de robots se chargeant de nos tâches humaines, sont particulièrement spectaculaires. Les chances qu'offre la numérisation sont bien réelles pour la Suisse aussi. Mais la numérisation comporte hélas aussi des risques, comme l'ont clairement montré les récentes cyberattaques. Les activités d'espionnage et de sabotage, de nouvelles variétés de maliciels jusque-là inconnues, et le chantage basé sur les attaques DDoS font partie du quotidien. Nous devons rester vigilants et continuer de renforcer notre cybersécurité, afin d'être prêts à réagir à la menace croissante due aux cyberattaques.

Il va de soi que le principal problème est de savoir si la Suisse est dans la bonne voie, et si les mesures de protection déjà prises suffiront à se prémunir durablement contre ces cyberrisques. En adoptant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) et son plan de mise en œuvre, nous avons pris la bonne direction et avons déjà obtenu de nombreux résultats. Concrètement, quinze des seize mesures prévues dans la SNPC étaient achevées à la fin de 2016. Les travaux réalisés ont été soumis en 2016 à une évaluation de l'efficacité, qui visait à montrer où les objectifs ont été atteints et où il convient encore d'agir. Le présent rapport résume brièvement les résultats de cette analyse.

Sans revenir ici sur les résultats de l'évaluation de l'efficacité, on peut dire que la mise en œuvre de la SNPC a conduit à des progrès notables dans beaucoup de domaines. Grâce à cette stratégie, nous avons jeté les bases d'une collaboration empreinte de confiance entre la Confédération, les cantons, l'économie et la société, afin de mieux protéger la Suisse contre les cyberattaques. Au niveau international également, la Suisse a poursuivi son engagement, dans le cadre de sa politique extérieure et de sa politique de sécurité, en faveur d'un cyberespace ouvert, libre et sûr. Elle a notamment été élue pour un an en tant que membre du Groupe d'experts gouvernementaux de l'ONU sur la sécurité internationale dans le cyberespace[1].

Or les événements des dernières années et les résultats de l'évaluation de l'efficacité l'ont clairement montré: malgré l'importance des acquis actuels, les travaux liés à la cybersécurité sont loin d'être terminés. Nous entreprendrons donc en 2017 toutes les démarches nécessaires afin qu'en Suisse, les acteurs économiques, les autorités et la population puissent continuer de se mouvoir en sécurité et librement dans Internet. Cela implique notamment de développer la SNPC. Les travaux liés à la stratégie actuelle s'achèveront à la fin de cette année, et nous sommes déjà en train de fixer les prochaines étapes, en étroite collaboration avec toutes les parties prenantes.

Dans cet esprit, nous nous réjouissons d'améliorer encore avec vous la protection de la Suisse face aux cyberrisques, afin de pouvoir tirer parti des chances que la numérisation nous offre, sans pour autant encourir de risques inconsidérés.

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

[1] UN Governmental Group of Experts on the Development in the field of information and telecommunications in the context of international security

1 Résumé

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

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

Les seize mesures portent sur quatre domaines: la prévention, la réaction, la continuité et les processus de soutien (coopération internationale, recherche et formation, et bases légales). D'importants objectifs ont été atteints dans tous les domaines au cours des dernières années, grâce notamment à l'étroite collaboration et à la bonne communication de tous les acteurs. C'est ainsi qu'à la fin de l'année 2016, quinze des seize mesures prévues dans la SNPC étaient achevées, et que le calendrier du plan de mise en œuvre a été dûment respecté. Il ressort encore de l'évaluation de l'efficacité menée en 2016 que la SNPC a eu un impact considérable et que l'approche décentralisée, basée sur le risque, a fait ses preuves.

En matière de **prévention**, l'Office fédéral de la protection de la population (OFPP) et l'Office fédéral pour l'approvisionnement économique du pays (OFAE) ont procédé à des analyses des risques et des vulnérabilités dans les secteurs identifiés comme d'importance vitale dans la stratégie pour la protection des infrastructures critiques (stratégie PIC), et les rapports sont d'ores et déjà disponibles.

La présentation de la situation globale de la menace est l'œuvre du Service de renseignement de la Confédération (SRC). Cette présentation interactive, appelée radar de la situation, permet de visualiser les différentes cybermenaces guettant les infrastructures de la Suisse et en montre à chaque fois l'importance relative. À partir de 2017, MELANI mettra le radar de la situation à la disposition des membres de son cercle fermé. Les rapports semestriels de MELANI et le rapport annuel de l'Office fédéral de la police (fedpol) offrent un bon aperçu des principales cybermenaces en 2016.

En ce qui concerne la **réaction**, les centres de compétences chargés d'analyser les logiciels malveillants de l'UPIC et du Département fédéral de la défense, de la protection de la population et des sports (DDPS), à l'instar de GovCERT, CSIRT-OFIT, milCERT-DDPS, ont continué d'être renforcés, et bien d'autres produits venus s'y ajouter ont accru la capacité de détection et de réaction. En outre, d'importants processus tant internes qu'externes ont été mis en place pour améliorer la communication, tandis que les coopérations internationales ont été renforcées.

Par ailleurs, l'unité Cyber du SRC a acquis des connaissances spécialisées et des aptitudes lui permettant d'analyser les objectifs, les méthodes et les acteurs d'une cyberattaque, ainsi que d'identifier les agresseurs potentiels. En outre, la loi fédérale sur le renseignement (LRens) acceptée par le peuple suisse confère au SRC la base juridique nécessaire, en cas de grave cyberattaque visant des infrastructures d'importance vitale, pour prendre des contre-mesures offensives, ce qui simplifie grandement sa recherche d'informations. Il est vrai qu'à l'heure actuelle, il faudrait notamment des analystes opérationnels et techniques supplémentaires et davantage de spécialistes des langues, afin de permettre au SRC d'analyser les cyberattaques de façon plus systématique et plus durable.

Dans le cadre de la **continuité**, l'OFPP et l'OFAE élaborent avec les exploitants d'infrastructures d'importance vitale, avec les autorités spécialisées ainsi qu'avec les autorités de surveillance et de régulation, des mesures propres à améliorer la résilience informatique des secteurs partiels. Ces travaux, qui reposent sur les résultats d'analyses des risques et de la vulnérabilité, servent à réduire les faiblesses et les risques identifiés. Sachant que l'adoption de directives et de normes minimales joue un rôle croissant dans beaucoup de secteurs, il faut veiller à coordonner les nouvelles mesures avec les prescriptions déjà en vigueur.

Pour ce qui est des **processus de soutien**, l'accent est mis sur la recherche et la formation, ainsi que sur la collaboration internationale. Le Secrétariat d'État à la formation, à la recherche et à l'innovation (SEFRI) et l'OC SNPC ont institué d'importants comités chargés de dresser, en collaboration avec les milieux économiques et l'administration, une vue d'ensemble des offres existantes en matière de formation des compétences, avec des propositions visant à en garantir le bon usage et à en combler les lacunes. C'est ainsi qu'un nouveau diplôme fédéral d'expert en sécurité informatique a vu le jour en un temps record, avec le concours de l'association ICT-Formation professionnelle Suisse et le soutien de nombreuses entreprises.

En parallèle, un rapport d'expert a permis d'identifier sur le plan suisse les principaux thèmes de recherche dans le domaine des cyberrisques. En outre, un comité interdépartemental et interoffices coordonne désormais dans toute l'administration les travaux des services spécialisés actifs dans la recherche (cyberrisques). Enfin, le réseau des chercheurs a resserré ses liens à la «Swiss Cyber Risk Research Conference».

