AWK GROUP

Consulting
Engineering
Project Management

Rapport

Évaluation de l’efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

Unité de pilotage informatique de la Confédération (UPIC)
Schwarztorstrasse 59
3003 Berne

30 novembre 2016, projet n° 12.415.14.01

Informations sur le document

Titre:	Évaluation de l’efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)	
Numéro du projet:	12.415.14.01	
Date de publication:	30 novembre 2016	
Nombre de pages:	83, hors annexes	
Nom du fichier:	_Ber_161201_WiÜ_NCS_V1.0.docx	
Responsable du document:	Markus Meier, AWK	
Vérifié par:	Co-auteur / chef de projet: Adrian Marti, AWK	Date: 18.11.2016

Versions

Version	Date	Principales modifications	Responsable
V0.8	31.08.2016	Premier projet complet du groupe de suivi	Mem, Sep
V0.15	20.09.2016	Projet présenté pour examen au CP SNPC	Mem
V0.25	16.11.2016	Version après feed-back de l’atelier SNPC II	Mem
V1.0	30.11.2016	Version finale	Mem

Abréviations et définitions

Abréviation	Description
BAC	Base d'aide au commandement
CdA	Chef de l'Armée
CDIP	Conférence suisse des directeurs cantonaux de l'instruction publique
CERT	Computer Emergency Response Team
ChF	Chancellerie fédérale
CI	Conseil de l'informatique de la Confédération
CNO	Computer Network Operations
COE	Centre des opérations électroniques
CoPIRFC	Comité de Pilotage Recherche et Formation Cyber
CP SNPC	Comité de pilotage de la SNPC
CPS	Conférence des procureurs de Suisse
CTI	Commission pour la technologie et l'innovation
CYD	Cyber Defence, centre de compétence de l'armée pour la planification de l'action, le suivi de la situation, la maîtrise d'événement et l'instruction dans le cyberespace
DFAE	Département fédéral des affaires étrangères
DFJP	Département fédéral de justice et police
DPS	Division Politique de sécurité
ECS	Exercice de conduite stratégique
EMCC	État-major cantonal de conduite
GCSP	Geneva Centre for Security Policy
GT	Groupe de travail
IC	Infrastructures critiques
ICANN	Internet Cooperation for Assigned Names and Numbers, Société pour l'attribution des noms de domaine et des numéros sur Internet
IOC	Indicator of Compromise, indicateur de compromission
LSCPT	Loi fédérale sur la surveillance de la correspondance par poste et télécommunication
MCC	Mécanisme de consultation et de coordination
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MISP	Malware Information Sharing Platform, plate-forme destinée à l'échange d'informations sur les maliciels
OC SNPC	Organe de coordination de la SNPC
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCOM	Office fédéral de la communication
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
OFROU	Office fédéral des routes
OIC	Operation Information Center
PPP	Partenariat public-privé

Abréviation	Description
RM	Service de renseignement militaire
RNS	Réseau national de sécurité
SCE	Swiss Cyber Experts
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
SIEM	Security Information and Event Management
SIGF	Swiss Internet Governance Forum
SMSI	Sommet mondial sur la société de l'information
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SOC	Security Operation Center
SPOC	Single Point of Contact
SRC	Service de renseignement de la Confédération
UCC	Unified Collaboration and Communication
UPIC	Unité de pilotage informatique de la Confédération

Table des matières

Condensé

Contexte et mandat
LeConseil fédéral a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) le 27 juin 2012 et son plan de mise en œuvre le 15 mai 2013. Ce plan comprend un mandat, à savoir présenter d'ici le printemps 2017 une évaluation de l'efficacité de la SNPC. Le présent rapport exécute ce mandat.

La SNPC fixe trois objectifs stratégiques:

- détection précoce des menaces et des dangers dans le cyberespace;
- augmentation de la capacité de résistance des infrastructures critiques;
- réduction des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

Ces objectifs doivent être atteints grâce à seize mesures dans les domaines «prévention et continuité», «réaction», «gestion des crises», «coopération internationale», «recherche et formation» et «bases juridiques».

Questions
Pour évaluer en détail l'efficacité de la SNPC, des analyses sont requises à trois niveaux:
1) Mesures de la SNPC: les seize mesures ont-elles été mises en œuvre comme prévu? Quels résultats ont été obtenus? À quel point les mesures ont-elles contribué à la réalisation des objectifs stratégiques de la SNPC?
2) Interfaces: les cantons et l'armée ont-ils suffisamment été associés aux travaux de la SNPC?
3) Aspects interdisciplinaires: la planification des ressources de la SNPC était-elle correcte? Le contenu et l'organisation de la SNPC ont-ils fait leurs preuves? La communication interne et externe a-t-elle fonctionné?

Méthode d'évaluation
L'évaluation de l'efficacité s'appuie sur une approche détaillée qui analyse les effets à trois niveaux (*output*, *outcome* et impact), définis comme suit:
- *output*: résultats de la mise en œuvre effective de la stratégie;
- *outcome*: groupes cibles touchés, connaissances nouvellement acquises, sensibilisations et changements comportementaux observés;
- impact: effets tangibles sur les objectifs stratégiques de la SNPC.

L'évaluation de l'*output* et de l'*outcome* se base sur les objectifs fixés dans le plan de mise en œuvre et utilise une échelle à quatre niveaux (objectifs non atteints, objectifs partiellement atteints, objectifs en majeure partie atteints, objectifs atteints). Concernant l'impact, on a examiné si celui-ci avait manifestement été obtenu ou non.

Collecte des données
Les résultats de l'évaluation de l'efficacité reposent en premier lieu sur une enquête menée auprès des responsables des mesures et des représentants des interfaces ainsi que sur une analyse approfondie des documents. Enfin, des entretiens supplémentaires ont été réalisés si cela était nécessaire et opportun. Les personnes interrogées ont été choisies en collaboration avec l'organe de coordination de la SNPC (OC SNPC). L'enquête s'est déroulée entre mars et fin juin 2016. À cette période, plusieurs mesures n'étaient pas encore achevées. L'évaluation de l'efficacité reflète donc l'avancement des travaux au moment de l'enquête.

Évaluation de la mise en œuvre des mesures
Le tableau 1 récapitule les résultats de l'évaluation de l'efficacité pour chaque mesure.

Légende			
✗✗	Objectifs non atteints	✗	Objectifs partiellement atteints
✓✓	Objectifs en majeure partie atteints	✓	Objectifs atteints
◎	Impact obtenu	☐	Actuellement non mesurable, non évaluable

Mesures	Office ou UO compétents	*Output*	*Outcome*	Impact
Mesures 2 et 12 – prévention et continuité: analyse des risques et vulnérabilités et continuité	OFPP, OFAE	✓✓	✓✓	☐
Mesure 3 – prévention et continuité: analyse de la vulnérabilité des infrastructures informatiques	UPIC	✗	☐	☐
Mesure 4 – prévention et continuité: établissement d'un tableau de la situation et de son évolution	MELANI (SRC)	✓	✓	◎
Mesure 5 – réaction: analyse et suivi des incidents	MELANI (SRC)	✓	✓	◎
Mesure 6 – réaction: concept de vue d'ensemble des infractions et coordination des cas intercantonaux complexes	SCOCI	✓	✗	☐
Mesure 14 – réaction: mesures actives d'identification des agresseurs	MELANI, SRC, UPIC	✓	✓	◎
Mesure 13 – gestion des crises: coordination des activités avec les acteurs directement concernés et soutien grâce à l'expertise requise	MELANI et SRC	✓	☐	☐
Mesure 15 – gestion des crises: concept pour les procédures et processus de conduite incluant les aspects cybernétiques	ChF	✓	✗	☐
Mesure 9 – coopération internationale: gouvernance d'Internet	OFCOM	✓✓	✓	☐
Mesure 10 – coopération internationale: coopération au niveau de la politique internationale de sécurité	DFAE	✓✓	✓✓	☐
Mesure 11 – coopération internationale: initiatives et processus internationaux de standardisation en matière de sécurité	OFCOM	✓	✗	☐
Mesure 1 – formation et recherche: identification des cyberrisques par la recherche	SEFRI	✓✓	✓	☐
Mesures 7 et 8 – formation et recherche: aperçu des offres de formation; usage accru des offres de formation et comblement des lacunes	OC SNPC	✓	✓✓	☐
Mesure 16 – bases juridiques: nécessité de modifier les bases juridiques	OC SNPC	✓✓	☐	☐

Tableau 1: Évaluation de la réalisation des objectifs visés par les mesures

On constate que la mise en œuvre des mesures est bien avancée. Les structures et les processus prévus sont majoritairement en place, et plusieurs produits (rapports et concepts) ont été fournis dans les délais. L'*output* obtenu s'est déjà traduit par un *outcome* notable puisque les capacités ont manifestement été développées, les connaissances se sont accrues et la coordination s'est améliorée.

L'impact direct des travaux sur les objectifs stratégiques est le plus difficile à mesurer. Dans le contexte dynamique et complexe des cyberrisques, il n'est guère possible de

mettre en évidence le lien de causalité entre les mesures prises et leur impact sur les objectifs de la SNPC. De plus, l'évaluation de l'efficacité a été réalisée trop tôt: en général, les mesures concernées déploient leurs effets après un certain laps de temps. C'est la raison pour laquelle un impact n'a pu être attesté que pour trois des seize mesures. Les modèles d'efficacité élaborés pour toutes les mesures dans le cadre de l'évaluation indiquent cependant l'impact concret qui peut être escompté au regard des résultats obtenus jusqu'à présent.

Évaluation des interfaces

Deux interfaces sont primordiales pour la mise en œuvre de la SNPC: l'interface avec les activités des cantons et l'interface avec le centre de compétence Cyber Defence de l'armée. L'évaluation de l'efficacité portait sur le degré d'intégration de ces interfaces.

Interface avec les cantons:

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome			✓	
Impact	☐ actuellement non énon llem			

Tableau 2: Évaluation de la réalisation des objectifs pour les interfaces avec les cantons – RNS

Interface avec l'armée:

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output		✗		
Outcome		✗		
Impact sur l'environnement CYD	☐ actuellement non énon llem			

Tableau 3: Évaluation de la réalisation des objectifs pour les interfaces avec l'armée

Évaluation des aspects interdisciplinaires

Les aspects interdisciplinaires ont été évalués pour déterminer si la planification des ressources de la SNPC était adéquate, le contenu et l'organisation de la SNPC avaient fait leurs preuves dans l'ensemble et la communication interne et externe avait fonctionné. On a examiné si les attentes étaient satisfaites, en majeure partie satisfaites, partiellement satisfaites ou non satisfaites. Le tableau 4 présente les résultats de l'évaluation:

Niveau	Attentes non satisfaites	Attentes partiellement satisfaites	Attentes en majeure partie satisfaites	Attentes satisfaites
Planification des ressources			✓	
Contenu				✓✓
Organisation			✓	
Communication		✗		

Tableau 4: Évaluation des aspects interdisciplinaires

De manière générale, le bilan concernant les aspects interdisciplinaires est également positif. Le contenu était bon, les ressources étaient à peine suffisantes et l'organisation

décentralisée a fait ses preuves. La communication externe s’est cependant avérée lacunaire, et plusieurs personnes interrogées estiment qu’il faut la renforcer.

1. Contexte et mandat

Le 27 juin 2012, le Conseil fédéral a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Il entend ainsi, en collaboration avec les autorités, les milieux économiques et les exploitants d'infrastructures critiques, réduire les cyberrisques auxquels ces acteurs sont exposés quotidiennement. Le 15 mai 2013, le Conseil fédéral a adopté le plan de mise en œuvre de la SNPC. Il y définit les ressources personnelles pour l'application de la SNPC et instaure un comité de pilotage interdépartemental de la SNPC (CP SNPC), qui surveille et coordonne les travaux.

Le CP SNPC est chargé de présenter une évaluation de l'efficacité au Conseil fédéral d'ici le printemps 2017 (p. 10 du plan de mise en œuvre). Cette évaluation permet de déterminer si les mesures prises ont déployé les effets escomptés et si les ressources ont été utilisées de manière appropriée.

Ce mandat fixe le contexte dans lequel l'évaluation de l'efficacité est réalisée. Dans un premier temps, les objectifs et les mesures qui ont été définis dans la SNPC ainsi que les personnes responsables de la mise en œuvre sont brièvement présentés. Les objectifs et l'organisation de l'évaluation sont ensuite décrits.

1.1. Contexte: contenu et organisation de la SNPC

1.1.1. Objectifs et mesures de la SNPC

Le Conseil fédéral a fixé trois objectifs stratégiques dans la SNPC:

- détection précoce des menaces et des dangers dans le cyberespace;
- augmentation de la capacité de résistance des infrastructures critiques;
- réduction des cyberrisques liés en particulier à la cybercriminalité, au cyberespionnage et au cybersabotage.

Seize mesures ont été définies pour atteindre ces objectifs. Elles sont variées, car les cyberrisques concernent les aspects les plus divers de la société civile ainsi que des milieux économiques et politiques. Ces mesures vont de l'exécution d'analyses de risques jusqu'à la promotion de la recherche et la mise en place d'une politique extérieure relative au cyberespace, en passant par le renforcement de la lutte contre les incidents.

Les seize mesures ont été réparties dans les six domaines suivants lors de l'élaboration du plan de mise en œuvre:

- Prévention et continuité:
  - Mesure 2: analyse des risques et vulnérabilités des secteurs partiels critiques
  - Mesure 3: analyse de la vulnérabilité des infrastructures informatiques
  - Mesure 4: établissement d'un tableau de la situation et de son évolution
  - Mesure 12: gestion de la continuité et amélioration de la résilience des secteurs partiels critiques
- Réaction:
  - Mesure 5: analyse et suivi des incidents
  - Mesure 6: concept de vue d'ensemble des infractions et de coordination des cas intercantonaux complexes
  - Mesure 14: mesures actives d'identification des agresseurs
- Gestion des crises:

  - Mesure 13: coordination des activités avec les acteurs directement concernés et soutien grâce à l'expertise requise
  - Mesure 15: concept pour les procédures et processus de conduite incluant les aspects cybernétiques
- Formation et recherche:
  - Mesure 1: identification des cyberrisques par la recherche
  - Mesure 7: aperçu des offres de formation
  - Mesure 8: usage accru des offres de formation et comblement des lacunes
- Coopération internationale:
  - Mesure 9: gouvernance d'Internet
  - Mesure 10: coopération au niveau de la politique internationale de sécurité
  - Mesure 11: initiatives et processus internationaux de standardisation en matière de sécurité
- Bases juridiques:
  - Mesure 16: nécessité de modifier les bases juridiques

1.1.2. Organisation et responsabilité de la mise en œuvre de la SNPC

La responsabilité stratégique de la mise en œuvre de la SNPC incombe au comité de pilotage de la SNPC (CP SNPC). Équivalent du CP SNPC sur le plan opérationnel, l'organe de coordination de la SNPC (OC SNPC) est chargé du contrôle de gestion stratégique des mesures et de la coordination entre les responsables des mesures.
L'OC SNPC est rattaché à l'Unité de pilotage informatique de la Confédération (UPIC), et plus précisément à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI).

Les unités d'organisation suivantes sont chargées de la mise en œuvre des mesures:

- OC SNPC (mesures 7, 8 et 16)
- MELANI (mesures 4, 5, 13 et 14)
- UPIC (mesure 3)
- SRC (mesures 4, 5 et 14)
- OFPP et OFAE (mesures 2 et 12)
- OFCOM (mesures 7, 9 et 11)
- DFAE (mesure 10)
- ChF (mesure 15)
- SEFRI (mesure 1)

1.2. Objectifs de l'évaluation de l'efficacité

Comme indiqué dans la décision du Conseil fédéral concernant le plan de mise en œuvre de la SNPC, l'évaluation de l'efficacité porte surtout sur les travaux qui ont été réalisés, sur les charges correspondantes et sur les résultats ainsi obtenus. Les trois principaux objectifs de cette évaluation sont donc les suivants:

- évaluation de la mise en œuvre des mesures: il convient de vérifier les travaux réalisés, les charges correspondantes ainsi que les résultats et les effets ainsi obtenus;
- évaluation des interfaces: il faut examiner si les cantons ont suffisamment été pris en compte dans la mise en œuvre de la SNPC et si l'interface avec le centre de compétence Cyber Defence de l'armée est assurée;
- évaluation des aspects interdisciplinaires: on détermine si la planification des ressources était adéquate pour la SNPC, si le contenu et la structure choisie pour la SNPC ont fait leurs preuves et si la communication interne et externe était suffisante.

2. Procédure

L'évaluation de l'efficacité a été réalisée conformément au concept détaillé [3] élaboré à l'automne 2015, qui fixait la procédure correspondante. Celle-ci comprend trois étapes, sur la base de ce document:

- conception;
- réalisation;
- établissement des rapports.

2.1. Conception

Le concept détaillé susmentionné divise l'évaluation en trois parties:

1) Évaluation des mesures (chap. 3)
2) Vérification des interfaces (chap. **Fehler! Verweisquelle konnte nicht gefunden werden.**)
3) Examen des aspects interdisciplinaires (chap. 5)

Cette structure est reprise dans le présent rapport.

Les mesures et les interfaces sont examinées à l'aide de modèles d'efficacité, qui présentent l'effet potentiel des mesures et la façon de l'obtenir. À cet égard, une distinction a été opérée entre les niveaux Concept, *Input*, *Output*, *Outcome* et Impact, comme le montre l'Illustration 1:

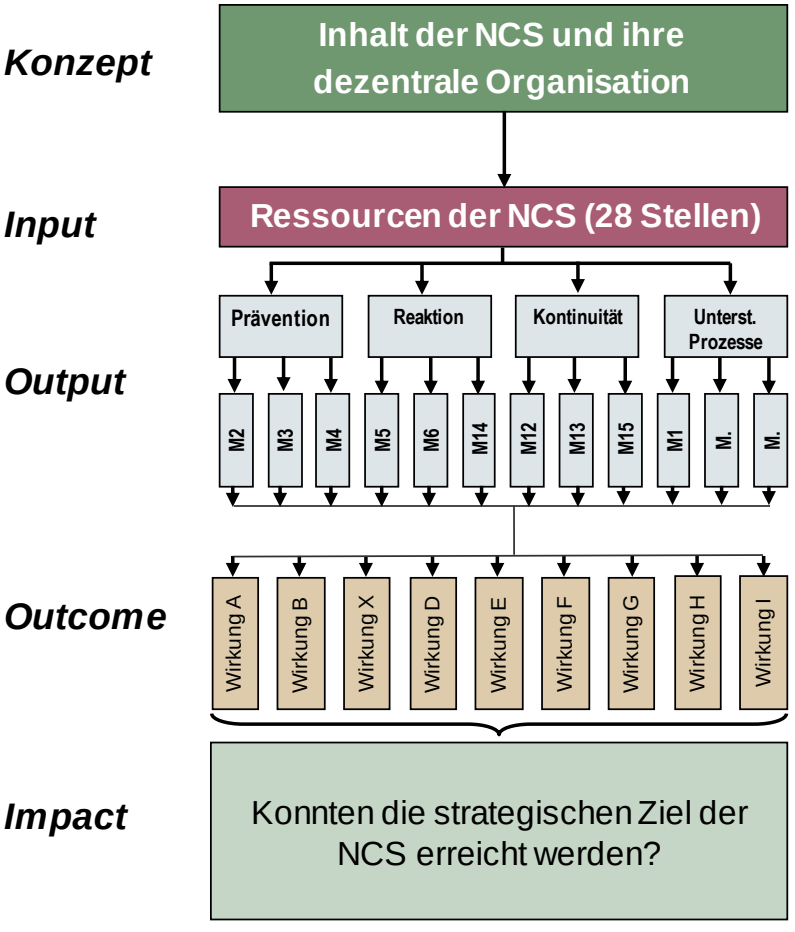

Illustration 1: Niveaux de l'évaluation de l'efficacité

- **Concept:** ce niveau concerne surtout les aspects interdisciplinaires et les interfaces. On évalue si le contenu et l'organisation de la SNPC sont adéquats et si la collaboration avec les tiers fonctionne. Les niveaux *Input*, *Output*, *Outcome* et Impact ont été examinés pour les seize mesures.
- ***Input*:** utilisation des ressources financières et personnelles pour mettre en œuvre la stratégie. L'évaluation porte sur l'utilisation des ressources allouées et sur leur soutien durable aux tâches de la SNPC.
- ***Output*:** résultats de la mise en œuvre effective de la stratégie, c'est-à-dire organisations établies, processus mis en place, offres de prestations et produits proposés, etc. Il s'agit d'évaluer l'avancement de l'application des mesures dans les différents domaines (réalisation des étapes).
- ***Outcome*:** groupes cibles touchés, connaissances nouvellement acquises, sensibilisations et changements comportementaux observés. L'évaluation est également axée sur les effets potentiels des différentes mesures (par ex. sensibilisation aux cyberrisques ou changements de comportement en la matière).
- **Impact:** la mise en œuvre des mesures a-t-elle permis d'atteindre les objectifs stratégiques de la SNPC? Quel impact effectif a eu l'application des mesures? On évalue également si cela a contribué à renforcer la résilience et à diminuer les cyberrisques.

Un modèle d'efficacité a été élaboré pour chaque mesure (et interface) en collaboration avec les responsables des mesures afin de pouvoir comprendre le but, la procédure et les résultats de ces dernières. L'évaluation des mesures s'appuie principalement sur les niveaux *Output*, *Outcome* et Impact, car ils permettent de mesurer directement les progrès réalisés et le résultat des travaux menés par les responsables de la mise en œuvre.

2.2. Réalisation

2.2.1. Procédure d'enquête

L'évaluation reposait sur un questionnaire type qui découlait du concept détaillé [3].

Des questionnaires individuels basés sur ce questionnaire type ont été établis pour chaque entretien ou, lorsque l'enquête a été menée par écrit, pour chaque destinataire.

Les questionnaires spécifiques ont ensuite été pré-remplis à l'aide des documents à disposition et, en général, envoyés aux personnes concernées au moins cinq jours ouvrés avant les entretiens afin qu'elles puissent se préparer. Les destinataires des questionnaires envoyés uniquement par écrit disposaient d'un délai d'environ dix jours ouvrés pour y répondre. À l'issue des entretiens, les questionnaires dûment complétés ont été soumis aux interlocuteurs pour qu'ils puissent vérifier leurs réponses.

2.2.2. Sélection des personnes interrogées

Les personnes interrogées ont été choisies en accord avec l'OC SNPC:

- **Entretiens individuels:** au total, quatorze entretiens ont été menés avec des représentants du SEFRI, de la DPS du DFAE, de la division SEC de l'UPIC, de MELANI, de l'OIC MELANI, du SRC, de fedpol, de l'OFCOM, de la ChF, du RNS, de l'OFPP, de l'OFAE, du RM, de la BAC et de l'OFEN.

- **Enquêtes écrites:** des représentants de six secteurs partiels critiques (approvisionnement en gaz naturel, approvisionnement électrique, transport aérien, banques, médias, santé) ont été interrogés par écrit.

La liste détaillée des entretiens figure à l'annexe A.1.

L'OC SNPC a fourni à AWK les documents nécessaires et disponibles sur chaque domaine thématique. Ceux-ci ont parfois été complétés par les propres recherches d'AWK (voir les documents référencés à l'annexe **Fehler! Verweisquelle konnte nicht gefunden werden.**).

2.2.3. Impression à l'issue de l'enquête

Le nombre de questions à poser selon les directives du concept détaillé [3] (plus de 280 au total) a constitué un défi particulier. Selon l'interlocuteur, un questionnaire pouvait souvent comprendre 100 questions, par exemple lorsque les responsables s'occupaient de plusieurs mesures. Très motivées, les personnes interrogées s'étaient bien préparées aux entretiens. La procédure retenue a été comprise et les participants ont activement soutenu l'enquête (réponse aux questions). Les personnes interrogées ont aussi parfois profité du contrôle des réponses après les entretiens pour apporter des précisions par écrit.

L'enquête purement écrite a également été menée sans problème particulier dans les secteurs partiels. Complétés rapidement, les questionnaires ont pu être évalués selon le calendrier prévu.

2.3. Établissement des rapports

Au cours de la dernière étape, les résultats ont été consolidés, puis compilés dans le présent rapport destiné au Conseil fédéral. Ce travail a été exécuté en étroite collaboration avec l'OC SNPC et les responsables de la mise en œuvre pour éviter toute ambiguïté, lacune ou contradiction.

Remarque: les déclarations figurant dans le rapport se basent sur les réponses des interlocuteurs lors des entretiens. AWK a intégré ces réponses dans le présent document sans en modifier le sens.

2.4. Principaux défis de l'évaluation

L'évaluation de l'efficacité s'appuie essentiellement sur l'appréciation des données collectées, celle-ci représentant également le principal défi de la procédure. Aux fins de transparence, AWK décrit ci-après certaines questions primordiales auxquelles l'équipe d'évaluation a été confrontée ainsi que les solutions retenues et les motifs correspondants.

2.4.1. Caractère hétérogène du contenu des mesures

Comme indiqué précédemment, le contenu des seize mesures couvre un éventail très large de sujets. La complexité de l'évaluation de l'efficacité tient notamment au fait que certaines mesures se traduisent par des produits finaux clairement définis, alors que d'autres visent à mettre en place de nouveaux processus ou à renforcer des processus existants. Pour un évaluateur, des produits sont plus facilement mesurables que des processus. Les mesures débouchant sur des produits risquent dès lors d'être évaluées différemment de celles qui sont plutôt axées sur des processus.

Pour désamorcer cette problématique, AWK se borne à évaluer les mesures en fonction des objectifs définis (étapes) dans la feuille de route SNPC **Fehler! Verweisquelle konnte nicht gefunden werden.**. Cela permet une évaluation équitable, car les ressources allouées se réfèrent aux mesures fixées. Par conséquent, AWK ne procède à aucune comparaison croisée entre les mesures lors de leur appréciation. L'évaluation de l'efficacité se contente de déterminer le degré de réalisation des objectifs de chaque mesure.

2.4.2. Évaluation de l'efficacité des mesures en cours

Le moment de la réalisation constitue le principal défi d'une évaluation de l'efficacité. En général, cette évaluation se déroule à la fin d'un programme. Lorsqu'elle est exécutée pendant la mise en œuvre d'un projet, deux difficultés fondamentales apparaissent:

- degré de mise en œuvre hétérogène des mesures: étant donné que plusieurs mesures sont encore en cours, l'évaluation porte souvent sur un résultat intermédiaire et non sur un résultat final;
- mesure de l'impact: en l'état actuel des choses, il est irréaliste de déterminer l'impact de la plupart des mesures, car elles ne déploieront leurs effets qu'ultérieurement.

AWK avait conscience de ces deux problèmes dès le départ. Concernant le degré de mise en œuvre hétérogène, la solution consiste à évaluer les mesures exclusivement en fonction des objectifs déjà atteints au printemps 2016, conformément à la feuille de route SNPC **Fehler! Verweisquelle konnte nicht gefunden werden.**. Les objectifs devant être réalisés ultérieurement d'après cette feuille de route ne sont pas pris en compte dans l'évaluation.

L'impact des mesures peut uniquement être évalué lorsqu'un effet direct peut être prouvé ou lorsque l'on constate de manière certaine que ce n'est pas le cas. Pour toutes les autres mesures, il est précisé qu'une appréciation n'est pas encore réalisable et que la mesure est évaluée sur la seule base de l'*output* et de l'*outcome*.

3. Évaluation de l'efficacité des mesures

L'objectif de chaque mesure tel qu'il est défini dans la feuille de route SNPC **Fehler! Verweisquelle konnte nicht gefunden werden.** et précisé par les responsables des mesures est déterminant pour évaluer ces dernières.

Les niveaux *Input*, *Output*, *Outcome*, Impact et Concept des seize mesures énoncées au chapitre 1.1.1 sont pris en considération selon la procédure exposée au chapitre 2.1.

Les chapitres du présent rapport qui sont consacrés aux différentes mesures sont tous structurés à l'identique:

- tableau décrivant la mesure et comportant les éléments suivants:
  - description des objectifs;
  - office responsable;
  - sources (documents consultés);
  - référence à l'entretien;
- effet escompté selon le modèle d'efficacité issu du concept détaillé [3];
- *input* (ressources utilisées);
- tableau concernant la réalisation des objectifs et l'impact;
- justification de l'évaluation, subdivisée en *output*, *outcome* et impact.

Les aspects relatifs aux interfaces sont exposés au chapitre 4, tandis que les aspects interdisciplinaires sont rassemblés au chapitre 5.

3.1. Mesures 2 et 12 – prévention et continuité: analyse des risques et vulnérabilités ainsi que continuité

Titre de la mesure	Analyse des risques et vulnérabilités ainsi que gestion de la continuité et amélioration de la résilience des secteurs partiels critiques
Objectifs	Objectifs de la mesure 2 «Analyse des risques et vulnérabilités»: • Des analyses des risques et vulnérabilités ont été effectuées dans les 28 secteurs partiels critiques, en collaboration avec les autorités compétentes et les associations faîtières et avec la participation des fournisseurs de prestations informatiques et des exploitants d'infrastructures critiques. Elles suivaient autant que possible une approche uniforme. – Les résultats de ces analyses ont été consolidés conjointement avec MELANI sous la forme d'une analyse globale de la menace. – Ils servent de base notamment aux travaux de réalisation de la mesure 12. Objectifs de la mesure 12 «Gestion de la continuité»: • Amélioration de la résilience des secteurs partiels critiques: des concepts comprenant d'éventuelles mesures d'amélioration de la résilience ont été élaborés dans les 28 secteurs partiels critiques sur la base des résultats des analyses des risques et vulnérabilités. – Il est indispensable de collaborer avec la branche et, si nécessaire, d'inclure les associations et les autorités spécialisées ainsi que les autorités de régularisation concernées. – Le concept peut comprendre, entre autres, des propositions concernant des mesures de prévention, la mise en place d'une gestion de la continuité et des crises dépassant le cadre de l'entreprise ou l'amélioration de la résilience de l'entreprise dans chaque secteur partiel critique.
Office / unité d'organisation responsable	OFPP, OFAE

Documents consultés pour l'évaluation de l'efficacité	Sources: **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**
Entretiens, questionnaires	Voir l'annexe A.1, entretiens I 3, I 8, et les questions aux secteurs partiels A.2

Remarques:

- Les 28 secteurs partiels ont été répartis comme suit entre l'OFPP et l'OFAE:
  - compétence de l'OFPP: représentations diplomatiques et sièges des organisations internationales, recherche et enseignement, biens culturels, Parlement, gouvernement, justice et administration, déchets, banques, assurances, soins médicaux et hôpitaux, laboratoires, médias, trafic postal, armée, services d'urgence, protection civile;
  - compétence de l'OFAE: approvisionnement en gaz naturel, approvisionnement en pétrole, approvisionnement électrique, industrie chimique et pharmaceutique, industrie des machines, des équipements électriques et des métaux (MEM), technologies de l'information, télécommunication, approvisionnement en denrées alimentaires, trafic routier, trafic maritime, trafic ferroviaire, trafic aérien, approvisionnement en eau, eaux usées.
- Pour évaluer les travaux relatifs aux mesures 2 et 12, treize représentants des secteurs partiels suivants ont été interrogés: soins médicaux et hôpitaux, laboratoires, banques, médias, approvisionnement électrique, gaz, trafic aérien.

3.1.1. *Effet escompté: modèle d'efficacité des mesures 2 et 12*

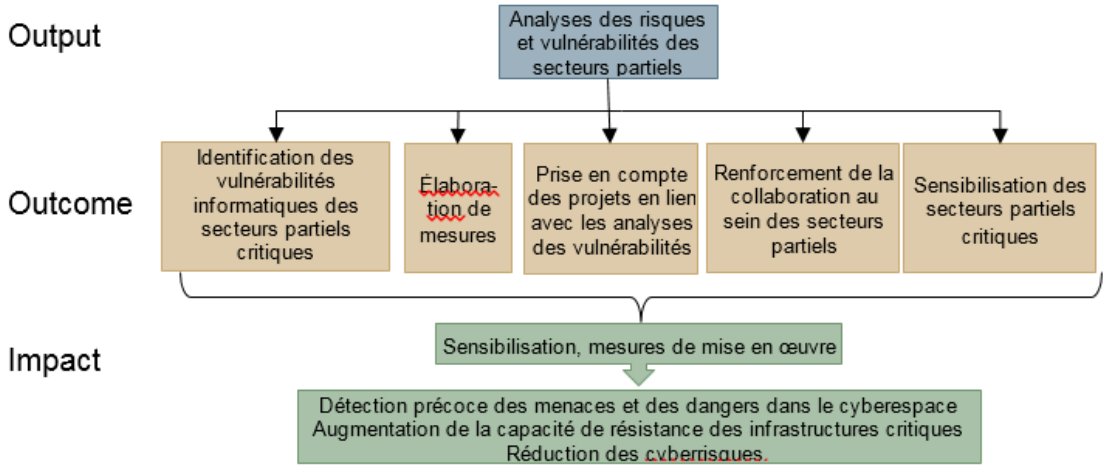

Illustration 2: Modèle d'efficacité des mesures 2 et 12

3.1.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	2 OFPP 2 OFAE 1 OFEN
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	Autorités spécialisées/régulateurs, MELANI, consultations de l'OFIT et de la BAC, associations professionnelles et représentants des infrastructures critiques, autres acteurs pertinents des secteurs partiels concernés

L'OFPP et l'OFAE ont chacun obtenu deux équivalents plein temps (EPT) pour la direction de projet et l'exécution des analyses des risques et vulnérabilités. L'OFEN s'est vu allouer un poste pour analyser les cyberrisques spécifiques au secteur énergétique, soutenir les mesures de résilience de la filière énergétique et, le cas échéant, préparer la modification du cadre légal. Les travaux n'auraient pas pu être réalisés sans ces créations de postes.

3.1.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome				✓✓
Impact	☐ actuellement non énon llem			

Remarque: les analyses des risques et vulnérabilités des secteurs partiels critiques n'étaient pas encore entièrement achevées au moment de l'évaluation de l'efficacité. Conformément aux prévisions, les travaux se poursuivent jusqu'en 2017 et respectent le calendrier fixé. Lorsque l'évaluation a été effectuée, les rapports finaux des analyses des risques et vulnérabilités des secteurs partiels suivants étaient disponibles:

- OFPP: protection civile, laboratoires, médias, banques ainsi que soins médicaux et hôpitaux. De plus, l'OFPP a mis à disposition des projets de rapport concernant les

services d'urgence, le Parlement, le gouvernement ainsi que la justice et l'administration;

- OFAE: approvisionnement électrique, approvisionnement en gaz naturel, trafic aérien, trafic routier, denrées alimentaires.

En plus des analyses des risques et vulnérabilités, un projet de rapport de l'OFAE sur la mesure 12 était déjà disponible pour le secteur du gaz naturel.

L'évaluation se base sur ces rapports.

3.1.4. Justification de l'évaluation

Output: objectifs atteints

Les analyses des risques et vulnérabilités des différents secteurs partiels étaient déjà réalisées en partie, tandis que d'autres étaient en cours d'élaboration au moment de l'évaluation de l'efficacité. Les experts interrogés considèrent que les rapports et la méthodologie retenue sont de bonne qualité. L'OFPP et l'OFAE appliquent des approches légèrement différentes pour leurs analyses, ce qui affecte un peu la cohérence et la transparence du projet global. À la fin des travaux, il sera cependant possible d'avoir une vue d'ensemble des risques et vulnérabilités informatiques dans les secteurs partiels critiques.

- **Évaluation des analyses des risques et vulnérabilités dans les secteurs partiels critiques:** les analyses des risques et vulnérabilités et les analyses de marché des secteurs partiels critiques sont en cours d'élaboration ou ont déjà été réalisées. Les rapports ont été établis par des groupes d'experts, sous la direction de l'OFPP ou de l'OFAE. Ces groupes ont reçu le soutien de représentants sectoriels (associations professionnelles ou principales entreprises), de représentants des autorités spécialisées et des régulateurs ainsi que de spécialistes en informatique. Les rapports ont fait l'objet d'un processus de feed-back à plusieurs niveaux, de sorte qu'ils ont été coordonnés de manière adéquate avec les experts des différents secteurs. Tous les rapports sont ensuite validés par l'OFPP ou l'OFAE et par l'UPIC.

  Les rapports terminés au moment de l'évaluation de l'efficacité ont permis de formuler l'évaluation suivante:

  – Procédure et structure: les experts des différents secteurs ont grandement apprécié l'étroite collaboration. Grâce à cette participation, les structures du marché ont pu être présentées intégralement dans chaque secteur, les risques et vulnérabilités ont fait l'objet d'une évaluation réaliste et la définition des mesures a été facilitée.
  – Méthodologie: dans chaque cas, le secteur partiel est d'abord présenté de manière générale; les processus critiques sont ensuite identifiés, puis une analyse des risques et vulnérabilités est réalisée. L'OFPP et l'OFAE ont appliqué des approches différentes pour évaluer les risques et les vulnérabilités (informations complémentaires ci-après).
  – Transparence et présentation des résultats: il est prévu d'élaborer, sur la base des rapports, des fiches d'information qui seront accessibles au grand public. Cela permettra d'obtenir une vue d'ensemble des analyses des risques et vulnérabilités et encouragera la transparence.

  Remarque concernant les approches divergentes de l'OFPP et de l'OFAE: ces deux offices ont appliqué une approche différente lors de l'évaluation des risques et vulnérabilités. L'OFPP se base sur les résultats des analyses des vulnérabilités pour

analyser les risques à l'aide de scénarios, l'évaluation du risque équivalant à la probabilité de survenance multipliée par le potentiel de dommages. L'OFAE évalue les vulnérabilités informatiques d'après le caractère critique et la menace potentielle qui pèse sur les processus partiels et renonce à analyser les risques à l'aide de scénarios. Ces divergences tiennent, d'une part, aux caractéristiques différentes des secteurs partiels concernés et, d'autre part, à une harmonisation avec des travaux existants dans les deux offices (OFPP: stratégie pour la protection des infrastructures critiques [stratégie PIC] et analyse nationale des dangers représentés par les catastrophes et les situations d'urgence en Suisse; OFAE: orientation stratégique de l'approvisionnement économique du pays). Compte tenu de ces différences, l'OFPP analyse les cyberrisques dans le contexte d'autres menaces potentielles, tandis que l'OFAE examine en profondeur les vulnérabilités informatiques spécifiques. Dans l'ensemble et malgré ces divergences, les analyses des deux offices permettent d'obtenir un aperçu des risques et vulnérabilités dans les secteurs partiels. De plus, les mesures informatiques spécifiques aux secteurs partiels seront elles aussi élaborées de manière similaire. Les procédures divergentes n'affectent donc pas la réalisation des objectifs des mesures.