La collaboration interétatique dans une optique de paix et de sécurité internationales a continué d'être renforcée et étendue sur une base bilatérale et multilatérale, sous la conduite de la Division Politique de sécurité (DPS) du Département fédéral des affaires étrangères (DFAE). L'Office fédéral de la communication (OFCOM) s'est par ailleurs chargé des questions de gouvernance d'Internet. De plus, les contacts bilatéraux existants ont été intensifiés et de nouveaux contacts ont été noués. Au niveau multilatéral, les travaux liés aux mesures de confiance de l'Organisation pour la sécurité et la coopération en Europe (OSCE) ont été poursuivis, et la Suisse a été élue en 2016 membre du Groupe d'experts gouvernementaux de l'ONU sur la sécurité internationale dans le cyberespace (UN Group of Governmental Experts on Cybersecurity, UNGGE).

Principales cybermenaces en 2016

L'année 2016 a été essentiellement marquée par des cybermenaces similaires à celles de 2015.[2] La principale différence réside toutefois dans l'intensité et la fréquence accrue des cyberattaques. Une spécialisation croissante a ainsi été constatée en 2016. De même, les attaques informatiques à des fins d'espionnage sont en hausse. Comme le relève le rapport semestriel 2016/2 de MELANI, le cyberespionnage constitue une menace à prendre au sérieux, et les entreprises doivent être conscientes qu'il s'agit d'un risque bien réel et non pas hypothétique. Les nombreux cas portés à la connaissance de MELANI attestent de cette prise de conscience. Autre sujet de préoccupation, les cybercriminels ont toujours plus tendance à lancer eux aussi des attaques complexes de type APT (advanced persistent threat).

Les principales cybermenaces constatées en 2016 ont été les suivantes[3]:

- **espionnage** (attaque contre une entreprise d'armement)
- **fuites d'information** (revente au noir de données d'accès à Twitter, vol de mots de passe)
- **attaques DDoS et chantage** (Cryptolocker, Locky, Armada Collective, KeRanger, CTB-Locker)

[2] MELANI rapport semestriel 2015/1 (janvier à juin): www.melani.admin.ch

[3] Pour plus de détails sur ces menaces, voir MELANI, rapport semestriel 2016/1 (janvier à juin): www.melani.admin.ch

- **Social Engineering, phishing** (arnaque au president ou CEO Fraud)
- **logiciels criminels** (chevaux de Troie bancaires comme Gozi, Conficker ou Dyre)
- **attaques contre les systèmes de contrôle industriels** (piratage de systèmes de commande de centrales électriques en Ukraine).

2 État de la mise en œuvre de la SNPC en 2016

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

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

Le présent chapitre propose une vue d'ensemble de la mise en œuvre (feuille de route). Les services responsables y exposent brièvement, à chaque fois, l'état actuel de la mise en œuvre des diverses mesures, regroupées par domaine.

Feuille de route de la SNPC

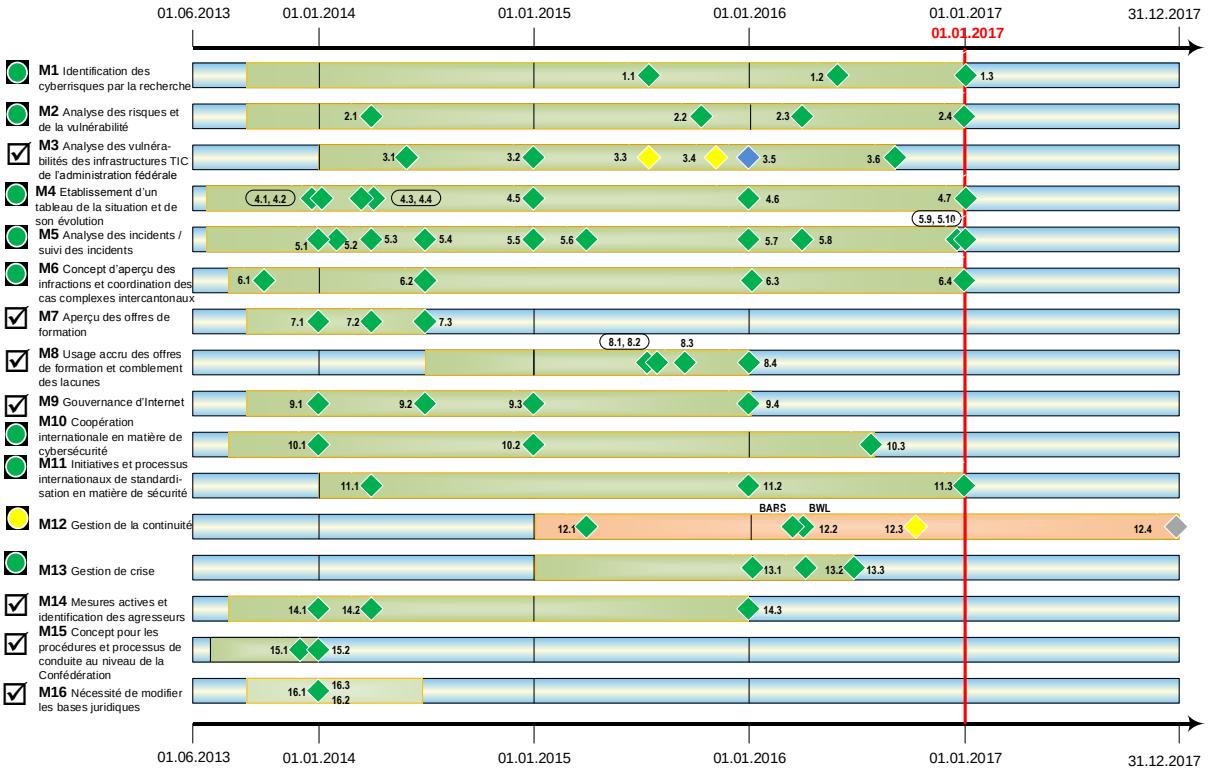

Illustration 1: Feuille de route de la SNPC

Légende: Etat des étapes

- Étape menacée
- Étape en retard
- Étape mise en œuvre selon le calendrier
- Mesure spécial

2.1 Prévention

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

2.1.1 Mesure 2: analyse des risques et vulnérabilités

Compétence: DEFR-OFAE, DDPS-OFPP, autorités spécialisées, autorités de surveillance et de régulation; DFF-MELANI

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

L'OFAE et l'OFPP se partagent les travaux à réaliser dans les 28 secteurs partiels définis en Suisse et coordonnent leur approche. Les analyses des risques et vulnérabilités ainsi effectuées ont généralement respecté le calendrier. De nombreux experts issus des entreprises, des associations de la branche, des autorités spécialisées ou encore des autorités de surveillance et de régulation compétentes à l'échelon tant de la Confédération que des cantons y ont participé. Les analyses reposent ainsi sur des bases solides, et ont confirmé le réel intérêt des services concernés.

État actuel:
La mesure a été achevée pour l'essentiel en 2016, mais des travaux de finalisation suivront encore. Des analyses de vulnérabilité ont été réalisées dans les 28 secteurs partiels. Ces analyses servent de base à la mise au point de mesures destinées à renforcer la capacité de résistance informatique (voir chapitre 3.3.1 Gestion de la continuité).

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

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

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

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

Dans l'exercice de sa mission, l'UPIC a établi à la fin de 2015 un concept de contrôle des infrastructures informatiques de l'administration fédérale (ci-après concept de contrôle), qui s'inspirait des normes fondées sur le risque ainsi que des bonnes pratiques établies dans le domaine de la gestion de la sécurité informatique (par ex. IRAM2 de l'ISF), et qui reflétait en ainsi la doctrine actuelle. Mais comme les travaux de mise en œuvre de ce concept s'annonçaient particulièrement lourds, le CP SNPC a décidé le 25 février 2016, sur proposition de l'OFAE, du DFAE et du SRC, que l'UPIC devait encore élaborer, à titre de mesure spéciale de la M3, une proposition alternative à son concept de contrôle pour la suite des travaux dans le domaine de l'analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale. Alors même que le poste temporaire créé pour la M3 avait déjà été supprimé à la fin de 2015, l'UPIC a élaboré dans le cadre de cette mesure spéciale le modèle demandé, soumis le 31 mai 2016 au CP SNPC. Ce dernier s'est prononcé en faveur du nouveau modèle. En substance, il renonce à une approche basée sur le risque, au profit

d'une analyse de la vulnérabilité.