Outcome: objectifs atteints

Les vulnérabilités informatiques dans les secteurs partiels traités ont été identifiées et évaluées de manière compréhensible. Les premières propositions ont déjà été formulées dans les rapports finaux relatifs à la mesure 2, alors qu'elles sont encore en cours d'élaboration dans les rapports distincts consacrés à la mesure 12. D'après les documents disponibles, des propositions concrètes bénéficiant d'une large assise dans les secteurs seront énoncées.
Le suivi de l'application des mesures et la mise à jour des analyses présentées constituent un défi. Les prochaines étapes doivent encore être définies à ce sujet.

- **Vulnérabilités informatiques identifiées dans les secteurs partiels critiques:** dans les rapports disponibles au moment de l'évaluation de l'efficacité, les vulnérabilités informatiques étaient analysées systématiquement et évaluées de manière compréhensible. Celles-ci n'ayant pas la même importance dans chaque secteur partiel, les rapports ne sont pas tous aussi détaillés les uns que les autres.
- **Élaboration de mesures:** les analyses comprennent déjà des propositions de mesures. L'élaboration de ces dernières s'effectue, elle aussi, en étroite collaboration avec les experts des secteurs, les autorités compétentes et les associations professionnelles. Elle est exposée dans les rapports sur la mesure 12. Au moment de l'évaluation de l'efficacité, seul un rapport de ce type (secteur partiel de l'approvisionnement en gaz naturel) et un concept général d'établissement des rapports étaient disponibles. Il est évident que des mesures concrètes pourront être formulées sur la base des analyses des risques et vulnérabilités, en collaboration avec les représentants sectoriels et les régulateurs (par ex. extension de Polycom aux exploitants des infrastructures critiques pour protéger la communication). Dans certains secteurs partiels, les résultats des travaux ont conduit à intégrer d'importants exploitants d'infrastructures critiques dans le cercle fermé des clients de MELANI.
- **Prise en compte des projets en cours:** la numérisation fait apparaître de nouvelles vulnérabilités informatiques dans de nombreux secteurs. Les analyses des risques et vulnérabilités laissent donc également entrevoir les futurs défis éventuels. Bien entendu, les analyses devront être régulièrement mises à jour en raison des évolutions technologiques, mais aucun rythme d'actualisation n'a encore été fixé.

- **Collaboration renforcée au sein des secteurs partiels:** la collaboration fonctionnait déjà dans les secteurs partiels avant la SNPC (notamment grâce aux travaux de l'OFPP en relation avec la stratégie PIC et à ceux de l'OFAE en rapport avec l'organisation de ses cadres), mais elle s'est désormais améliorée. Les travaux ont en particulier contribué à mieux intégrer les acteurs des différents secteurs partiels dans les analyses des risques et vulnérabilités.
- **Sensibilisation des secteurs partiels critiques:** certains secteurs partiels (banques par ex.) sont déjà fortement sensibilisés aux cyberrisques alors que d'autres ne le sont guère (par ex. trafic routier ou médias). Un important travail de sensibilisation a pu être réalisé dans ces secteurs. Plusieurs demandes à l'OFPP et à l'OFAE ont confirmé que les exploitants d'infrastructures critiques étaient désormais bien plus sensibles qu'avant à ces questions.

Impact: actuellement non évaluable

Les mesures 2 et 12 auront un impact lorsque les secteurs partiels appliqueront des mesures concrètes pour diminuer les risques et vulnérabilités informatiques et, partant, les cyberrisques auxquels ils sont exposés. C'est déjà le cas à titre individuel (par ex. dans le secteur du gaz naturel), mais il est encore trop tôt pour évaluer de manière globale l'impact de ces efforts et donc des mesures.

3.2. Mesure 3 – prévention et continuité: analyse de la vulnérabilité des infrastructures informatiques

Titre de la mesure	Mesure 3: analyse de la vulnérabilité des infrastructures informatiques
Domaine	Prévention
Objectifs	Les responsables des secrétariats généraux et les fournisseurs de prestations compétents reçoivent un concept de contrôle afin d'examiner les vulnérabilités systémiques, organisationnelles et techniques des infrastructures informatiques de l'administration fédérale et d'identifier les risques informatiques. Le concept de contrôle a été élaboré avec le soutien de l'OFIT et de la BAC, en coordination avec les projets en cours. Les résultats ont été consolidés en collaboration avec MELANI, sous forme d'analyse globale de la menace. Le concept de contrôle identifie les risques informatiques de chaque processus critique et définit les exigences minimales systémiques correspondantes. Les cantons, les milieux économiques et les exploitants d'IC intéressés recevront le concept de contrôle des infrastructures informatiques conçu par l'administration fédérale et utile à leurs propres vérifications des vulnérabilités.
Office / unité d'organisation responsable	UPIC
Documents consultés pour l'évaluation de l'efficacité	Sources: **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**
Entretiens	Voir l'annexe A.1, entretien I 7

3.2.1. Effet escompté: modèle d'efficacité de la mesure 3

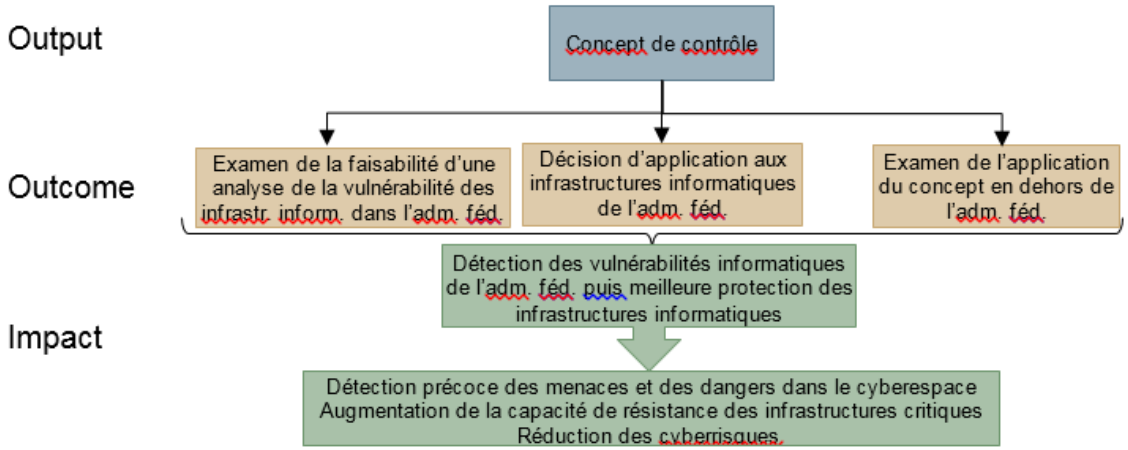

Illustration 3: Modèle d'efficacité de la mesure 3

3.2.2. Input: ressources utilisées

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Un poste (100 %) à l'UPIC, durée limitée jusqu'au 31.12.2015
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	Consultations auprès de l'OFIT, de la BAC et du Conseil de l'informatique de la Confédération (CI)

Remarques:

Une personne dûment qualifiée a occupé un poste supplémentaire d'une durée limitée jusqu'à fin 2015 pour élaborer le concept de contrôle. Les fournisseurs de prestations OFIT et BAC ainsi que le Conseil de l'informatique de la Confédération (CI) ont participé à cette élaboration. De manière générale, les ressources requises, en particulier les moyens nécessaires au contrôle de la faisabilité, ont été nettement sous-estimées.

3.2.3. Évaluation de la réalisation des objectifs et de l'impact

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output		✖		
Outcome	☐ actuellement non énon llem			
Impact	☐ actuellement non énon llem			

3.2.4. Justification de l'évaluation

Output: objectifs partiellement atteints

> Un concept d'analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale a certes été élaboré, mais le CP SNPC l'a refusé, car il estimait que sa mise en œuvre était irréaliste en raison des charges élevées. Une alternative a ensuite été développée dans le cadre d'une mesure particulière prise par le CP SNPC. Dans l'ensemble, les travaux sont en retard par rapport aux prévisions initiales.

Un concept de contrôle destiné au recensement complet et à l'évaluation systématique des vulnérabilités des infrastructures informatiques de l'administration fédérale a été élaboré dans le cadre de la mesure 3. Il s'appuie sur l'«Information Risk Assessment Methodology» (IRAM), qui est reconnue sur le plan international, et sur les normes d'analyse des risques informatiques qui ont été définies par le Bundesamt für Sicherheit in der Informationstechnik (BSI) en Allemagne.

Le concept sommaire a révélé que le mandat initial d'analyse des vulnérabilités des infrastructures informatiques devrait être étendu en cas de strict respect des normes, car il n'exigeait aucune prise en compte systématique des processus opérationnels, des dangers et des menaces, mais considérait uniquement les vulnérabilités. Par la suite, l'élaboration du concept de contrôle a cependant mis en évidence les importantes ressources personnelles et financières nécessaires à la réalisation d'une analyse détaillée des risques informatiques. Les consultations menées auprès des fournisseurs de prestations OFIT et BAC conformément au mandat ont également confirmé que le concept répondait certes aux objectifs, mais utilisait énormément de ressources. Ces dernières n'étant pas modifiables, les membres du CI ont estimé que le concept était théoriquement approprié, mais ils ont remis en question sa proportionnalité réelle et sa plus-value effective.

Le concept s'est heurté aux critiques du CP SNPC [65]. Les principaux reproches portaient sur le manque d'attention portée à l'identification des vulnérabilités des infrastructures informatiques, l'absence d'instructions claires et la plus-value discutable d'une analyse globale et fortement standardisée des risques informatiques. Le CP SNPC a donc pris une mesure particulière concernant la mesure 3 afin d'élaborer une alternative à ce concept de contrôle. Cette dernière définirait une procédure pragmatique et facilement

réalisable pour recenser les vulnérabilités des infrastructures informatiques. L'UPIC a développé un concept correspondant qui peut être appliqué en mobilisant beaucoup moins de ressources. Ce concept n'avait pas encore été approuvé par le CP SNPC au moment de l'évaluation de l'efficacité, mais il bénéficiait d'une large approbation lors des consultations préalables. Étant donné qu'il ne s'agit que d'une ébauche de procédure, d'autres travaux seront nécessaires avant la mise en place systématique d'une analyse de la vulnérabilité des infrastructures informatiques dans l'administration fédérale. Dans l'ensemble, force est de constater que les travaux sont en retard par rapport aux prévisions initiales.

Outcome: actuellement non évaluable

> Au moment de l'évaluation de l'efficacité, l'alternative n'existait que sous forme d'ébauche, mais les premières prises de position estiment qu'elle est réalisable. Il faut encore la concrétiser avant que son utilisation ne soit éventuellement décidée. L'applicabilité du concept en dehors de l'administration fédérale n'a pas encore été vérifiée.

- Faisabilité du concept de contrôle dans l'administration fédérale: la vérification systématique qui avait été élaborée n'a jamais eu lieu, car sa réalisation aurait mobilisé trop de ressources par rapport aux moyens limités et au budget défini. Seule l'alternative développée permettra d'examiner en détail la faisabilité d'une analyse de la vulnérabilité des infrastructures informatiques dans l'administration fédérale.
- Décision d'application aux infrastructures informatiques de l'administration fédérale: aucune décision n'a été prise, car le concept alternatif doit d'abord être examiné.
- Examen de l'application du concept en dehors de l'administration fédérale: cet examen est inopportun tant que l'application au sein de l'administration fédérale n'a pas été décidée.

Impact: actuellement non évaluable

> L'impact ne peut pas être évalué, car l'application du concept de contrôle n'a fait l'objet d'aucune décision et une alternative est en cours d'élaboration. Jusqu'à présent, l'impact de la mesure se limite à la sensibilisation des responsables hiérarchiques des départements à l'importance des analyses des vulnérabilités.

3.3. Mesure 4 – prévention et continuité: établissement d'un tableau de la situation et de son évolution

Titre de la mesure	Mesure 4: établissement d'un tableau de la situation et de son évolution
Domaine	Prévention
Objectifs	Les acteurs pertinents et responsables issus de la politique, de l'économie et de la société civile peuvent se renseigner sur les cyberincidents de portée nationale. Des analyses informant sur la situation et son évolution et adaptées à leur domaine de responsabilité sont mises à leur disposition. Ces informations sont collectées, évaluées, analysées, puis fusionnées dans un tableau de la situation dans le cadre du modèle de partenariat public-privé de MELANI. À cet effet, les connaissances spéciales requises sur le cyberespace et les capacités techniques sont développées, et la plate-forme d'échange volontaire d'informations avec des exploitants sélectionnés d'infrastructures critiques et l'économie est renforcée.

Titre de la mesure	Mesure 4: établissement d'un tableau de la situation et de son évolution
Office / unité d'organisation responsable	MELANI (SRC)
Documents consultés pour l'évaluation de l'efficacité	Sources: **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, [76], [77], [78], [79]
Entretiens	Voir l'annexe A.1, entretien I 2

3.3.1. *Effet escompté: modèle d'efficacité*

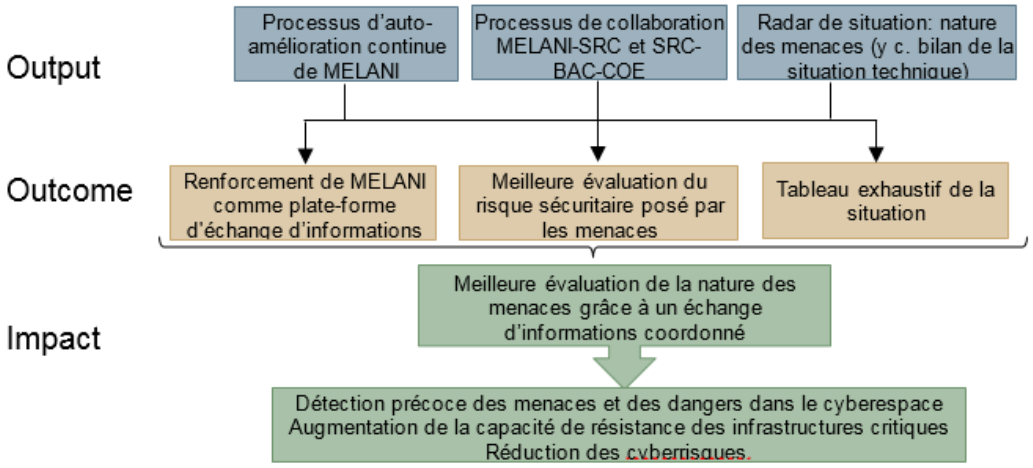

Illustration 4: Modèle d'efficacité de la mesure 4

3.3.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel [pool de ressources pour les mesures 4, 5 et 14]	3 MELANI UPIC 3 OIC MELANI (SRC) 7 SRC 1 RM 4 BAC
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	Services participants en plus de MELANI, SRC, RM et BAC: OFIT, SCOCI

Remarques concernant les postes alloués au SRC: les postes créés dans la cybernétique sont regroupés dans une nouvelle unité d'organisation (Cyber SRC), à l'exception des services d'achat. De plus, le commissariat spécialisé Cyber a été mis en place.

Les collaborateurs embauchés sont dûment qualifiés pour cette tâche spécialisée. Ils disposent non seulement des capacités techniques, mais également des compétences relationnelles nécessaires. La durée déterminée des contrats était un obstacle lors du recrutement.

Les ressources nécessaires en personnel ont été correctement évaluées (les mêmes ressources sont également utilisées pour les mesures 5 et 14; voir les chap. 3.4.2 et 3.6.2).

De nouveaux besoins ont toutefois été identifiés, par exemple en vue de l’élaboration de nouveaux produits ou d’une analyse approfondie plus stricte.

3.3.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✓	
Outcome			✓	
Impact	◎ Impact obtenu			

3.3.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

> Les processus d'auto-amélioration de MELANI et de renforcement de la collaboration MELANI-SRC et SRC-BAC-COE sont définis ou les travaux correspondants sont bien avancés. Un prototype du radar de la situation a été élaboré. Il devra toutefois être encore développé afin de fournir une image exhaustive de la situation.

Les *outputs* définis dans le modèle d'efficacité ont été en majeure partie atteints:

- **Processus d'auto-amélioration continue de MELANI:** le programme d'auto-amélioration continu de MELANI est en cours d'élaboration. Il devrait être présenté d'ici fin 2016 et être expertisé séparément par une entreprise externe. Il se base sur les besoins des clients recensés dans le cadre de la mesure 13 et sur le concept existant visant à renforcer MELANI en tant que plate-forme d'échange d'informations. Les processus définis dans le concept d'auto-amélioration seront examinés lors de séances régulières et, le cas échéant, adaptés à une nouvelle menace.
- **Processus de collaboration MELANI-SRC et SRC-BAC-COE:** les processus de collaboration entre MELANI et le SRC, entre ce dernier et BAC-COE ainsi que ceux concernant la participation de partenaires internationaux sont définis dans un guide et sont également mis en œuvre. Très bonne, la collaboration entre MELANI et le SRC est étroite et fait ses preuves depuis plusieurs années. Des conventions de prestations correspondantes ont renforcé la collaboration entre le SRC et BAC-COE.

  Les responsables des mesures estiment que la collaboration est aussi bonne, car les personnes se connaissent bien dans la cybernétique et peuvent échanger bilatéralement. La convention de prestations est considérée comme suffisante, mais doit être examinée régulièrement et adaptée le cas échéant. Tous les acteurs pertinents au sein de la Confédération sont identifiés et participent activement. La collaboration en la matière est très conviviale et professionnelle. Il est également important que des réunions de coordination régulières soient organisées sous l'égide de l'OIC MELANI entre les principaux acteurs techniques et opérationnels (GovCERT, BAC-COE CNO, Cyber SRC, OFIT-CSIRT, MilCERT et Cyber RM) afin d'analyser globalement le niveau de menace et de coordonner le traitement des incidents.
- **Tableau global de la situation** (y compris au niveau technique): un prototype destiné à représenter le niveau de menace (radar de la situation) a été développé et sa version finale a été présentée à l'automne 2016. Ce produit est mis à la disposition des infrastructures critiques en tant qu'outil de monitoring avec des informations spécifiques aux secteurs. Les informations du radar s'appuient sur les connaissances du SRC, les analyses techniques du GovCERT et les renseignements des enquêteurs de la police, qui sont fournis par l'intermédiaire du SCOCI.

Le radar de la situation devra cependant être encore développé afin de fournir effectivement un tableau exhaustif de la situation. Actuellement, les cas complexes et leurs interactions ne peuvent pas encore être représentés. De plus, la qualité du radar dépend de MELANI, qui doit disposer de ressources suffisantes pour traiter les informations pertinentes et les saisir dans le système ainsi que pour renforcer l'échange d'informations avec les infrastructures critiques.

Outcome: objectifs en majeure partie atteints

Le radar de la situation constitue un outil important pour présenter un tableau exhaustif de la situation. L'échange d'informations entre les participants et les exploitants d'infrastructures critiques doit encore être renforcé pour que l'évaluation de la situation exposée dans le radar soit précise et à jour.
La nouvelle extension du cercle fermé des clients de MELANI représente un premier pas dans ce sens. Une orientation stratégique claire pour la future croissance de ce cercle fait cependant encore défaut.

- **Renforcement de MELANI en tant que plate-forme d'échange d'informations:** depuis sa création en 2004, MELANI a connu une forte expansion et a pu étendre le «cercle fermé des clients», qui comprend des représentants des infrastructures critiques. Actuellement, plus de 190 grandes entreprises suisses et unités administratives issues de dix secteurs y sont représentées et peuvent partager et obtenir des informations concernant la sécurité. Une nouvelle extension de ce cercle est nécessaire pour renforcer l'échange d'informations. Il n'existe toutefois encore aucune stratégie précise sur l'exécution de cette extension. La question de la participation éventuelle d'entreprises ne faisant pas partie des infrastructures critiques n'a pas été tranchée. Il faut davantage développer les idées relatives à un «modèle de cercle» qui rassemblerait plusieurs cercles de clients (avec des droits et obligations correspondants).
- **Meilleure évaluation de la pertinence des menaces pour la sécurité:** l'extension du cercle fermé des clients a permis de mieux évaluer la pertinence des menaces pour la sécurité. Plus le nombre d'acteurs échangeant des informations est grand, plus la situation présentée en matière de menaces est précise. Les informations collectées doivent cependant être interprétées avec la diligence requise, ce qui implique une charge supplémentaire. Les ressources disponibles limitent l'ampleur et la précision de l'analyse [73]. Une nouvelle extension est difficilement réalisable avec les ressources actuelles.
- **Tableau exhaustif de la situation et de son évolution:** le radar de la situation qui a été développé permet d'obtenir une vue d'ensemble actualisée, car il propose une représentation en temps réel. De plus, les acteurs concernés peuvent être contactés rapidement, car l'OIC MELANI a un service de permanence qui est opérationnel 24 heures sur 24 et sept jours sur sept (y compris le service par SMS). Grâce aux informations, la capacité d'action a progressé, comme en attestent les exemples suivants:
  - attaques DDoS: la coopération internationale a permis d'informer à temps et préalablement des entreprises, qui ont dès lors pu prendre les contre-mesures correspondantes;
  - Heartblead: le tableau de la situation a contribué à une meilleure évaluation des menaces;
  - menace concernant le WEF dans la presse: les déclarations précises basées sur le tableau de la situation ont conduit à une évaluation appropriée, à savoir qu'aucune menace réelle ne visait le WEF.

L'objectif suprême d'un tableau exhaustif de la situation n'est cependant réalisable que si l'échange d'informations et la collaboration entre tous les partenaires concernés sont encore renforcés. Des ressources supplémentaires devraient être allouées pour exécuter entièrement le mandat relatif à la mesure 4.

Impact: objectif atteint

> Aujourd'hui, la menace peut être mieux évaluée, car l'échange d'informations entre le SRC, MELANI, le RM, les fournisseurs de prestations et les exploitants d'infrastructures critiques est coordonné. La mise en place de l'unité Cyber SRC a permis à de nombreuses reprises d'identifier précocement des attaques et des menaces. Grâce au radar de la situation, il est possible d'avoir une vue d'ensemble des menaces et d'évaluer leur pertinence pour la sécurité de la Suisse.

La meilleure capacité d'attribution du SRC joue également un rôle essentiel dans l'évaluation plus précise de la situation. L'étroite collaboration entre les acteurs et les liens importants entre le SRC et les services partenaires ont conduit à une identification accrue des agresseurs. Ces informations sont primordiales pour évaluer la situation (informations complémentaires au chap. 3.6).

3.4. Mesure 5 – réaction: analyse et suivi des incidents

Titre de la mesure	Analyse et suivi des incidents
Domaine	Réaction
Objectifs	La Confédération, les cantons et les exploitants d'IC ont réexaminé et affiné leurs propres mesures visant à gérer les incidents. Les enseignements tirés des incidents pertinents (dus à des maliciels, des réseaux de zombies ou des chevaux de Troie) sont transmis à MELANI selon des processus bien établis au sein et en dehors de la Confédération. Lors du traitement ultérieur de ces incidents, les exploitants d'infrastructures critiques et les fournisseurs de prestations informatiques peuvent bénéficier, sur demande, du soutien technique de MELANI. Le SRC transmet à MELANI les enseignements relatifs à la protection de l'État qui sont tirés d'incidents pertinents en lien avec des cyberrisques. Les fournisseurs de prestations (CERT) se dotent des capacités techniques de surveillance des réseaux fédéraux. Les plates-formes et les infrastructures destinées à l'identification et à la réduction des cybermenaces ainsi que le soutien technique apporté aux exploitants d'infrastructures critiques sont en place. De même, les connaissances spécifiques et les capacités scientifiques inhérentes à la détection et à la lutte contre les cybermenaces ont été développées dans les services concernés de la Confédération.
Office / unité d'organisation responsable	MELANI et SRC
Documents consultés pour l'évaluation de l'efficacité	Sources: [80], [81], [82], [83]
Entretiens	Voir l'annexe A.1, entretien I 10

3.4.1. *Effet escompté: modèle d'efficacité de la mesure 5*

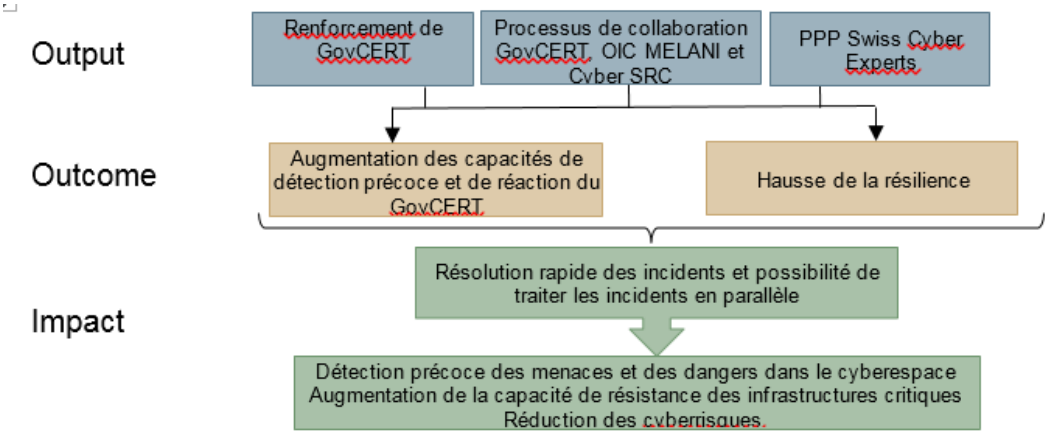

Illustration 5: Modèle d'efficacité de la mesure 5

3.4.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel [pool de ressources pour les mesures 4, 5 et 14]	3 MELANI UPIC 3 OIC MELANI (SRC) 7 SRC 1 RM 4 BAC
Ressources financières	Aucune
Collaboration avec d'autres offices / unités d'organisation	Collaboration avec le CSIRT de l'OFIT

<u>Remarques concernant les postes alloués à MELANI UPIC et à l'OIC MELANI:</u>

Trois postes supplémentaires ont été approuvés dans le GovCERT (MELANI UPIC) pour mettre en œuvre la SNPC. Trois postes ont également été alloués à l'OIC MELANI du SRC. Actuellement (au 1er août 2016), le GovCERT comprend au total l'équivalent de 4,6 postes à 100 % (prévisions: équivalent de 5,6 postes à 100 %). L'OIC compte 8 EPT. Dans un premier temps, cela garantissait le traitement normal des incidents. Il est désormais possible de traiter en parallèle deux incidents de plus grande ampleur.

Grâce aux liens étroits noués avec des services connexes tels que le CSIRT de l'OFIT et le COE, il est possible en cas de crise de faire appel à d'autres personnes dûment qualifiées de l'administration fédérale pour maîtriser la situation.

Si les ressources correspondantes n'étaient plus disponibles après 2017, le mandat de base de MELANI (protection des infrastructures critiques en Suisse et soutien en cas de cybercrise) ne pourrait plus être réalisé avec la même qualité. Les connaissances techniques viendraient à manquer et la qualité du réseautage national et international diminuerait sensiblement.

3.4.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✓	
Outcome			✓	
Impact	◎ Impact obtenu			

3.4.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

Les capacités destinées à la résolution des incidents ont indéniablement pu être renforcées grâce à une extension des ressources allouées au GovCERT et à l'OIC MELANI ainsi qu'à une meilleure collaboration entre tous les acteurs. Un élément manque pour compléter la mise en œuvre: la création prévue d'une plate-forme sécurisée de communication en vue d'un échange d'informations sur les incidents.

- **Renforcement des unités opérationnelles de MELANI (GovCERT et OIC MELANI):** le Swiss Government Computer Emergency Response Team (GovCERT) a clairement pu étendre ses opérations grâce au renforcement des effectifs de MELANI. Il est donc aujourd'hui indéniablement plus résilient que quelques années auparavant. De plus, l'organisation du GovCERT a été définie en 2013. Le renforcement de la partie analytique de MELANI au SRC (OIC MELANI) a permis de surmonter la charge de travail supplémentaire connexe et de traiter les informations obtenues dans les domaines de l'évaluation, de l'estimation et de la communication avec les infrastructures critiques.
- **Début des opérations de Cyber SRC:** très active sur le plan international, la nouvelle unité Cyber SRC a trouvé sa place au sein du SRC. Les analyses, le réseau de sources et les contacts internationaux ont contribué à la détection précoce d'incidents, à des attributions et à la catégorisation de menaces en temps opportun.
- **Définition des processus de collaboration GovCERT, OIC MELANI et Cyber SRC:** parallèlement au renforcement du GovCERT et de l'OIC MELANI, le SRC a achevé l'élaboration d'un concept visant à structurer ses capacités cybernétiques ainsi que la création des descriptions de postes pour l'analyse des incidents. Il a également mis en place ou développé activement le transfert de savoir sur différentes plates-formes de communication, un site Internet comprenant un formulaire de déclaration d'incident et une plate-forme destinée à l'échange d'informations sur les maliciels (Malware Information Sharing Platform, MISP). Par ailleurs, les processus de transfert de savoir ont été renforcés, les capacités de résistance et de détection ont été accrues et l'interaction des différents CERT nationaux et internationaux a été améliorée (grâce à des contacts personnels et à l'adhésion au Forum for Incident Response and Security Teams [FIRST] et à l'European Government CERTs [EGC]). En cas d'incident, les données peuvent être analysées et préparées de telle sorte que l'organisation attaquée soit capable de prendre des contre-mesures techniques. Grâce à des plates-formes, des structures et des processus établis, les incidents traités alimentent la prévention en tant qu'enseignements tirés (*lessons learned*) et permettent d'actualiser la menace. Dans l'ensemble, les acteurs sont ainsi mieux préparés. La réalisation prévue d'une plate-forme sécurisée de communication sur laquelle tous les acteurs pertinents pourront échanger facilement et rapidement des informations sur des incidents ne s'est pas encore concrétisée.

- **Création du partenariat public-privé (PPP) Swiss Cyber Experts:** la création du PPP Swiss Cyber Experts (association regroupant des représentants du secteur informatique) a permis d'établir une organisation supplémentaire dotée d'un savoir-faire spécialisé, à laquelle on peut faire appel en cas de cyberincident grave.

Outcome: objectifs en majeure partie atteints

Les capacités accrues permettent aujourd'hui de détecter plus rapidement les incidents et de réagir plus vite. La résilience face aux menaces durables a également été renforcée. Les ressources demeurent cependant trop limitées pour surmonter des situations exceptionnelles. De plus, il faut examiner régulièrement les compétences spécialisées supplémentaires dont ont besoin le GovCERT et l'OIC MELANI.

- **Augmentation des capacités de détection précoce et de réaction:** l'adoption de la SNPC a étendu le mandat de MELANI concernant le traitement des incidents. Pour exécuter ce mandat, les capacités de gestion des menaces (*threat management*) ainsi que les capacités analytiques et scientifiques ont été développées au sein du GovCERT et de l'unité Cyber SRC. Grâce à ce développement et au renforcement de la collaboration entre le GovCERT, le CSIRT de l'OFIT et l'OIC MELANI, qui assume la coordination et est rattaché au Service de renseignement, les incidents peuvent désormais être détectés plus rapidement. Il est également possible d'y apporter une réponse ciblée. Les exploitants d'infrastructures critiques sont très satisfaits de l'aide fournie par MELANI en cas d'incident (source: enquête auprès du cercle fermé des clients).

  Malgré le développement des connaissances, des lacunes demeurent au niveau du savoir-faire technique, et en particulier de la sécurité des systèmes de contrôle et d'acquisition de données (*supervisory control and data acquisition*, SCADA), qui constitue un élément important. En l'espèce, la complexité tient aux connaissances très spécialisées qui sont requises selon le système. La collaboration avec des spécialistes des domaines correspondants doit donc être encore renforcée.

- **Hausse de la résilience:** le nombre actuel de postes est suffisant dans une situation normale. Les ressources disponibles sont cependant insuffisantes en cas de situations exceptionnelles qui s'étendraient sur plusieurs jours ou semaines. Elles atteindraient même rapidement leurs limites en cas d'incidents simultanés. Il faut donc renforcer le réseautage avec les CERT de l'économie privé. En plus des bonnes relations qui ont déjà été nouées avec les principaux CERT, il conviendrait d'intégrer des *response teams* de plus petite taille dans le réseau de MELANI, et notamment du centre de compétence technique GovCERT.

Impact: objectif atteint

Les capacités accrues de résolution des incidents ont déjà été utilisées lors de plusieurs incidents, démontrant ainsi l'efficacité des mesures prises.

Les connaissances spécialisées, les capacités et la résilience des unités opérationnelles de MELANI (GovCERT et OIC MELANI) ont déjà été utilisées pour résoudre efficacement des incidents. L'extension des ressources permet également de traiter désormais plusieurs incidents en parallèle. Grâce à l'amélioration de la détection précoce, il est possible de réagir plus rapidement aux incidents et de les maîtriser plus vite.

3.5. Mesure 6 – réaction: concept de vue d'ensemble des infractions et coordination des cas intercantonaux complexes

Titre de la mesure	Concept de vue d'ensemble des infractions et coordination des cas intercantonaux complexes
Objectifs	La Confédération et les cantons ont défini, dans un concept soumis au Conseil fédéral, les modalités de leur future collaboration à des fins de coordination des cas intercantonaux complexes. Ce concept indique comment obtenir au niveau national une vue d'ensemble aussi complète que possible des cas (infractions), et donc précise tant les interfaces prévues avec d'autres acteurs pour réduire les cyberrisques que le flux des informations destinées à l'état des lieux. La coordination des cas intercantonaux complexes tiendra aussi compte des efforts déjà déployés au niveau international pour que les cyberrisques donnent lieu à des poursuites pénales. Le concept précisera s'il convient de modifier le droit fédéral ou cantonal, et quelles ressources il faudra consacrer à sa mise en œuvre. Les informations acquises à partir de la vue d'ensemble (infractions) et les résultats sur les cas complexes obtenus par l'analyse technico-opérative dans le cadre d'une procédure pénale sont transmis en permanence à MELANI. En contrepartie, MELANI fournit régulièrement au SCOCI les informations pénales pertinentes qui proviennent de ses propres travaux (informations des CERT et du Service de renseignement). Les processus tant internes qu'externes à la Confédération seront établis à cet effet.
Office / unité d'organisation responsable	SCOCI
Documents consultés pour l'évaluation de l'efficacité	Sources: [84], [85], **Fehler! Verweisquelle konnte nicht gefunden werden.**, [87], [88], [89]
Entretiens	Voir l'annexe A.1, entretien I 6

3.5.1. Effet escompté: modèle d'efficacité de la mesure 6

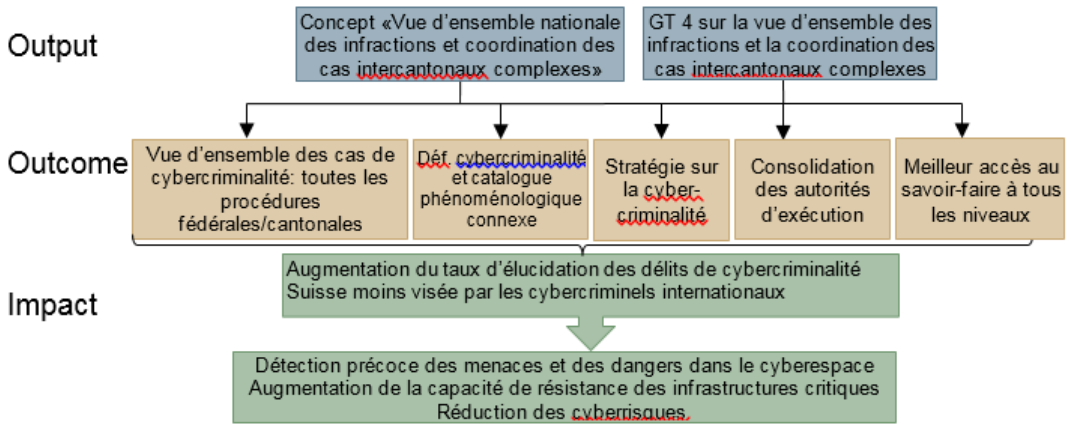

Illustration 6: Modèle d'efficacité de la mesure 6

3.5.2. Input: ressources utilisées

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Un poste (100 %), durée limitée à deux ans
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	

Un poste à durée limitée (deux ans) a été approuvé pour l'élaboration du concept en vue de la mise en œuvre de la SNPC. Il n'a toutefois été occupé que six mois. Le recrutement d'une personne adéquate s'est révélé difficile.

3.5.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✔	
Outcome		✖		
Impact	☐ actuellement non énon llem			

3.5.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

Achevé, le concept de vue d'ensemble nationale des infractions doit encore être approuvé. Au cours de son élaboration, la nécessité d'une stratégie globale sur la cybercriminalité qui irait au-delà de ce concept a été constatée. Les échanges avec les cantons dans le groupe de travail 4 ont été fructueux, mais il existait déjà grâce au SCOCI une bonne coordination entre la Confédération et les cantons en matière de cybercriminalité.

- **Concept «Vue d'ensemble nationale des infractions et coordination des cas intercantonaux complexes»:** le document est prêt et semble actuellement complet. Il doit être soumis à la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) à l'automne 2016, puis au Conseil fédéral. Son approbation était initialement prévue au printemps 2016, mais elle a été retardée, car les discussions avec les cantons, qui jouent un rôle déterminant dans la mise en œuvre du concept, se sont prolongées.

  Toutes les parties concernées ont dûment participé à l'élaboration. MELANI a fourni la liste des exigences pour la vue d'ensemble et contribué à la rédaction du concept par l'intermédiaire du groupe de travail 4 (GT 4) du RNS. Au début, les cantons participaient plutôt passivement, car l'utilité et l'objectif de cette mesure n'étaient pas évidents à leurs yeux. Ils n'en ont pris conscience qu'après l'établissement d'un catalogue phénoménologique définissant clairement les différentes formes de cybercriminalité, et ont ensuite activement pris part à la création du concept.

  Ce dernier ne définit toutefois aucun processus de recensement des cas et de réalisation d'une vue d'ensemble des infractions. Il ne présente que des variantes indiquant qui fournit quelles informations, à quel moment, et où celles-ci sont consolidées dans une vue d'ensemble des infractions. Ces questions seront examinées dans le sillage de la future stratégie globale Cybercrime.