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

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

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

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

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

La présentation de la situation globale de la menace a vu le jour. À partir de 2017, MELANI mettra cette présentation interactive (radar de la situation) à la disposition des membres de son cercle fermé. Une version publique suivra plus tard.

Une expertise externe a également été réalisée pour juger des processus d'autoamélioration mis en place par MELANI.

2.2 Réaction

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

2.2.1 Mesure 5: analyse et suivi des incidents

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

La capacité à se préparer et à réagir aux cyberincidents est une condition essentielle de la réduction des cyberrisques. Le plan de mise en œuvre de la SNPC prévoit donc le développement de l'analyse et du suivi des incidents. Les divers centres d'alerte et de réaction aux attaques informatiques (GovCERT, CSIRT-OFIT, milCERT-DDPS) doivent renforcer leurs capacités d'analyse des maliciels, afin de pouvoir traiter les données en cas d'incident et adopter les contre-mesures indiquées sur le plan technique. L'accomplissement de ce mandat exige en premier lieu un renforcement des capacités techniques et des connaissances spécialisées, de même qu'une analyse exhaustive et une évaluation des menaces. S'ajoutent à cela un renforcement de l'endurance et de la capacité de réaction de tous les CERT, de même qu'un réseautage plus marqué de ces derniers.

État actuel:

La mise en œuvre de la mesure a pris fin en 2016.

Globalement, les centres de compétences spécialisés (GovCERT, CSIRT-OFIT, milCERT) ont encore accru leurs capacités de détection et de réaction.

En outre, la LRens acceptée par le peuple suisse en 2016 prévoit expressément que le SRC protège les infrastructures d'importance vitale face aux cyberattaques, et confère désormais au SRC la base juridique nécessaire, en cas de grave cyberattaque visant des infrastructures d'importance vitale, pour prendre des contre-mesures offensives. La recherche d'information et l'infiltration dans des systèmes et réseaux informatiques sont également prévues dans la LRens.

Le poste créé dans le cadre de la SNPC afin d'élucider les cyberincidents a été pourvu en 2016. Les tâches assumées sont les suivantes:

- recrutement et gestion de sources d'informations (experts externes),
- recherche d'informations (sans les mesures soumises à autorisation selon la LRens),
- analyses stratégiques,
- analyses techniques,
- identification des agresseurs (attribution) par les moyens du SRC,
- coopération internationale.

La constitution d'un réseau de sources et le resserrement des liens avec les services partenaires à l'étranger ont régulièrement permis au SRC de découvrir de bonne heure des cyberattaques. Or à l'heure actuelle, avec les moyens et capacités à sa disposition, le SRC ne parvient à traiter qu'une petite partie des informations recherchées. Et comme les cyberattaques durent souvent plusieurs années, les rares spécialistes sont durablement occupés. Face au risque croissant de ne pas reconnaître à temps de nouvelles attaques, il est donc essentiel d'analyser les cyberattaques de façon plus systématique et plus durable. Le SRC aurait notamment besoin aujourd'hui d'analystes opérationnels et techniques supplémentaires et de davantage de spécialistes des langues pour mener à bien cette tâche.

2.2.2 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. À cette fin, la SNPC prévoit (M6) que le Service de coordination de la lutte contre la criminalité sur Internet (SCOCI), rattaché au Département fédéral de justice et police (DFJP), présente fin 2016, en collaboration avec les cantons, un concept intitulé «Vue d'ensemble des infractions et coordination des cas intercantonaux complexes».

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

Tant la coordination des enquêtes liées à la cybercriminalité, prévue par la mesure 6 de la SNPC, que le tableau de la situation en Suisse font déjà l'objet de l'arrangement administratif conclu entre le DFJP et la Conférence des directrices et directeurs cantonaux de justice et de police (CCDJP), au sujet des missions du SCOCI, rattaché à fedpol. Or ces missions du SCOCI, financées conjointement par la Confédération et les cantons, n'ont été qu'en partie réalisées à ce jour. Aussi le concept M6 de la SNPC, élaboré en commun par les autorités de poursuite pénale de la Confédération et des cantons, prévoit-il des mesures visant la saisie uniforme, la coordination et la diffusion des informations requises pour établir un tableau d'ensemble exhaustif de la cybercriminalité. Quant à la coordination intercantonale visée pour tous les cyberdélits, le concept décrit de premières mesures de police destinées à

déterminer les autorités localement et matériellement compétentes pour la poursuite des agresseurs, qui agissent souvent depuis l'étranger et à partir de cyberinfrastructures étrangères. La CCDJP a fait savoir à sa réunion du 18 novembre 2016 qu'elle soutient le concept.

Le tableau de la situation en Suisse et la coordination des cas intercantonaux ne constituent toutefois que deux aspects du défi soulevé par la cybercriminalité. La Conférence des commandants des polices cantonales de Suisse (CCPCS) met encore sur pied un dispositif national relatif à la cybercriminalité et à la forensique informatique. Ces travaux serviront à clarifier dans leur globalité les questions d'organisation et d'infrastructure. Fedpol participera à ces travaux. La question de la mise en œuvre du concept lié à la mesure M6 sera donc examinée dans le cadre de ce dispositif de la CCPCS.

2.2.3 Mesure 14: mesures actives d'identification des agresseurs

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

La SNPC entend renforcer les capacités du 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.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

Il convient d'ajouter aux explications figurant au point 3.2.1 qu'en 2016, le SRC a pu attribuer certaines cyberattaques lancées contre la Suisse à des agresseurs étatiques ou soutenus par un État. Ces découvertes ont été reprises dans de brèves analyses, des rapports et des notes d'information adressés aux autorités compétentes. L'attribution est un processus du renseignement permettant d'identifier les agresseurs avec un degré de probabilité suffisant. L'objectif premier n'est pas de lancer des poursuites pénales, mais de préserver la marge de manœuvre politique. En ce sens, les résultats s'adressent en premier lieu aux décideurs politiques.

2.3 Gestion de la continuité et des crises

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

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

Compétence: DEFR-OFAE, DDPS-OFPP, autorités spécialisées, autorités de surveillance et de régulation; DFF-MELANI

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

État actuel:
L'OFPP et l'OFAE élaborent avec les exploitants d'infrastructures d'importance vitale, avec les autorités spécialisées ainsi qu'avec les autorités de surveillance et de régulation, des mesures propres à améliorer la résilience informatique des secteurs partiels. Ces travaux, qui reposent sur les résultats d'analyses des risques et de la vulnérabilité, servent à réduire les faiblesses et les risques identifiés.

Les rapports renfermant les mesures à prendre pour améliorer la résilience informatique de tous les secteurs partiels définis dans la stratégie pour la protection des infrastructures critiques (stratégie PIC) seront disponibles à la fin de 2017. Diverses mesures ont déjà été réalisées ou sont en train de l'être. Ces travaux permettront d'accroître la capacité de résistance aux perturbations ou attaques informatiques des secteurs partiels assurant l'approvisionnement de notre pays en biens et services de nécessité vitale.

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

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

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

Dans les cas susceptibles d'avoir des conséquences sur la politique étrangère, le DFAE est informé et associé à l'élaboration d'une planification préventive.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

L'enquête réalisée en novembre 2015 auprès des membres du cercle fermé a été évaluée en 2016, et les principaux résultats ont été consignés dans un rapport. Il en ressort que le modèle de partenariat public-privé de MELANI continue de bien fonctionner. En outre, MELANI a bien géré la forte expansion de son cercle fermé survenue ces dernières années. Les défis actuels consistent à renforcer les secteurs encore peu établis.

À partir des résultats de cette enquête, MELANI a élaboré un concept visant à renforcer son rôle de plateforme d'échange d'informations. Le concept précise la mission de base et les objectifs de MELANI et indique les mesures utiles au développement de MELANI, sur le plan tant opérationnel que stratégique. Les mesures préconisées ont encore fait l'objet d'une expertise externe.

2.3.3 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 déjà en place.

État actuel:
La mise en œuvre de la mesure a pris fin en 2014.

La mesure 15 s'est terminée au niveau de la Confédération avec l'adoption d'un concept pour les procédures et processus de conduite incluant les aspects cybernétiques. Mais la collaboration avec les cantons et les exploitants d'infrastructures d'importance vitale s'est poursuivie, dans le cadre de la mise en œuvre de la SNPC incombant au Réseau national de

sécurité, au sein du groupe de travail 3 Gestion des crises. Les activités de ce groupe de travail ont également leur place dans le rapport annuel sur la SNPC. Les détails sont résumés au chapitre 3.6.

En novembre 2016, l'exercice Popula a simulé une cyberattaque contre le système suisse de retraites. La FEAS a assuré, en collaboration avec la Confédération, les cantons et les exploitants d'infrastructures concernés, la conduite de l'exercice qui visait à tester l'état de préparation et la gestion des crises à l'échelon de la Confédération et des cantons.

2.4 Processus de soutien

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

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

2.4.1 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. À cet effet, il s'agit d'exploiter et d'encourager de façon ciblée les travaux de recherche (tant fondamentale qu'appliquée) consacrés à la protection contre les cyberrisques. Le SEFRI est responsable de la mise en œuvre, en collaboration avec l'OC SNPC.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

D'importants progrès ont été réalisés dans les travaux visant à identifier les thèmes de recherche prioritaires. Le comité interdépartemental de pilotage Recherche et Formation Cyber (CoPIRFCyber) a désigné un groupe de quinze experts issus des hautes écoles suisses, qu'il a chargé d'identifier les principaux thèmes de la recherche. Ce groupe d'experts aux compétences diversifiées a passé au crible les disciplines, perspectives et enjeux du paysage scientifique et a identifié neuf domaines où il faudrait intensifier à l'avenir les travaux de recherche. En outre, comme cette thématique est au carrefour de plusieurs disciplines, trois grands thèmes à la fois interprofessionnels et interdisciplinaires ont été recommandés comme axes de recherche prioritaires pour l'avenir. Le rapport consolidé en 2016 par le groupe d'experts paraîtra probablement à l'été 2017.

Sur la base des travaux de fond menés en 2016 par le SEFRI et le Secrétariat d'État à l'économie (SECO), le Conseil fédéral a approuvé le 11 janvier 2017 le rapport sur les principales conditions-cadre pour l'économie numérique, chargeant au passage le Département fédéral de l'économie, de la formation et de la recherche (DEFR) d'examiner en détail les défis qui s'ensuivent pour la formation et la recherche. Son mandat implique en substance d'analyser, avec la participation des offices fédéraux compétents, des cantons et de la Conférence suisse des hautes écoles (CSHE), les effets systémiques de la numérisation sur le domaine de la formation, et d'identifier les éventuelles lacunes à combler au sein des hautes écoles pour négocier avec succès le virage numérique. Les travaux liés au rapport d'audit (volet de recherche) reprendront les conclusions du rapport d'expert sur la recherche dans le domaine des cyberrisques (voir plus haut) et les affineront le cas échéant.

La Swiss Cyber Risk Research Conference, menée le 20 mai 2016 à l'EPFL, a en outre constitué une étape importante vers la mise en réseau et la sensibilisation des chercheurs étudiant les cyberrisques. Plus de 300 participants ont assisté aux exposés de spécialistes tant suisses qu'étrangers. La conférence a lancé un signal clair en faveur du renforcement de la recherche sur les cyberrisques en Suisse, réunissant pour la première fois des spécialistes de toutes les disciplines concernées.

2.4.2 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 DFAE.

État actuel:

La mise en œuvre de la mesure 7 a pris fin en 2015.

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

Compétence: OC SNPC; SEFRI, DFAE-DP

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

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

La mesure 8 a été achevée comme prévu en 2016. Le comité interdépartemental de pilotage Recherche et Formation Cyber a adopté un concept montrant où il y a lieu d'encourager la formation dans le domaine des cyberrisques.

Cette mesure a principalement abouti à la création d'un nouveau diplôme fédéral d'expert en sécurité informatique, délivré par l'association ICT-Formation professionnelle Suisse. Avec l'aide de la SNPC, cette association a réussi à créer dans le secteur privé un large partenariat en faveur du nouveau diplôme, ainsi qu'à formuler avec ces partenaires le profil de qualification correspondant. Ce profil est désormais défini, et les premiers examens pourront avoir lieu à partir de l'automne 2018.

2.4.4 Mesure 9: gouvernance d'Internet

Compétence: DETEC-OFCOM; DFAE-DP, 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'État de droit. L'OFCOM est chef de file et participe aux processus internationaux et régionaux concernés tels que l'ICANN, 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 et le Conseil de l'Europe.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

La dernière étape, réalisée en 2016, a été une analyse de l'efficacité. Il en ressort que l'engagement de la Suisse dans le domaine de la gouvernance d'Internet, par le biais de la mise en œuvre de la mesure 9, correspond aux objectifs de fond et qu'il est globalement mieux coordonné. En effet, la collaboration au sein de l'administration ainsi qu'avec les divers groupes d'intérêt a été institutionnalisée et structurée, et les synergies mieux exploitées. La collaboration devra être étendue encore à l'avenir, pour permettre à la Suisse de s'engager de manière active et coordonnée même quand la gouvernance d'Internet la confrontera à de nouveaux défis.

2.4.5 Mesure 10: coopération internationale en matière de cybersécurité

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 l'intermédiaire d'initiatives et de ses relations internationales, la Suisse participe aux efforts visant à éviter que le cyberespace ne soit utilisé de manière abusive à des fins criminelles, politiques, terroristes ou de renseignement.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

En 2016, la Suisse a poursuivi son engagement, dans le cadre de sa politique extérieure et de sa politique de sécurité, en faveur d'un cyberespace ouvert, libre et sûr, dont l'utilisation repose sur des règles claires. Elle s'est surtout impliquée dans le Groupe d'experts gouvernementaux de l'ONU sur les progrès de la téléinformatique dans le contexte de la sécurité internationale (Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UNGGE), seul comité des Nations Unies à s'occuper de l'élaboration, au niveau mondial, de normes de conduite pour les États, de l'applicabilité du droit international public, de l'instauration d'un climat de confiance et du développement des capacités dans le cyberespace. La Suisse a été désignée membre pour la première fois pour la période 2016-2017. Ses priorités résident dans la consolidation et la concrétisation des travaux conceptuels déjà réalisés par le groupe, d'une part, et dans l'intégration au processus des États ne faisant pas partie de l'UNGGE et des acteurs non étatiques, d'autre part.

La Suisse a également participé activement au processus de l'OSCE visant à instaurer un climat de confiance dans le cyberespace, en améliorant la transparence, la coopération et la stabilité. Sachant que plus la confiance règne entre les États, moins les erreurs d'appréciation et les malentendus sont à craindre. Dans ce cadre, la Suisse a encouragé la mise en œuvre des mesures de confiance déjà adoptées et soutenu en parallèle la mise au point de mesures additionnelles. Compte tenu de la portée planétaire des cyberrisques, la Suisse s'est encore mobilisée en faveur de l'universalisation du processus de l'OSCE.