- **GT 4 sur la vue d'ensemble des infractions et la coordination des cas intercantonaux complexes:** le groupe de travail 4 du RNS a contribué à l'élaboration du catalogue phénoménologique, car les cantons ont pris part à la définition des cas de cybercriminalité. Le GT 4 a été consulté dans le cadre des travaux relatifs au concept de vue d'ensemble des infractions, mais ses membres n'y ont pas participé directement. De manière générale, une étroite collaboration entre la Confédération et les cantons existe déjà par l'intermédiaire du SCOCI. Le GT 4 n'a apporté qu'une plus-value limitée en vue du renforcement de la collaboration.

Outcome: objectifs partiellement atteints

Il n'y a aucune vue d'ensemble exhaustive des infractions relatives à la cybercriminalité en Suisse, car tous les cantons ne saisissent pas encore les données correspondantes. Grâce aux nouvelles fiches phénoménologiques, les différentes formes de cybercriminalité sont désormais décrites et clairement délimitées. Les compétences n'ont pas encore été réglementées; cela reste un défi majeur qui sera abordé dans le cadre de l'élaboration de la stratégie globale sur la cybercriminalité.

- **Vue d'ensemble nationale des infractions:** les cantons ont été consultés lors de l'élaboration du concept de vue d'ensemble des infractions. Ils ont également donné leur avis lors de la procédure de consultation. Tous les cantons ne saisissent pas encore les données concernant la cybercriminalité, de sorte qu'aucune vue exhaustive des infractions n'est possible pour le moment. Les données sont collectées manuellement (le SCOCI prend contact avec les cantons). La procédure de coordination en vue de la création d'une vue d'ensemble des infractions a été examinée avec les cantons et avec le Ministère public de la Confédération.
- **Définition de la cybercriminalité et catalogue phénoménologique connexe:** la création d'un catalogue phénoménologique détaillé sur les différentes formes de cybercriminalité est un pas important dans l'élaboration de la vue d'ensemble des infractions et dans le renforcement de la collaboration en cas de poursuite pénale. Ce catalogue favorise une compréhension commune et contribue à définir les compétences. La mise en place d'une offre de formation destinée aux policiers constitue également un objectif (module intégré à l'offre de l'Institut suisse de police).
- **Stratégie sur la cybercriminalité:** les travaux relatifs à la mesure 6 ont conduit à reconnaître la nécessité d'une stratégie globale des cantons sur la cybercriminalité. Cette stratégie est en cours d'élaboration et sera harmonisée avec la SNPC. Tant la mesure 6 que la stratégie globale seront présentées au DFJP et à la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) de sorte qu'il ne devrait y avoir aucune divergence. Les travaux concernant la stratégie n'en sont toutefois qu'à leurs balbutiements.
- **Consolidation des autorités de poursuite pénale:** les travaux relatifs à la mesure 6 ont mis en lumière la définition encore insuffisante des compétences. À cela s'ajoute la jurisprudence du Tribunal fédéral, par exemple en relation avec les cas d'hameçonnage (*phishing)*. La collaboration entre les cantons et la Confédération fonctionne toutefois grâce au SCOCI.
- **Meilleur accès au savoir-faire:** la formation technique et analytique ne relève pas directement de la mesure 6. Les fiches phénoménologiques contribueront à l'avenir à renforcer la formation des policiers dans le domaine de la cybercriminalité.

Impact: non évaluable

L'objectif de réduction de la cybercriminalité n'est pas mesurable pour le moment. Les autorités de poursuite pénale ne disposent pas encore aujourd'hui de données suffisantes pour évaluer cette question. Compte tenu de la forte progression des activités des cybercriminels, la limitation des cas de cybercriminalité constituera un objectif plus réaliste que leur diminution effective.

3.6. Mesure 14 – réaction: mesures actives d'identification des agresseurs

Titre de la mesure	Mesures actives d'identification des agresseurs
Objectifs	En cas de menace spécifique liée à des cyberrisques, le SRC a les moyens d'identifier l'agresseur, en coopération avec ses partenaires étrangers. Avec le soutien de la BAC et du RM comme fournisseurs de prestations. Le Ministère public de la Confédération reçoit du SRC, dans la mesure où la loi le permet, des informations sur l'agresseur. Lorsqu'aucune procédure pénale n'est engagée, le SRC prépare des contre-mesures actives si la base juridique correspondante (loi fédérale sur le renseignement) existe.
Office / unité d'organisation responsable	OIC MELANI, SRC, UPIC
Documents consultés pour l'évaluation de l'efficacité	Sources: **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, [76], [77], [78], [79]
Entretiens	Voir l'annexe A.1, entretien I 2

3.6.1. Effet escompté: modèle d'efficacité de la mesure 14

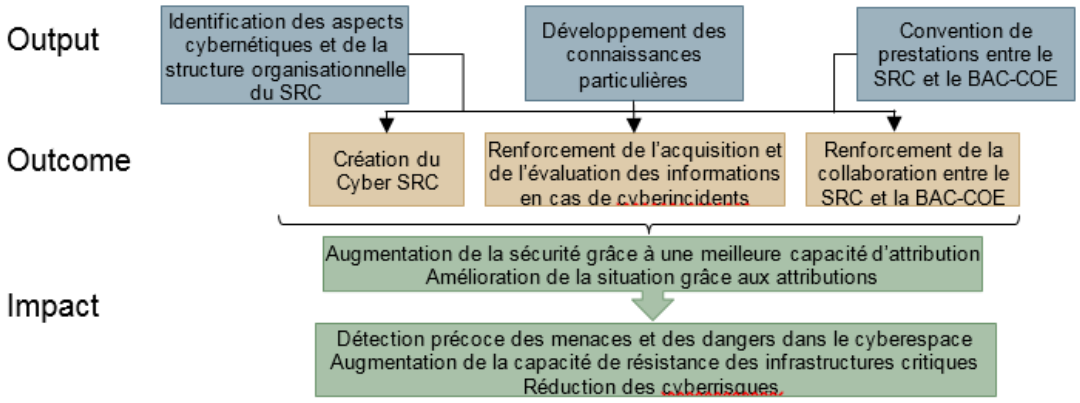

Illustration 7: modèle d'efficacité de la mesure 14

3.6.2. Input: ressources utilisées

Type de ressources	Ressources SNPC utilisées
Ressources en personnel [pool de ressources pour les mesures 4, 5 et 14]	3 UPIC MELANI 3 OIC MELANI (SRC) 7 SRC 1 RM 4 BAC
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	BAC, RM, MELANI

Remarques:

Voir les mesures 4 (chap. 3.3) et 5 (chap. 3.4).

3.6.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✓	
Outcome			✓	
Impact	◎ Impact obtenu			

3.6.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

Le SRC a défini les compétences dont il doit disposer pour identifier les agresseurs. Il a acquis et développé les connaissances spécifiques nécessaires à cette tâche. Le principal défi demeure l'analyse des acteurs et de leur environnement, car ils proviennent de régions très diverses. Des connaissances spécifiques doivent encore être obtenues en la matière.

- **Identification des aspects cybernétiques:** le SRC a identifié les huit compétences-clé suivantes pour son travail lié au cyberespace **Fehler! Verweisquelle konnte nicht gefunden werden.**:
  - évaluation technique des moyens utilisés par les agresseurs;
  - obtention d'informations pour tirer des enseignements supplémentaires sur le mode opératoire, les objectifs et les motivations des agresseurs;
  - rapprochement avec les renseignements existants sur les acteurs et les infrastructures du cyberespace;
  - rapprochement avec les renseignements existants sur des incidents similaires en Suisse et à l'étranger;
  - échange d'informations avec les services partenaires en fonction de la situation et coordination avec les autorités de poursuite pénale;
  - évaluation et actualisation des informations et renseignements existants aux niveaux stratégique et opérationnel à l'intention des décideurs politiques et adaptation de l'évaluation de la menace;
  - prise en compte des implications concernant les traités internationaux;
  - densification des connaissances liées aux rapports d'analyse et aux rapports sur les menaces.

  Lorsque la nouvelle loi fédérale sur le renseignement entrera en vigueur, d'autres compétences concernant les contre-mesures actives pourront être développées.
- **Développement des connaissances particulières:** le SRC pourrait acquérir et développer ses connaissances techniques dans les domaines suivants, en collaboration avec ses partenaires d'OIC MELANI, de GovCERT et du BAC-COE:
  - analyse des données réseau (analyse technique des objectifs et des méthodes de cyberattaque);
  - analyse des maliciels (accent mis sur la rétro-ingénierie ou ingénierie inversée et sur la classification des agresseurs);
  - analyse des acteurs (analyse de la menace et classification des agresseurs);
  - analyse du contexte (environnement et conditions-cadres d'une cyberattaque).

Actuellement, les capacités d'analyse des acteurs restent limitées en raison de ressources restreintes.

- **Convention de prestations entre le SRC et le BAC-COE:** pour exécuter ses tâches dans le cyberespace, le SRC fait parfois appel au savoir-faire technique du BAC-COE. Cette collaboration repose sur une convention de prestations spécifique.

Outcome: objectifs en majeure partie atteints

La création de l'unité Cyber SRC a permis de renforcer et de regrouper les compétences du SRC concernant le cyberespace. Les informations sont obtenues correctement, mais leur évaluation demeure difficile en raison de ressources limitées. L'échange de renseignements avec le Ministère public de la Confédération n'est pas encore optimal.

- **Cyber SRC:** la nouvelle unité d'organisation Cyber SRC a été créée pour exécuter les tâches du SRC relatives au cyberespace. Elle est bien établie et pleinement intégrée dans les procédures du SRC. Cela ressort également des cas traités en 2015, qui ont permis d'identifier et d'analyser des attaques étatiques pertinentes pour la Suisse. De plus, l'unité Cyber SRC a réalisé plusieurs analyses pour le Conseil fédéral et rédigé des rapports destinés aux autorités de poursuite pénale.
- **Acquisition et évaluation des informations:** l'OIC MELANI est l'interlocuteur central pour toutes les informations concernant des cyberattaques. L'obtention de renseignements pertinents par l'intermédiaire de Cyber SRC fonctionne bien. La qualité de ces derniers est généralement suffisante, notamment grâce au réseau adéquat de sources d'information nationales et internationales de Cyber SRC et, dans le domaine technique, de GovCERT. L'appréciation, l'évaluation et la contextualisation de ces informations requièrent cependant beaucoup de ressources et demeurent un défi majeur. Les processus de transfert des informations traitées aux services adéquats sont définis.
- **Collaboration entre le SRC et le Ministère public de la Confédération:** le SRC remet des rapports au Ministère public de la Confédération et veille à une saisie et un enregistrement corrects des données nécessaires à une poursuite pénale. Actuellement, le retour d'informations depuis le Ministère public de la Confédération n'est pas optimal. Ce dernier n'indique pas toujours s'il a clôturé un dossier.

Impact: objectif atteint

L'impact a été illustré à l'aide d'exemples qui ne peuvent être reproduits dans le présent rapport pour des questions de confidentialité. Ces exemples attestent cependant l'identification des agresseurs. Les informations concernant ces derniers ont également été prises en compte dans l'évaluation de la situation, apportant ainsi une contribution substantielle à la détection précoce des risques.

3.7. Mesure 13 – gestion des crises: coordination des activités avec les acteurs directement concernés et soutien grâce à l'expertise requise

Titre de la mesure	Coordination des activités avec les acteurs directement concernés et soutien grâce à l'expertise requise
Objectifs	En cas de crise, MELANI apporte un soutien subsidiaire aux acteurs concernés en leur offrant son expertise. MELANI soutient l'échange volontaire d'informations entre les exploitants d'IC, 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 ce faire, les prestations actuellement disponibles ont été développées. Dans les cas susceptibles d'avoir des conséquences sur la politique étrangère, le DFAE est informé et associé à l'élaboration des planifications préventives correspondantes.
Office / unité d'organisation responsable	MELANI
Documents consultés pour l'évaluation de l'efficacité	Sources: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Entretiens	Voir l'annexe A.1, entretien I 12

3.7.1. Effet escompté: modèle d'efficacité de la mesure 13

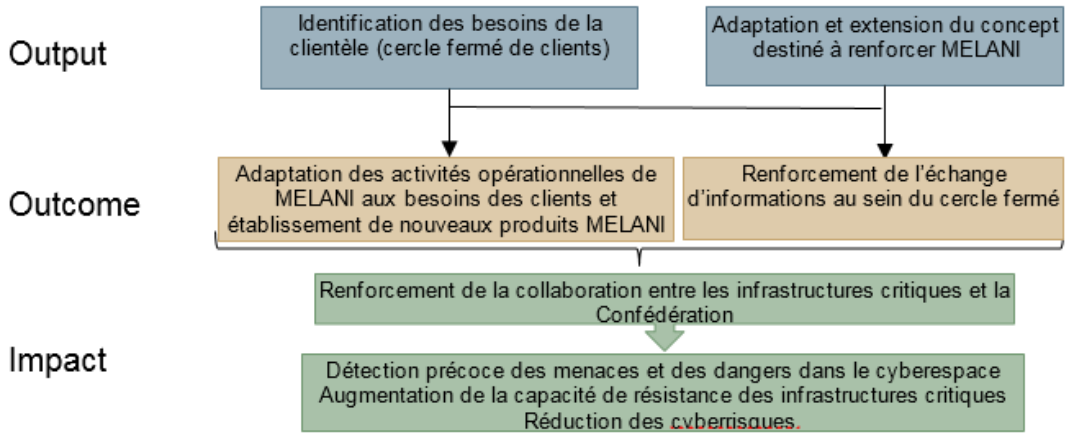

Illustration 8: Modèle d'efficacité de la mesure 13

3.7.2. Input: ressources utilisées

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucun moyen supplémentaire
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	OC SNPC

3.7.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✔	
Outcome	☐ actuellement non mesurable			
Impact	☐ actuellement non mesurable			

3.7.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

MELANI a mené une enquête dans son cercle fermé de clients pour mieux cerner les besoins des exploitants d'infrastructures critiques qui y sont représentés. Sur cette base, MELANI peut désormais adapter ses prestations de manière à apporter un soutien optimal aux exploitants d'infrastructures critiques. Au moment de l'évaluation de l'efficacité, les résultats de l'enquête avaient été analysés, mais aucune mesure d'adaptation concernant MELANI n'avait encore été formulée.

- **Identification des besoins du cercle fermé de clients:** en novembre 2015, une enquête en ligne a permis de mieux cerner les besoins des exploitants d'infrastructures critiques, qui constituent le cercle fermé des clients de MELANI. Sur les 424 membres, 260 ont répondu. L'enquête révèle les points forts actuels de MELANI, les domaines pouvant être améliorés et les souhaits des membres du cercle fermé. Ses résultats offrent une base adéquate pour le développement futur de MELANI.

  Les membres du cercle fermé sont satisfaits des prestations de MELANI et estiment que cette dernière est utile et importante. Le renforcement des secteurs comprenant peu de membres, l'extension du cercle à d'autres exploitants d'infrastructures critiques et l'acquisition d'autres enseignements issus de l'inventaire PIC, la promotion de la confiance entre les membres du cercle fermé, l'amélioration de la plate-forme d'échange d'informations et la diffusion rapide d'informations vérifiées sur les nouvelles menaces constituent les futurs défis.

  L'analyse des résultats de l'enquête est achevée. Au moment de l'évaluation de l'efficacité, aucune mesure concrète n'avait encore été formulée.

- **Concept destiné à renforcer MELANI:** dans le cadre de la mesure 4, un concept destiné à renforcer MELANI en tant que plate-forme d'échange d'informations a été élaboré en février 2014. Il ne tient pas compte des résultats de l'enquête. Le concept a été adapté à l'été 2016 sur la base de ces derniers et met donc l'accent sur les besoins du cercle fermé de clients. D'après les renseignements de l'auteur, le concept devrait porter sur les sujets suivants:
  - garantie des prestations actuellement disponibles;
  - développement des secteurs existants;
  - développement des prestations de GovCERT.ch;
  - participation d'exploitants d'infrastructures non critiques à MELANI.

Outcome: actuellement non mesurable

La mise en œuvre de la mesure 13 a commencé peu avant l'évaluation de l'efficacité. On ne peut donc pas encore déterminer si les prestations de MELANI ont été adaptées aux besoins du cercle fermé de clients et si l'échange d'informations s'est renforcé.

Impact: actuellement non mesurable

L'impact de la mesure 13 ne pouvait pas encore être estimé au moment de l'évaluation de l'efficacité.

3.8. Mesure 15 – gestion des crises: concept pour les procédures et processus de conduite incluant les aspects cybernétiques

Titre de la mesure	Concept pour les procédures et processus de conduite incluant les aspects cybernétiques
Objectifs	Un concept est élaboré pour des procédures et processus de conduite permettant de résoudre en temps adéquat les problèmes, compte tenu des aspects cybernétiques. De même, la gestion générale des crises est adaptée en matière de cyberrisques et englobe les aspects cybernétiques.
Office / unité d'organisation responsable	Chancellerie fédérale
Documents consultés pour l'évaluation de l'efficacité	Sources: [117], [118], [119], [120], [121], [122], [123], [124], [125], [126]
Entretiens	Voir l'annexe A.1, entretien I 9

3.8.1. Effet escompté: modèle d'efficacité de la mesure 15

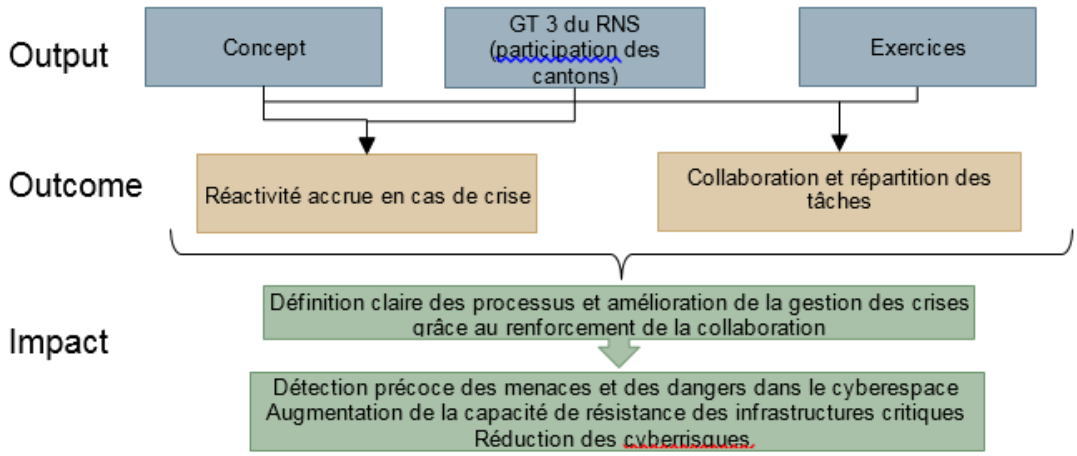

Illustration 9: Modèle d'efficacité de la mesure 15

3.8.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucune ressource spécifique à la SNPC
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	OC SNPC

3.8.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✔	
Outcome		✖		
Impact	☐ actuellement non énon llem			

3.8.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

La Chancellerie fédérale a rédigé un concept de gestion des crises incluant les aspects cybernétiques. Il est important de souligner que ces derniers ne requièrent aucune nouvelle forme de gestion des crises. L'actuelle gestion des crises demeure donc valable. Le tableau de la situation doit être étendu pour gérer des crises dans le cyberespace; de même, les processus décisionnels et la responsabilité en matière de communication doivent être définis plus précisément. Le concept a été développé, puis testé par le GT 3 du RNS. D'autres exercices reposant si possible sur une large assise sont toutefois encore nécessaires.