La Suisse s'est ponctuellement engagée pour le développement des cybercapacités. Elle a soutenu les projets du Forum mondial sur la Cyber Expertise (Global Forum on Cyber Expertise, GFCE), à l'instar de l'initiative Meridian axée sur la protection des infrastructures d'information d'importance vitale. Par ailleurs, afin d'assurer le développement de ses propres capacités nationales, la Suisse a intensifié sa collaboration avec le Centre d'excellence de l'OTAN pour la cyberdéfense en coopération (CCDCoE) basé à Tallin, en Estonie.

Cette année aussi, la Suisse a participé activement au dialogue noué entre des États

européens et la Chine pour mieux comprendre les perceptions respectives des menaces et identifier les questions dont l'approfondissement présente un intérêt commun.

Enfin, la Suisse a procédé au niveau bilatéral à des consultations avec des pays spécifiques sur des questions liées au cyberespace.

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

Compétence: DETEC-OFCOM; OC SNPC, autorités spécialisées, DFAE-DP, 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.

État actuel:
La mise en œuvre de la mesure a pris fin en 2016.

Dans le cadre de la mesure 11, un atelier organisé en 2016 a réuni les acteurs concernés à des fins d'échange d'informations, et l'efficacité a été analysée lors d'une enquête. Les résultats ont été exploités à la fin de 2016 et mis en forme au début de décembre avec les réactions des acteurs. Avec la remise en fin d'année du rapport sur l'analyse de l'efficacité à l'OC SNPC, les délais seront vraisemblablement respectés pour toutes les étapes prescrites et pour les divers objets à fournir.

La mesure peut être considérée comme terminée en ce qui concerne la planification de projets de la SNPC. L'évaluation des résultats et les activités en cours seront poursuivies en 2017.

2.4.7 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, puis 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.

État actuel:
La mise en œuvre de la mesure a pris fin en 2014.

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

2.5 Mise en œuvre par l'armée

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

L'armée dispose de connaissances et d'aptitudes étendues auxquelles les offices responsables peuvent recourir de manière subsidiaire en cas de nécessité, pour autant que

l'armée n'en ait pas elle-même besoin.

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

État actuel:
En 2016, l'armée a poursuivi la mise en œuvre de son concept de cyberdéfense et procédé à différentes améliorations organisationnelles. L'augmentation constante des cybermenaces et des cyberincidents, le oui du peuple à la LRens, l'adoption par le Parlement de la loi sur l'armée (LAAM) et les suites de la cyberattaque contre RUAG font partie des principaux éléments que l'armée n'a jamais perdus de vue, dans ses efforts déployés au titre de la cyberdéfense.

Selon ses objectifs 2016, le DDPS a ordonné l'établissement d'un plan d'action cyberdéfense du DDPS (PACD). Ce plan est conforme à la SNPC: il satisfait concrètement à ses attentes et n'entrave pas son développement.

Le plan poursuit trois objectifs:

- renforcement du DDPS, de l'armée notamment, pour venir à bout des cybermenaces croissantes, au quotidien comme en situation de crise et de conflit;
- aide concrète, dans le cyberespace, à la mise en œuvre de la LRens et des dispositions de la LAAM, pour permettre à l'armée de se défendre activement, à partir de 2018 et à certaines conditions, contre les cyberattaques;
- création de conditions propices afin que le DDPS puisse soutenir les exploitants d'infrastructures d'importance vitale (conformément à la LRens) face aux cyberattaques.

L'élaboration de ce plan d'action a déjà conduit à optimiser les ressources à disposition; elle a en outre poussé à introduire une bonne gouvernance au DDPS. La concrétisation du plan d'action nécessitera toutefois une redistribution conséquente des ressources au DDPS. L'état final visé devrait être atteint en 2020.

L'armée compte aussi, pour gagner en maturité et renforcer sa préparation, sur les activités d'instruction et de sensibilisation aussi bien de son personnel de milice que de son personnel professionnel. L'armée a ainsi participé en 2016 à divers exercices, dont l'exercice international LOCKED SHIELD 16 et celui du RNS, qui portait sur une cyberattaque contre le système suisse de retraites avec des retombées sur le numéro AVS. En outre, l'état-major Cyber Defence de l'armée a organisé l'exercice CYBER PAKT 16, comportant divers scénarios d'une grande complexité et gourmands en ressources. Ces diverses mesures ont permis de tester les processus élaborés dans le cadre du PACD, d'améliorer la compréhension des nouvelles bases juridiques et de préciser les principes de subsidiarité applicables à l'armée. Outre ces exercices, de nombreuses actions de sensibilisation ont été lancées auprès du personnel du DDPS, des troupes (par ex. durant l'engagement de sécurité de l'armée au World Economic Forum), mais aussi de la population lors de manifestations publiques de l'armée organisées à Meiringen et à Thoune.

2.6 Mise en œuvre par les cantons

Le RNS est l'interface entre la SNPC et les cantons. Le groupe spécialisé Cyber du 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. L'OC SNPC est membre du groupe spécialisé Cyber et joue, au niveau de la Confédération, le rôle de passerelle pour les travaux de projet menés avec les cantons. Quatre groupes de travail ont été créés, sous la conduite du groupe spécialisé Cyber, en vue de la mise en œuvre dans les cantons de la SNPC.

État actuel:
L'analyse de la situation actuelle en matière de cyberrisques dans les cantons a servi de base à l'élaboration d'un outil spécifique. Celui-ci permet d'inventorier les processus importants dans les cantons, et donc de franchir une étape importante vers une meilleure gestion des cyberrisques. Trois cantons le testent actuellement, après quoi il sera proposé à tous les cantons.

Les descriptions des processus servant à traiter les cyberincidents conçues par le groupe de travail compétent ont été en partie adaptées ou améliorées.

En novembre 2016, l'exercice-cadre d'état-major de deux jours Popula a servi à tester le concept d'opérations et de processus de conduite de la Confédération dans une situation de crise à composante cybernétique; pour compliquer les choses, il prévoyait des retombées dans les cantons et une mise en danger de certaines infrastructures d'importance vitale. Outre la Confédération, les cantons, des exploitants d'infrastructures d'importance vitale et les tiers concernés par le scénario «Cyberattaque contre le système de retraites» ont pris part à l'exercice. Près de 50 participants de diverses organisations entretenant des contacts plus ou moins étroits au quotidien étaient présents. À titre d'introduction, le groupe industriel et d'armement RUAG a montré en direct une simulation technique de cyberattaque. L'exercice avait pour but de tester les interfaces entre les diverses organisations touchées par le scénario. Les participants ont dû solliciter leurs partenaires, partager des informations et faire remonter le cas au sein de leur hiérarchie. D'utiles leçons ont été tirées pour le concept et pour la gestion nationale des crises à composante cybernétique. Le déroulement de l'exercice n'a toutefois pas permis de tester tous les aspects du concept.

Le groupe de travail sur la cybercriminalité a décidé que les feuilles d'information rédigées par le SCOCI avec l'aide des cantons, qui décrivent les principaux phénomènes touchant à la cybercriminalité, seront systématiquement envoyées aux autorités de poursuite pénale, afin qu'elles s'y réfèrent dans leur travail de tous les jours.

3 Comité de pilotage et contrôle de gestion stratégique

Le Conseil fédéral a chargé le CP SNPC de suivre la mise en œuvre de la stratégie, grâce à un contrôle de gestion stratégique. Ledit contrôle vise à s'assurer tous les six mois, pour chaque mesure de la SNPC, que les progrès sont conformes aux objectifs et aux délais fixés. Le Conseil fédéral reçoit des rapports à ce sujet par l'intermédiaire de la Conférence des secrétaires généraux (CSG), en vertu du plan de mise en œuvre de la SNPC du 15 mai 2013. Comme le montre le contrôle de gestion en date du 31 décembre 2016, quinze des seize mesures de la SNPC sont déjà terminées, et la dernière portant sur la gestion de la continuité s'achèvera comme prévu d'ici la fin de 2017.

Durant cette année, le CP SNPC a examiné en détail le développement de la SNPC à partir de 2018. Il a discuté des prochaines étapes lors d'une séance spéciale fixée au 30 juin 2016, à sa 7e séance ordinaire le 17 août 2016, ainsi que le 26 octobre 2016, lors d'un atelier organisé avec un cercle de participants élargi. Compte tenu des résultats de l'évaluation de l'efficacité, le CP SNPC et le cercle de participants élargi ont reconnu que la stratégie avait eu un impact considérable, que l'approche décentralisée et basée sur le risque a fait ses preuves et qu'il faut reconduire la SNPC.

4 Évaluation de l'efficacité

En adoptant le plan de mise en œuvre de la SNPC, le Conseil fédéral avait chargé l'UPIC de

lui soumettre en avril 2017 une évaluation de l'efficacité de cette stratégie. L'évaluation a eu lieu en 2016 déjà, afin que le délai puisse être respecté. Entre mars et juillet, l'entreprise externe mandatée a mené quatorze entretiens, elle a fait remplir par écrit quinze questionnaires et analysé au total 130 documents créés dans le cadre de la SNPC.

La SNPC a été évaluée à trois niveaux: succès dans la mise en œuvre des seize mesures, aspects transversaux (planification des ressources, contenus, structure organisationnelle, communication), et enfin interfaces avec les activités des cantons et de l'armée. L'analyse a abouti aux résultats suivants:

- **Mesures adoptées**: la mise en œuvre des seize mesures de la SNPC a été globalement fructueuse, et les objectifs ont été atteints pour l'essentiel. Les résultats tangibles incluent un renforcement des capacités, l'acquisition de connaissances spécialisées et une meilleure coordination. Comme l'évaluation a eu lieu de bonne heure, l'effet direct des mesures adoptées sur les objectifs stratégiques est difficile à démontrer. Des modèles d'impact indiquent toutefois de manière plausible les effets pouvant être attendus. Les objectifs fixés n'ont pas tous été atteints pour quatre mesures. Pour celles-ci, le besoin d'efforts supplémentaires est avéré.
- **Contenus, ressources, structure organisationnelle et communication**: dans l'ensemble, l'évaluation de l'efficacité relève que les objectifs stratégiques fixés en 2012 par le Conseil fédéral étaient appropriés. Les ressources destinées à la réalisation des mesures ont tout juste suffi, et la structure organisationnelle décentralisée a globalement bien fonctionné. Par contre, la communication externe au niveau national laisse à désirer. Le grand public méconnaît la SNPC; il ignore ce que la Confédération entreprend face aux cyberrisques et où s'arrêtent ses compétences.
- **Interfaces avec les activités des cantons et de l'armée**: le RNS a assuré la coordination des travaux de la SNPC avec ceux des cantons. Comme l'a montré l'évaluation, la collaboration fonctionne bien et une prise de conscience s'est faite dans les cantons. Par contre, d'importantes questions restent à régler en ce qui concerne l'interface avec les travaux de l'armée. Il faudra dûment clarifier les tâches civiles du ressort de la SNPC et les compétences de l'armée en cas de crise, et préciser à propos de l'appui subsidiaire de l'armée quelles sont les attentes raisonnables et les possibilités effectives.

Les résultats de l'évaluation de l'efficacité montrent que l'approche stratégique a été correctement choisie, et que la mise en œuvre décentralisée mais étroitement coordonnée de la SNPC fonctionne globalement bien. Dans tous les domaines, il a été possible d'établir des processus et des structures qui fonctionnent, et d'acquérir les connaissances spéciales requises, avec pour effet que la Suisse est mieux préparée à affronter les cyberrisques qu'elle ne l'était en 2012. En même temps, il est clair que la SNPC ne constitue qu'une base, et qu'il faudra renforcer encore la protection face aux cyberrisques.

5 Conférences et Manifestations

Ce chapitre présente quelques conférences ou manifestations importantes, ayant eu lieu en 2016 au niveau national ou international.

5.1 Niveau national

La quatrième cyber-landsgemeinde s'est déroulée le 6 avril 2016. Quelque 100 responsables de la Confédération et de tous les cantons, et d'étroits partenaires du Réseau national de sécurité (RNS) ont participé cette année à cette manifestation de réseautage. Comme les années précédentes, les discussions ont principalement porté sur l'état d'avancement des

projets menés au niveau cantonal ou dans le cadre de la SNPC, ainsi que sur l'évaluation de l'efficacité de la SNPC.

Le Cyber 9/12 Student Challenge a eu lieu les 7 et 8 avril 2016 à Genève. Comme l'année précédente, l'Atlantic Council et le Geneva Centre for Security Policy (GCSP) étaient les hôtes de la manifestation. Cette année aussi, 28 équipes de treize pays d'Europe, du Moyen-Orient et des États-Unis ont dû se préparer à une vaste cyberattaque et formuler des recommandations adéquates. L'équipe britannique s'est imposée cette année. La Confédération a soutenu la manifestation, à travers la participation de l'OC SNPC et d'autres représentants comme jurés.

Le 20 mai 2016, l'École polytechnique fédérale de Lausanne (EPFL) a accueilli la première Swiss Cyber Risk Research Conference, organisée par le SEFRI. La conférence visait à encourager la recherche sur le thème des cyberrisques et à consolider le réseau de chercheurs en Suisse.

Le 18 septembre 2016, Lucerne a accueilli une épreuve du troisième European Cyber Security Challenge. Dans cette compétition internationale, des écoliers ou étudiants venus d'Autriche, d'Allemagne, de Roumanie, de Grande-Bretagne, d'Espagne et de Suisse devaient découvrir, exploiter et corriger les vulnérabilités de systèmes informatiques. Les hôtes de la manifestation étaient l'association Swiss Cyber Storm, le DFAE et le Département fédéral des finances (DFF). L'Espagne s'est imposée cette année.

La troisième conférence sur les cyberrisques en Suisse s'est tenue le 26 octobre, selon une formule différente des années précédentes: le matin, un atelier interne a réuni les responsables des diverses mesures de la SNPC, afin de définir les prochaines étapes à partir du 1er janvier 2018. Il s'agissait de déterminer ensemble le besoin de mesures supplémentaires pour une possible stratégie subséquente à la SNPC. La partie officielle de la conférence s'est déroulée l'après-midi, afin de donner aux représentants de l'économie et de la politique un aperçu détaillé de la mise en œuvre des mesures de la SNPC et de leur présenter les premiers résultats de l'évaluation de l'efficacité.

Les 23 et 24 novembre 2016, l'exercice de gestion de crise Populа a simulé une cyberattaque contre le système suisse de retraites. La Fédération suisse des employés en assurances sociales (FEAS) a assuré, en collaboration avec la Confédération, les cantons et les exploitants d'infrastructures concernés, la conduite de l'exercice qui visait à tester l'état de préparation et la gestion des crises à l'échelon de la Confédération et des cantons.

5.2 Niveau international

Du 14 au 18 mars 2016, Hanovre a accueilli le salon CeBIT, dont la Suisse était le pays partenaire. L'accent y a été mis sur les processus au sein des entreprises et la connexion du quotidien, sur l'Internet des objets ainsi que sur «Industrie 4.0».

Les 10 et 11 mai ainsi que les 14 et 15 novembre 2016, comme déjà dans le passé, la Suisse a participé au Sino-European Cyber Dialogue (5e et 6e éditions), auquel elle a apporté une contribution déterminante. Il s'agit d'un dialogue multilatéral noué entre des États européens et la Chine pour mieux comprendre les perceptions respectives des menaces et identifier les questions dont l'approfondissement présente un intérêt commun.