Concept: le concept de gestion nationale des crises à caractère cybernétique a été élaboré. Les travaux correspondants ont notamment révélé que la gestion des crises doit s'appuyer sur des processus et non sur des scénarios. Cela signifie que les processus de conduite et les processus décisionnels ne changent pas lorsqu'une crise comporte également des aspects cybernétiques. Dans de tels cas, il est important d'intégrer à la gestion des crises les acteurs compétents en matière de cyberespace (en particulier MELANI).

Le concept décrit deux processus essentiels pour surmonter les crises:

– **Tableau uniforme de la situation:** la diffusion d'un tableau de la situation actualisé, uniforme et exhaustif est primordiale en cas de crise. Les processus cybernétiques correspondants sont définis dans ce tableau (mesure 4).
– **Coordination:** jusqu'à présent, aucun mécanisme décisionnel n'a été clairement défini au niveau stratégique. La Confédération comprend de nombreux états-majors de crise (sur le plan opérationnel). On ignore souvent quels sont les interlocuteurs compétents. Il n'y a aucune vue d'ensemble des processus définis, de sorte que des canaux de communication privés sont généralement utilisés (les interlocuteurs se connaissent).

– **Exercices:** il est parfois difficile d'intégrer tous les acteurs concernés. Souvent, seuls des contacts personnels permettent d'y parvenir, ce qui restreint le cercle des parties prenantes. La sensibilisation des acteurs à la prise en compte du risque constitue également un défi. L'exercice de conduite stratégique 13 (ECS 13), qui testait la gestion des crises au niveau de la Confédération en cas de cyberattaque d'envergure contre la Suisse, était le principal exercice relatif aux crises comportant des aspects cybernétiques. Il portait principalement sur la collaboration entre les différents départements.

Outcome: objectifs partiellement atteints

La réactivité ne peut pas être évaluée en fonction des seuls aspects cybernétiques d'une crise. En général, les concepts de résolution de crise doivent présenter une large assise, notamment afin de gérer des crises multiples et complexes. La collaboration a révélé que les processus de plusieurs services étaient flous. Par ailleurs, les aspects cybernétiques sont encore trop peu pris en compte par les états-majors de crise cantonaux, ce qui aggrave la situation.

- **Réactivité accrue en cas de crise:** les travaux ont mis en évidence que l'évaluation de la réactivité ne devait pas porter uniquement sur les aspects cybernétiques. Les crises touchent très rapidement les domaines les plus divers (crises multiples). Le concept de résolution de crise doit donc reposer sur une large assise et mettre également l'accent sur d'autres domaines que la cybernétique (par ex. gestion de crise lorsqu'une panne d'infrastructures critiques a des répercussions sur l'économie et la société).
- **Collaboration:** des défis majeurs liés à la collaboration demeurent. Au niveau fédéral, il faut clarifier la coordination entre les différents états-majors de crise existants. Les structures de conduite de la Confédération sont certes définies sommairement en tant que base de la gestion interdépartementale des crises, y compris les différents rôles et tâches (voir [117]), mais plusieurs questions restent en suspens.

  La cybernétique n'est pas encore d'actualité dans la plupart des états-majors de conduite cantonaux. Dès lors, les cyberspécialistes ne sont pas encore intégrés dans tous les organes de conduite des cantons. De même, le soutien mutuel de ces derniers n'est pas réglementé. Il convient de mettre en place une structure adéquate en vue d'un échange d'informations, par exemple par l'intermédiaire du GT Sécurité de la Conférence suisse sur l'informatique (CSI) ou de la Conférence des chefs d'états-majors cantonaux.

Impact: non évaluable

La collaboration a été renforcée dans le sillage des travaux d'élaboration du concept et dans le cadre des exercices. Les processus sont désormais définis plus clairement. Il faut encore déterminer si cela se traduira par une amélioration de la gestion des crises. En l'état actuel des choses, l'impact ne peut donc pas être évalué.

3.9. Mesure 9 – coopération internationale: gouvernance d'Internet

Titre de la mesure	Gouvernance d'Internet
Objectifs	Les intérêts suisses (autorités, économie, société civile) concernant la gouvernance d'Internet sont coordonnés. Des processus sont définis à cet effet. La plate-forme d'échanges multilatérale gérée par le DETEC permet aux acteurs concernés de discuter de sujets liés à la gouvernance d'Internet. Les intérêts suisses en la matière sont représentés dans les manifestations et comités internationaux correspondants, et la coopération avec les partenaires est garantie au niveau international.
Office / unité d'organisation responsable	OFCOM
Documents consultés pour l'évaluation de l'efficacité	Sources: [90], [91], [92]
Entretiens	Voir l'annexe A.1, entretien I 6

3.9.1. *Effet escompté: modèle d'efficacité de la mesure 9*

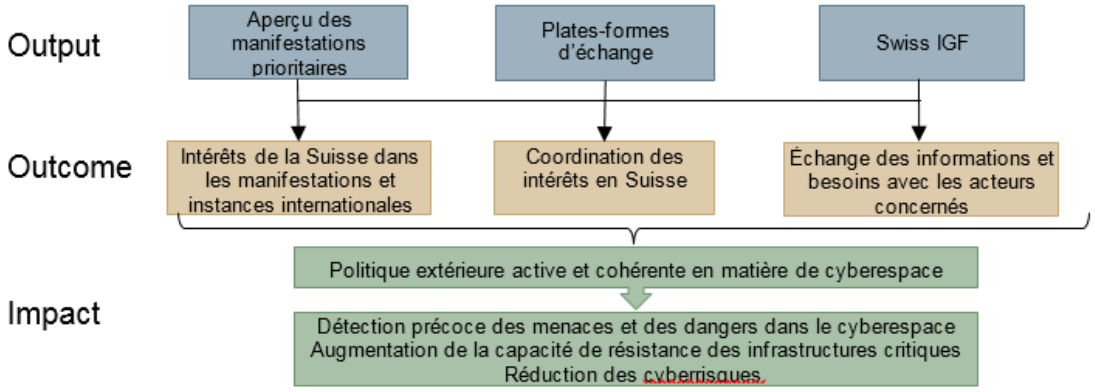

Illustration 10: Modèle d'efficacité de la mesure 9

3.9.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Un poste supplémentaire (budget de l'OFCOM)
Ressources financières	Aucun moyen supplémentaire (budget ordinaire de l'OFCOM)
Collaboration avec d'autres offices / unités d'organisation	DFAE, MELANI

3.9.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome			✓	
Impact	☐ actuellement non énon llem			

3.9.4. *Justification de l'évaluation*

Output: objectifs atteints

> Une vue d'ensemble des principaux acteurs et des principales manifestations concernant la gouvernance d'Internet a été réalisée. Les échanges entre toutes les parties prenantes issues de l'administration, de l'économie et de la société civile reposeront sur des formats existants ou nouveaux.

- **Gouvernance d'Internet et manifestations:** toutes les organisations pertinentes qui s'occupent de la gouvernance d'Internet ont été répertoriées. Priorité est donnée aux organisations et aux instances internationales qui jouent un rôle central dans la gouvernance d'Internet et qui s'occupent principalement des requêtes concernant Internet, que celles-ci soient de nature technique ou politique. Tous les autres organismes ont une priorité 2 ou 3. Cette vue d'ensemble sera actualisée régulièrement après sa mise en place.
- **Plates-formes d'échange:** l'échange d'informations est défini dans la liste des organisations (voir [91]).
  - Échanges internes à la Confédération: la plate-forme ch@world est utilisée comme canal d'information au sein de la Confédération. Elle permet d'informer les différents services fédéraux en cas de consultations importantes afin que les avis soient remis dans les délais. En plus de cette plate-forme, les échanges s'effectuent sur les canaux habituels (courriel, téléphone) et sont approfondis sporadiquement dans le cadre de rencontres thématiques organisées pendant le repas de midi (*brown-bag lunches*).
  - Échanges avec l'économie et la société civile: créée en 2003, la plate-forme tripartite est utilisée par l'OFCOM pour discuter et diffuser des informations concernant la gouvernance d'Internet. Elle s'appuie sur des réunions organisées deux fois par an et sur une liste de distribution qui regroupe actuellement 100 personnes (dont près de la moitié font partie de l'administration fédérale).
  - Swiss Internet Governance Forum (Swiss IGF): le Swiss IGF a été mis en place en tant que nouvelle plate-forme d'échange. Il permet à toutes les personnes intéressées de diffuser des informations sur leurs propres activités en relation avec la gouvernance d'Internet (approche ascendente). Le Swiss IGF est donc complémentaire à la plate-forme tripartite, sur laquelle l'OFCOM est le principal informateur. Ce format a fait ses preuves: en 2016, près de 100 personnes ont assisté à la manifestation annuelle du Swiss IGF.

Outcome: objectifs en majeure partie atteints

> Les intérêts de la Suisse concernant la gouvernance d'Internet sont coordonnés. Les échanges fonctionnent bien, en particulier entre la DPS-DFAE et l'OFCOM. Actuellement, cette coordination n'intègre pas suffisamment la Direction du développement et de la coopération (DDC) et le Secrétariat d'État à l'économie (SECO).
> Les intérêts de l'économie et de la société civile sont recensés, mais l'économie privée a été plutôt réticente à s'engager jusqu'à présent.

- **Coordination des intérêts de la Suisse dans les instances et les conférences internationales:** des informations sur la gouvernance d'Internet sont échangées régulièrement au sein de l'administration fédérale. C'est notamment le cas de l'OFCOM et du DFAE, qui ont intensifié les bonnes relations existantes depuis le début de la mise en œuvre de la mesure 9. Il en découle des échanges assidus avant

les conférences internationales, de sorte que les délégations suisses peuvent présenter des positions consolidées. La coordination s'effectue dans le cadre du groupe spécialisé Cyber International (voir le chap. 3.10), qui est dirigé par la DPS. Le siège attribué au représentant suisse dans le comité consultatif gouvernemental de l'ICANN, la participation coordonnée au processus SMSI de l'ONU et le lancement de la Geneva Internet Platform par le DFAE et l'OFCOM illustrent la réussite d'une représentation harmonisée des intérêts.

MELANI participe également à la coordination, en plus des échanges entre l'OFCOM et la DSP-DFAE. En revanche, il n'y a aucun échange régulier sur la gouvernance d'Internet avec la DDC et le SECO.

- **Coordination des intérêts en Suisse et échange d'informations:** l'utilisation de la plate-forme tripartite et le nouveau Swiss IGF permettent de recenser précocement les différents intérêts et d'en tenir compte. De plus, l'OFCOM informe activement à l'aide de newsletters et d'articles dans des revues spécialisées. Il est cependant difficile d'intégrer un public aussi large que possible dans les activités concernant la gouvernance d'Internet. L'économie privée est réticente à s'engager, car les processus des instances internationales sont souvent très longs et plutôt abstraits. Ses intérêts sont donc généralement pris en compte de manière indirecte uniquement.

Impact: non évaluable

Le renforcement de la coordination s'est traduit par une politique extérieure cohérente en matière de cyberespace. Les principes fondamentaux de la Suisse concernant la gouvernance d'Internet (approche englobant plusieurs parties prenantes ou *multistakeholder approach*) sont connus et représentés uniformément. Pour le moment, on ne saurait toutefois déterminer si la position de la Suisse s'en trouve renforcée. L'impact n'est donc pas encore évaluable.

3.10. Mesure 10 – coopération internationale: coopération au niveau de la politique internationale de sécurité

Titre de la mesure	Coopération au niveau de la politique internationale de sécurité
Objectifs	Face aux cyberrisques, les intérêts de l'économie, de la société civile et des autorités sont coordonnés au niveau de la politique de sécurité internationale. La coopération internationale est dûment garantie afin de réagir aux cybermenaces conjointement avec d'autres États ou des organisations internationales.
Office / unité d'organisation responsable	DFAE
Documents consultés pour l'évaluation de l'efficacité	Sources: [98], **Fehler! Verweisquelle konnte nicht gefunden werden.**, [100], [101], [102], **Fehler! Verweisquelle konnte nicht gefunden werden.**, [104], **Fehler! Verweisquelle konnte nicht gefunden werden.**, [106], [107], [108], [109], [110], [111], [112], [113], [114], [115], [116]
Entretiens	Voir l'annexe A.1, entretien I 4

3.10.1. *Effet escompté: modèle d'efficacité de la mesure 10*

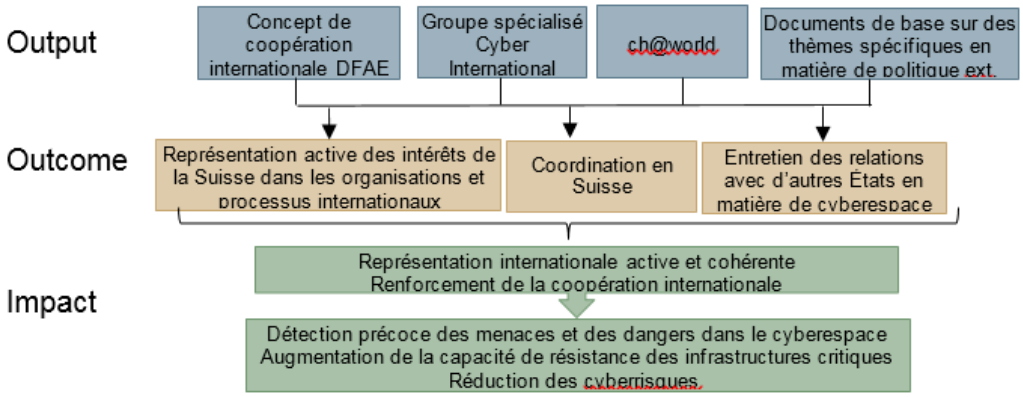

Illustration 11: modèle d'efficacité de la mesure 10

3.10.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	2 employés
Ressources financières	150 000 francs par an
Collaboration avec d'autres offices / unités d'organisation	MELANI, OC SNPC, DFJP, DDPS, OFCOM, IFSN

3.10.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome				✓✓
Impact	☐ actuellement non énon llem			

3.10.4. *Justification de l'évaluation*

<u>*Output*: objectifs atteints</u>

Les bases d'une politique extérieure relative au cyberespace et d'une politique de sécurité coordonnées et cohérentes ont été mises en place. Le rôle de la division Politique de sécurité (DPS) du DFAE est clairement défini dans un concept de coopération internationale. Un organe d'échange a été établi à travers le groupe spécialisé Cyber International, et la communication a été renforcée grâce à la plate-forme ch@world. Des documents de base sur la politique extérieure relative au cyberespace ont également été rédigés.

- **Concept de coopération internationale:** le concept a été élaboré. Il s'agit d'un document exposant le rôle du DFAE ainsi que les activités et les initiatives qu'il dirige ou auxquelles il apporte son soutien. De plus, la DPS établit une fois par an, en tant

que «mise à jour», un aperçu des principales activités, procédures et initiatives relatives au cyberespace pour le chef du département, le secrétaire d'État et le CP SNPC (voir [98] pour 2014 et **Fehler! Verweisquelle konnte nicht gefunden werden.** pour 2015).

- **Groupe spécialisé Cyber International (GS-CI):** le GS-CI est composé de représentants du DFAE (Direction politique et Direction du droit international public), du DDPS (SIPOL, OFPP, groupement de la Défense et SRC), du DETEC (OFCOM et OFEN), du DFF (UPIC), du DFJP (OFJ et fedpol) et, depuis peu, de l'IFSN également. Tous les représentants y participent activement. Cet organe est ouvert à d'autres services fédéraux qui s'occupent de la cybersécurité et de la gouvernance d'Internet au niveau international. La DPS préside le GS-CI, qui se réunit deux fois par an. En cas de besoin, un membre peut demander la tenue d'une réunion extraordinaire.
- **ch@world:** pour faciliter l'échange d'informations, une plate-forme correspondante destinée aux membres du GS-CI a été développée sur ch@world. Les membres peuvent charger eux-mêmes des documents. Cette plate-forme est utilisée régulièrement, notamment pour participer à des consultations (par ex. sur la Geneva Declaration for Cyberspace).
- **Documents de base concernant la politique étrangère:** ils couvrent les principaux champs d'action, qui sont définis et développés en fonction de leur importance dans la politique étrangère et en cas de besoin. Le traitement des contenus extrémistes violents sur Internet et sur les réseaux sociaux est un sujet d'actualité (*preventing violent extremism*).

Outcome: objectifs atteints

La Suisse défend ses intérêts de manière cohérente et active dans les instances internationales chargées de la cybersécurité et entretient de bonnes relations bilatérales. Elle est considérée comme un acteur actif et fiable.
Les échanges entre tous les services fédéraux participants sont bien établis. Cela tient directement à la création du groupe spécialisé Cyber International et à l'utilisation de la plate-forme ch@world.

- **Représentation active des intérêts de la Suisse dans les instances internationales et entretien des relations avec d'autres États en matière de cyberespace:** la DPS a représenté la Suisse dans plusieurs négociations et procédures internationales consacrées à la politique de cybersécurité. Des relations bilatérales avec différents pays se sont également nouées dans le sillage de ces activités. La Suisse est considérée comme un acteur actif et fiable en matière de cyberespace, comme en attestent plusieurs requêtes émanant d'États qui souhaitent son soutien dans l'élaboration de cyberstratégies (par ex. participation de la Suisse à des auditions publiques en Arménie et en Serbie, soutien lors de la mise en place de CERT, etc.).
  Les principales activités et leurs résultats sont brièvement exposés ci-après:
  – Processus de l'OSCE: instauration d'un climat de confiance dans le cyberespace. Promotion de mesures de confiance dans le cadre de la présidence suisse de l'OSCE en 2014. Deux trains de mesures ont été adoptés.
    - Participation active de la Suisse à la Conférence mondiale sur le cyberespace et organisation de l'atelier «Mechanisms for Confidence-Building and Cooperation in Cyberspace» à Genève dans le cadre de cette conférence.
    - Participation du Geneva Center for Security Policy (GCSP) au dialogue sur le cyberespace entre la Chine et l'Europe (2014-2016), dans le cadre duquel

un groupe de travail a été mis sur pied pour examiner l'applicabilité du droit international public au cyberespace.

  - ICT4Peace: projets pour développer les capacités cybernétiques des pays en développement.
  - Participation à la rédaction du Manuel de Tallinn de l'OTAN (étude sur l'applicabilité du droit international public au cyberespace).

- **Coordination des intérêts en Suisse en vue d'une représentation internationale plus cohérente:** les échanges réguliers entre les services constituent une plus-value importante du groupe spécialisé Cyber International. La plate-forme ch@world, qui est devenue une base de données regroupant les principaux documents, poursuit le même objectif. Ces instruments ont contribué à accroître la cohérence de la politique extérieure relative au cyberespace. La fréquence des réunions devrait toutefois être augmentée en fonction des besoins. De plus, selon le sujet abordé, il convient de faire appel à des partenaires de projet qui ne sont pas membres du groupe spécialisé Cyber International.

Impact: actuellement non évaluable

La Suisse applique une politique extérieure active et cohérente en matière de cyberrisques. Elle s'investit dans le renforcement des relations avec d'autres États et s'efforce de contribuer à la cybersécurité sur le plan international. Ces efforts étant déployés sur le long terme, aucun impact n'est mesurable pour le moment.

3.11. Mesure 11 – coopération internationale: initiatives et processus internationaux de standardisation en matière de sécurité

Titre de la mesure	Initiatives et processus internationaux de standardisation en matière de sécurité
Objectifs	Les intérêts de la place économique suisse sont exposés de manière coordonnée dans les instances internationales privées ou étatiques qui s'occupent de la sécurité, de la sûreté et de la standardisation. À cet effet, l'échange d'informations est renforcé entre les exploitants d'IC, les fournisseurs de prestations informatiques, les fournisseurs de systèmes, les associations faîtières, les organisations nationales de standardisation, les autorités et les régulateurs. Un processus est établi à cet effet.
Office / unité d'organisation responsable	OFCOM
Documents consultés pour l'évaluation de l'efficacité	Sources: [93], [94], [95], [96], [97]
Entretiens	Voir l'annexe A.1, entretien I 6

3.11.1. *Effet escompté: modèle d'efficacité de la mesure 11*

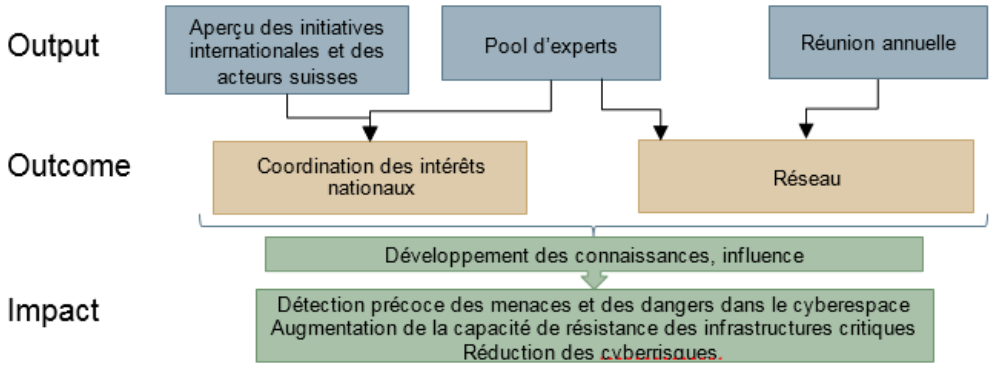

Illustration 12: Modèle d'efficacité de la mesure 11

3.11.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucune; l'OFCOM a assumé cette tâche sans ressources supplémentaires en personnel
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	OC SNPC

3.11.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✔	
Outcome		✖		
Impact	☐ actuellement non énon llem			

3.11.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

Les étapes de la planification stratégique ont été définies, et un réseau d'acteurs souhaitant s'entretenir sur les initiatives et processus internationaux de standardisation a été mis en place. L'économie privée semble peu intéressée par une participation active. Un premier atelier (qui pourrait devenir annuel) consacré aux récents développements internationaux a eu lieu.
Aucun besoin concret de coordination n'a pu être identifié parmi les acteurs de la mesure 11 et personne d'autre n'a formulé un tel besoin en rapport avec cette mesure. L'expertise disponible au sein du réseau est documentée à l'aide de listes et d'exposés. On ignore encore si elle servira à la SNPC dans un contexte plus large.

- **Aperçu des initiatives internationales auxquelles participent des acteurs suisses:** l'aperçu a été réalisé ([96]) et devrait être mis à jour chaque année. Il comprend une liste d'acteurs qui suivent les développements au niveau des organisa-

tions et initiatives internationales en matière de cybersécurité et exercent une influence dans ce domaine. Cette liste comprend deux catégories aux intentions distinctes:

– acteurs des autorités, offices spécialisés et régulateurs;
– acteurs des organisations économiques privées et des établissements de formation.

La liste s'appuie sur une inscription volontaire. Seul un tiers environ des organisations contactées dans le cadre de la mesure 11 a répondu. On note l'absence de grandes entreprises qui ont des succursales en Suisse, sont représentées dans les instances internationales, mais ne se considèrent pas comme des acteurs suisses (par ex. Google, Microsoft, Cisco).

- **Pool d'experts sur les questions de standardisation en matière de sécurité:** on compte parmi les participants des experts dans différents domaines des processus internationaux liés aux cyberrisques. En accord avec les participants, le groupe doit encore affiner son orientation. Un premier atelier portait principalement sur les questions concernant la mise en place de CERT. Il n'existe guère de besoins de coordination supplémentaires en relation avec la SNPC, car les représentants ont déjà des échanges détaillés dans les organisations internationales de standardisation.

Outcome: objectifs partiellement atteints

Le réseau a été renforcé au cours d'un premier atelier qui a attiré un groupe de 30 à 40 participants intéressés par la standardisation et les meilleures pratiques. Les besoins de coordination relatifs à la standardisation internationale sont encore faibles, l'intérêt portant plutôt sur les développements nationaux.

- **Coordination des intérêts nationaux:** aucun résultat n'a été obtenu à ce sujet et aucun besoin n'est identifiable pour le moment. Jusqu'à présent, l'accent a été mis sur le développement et le renforcement du réseau. La plupart des participants s'intéressent aux développements nationaux, mais pas à la coordination internationale.
- **Réseau:** un premier atelier rassemblant plus de 40 participants a été organisé. Il était consacré à la surveillance et à la réaction (*monitoring and response*). Il a permis de renforcer le réseau. On ignore toutefois si la standardisation est un sujet suffisamment important pour inciter les participants à poursuivre leur engagement dans le cadre de la mesure 11.

Impact: actuellement non évaluable

Il est encore trop tôt pour évaluer l'impact de manière exhaustive. Le réseau mis en place est certes doté d'une grande expertise et influence, mais il n'existe jusqu'à présent aucun besoin pour les représentants suisses de coordonner leur influence sur le plan international.

3.12. Mesure 1 – formation et recherche: identification des cyberrisques par la recherche

Titre de la mesure	Identification des cyberrisques par la recherche
Objectifs	Les offices fédéraux compétents procèdent à des échanges, tant entre eux qu'avec des acteurs extérieurs à l'administration fédérale, sur les développements actuels ou à explorer en Suisse et à l'étranger en matière de cyberrisques; ils effectuent le cas échéant des recherches intramuros ou donnent des mandats de recherche.
Office / unité d'organisation responsable	SEFRI, OC SNPC
Documents consultés pour l'évaluation de l'efficacité	Sources: [16], [17], [18], [19], **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, [30], **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**
Entretiens	Voir l'annexe A.1, entretien I 1

3.12.1. *Effet escompté: modèle d'efficacité de la mesure 1*

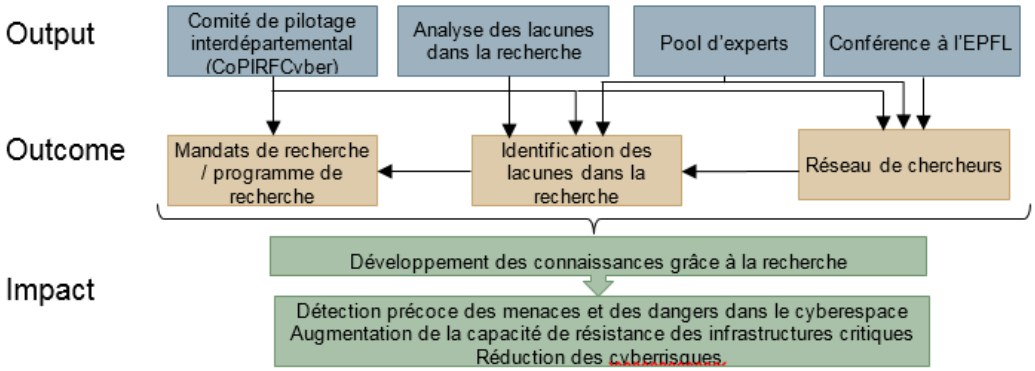

Illustration 13: modèle d'efficacité de la mesure 1

3.12.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucun poste supplémentaire
Ressources financières	Aucun moyen supplémentaire; les experts des hautes écoles travaillent bénévolement
Collaboration avec d'autres offices / unités d'organisation	DSP DFAE, OFCOM, BAC-COE, RM, CTI, OFAE, MELANI, RNS

Le SEFRI est chargé de la mise en œuvre de la mesure depuis 2014 et assume les charges de personnel.

3.12.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome			✓	
Impact	☐ actuellement non énon llem			

3.12.4. *Justification de l'évaluation*

Output: objectifs atteints

Créé sous l'égide du SEFRI, un comité de pilotage interdépartemental pour la recherche et la formation en matière de cyberrisques assure la coordination dans ce domaine. Les premières étapes destinées à renforcer la recherche sont franchies: un groupe d'experts composé de représentants des hautes écoles suisses a été mis en place pour identifier les besoins prioritaires dans la recherche en Suisse. La première Swiss Cyber Risk Research Conference a contribué à renforcer le réseau parmi les chercheurs, soulignant la volonté de la Confédération de promouvoir la recherche sur les cyberrisques.

- **Mise en place d'un comité de pilotage interdépartemental:** le Comité de Pilotage Interdépartemental Recherche et Formation dans le domaine de la protection contre les Cyberrisques (CoPIRFCyber) a été créé sous l'égide du SEFRI. Y sont représentés les offices fédéraux qui s'intéressent à la formation et à la recherche en matière de cyberrisques. Le comité siège quatre fois par an (ou en cas de besoin) et coordonne les principales activités de l'administration fédérale dans ce domaine.
- **Pool d'experts et analyse des lacunes dans la recherche:** le CoPIRFCyber a nommé un groupe d'experts pour le soutenir sur le plan technique, en particulier dans l'identification des besoins dans la recherche. Quatorze spécialistes issus de hautes écoles suisses ont accepté de participer à ce groupe d'experts. Celui-ci a déjà identifié les principaux axes de recherche; il remettra un rapport d'ici fin 2016 pour présenter les défis majeurs de la recherche sur le plan national et international.
- **Conférence sur les cyberrisques:** la première Swiss Cyber Risk Research Conference s'est déroulée le 25 mai 2016 à l'École polytechnique fédérale de Lausanne (EPFL). Organisée par le CoPIRFCyber sous l'égide du SEFRI, la conférence a accueilli 350 personnes issues de la recherche en Suisse. Des experts internationalement reconnus étaient invités en tant qu'intervenants. À l'avenir, la conférence devrait avoir lieu tous les deux ans et contribuer à renforcer le réseau de chercheurs dans le domaine des cyberrisques.

Outcome: objectifs en majeure partie atteints

La Swiss Cyber Risk Research Conference a permis d'aborder le thème des cyberrisques avec des chercheurs venant de domaines extrêmement variés. La mise en place d'un groupe d'experts a contribué à tisser un réseau dense de spécialistes. Ce groupe a identifié les principaux thèmes de recherche et défis et doit les présenter en détail d'ici fin 2016. Ces travaux aideront la Confédération à fixer les priorités dans la promotion de la recherche.

- **Réseau de chercheurs:** des chercheurs de différentes disciplines et hautes écoles ont assisté pour la première fois à la Swiss Cyber Risk Research Conference consacrée aux cyberrisques. Celle-ci marquait le lancement du réseau de chercheurs. Au-delà de cette conférence, il est primordial de continuer à promouvoir les échanges entre les chercheurs. La forme de ces échanges n'a toutefois pas encore été définie. La mise en place d'un groupe d'experts en tant que réseau dense de spécialistes constitue une bonne base de départ.
- **Identification des lacunes dans la recherche:** le groupe d'experts mis en place a identifié les principaux thèmes et défis de la recherche suisse et publiera un rapport à ce sujet d'ici fin 2016. Il convient de déterminer si et comment ces travaux seront actualisés régulièrement.
- **Mandats de recherche / programme de recherche:** aucun mandat de recherche concret n'a été formulé pour le moment, car les principaux sujets de recherche doivent encore être décrits. La recherche sur les cyberrisques est déjà encouragée dans le cadre du programme «Big Data» du Fonds national suisse de la recherche scientifique.

Impact: actuellement non évaluable

Les structures mises en place semblent adéquates pour déterminer l'état actuel de la recherche et identifier d'éventuels besoins supplémentaires dans la recherche sur les cyberrisques. Il est cependant encore trop tôt pour savoir si la mesure a déployé ses effets.

3.13. Mesures 7 et 8 – formation et recherche: aperçu des offres de formation ainsi qu'usage accru des offres de formation et comblement des lacunes

Titre de la mesure	Aperçu des offres de formation ainsi qu'usage accru des offres de formation et comblement des lacunes
Objectifs	Mesure 7: les milieux économiques, l'administration et la société civile trouvent des informations conformes à leurs besoins sur des offres de qualité destinées à la formation des compétences en gestion des cyberrisques. Les lacunes de l'offre sont identifiées et servent de base à la mise en œuvre de la mesure 8. Mesure 8: d'entente avec les cantons et l'économie, la Confédération a indiqué dans un concept de mise en œuvre comment elle entendait accroître le recours aux offres destinées à la formation des compétences en gestion des cyberrisques. Le concept précisera encore comment les lacunes de l'offre seront comblées et quelles nouvelles offres sont prévues.
Office / unité d'organisation responsable	SEFRI, OC SNPC
Documents consultés pour l'évaluation de l'efficacité	Sources: [16], [17], [18], [19], **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**, [30], **Fehler! Verweisquelle konnte nicht gefunden werden.**, **Fehler! Verweisquelle konnte nicht gefunden werden.**
Entretiens	Voir l'annexe A.1, entretien I 1

3.13.1. *Effet escompté: modèle d'efficacité des mesures 7 et 8*

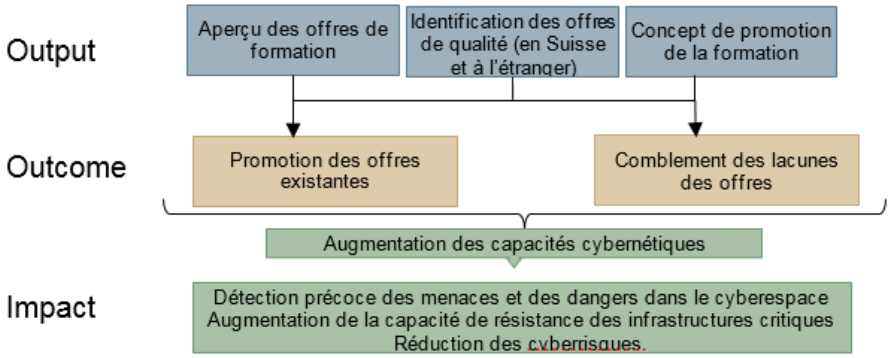

Illustration 14: Modèle d'efficacité des mesures 7 et 8

3.13.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucun poste supplémentaire
Ressources financières	Aucun moyen supplémentaire
Collaboration avec d'autres offices / unités d'organisation	OFCOM, DFAE, OFAS

3.13.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output			✓	
Outcome				✓✓
Impact	☐ actuellement non énon llem			

3.13.4. *Justification de l'évaluation*

Output: objectifs en majeure partie atteints

Une vue d'ensemble des offres existantes en matière de formation a été élaborée et des offres de grande qualité ont été identifiées grâce à des entretiens avec des experts. Ces travaux ont surtout contribué à déterminer comment la Confédération pouvait promouvoir la formation dans le domaine des cyberrisques. On a renoncé à mentionner spécifiquement les offres de grande qualité, car une évaluation de la Confédération serait licite uniquement dans le cadre d'un processus exhaustif de certification. Un concept de mise en œuvre précise comment la Confédération entend promouvoir les compétences en matière de cyberrisques. Le processus concernant le perfectionnement, la formation professionnelle et les hautes écoles a été concrétisé dans ce domaine.

- **Aperçu des offres:** les offres de formation existant en Suisse et dans les pays voisins ont été identifiées grâce à des entretiens avec des experts. Une distinction est

opérée entre les offres destinées à la population, à l'administration et à l'économie. Les besoins des groupes cibles, les offres recensées et leurs lacunes ont été présentés dans un rapport. Compte tenu du dynamisme du marché de la formation, il est toutefois évident qu'un tel aperçu ne saurait être exhaustif. Aucune mise à jour régulière n'est cependant prévue, car plusieurs associations et fédérations publient elles aussi des vues d'ensemble des offres de formation sur leur site Internet.

- **Identification des offres de grande qualité:** sur la base des entretiens susmentionnés, on a tenté d'identifier des exemples d'offres appropriées. On a finalement renoncé à une évaluation qualitative systématique des différentes offres et à la publication des meilleures. Pour des raisons d'ordre institutionnel, la Confédération ne devrait pas intervenir sur le marché actuel de la formation. Une évaluation complète ne serait licite que dans le cadre d'un processus de certification, ce qui dépasserait les objectifs fixés pour les mesures 7 et 8.
- **Concept de promotion de la formation:** le concept visant à promouvoir la formation en matière de cyberrisques a été établi par CoPIRFCyber (voir le chap. 3.12). Il présente les mesures que la Confédération prendra pour encourager la formation dans ce domaine. La Confédération entend tout d'abord renforcer le développement des compétences au niveau du perfectionnement, de la formation professionnelle et des hautes écoles. Le concept expose déjà des étapes concrètes en ce sens. La formation de base relevant principalement de la compétence des cantons, elle n'a pas été examinée jusqu'à présent.

Outcome: objectifs atteints

Le lancement de la filière débouchant sur le diplôme fédéral d'ICT Security Expert, un projet mené en collaboration avec l'association ICT-Formation professionnelle, a permis de franchir un pas important dans la promotion du développement des compétences au niveau du perfectionnement et de la formation professionnelle. Concernant les hautes écoles, la formation est surtout renforcée de manière indirecte, grâce à la promotion de la recherche (voir la mesure 1, chap. 3.12).

- **Promotion des offres existantes et comblement des lacunes:** le nouveau profil professionnel «ICT Security Expert» a été créé en collaboration avec l'association ICT-Formation professionnelle pour encourager l'utilisation des offres disponibles et combler les lacunes correspondantes en matière de cyberrisques (voir **Fehler! Verweisquelle konnte nicht gefunden werden.**). Les premiers diplômes devraient être décernés à l'automne 2018. Le projet suscite un grand intérêt dans l'économie privée et plusieurs entreprises le cofinancent. Il s'appuie sur les formations existantes et les complètent lorsque des lacunes ont été recensées. Le profil de qualification a été défini avec des représentants de l'économie privée.

  Pour ce qui est des hautes écoles, la Confédération encourage la formation dans le cadre de la recherche. Coordonnée par le CoPIRFCyber, la mise en œuvre de cette mesure est donc étroitement liée à la mesure 1 (voir cette dernière au chap. 3.12). La promotion ciblée de projets de recherche renforcera la formation dans les hautes écoles, l'accent étant mis sur l'encouragement des formations interdisciplinaires.

Impact: actuellement non évaluable

La formation est une tâche de longue haleine. Il est donc encore trop tôt pour mesurer un quelconque impact.