Le Forum européen sur la gouvernance d'Internet (European Dialogue on Internet Governance, EuroDIG) a été organisé du 8 au 10 juin 2016 à Bruxelles. Ce réseau s'inspirant du Forum des Nations Unies sur la gouvernance d'Internet (FGI) joue un rôle pionnier, en proposant des solutions d'avant-garde pour que les divers groupes d'intérêt puissent débattre sur les thèmes liés à Internet. L'OFCOM fait partie des fondateurs de l'EuroDIG et cette année aussi, la Suisse a participé activement sur place aux discussions menées.

Le Groupe d'experts gouvernementaux de l'ONU sur la sécurité internationale dans le

cyberespace s'est réuni du 29 août au 2 septembre et du 28 novembre au 2 décembre 2016 à New York et Genève. La Suisse, qui y siégeait pour un an en 2016, a formulé des recommandations portant sur l'utilisation du cyberespace pour chacun des cinq axes thématiques définis (menace actuelle, normes de bonne gouvernance, droit international public, instauration d'un climat de confiance, développement des capacités).

Le 18 septembre 2016, en amont de l'Assemblée générale des Nations Unies, la Commission «Le large bande au service du développement numérique» (Broadband Commission for Sustainable Development, BBCOM) créée par l'Union internationale des télécommunications (UIT) et l'UNESCO a tenu son assemblée annuelle à New York. La BBCOM et ses groupes de travail s'engagent notamment en vue du déploiement à l'échelle mondiale des infrastructures à large bande.

La conférence indienne sur la cybersécurité (CyFy), dont la Suisse était pays partenaire, s'est tenue du 28 au 30 septembre 2016 à New Delhi. Il s'agit de la plus grande conférence d'Asie sur la cybersécurité et la gouvernance d'Internet, réunissant des délégués aussi bien des gouvernements que du secteur privé et de la recherche.

Depuis le 30 septembre 2016, les États-Unis ne jouent plus le rôle de surveillant de l'Internet Corporation for Assigned Names and Numbers (ICANN), la société de gestion des adresses Internet au niveau mondial. Celle-ci est désormais dirigée par une communauté mondiale, où sont représentés tous les groupes d'intérêts. Un pas important a ainsi été franchi vers une gestion internationale du système des noms de domaines (DNS), un objectif poursuivi par la Suisse.

Le 4 novembre 2016, Vienne a accueilli le Cyber Showcase Event de l'OSCE, placé sous la présidence de l'Allemagne. La rencontre avait pour thème principal la difficulté d'attribuer les cyberdélits à des personnes déterminées, et donc d'identifier l'agresseur. De l'avis de tous les États membres, il faut trouver des solutions communes pour surmonter ce défi. L'OSCE semble offrir un cadre adéquat à des discussions approfondies sur la question.

Du 3 au 9 novembre 2016, Hyderabad (Inde) a accueilli une réunion de l'ICANN57. Après Marrakech (du 5 au 10 mars) et Helsinki (du 27 au 30 juin) il s'agissait de sa troisième séance de l'année. Depuis le transfert à la communauté mondiale du rôle de haute surveillance assuré jusque-là par les États-Unis, il s'agit d'en concrétiser les modalités et de poursuivre les réformes internes à l'ICANN. La Suisse a été réélue par acclamation, pour deux années supplémentaires, à la présidence du Comité consultatif gouvernemental de l'ICANN.

Du 16 au 18 novembre 2016, le gouvernement chinois a organisé la troisième Conférence mondiale de l'Internet (World Internet Conference, WIC) à Wuzhen, petite ville proche de Shanghai. Contre-projet au Forum des Nations Unies sur la gouvernance de l'Internet (FGI), la WIC est à la botte du Parti communiste chinois. À travers de telles initiatives et les investissements qui s'ensuivent, la Chine affiche sa détermination à jouer un rôle de premier plan dans les débats sur la gouvernance d'Internet. Le président Xi Jinping a fait de ce thème une priorité politique de son pays, et donc la Chine ne ménage pas ses efforts sur ce plan.

Du 6 au 9 décembre 2016, Guadalajara (Mexique) a accueilli le premier FGI depuis la prolongation, par les États membres, de son mandat qui avait expiré en décembre 2015. Le FGI est l'une des principales conférences du monde dans le domaine de la gouvernance de l'Internet, et offre à tous les groupes d'intérêt un espace de dialogue sur les questions en la matière. La Suisse a annoncé au Mexique son intention de soutenir, en tant que pays hôte, l'organisation du FGI 2017 à Genève, au siège des Nations Unies.

En août 2016, la Commission européenne a adopté la directive sur la sécurité des réseaux et de l'information (directive SRI), que tous les États membres sont tenus de transposer dans leur législation nationale. La Suisse ne devra pas perdre de vue les développements de cette directive, sachant que l'obligation de notifier les incidents pourrait avoir des répercussions pour la Suisse et les entreprises helvétiques actives dans l'UE. L'organe de coordination de

la SNPC est membre du groupe de cyberexperts de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) et prend part aux conférences et activités régulièrement organisées.

6 Considérations finales

La mise en œuvre de la SNPC touche à sa fin. Quinze des seize mesures définies étaient terminées à la fin de 2016, et la dernière s'achèvera comme prévu d'ici la fin de 2017. Selon les premiers résultats de l'évaluation de l'efficacité, la SNPC a eu un impact significatif, les objectifs stratégiques du Conseil fédéral étaient appropriés et la Suisse est mieux armée face aux cyberrisques qu'en 2012. En plus de renforcer et de développer les structures et les processus existants, la SNPC en a défini d'autres encore, dans le but d'améliorer la collaboration, la coopération et la communication des acteurs concernés et, le cas échéant, de rallier à l'avenir d'autres acteurs à la stratégie.

La recrudescence de cyberattaques en 2016 confirme que la vigilance reste de mise et qu'il faudra encore approfondir la coopération bien établie avec nos partenaires au niveau tant national qu'international. Il s'agira comme jusqu'ici d'intensifier la précieuse collaboration instaurée avec les exploitants d'infrastructures d'importance vitale, avec l'économie et les cantons, et de renforcer constamment les échanges d'informations non seulement avec les organisations de police et les ministères publics, mais aussi avec les prestataires informatiques, les fournisseurs de systèmes, les autorités spécialisées ainsi qu'avec les autorités de surveillance et de régulation, de façon à accroître la résilience de la Suisse.

Au niveau international également, la Suisse s'est à nouveau montrée active. Elle s'est engagée pour la création d'un dispositif normatif destiné à régler, à l'aide d'instruments politiques et juridiques, l'utilisation et les frontières du cyberespace, ainsi qu'à concrétiser sa vision d'un cyberespace ouvert, libre et sûr.

D'autres défis s'annoncent à l'avenir. Les menaces se sont faites plus pressantes ces dernières années, et elles ne cessent d'évoluer: les menaces d'hier ne sont pas celles d'aujourd'hui, encore moins celles de demain. La Suisse doit donc soigneusement se préparer à affronter les cybermenaces à venir. De l'avis tant des responsables des mesures réalisées que des acteurs au niveau fédéral et dans les cantons, les résultats de la SNPC doivent être pérennisés au-delà de l'horizon actuel, fixé à la fin de 2017. À cet effet, le comité de pilotage de la SNPC prépare un état des lieux en vue du développement ultérieur de la stratégie, qu'il soumettra au Conseil fédéral.

7 Annexes

7.1 Documents de base relatifs à la SNPC

«Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)»:
https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html

«Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques»:
https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/umsetzungsplan.html

«Rapport annuel SNPC 2013»:
https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

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

7.2 Récapitulation des interventions parlementaires relatives aux cyberrisques

Intervention Ip. = Interpellation; Mo. = Motion; Po. = Postulat; Qu. = Question	Date du dépôt	État au 31.12.2015
08.3050 Po. Schmid-Federer. Protection contre la cyberintimidation	11.03.2008	liquidé
08.3100 Mo. Burkhalter. Stratégie nationale de lutte contre la criminalité par Internet; délibérations du Conseil des États 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. Évaluation 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),	29.06.2010	liquidé

rapport de la CPS-CN du 11 janvier 2011 et délibérations du Conseil des États du 15 mars 2011 (BO CE 15.03.2011)		
10.3872 Ip. Recordon. Risque de panne de grande ampleur du réseau électrique en Suisse	01.10.2010	liquidé
10.3910 Po. Groupe libéral-radical. Organe de direction et de coordination pour contrer les cybermenaces	02.12.2010	liquidé
10.4020 Mo. Glanzmann. MELANI pour tous	16.12.2010	liquidé
10.4028 Ip. Malama. Risque d'une cyberattaque contre les centrales nucléaires suisses	16.12.2010	liquidé
10.4038 Po. Büchler. Compléter le rapport sur la politique de sécurité en y ajoutant un chapitre sur la cyberguerre	16.12.2010	liquidé
10.4102 Po. Darbellay. Élaboration d'une stratégie visant à protéger l'infrastructure numérique de la Suisse	17.12.2010	liquidé
11.3906 Po. Schmid-Federer. Loi-cadre sur les TIC	29.09.2011	liquidé
12.3417 Mo. Hodgers. Marchés ouverts de la télécommunication. Stratégies pour la sécurité numérique nationale	30.05.2012	liquidé
12.4161 Mo. Schmid-Federer. Pour une stratégie nationale contre le cyberharcèlement	13.12.2012	liquidé
13.3228 Ip Recordon. Système d'écoutes téléphoniques fédéral et carences générales de la Confédération en informatique et en télécommunication	22.03.2013	liquidé
13.3229 Ip. Recordon. Ampleur de la menace et mesures de lutte contre la cyberguerre et la cybercriminalité	22.03.2013	liquidé
13.5224 Qu. Reimann. Cyberactivités des services secrets américains en Suisse	10.06.2013	liquidé
13.3558 Ip. Eichenberger. Cyberespionnage. Evaluation et stratégie	20.06.2013	liquidé
13.3677 Ip. Groupe socialiste. Certains services de renseignement étrangers, tels que la NSA, furètent-il également en Suisse?	11.09.2013	liquidé
13.5325 Qu. Sommaruga. Le Service de renseignement de la Confédération utilise-t-il des données collectées illégalement par la NSA?	11.09.2013	liquidé
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. Élaborer 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
14.3654 Ip. Derder. Sécurité numérique. Faisons-nous fausse route?	20.06.2014	non encore traité au conseil
14.5569 Qu. Leutenegger. Affaire Snowden. Ampleur des agissements des États-Unis	26.11.2014	liquidé
14.4138 Ip. Noser. Procédure d'adjudication pour les infrastructures TIC critiques de l'administration fédérale	10.12.2014	non encore traité au conseil
14.1105 Qu. Buttet. Moyens dédiés à la cyberdéfense dans la politique de sécurité de la Suisse	10.12.2014	liquidé
14.4299 Ip. Derder. Veille transversale de la révolution numérique. Faut-il créer un secrétariat d'État de la société numérique?	12.12.2014	non encore traité au conseil
15.3359 Po. Derder. Pour une armée innovante	20.03.2015	non encore traité au conseil
15.3375 Ip. Recordon. Subtilisation de codes SIM par la NSA et le GCHQ auprès de la société Gemalto	20.03.2015	liquidé
15.5299 Qu. Leutenegger. Protection contre l'espionnage de la NSA	09.06.2015	liquidé
15.3656 Ip. Munz. La télémaintenance des systèmes informatiques représente un danger pour la centrale nucléaire de Mühleberg. Surveillance de l'IFSN remise en cause	18.06.2015	non encore traité au conseil
15.1059 Qu. Berberat. Aide financière d'urgence de la Confédération suite à la cyberattaque contre TV5 Monde	10.09.2015	liquidé
15.4073 Ip. Derder. L'armée est-elle réellement capable de protéger l'espace cybernétique helvétique?	25.09.2015	non encore traité au conseil
16.3186 Mo. Eichenberger. Cyberrisques. Échange d'informations techniques	17.03.2016	liquidé
16.3348 Po. Béglé. Création d'un conseil de cyberdéfense. Une priorité pour notre souveraineté et notre sécurité	27.04.2016	non encore traité au conseil

16.3353 Ip. Salzmann. À quoi sert le Réseau national de sécurité?	30.05.2016	non encore traité au conseil
16.3356 Ip. Nordmann. Redéployer enfin les moyens humains et financiers en faveur de la cybersécurité	31.05.2016	non encore traité au conseil
16.3363 Ip. Glättli. Cyberattaque contre l'entreprise RUAG et le DDPS. Il faut tirer les conséquences qui s'imposent!	31.05.2016	liquidé
16.3364 Ip. Glanzmann-Hunkeler. Faire toute la lumière sur la cyberattaque contre l'entreprise RUAG	31.05.2016	liquidé
16.1020 Qu. urgente Groupe BD. Lutte contre les cyberrisques. Institution d'un système de contrôle et d'un centre de compétences en vue de relever les défis à venir	02.06.2016	liquidé
16.1021 Qu. urgente Groupe des Verts.	02.06.2016	liquidé
16.1022 Qu. urgente Groupe PDC. Faire toute la lumière sur la cyberattaque contre l'entreprise RUAG	02.06.2016	liquidé
16.1024 Qu. Knecht. Interpol, cyberrisques et cybercriminalité	07.06.2016	liquidé
16.3413 Ip. Heim. Cyberrisques et installations nucléaires	09.06.2016	liquidé
16.3528 Mo. Glanzmann-Hunkeler. Compétence en matière de cyberdéfense	16.06.2016	non encore traité au conseil
16.3561 Ip. Dittli. Élargissement de la clause de défense mutuelle de l'OTAN aux cyberattaques. Et la Suisse?	17.06.2016	liquidé
16.061 Objet du Conseil fédéral. Politique de sécurité de la Suisse. Rapport	24.08.2016	non encore traité au conseil
16.3706 Po. Vonlanthen. Économie numérique et marché du travail	27.09.2016	adopté
16.4073 Po. Golay. Cyberrisques. Pour une protection globale, indépendante et efficace	15.12.2016	non encore traité au conseil
16.4115 Ip. Quadranti. Identité électronique	16.12.2016	non encore traité au conseil

7.3 Liste des abréviations

AEP	Approvisionnement économique du pays
BAC	Base d'aide au commandement de l'armée
BAC COE	Base d'aide au commandement de l'armée – 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-SIPOL	Département fédéral de la défense, de la protection de la population et des sports – 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-DP	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
EC CYD	Étude conceptuelle sur la cyberdéfense
ENISA	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 d'Internet
GAC	Comité consultatif gouvernemental (Governmental Advisory Committee)
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
ICT	Information and Communication Technology
LRens	Loi fédérale sur le renseignement
MCC RNS	Mécanisme de consultation et de coordination du Réseau national de sécurité
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MELANI OIC	Centrale d'enregistrement et d'analyse pour la sûreté de l'information Operation – Information Center
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
ONU	Organisation des Nations Unies

OrgN	Organisation de normalisation
OSCE	Organisation pour la sécurité et la coopération en Europe
OTAN	Organisation du traité de l'Atlantique Nord
PM SNPC	Plan de mise en œuvre de la SNPC
RM	Service de renseignement militaire
RNS	Réseau national de sécurité
SCOCI	Service national de coordination de la lutte contre la criminalité sur Internet
SEFRI	Secrétariat d'État 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 de niveau 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 de 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 – Sécurité informatique