3.14. Mesure 16 – bases juridiques: nécessité de modifier les bases juridiques

Titre de la mesure	Nécessité de modifier les bases juridiques
Objectifs	Les départements compétents ont identifié les lacunes législatives considérées comme prioritaires, effectué les adaptations juridiques nécessaires et élaboré les projets requis à l'échelon normatif adéquat. Un concept de réglementation est soumis au Conseil fédéral.
Office / unité d'organisation responsable	UPIC
Documents consultés pour l'évaluation de l'efficacité	Sources: [127]
Entretiens	Voir l'annexe A.1, entretien I 13

3.14.1. Effet escompté: modèle d'efficacité de la mesure 16

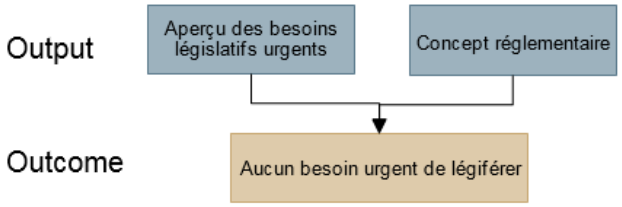

Illustration 15: Modèle d'efficacité de la mesure 16

3.14.2. Input: ressources utilisées

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Traitement par l'OC SNPC
Ressources financières	Aucune
Collaboration avec d'autres offices / unités d'organisation	Il a été fait appel aux services fédéraux compétents (voir la liste figurant à l'annexe 16 1)

3.14.3. Évaluation de la réalisation des objectifs et de l'impact

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome	☐ actuellement non énon llem			
Impact	☐ actuellement non énon llem			

3.14.4. Justification de l'évaluation

Output: objectifs atteints

Un aperçu des besoins législatifs urgents a été établi. Pour ce faire, tous les services fédéraux compétents ont été interrogés. Aucun besoin impératif de révision ou de nouvelle législation n'a été constaté.

- **Aperçu des besoins législatifs urgents:** le document «Übersicht zum vordringlichen Gesetzgebungs- und Revisionsbedarf zum Meilenstein 16.1» (voir [127]) comprend l'aperçu requis. Tous les services fédéraux compétents ont participé aux travaux. Grâce aux secrétariats généraux et à la Chancellerie fédérale, l'OC SNPC a établi avec tous les services fédéraux concernés une vue d'ensemble des bases légales comportant des aspects cybernétiques et déterminé s'il existait un besoin urgent de révision ou de nouvelle législation.
- **Concept réglementaire:** le groupement Défense du DDPS a été le seul service fédéral à indiquer une nécessité urgente de légiférer. Ce point a été réglé dans l'intervalle grâce à l'art. 100 de la nouvelle loi sur l'armée. L'ordonnance correspondante est en cours d'élaboration.

Le CP SNPC a pris acte de l'aperçu des besoins législatifs et décidé de suspendre la poursuite de la mise en œuvre de la mesure 16. Il incombe aux services fédéraux compétents, et non à la SNPC, de déterminer le besoin de légiférer.

Outcome: non évaluable

Aucun besoin urgent de légiférer n'a été constaté. L'étape de formulation des adaptations juridiques est donc caduque. Il est dès lors impossible d'évaluer l'*outcome* de la mesure 16.

- **Il n'existe aucun besoin urgent de légiférer.** La mesure est mise en œuvre, mais elle doit être contrôlée régulièrement, comme toute mesure de la SNPC. Seule une première analyse ressort de la vue d'ensemble établie. La situation juridique doit cependant s'adapter aux cybermenaces, qui changent constamment (voir par ex. la loi sur la sécurité des informations [LSI] ou la directive sur la sécurité des réseaux et de l'information [SRI] que l'UE a approuvée en juin 2016).

Impact: ne doit pas être évalué

La mesure s'étant achevée par l'élaboration de la vue d'ensemble, aucun impact ne peut être mesuré.

4. Interfaces

Les mesures de la SNPC sont axées sur les tâches de l'administration fédérale civile et entendent contribuer au renforcement de la protection des infrastructures critiques. Deux interfaces sont primordiales dans le cadre de ces tâches: l'interface avec les activités des cantons et l'interface avec les activités de l'armée dans la cyberdéfense. Elles ont toutes deux été analysées afin d'évaluer de manière exhaustive l'impact de la SNPC.

4.1. Interface avec les cantons – travaux du Réseau national de sécurité

Type d'interface	Interface concernant la mise en œuvre de la SNPC dans les cantons
Objectifs	Participation des cantons à toutes les mesures d'application de la SNPC les concernant, coordination des activités en cours des cantons dans la protection contre les cyberrisques, échange d'informations et de savoir
Office / unité d'organisation responsable	Réseau national de sécurité (RNS)

Documents consultés pour l'évaluation de l'efficacité	Sources: [128], [129], [130]
Entretiens	

4.1.1. *Effet escompté: modèle d'efficacité de l'interface avec les cantons*

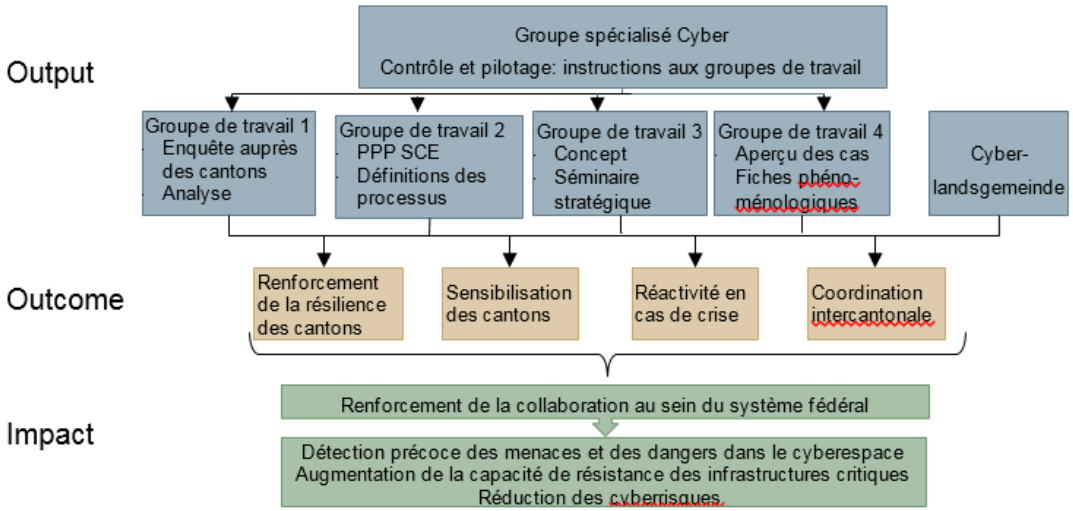

Illustration 16: Modèle d'efficacité du RNS

4.1.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Le RNS a entièrement assumé les travaux de coordination sans ressources supplémentaires.
Ressources financières	À la charge du RNS
Collaboration avec d'autres offices / unités d'organisation	Services de l'administration fédérale ayant pris part à la collaboration: OC SNPC, MELANI, SCOCI, ChF, OFPP, armée.

4.1.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output				✓✓
Outcome			✓	
Impact	☐ actuellement non énon llem			

4.1.4. *Justification de l'évaluation*

Output: objectifs atteints

Le groupe spécialisé Cyber et ses quatre groupes de travail ont été mis en place et ont contribué de manière importante à ancrer la SNPC dans les cantons. La cyber-landsgemeinde qui se déroule chaque année garantit un échange mutuel.

- **Groupe spécialisé Cyber:** dans le plan de mise en œuvre de la SNPC, le RNS est chargé de constituer un groupe spécialisé Cyber (GS-C), qui servira d'interface entre l'application de la SNPC et les activités des cantons.

  Créé en 2013, le GS-C est composé des organisations suivantes: le RNS, la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), l'OC SNPC, la Conférence suisse des chanceliers d'État (CDE), MELANI, la Conférence suisse sur l'informatique (CSI), l'armée, la Conférence des gouvernements cantonaux (CDC), l'Union des villes suisses et l'Association des communes suisses. Le groupe spécialisé se réunit deux fois par an et assure ainsi la coordination de tous les travaux en cours. Concernant les aspects opérationnels des interfaces avec la SNPC, le GS-C a mis en place quatre groupes de travail dont les responsables sont également représentés en son sein.

  Groupes de travail: les quatre groupes de travail ont été définis conformément aux principales interfaces de la SNPC avec les cantons. Ils ont atteint les objectifs suivants:

  – **GT 1 Analyse des risques et prévention** (interface avec les mesures 2 et 3 de la SNPC): les cantons ont reçu, sous la forme d'un questionnaire, un outil pour auto-évaluer la gestion des cyberrisques. Le groupe de travail a analysé les réponses et soumis aux cantons des propositions visant à réduire les cyberrisques identifiés. Lors d'une prochaine étape, le groupe de travail aidera les cantons à intégrer les cyberrisques dans leur gestion générale des risques.
  – **GT 2 Gestion des incidents** (interface avec les mesures 4 et 5 de la SNPC): le groupe de travail a décrit dans plusieurs documents les processus de traitement des cyberincidents. Par exemple, les processus de collaboration entre MELANI et les cantons en cas d'incident sont dûment consignés (document IMTP6 [130]). Dans le cadre du GT 2, les cantons ont souhaité pouvoir accéder à de vastes connaissances spécialisées. La mise en place du partenariat public-privé Swiss Cyber Experts répond à ce souhait.
  – **GT 3 Gestion des crises de la Confédération et des cantons** (interface avec la mesure 15 de la SNPC): le groupe de travail a étendu aux cantons le champ d'application de la gestion des crises et y a également intégré les infrastructures critiques. Le concept a été testé lors de deux manifestations: un séminaire stratégique organisé le 11 juin 2015 et un test dans le cadre de RUAG Cyber Range le 23 février 2016. Le séminaire stratégique a mis en évidence certaines ambiguïtés. Le cas d'étude simulait une attaque contre le système de rente de la Suisse. L'intégration des secteurs spécialisés concernés dans la gestion des crises a été analysée, l'accent étant mis sur la coordination entre la Confédération et les cantons en leur qualité de principaux partenaires du RNS. Les différents acteurs ont pu examiner et traiter les points faibles et les zones d'ombre identifiées dans leur organisation.
  – **GT 4 Vue d'ensemble des infractions et coordination des cas intercantonaux complexes** (interface avec la mesure 6 de la SNPC): sous l'égide du Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) et avec la participation des cantons, ce groupe de travail a élaboré un concept de gestion nationale des infractions pénales et de coordination des cas intercantonaux complexes. Les fiches phénoménologiques qui décrivent les différentes formes de cybercriminalité sont également importantes pour les cantons, qui ont participé à leur rédaction. Ils les ont reçues en vue d'une prise de position et en ont validé le contenu lors de la consultation. La question de la compétence des ministères publics n'a pas encore été résolue. Étant donné que le SCOCI est déjà une unité d'organisation conjointe de la Confédération et des cantons, un vaste travail de coordination a pu être accompli directement par son intermédiaire.

– **Cyber-landsgemeinde:** la première cyber-landsgemeinde a eu lieu en 2013; elle est désormais organisée chaque année. Cette manifestation bien établie accueille un grand nombre de participants issus des cantons. Elle contribue sensiblement à l'échange d'informations sur les cyberrisques entre la Confédération et les cantons.

Outcome: objectifs en majeure partie atteints

La collaboration entre la Confédération et les cantons et entre ces derniers a été renforcée. Tous les cantons étant désormais membres de MELANI, la réactivité s'est améliorée. La participation des cantons aux exercices de gestion de crise contribue à identifier et à surmonter les points faibles dans la gestion de la résilience. La collaboration pourrait néanmoins être encore plus poussée dans tous les domaines.

- **Collaboration:** les groupes de travail et la cyber-landsgemeinde ont sensiblement renforcé la collaboration et le réseautage entre les cantons et la Confédération, comme l'illustre l'amélioration notable de la participation des cantons à MELANI: au début de la mise en œuvre de la SNPC, dix cantons n'avaient pas encore pris part à MELANI. Grâce au soutien du RNS, tous les cantons sont membres du cercle fermé des clients de MELANI depuis fin 2015.

  Les travaux ont également mis en évidence un besoin de coordination supplémentaire entre la Confédération et les cantons. La collaboration pourrait être plus soutenue dans les domaines suivants:
  – tableau commun et évaluation de la situation;
  – harmonisation des actions possibles et synchronisation des décisions;
  – aperçu et gestion des ressources;
  – harmonisation de la gestion de la continuité;
  – élaboration de messages communs et communication correspondante.
- **Gestion de la résilience:** l'auto-évaluation initiée par le GT 1 a contribué à renforcer la résilience des cantons face aux cyberrisques. Les cantons ont désormais un meilleur aperçu de leur propre situation et des mesures supplémentaires qu'ils devraient prendre. La réalisation d'exercices de gestion de crise avec la participation des cantons et des infrastructures critiques a également joué un rôle important, car elle a révélé les points faibles des différents processus.
- **Réactivité:** l'adhésion à MELANI permet désormais à tous les cantons de bénéficier directement de son service de permanence, disponible 24 heures sur 24, sept jours sur sept. De plus, certains cantons mettent en place des Security Operation Centers (celui du canton de Vaud est déjà opérationnel). Grâce aux échanges mutuels, il est possible de profiter des expériences et d'identifier les solutions les plus appropriées. La définition des processus applicables en cas de cyberincident contribue à une gestion adéquate de ce dernier et à une réaction rapide.
- **Coordination intercantonale:** les discussions au sein des groupes de travail auxquels participent les cantons ont permis d'échanger des connaissances et des expériences. Les produits élaborés sont mis à la disposition de tous les cantons. Le fait de se connaître contribue à nouer une relation de confiance et facilite l'échange d'informations.

Impact: non évaluable

La collaboration avec les cantons s'est sensiblement améliorée. On ne peut toutefois pas encore évaluer dans quelle mesure cela a contribué à ancrer une collaboration fédéraliste en matière de cyberrisques, car la plupart des travaux correspondants ne sont pas entièrement achevés. Actuellement, les activités des groupes de travail dépendent fortement du travail bénévole de certaines personnes.

4.2. Interface avec l'armée

Type d'interface	Interface concernant la mise en œuvre de la SNPC à l'armée
Objectifs	En cas de besoin, les offices responsables peuvent intégrer et utiliser les capacités existantes de l'armée dans leurs processus de mise en œuvre. Cette approche est conforme au modèle éprouvé de subsidiarité de l'armée lors de catastrophes naturelles, par exemple.
Office / unité d'organisation responsable	Unité d'organisation Cyber Defence du RM, OC SNPC
Documents consultés pour l'évaluation de l'efficacité	Sources: entretiens, documents confidentiels
Entretiens	I 10

L'armée fait partie des infrastructures critiques du pays. Compte tenu de ses missions, l'utilisation du cyberespace en général et les cybermenaces en particulier constituent des thèmes centraux. Les principales tâches immédiates de l'armée englobent la protection de ses systèmes et infrastructures informatiques dans toutes les situations afin de garantir en permanence sa capacité et sa liberté d'action.

Le SRC exclut explicitement une guerre ou un conflit et délègue la compétence à l'armée en cas de cyberattaque correspondante. Le transfert des compétences des services civils à l'armée et le moment de ce transfert ne sont toutefois pas définis, pas plus que le fonctionnement de la collaboration formelle en cas de crise.

L'armée a un rôle subsidiaire dans les crises qui n'ont pas le niveau d'un conflit. Son action subsidiaire dans le cadre de la SNPC suppose une identification et une exploitation précoces des synergies. La participation de l'armée en amont devrait également se traduire par une harmonisation du système global suisse avec l'étude conceptuelle sur la cyberdéfense (*Konzeptionsstudie Cyber-Defence*) réalisée par l'armée en 2013.

4.2.1. Effet escompté: modèle d'efficacité de l'interface avec l'armée

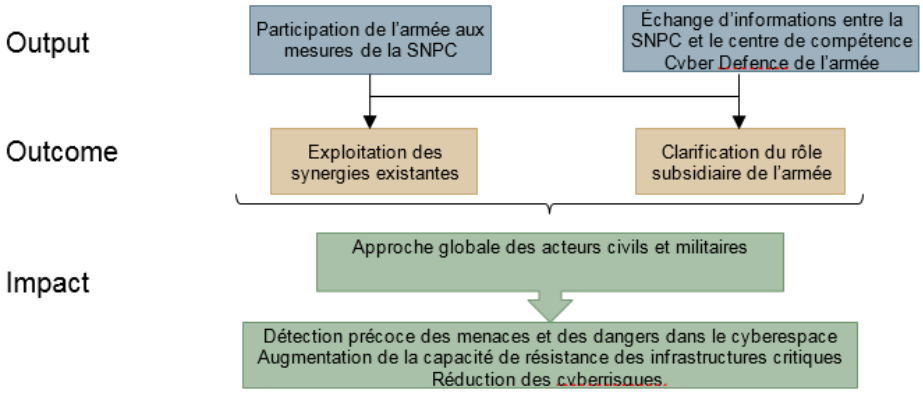

Illustration 17: Modèle d'efficacité de l'interface avec l'armée

4.2.2. *Input: ressources utilisées*

Type de ressources	Ressources SNPC utilisées
Ressources en personnel	Aucune ressource supplémentaire. Au sein de l'armée, l'unité d'organisation Cyber Defence assume les charges liées à la coordination avec la SNPC. Concernant cette dernière, cela incombe à l'OC SNPC.
Ressources financières	Aucune
Collaboration avec d'autres offices / unités d'organisation	Unités d'organisation prenant part à la collaboration: MELANI, SRC, SEFRI, DFAE, ChF

4.2.3. *Évaluation de la réalisation des objectifs et de l'impact*

Niveau	Objectifs non atteints	Objectifs partiellement atteints	Objectifs en majeure partie atteints	Objectifs atteints
Output		✖		
Outcome		✖		
Impact	☐ actuellement non énon llem			

4.2.4. *Justification de l'évaluation*

Output: objectifs partiellement atteints

L'armée collabore dans une large mesure à la SNPC. L'échange d'informations est donc adéquat sur le plan opérationnel. Compte tenu des ressources limitées, on se concentre cependant sur les principales tâches, et les compétences sont fortement restreintes. Les différents responsables connaissent leurs capacités et activités mutuelles. Les échanges sont en revanche sporadiques sur le plan stratégique, de sorte que plusieurs questions relatives aux compétences et aux attentes envers l'armée ne sont pas clarifiées de manière suffisante.

- **Participation de l'armée aux mesures de la SNPC:** l'armée participe directement ou indirectement à plusieurs mesures, à savoir:
  - mesures 1, 7 et 8: l'armée s'est fortement engagée en faveur de ces mesures et a financé la première collecte d'informations. Elle a incité à la création de CoPIRFCyber (voir le chap. 0), qui relève désormais du SEFRI. Les représentants de l'armée poursuivent leur participation;
  - mesures 4, 5 et 14: l'armée y participe directement, notamment à travers la convention de prestations conclue entre le SRC et le BAC-COE. L'armée ne contribue que de manière restreinte au tableau de la situation, car celui-ci n'est pas encore suffisamment consolidé. Les rares informations disponibles sont cependant échangées chaque semaine avec le SRC. Les échanges avec MELANI sont réguliers au niveau opérationnel; les informations provenant du réseau de MELANI ne sont pas fournies à l'UO CYD RM. Sur le plan stratégique, les échanges sont sporadiques et une compréhension mutuelle des rôles et des compétences fait encore défaut;
  - mesures 2 et 12: l'armée a participé de manière décisive à la réalisation de l'analyse des risques et vulnérabilités du secteur partiel critique correspondant.

Dans le cadre de ses propres projets, elle effectue déjà des analyses et applique des mesures (concept de sécurité intégrale du DDPS) afin d'améliorer la résilience de ses infrastructures;

- mesure 10: l'armée assiste aux réunions du groupe spécialisé Cyber International et est donc bien informée. À l'inverse, elle fournit au groupe des informations sur les aspects internationaux des activités de cyberdéfense;
- mesure 15: l'armée y participe, mais on ignore dans une large mesure quelle contribution subsidiaire elle pourrait apporter pour surmonter une éventuelle crise ayant des aspects cybernétiques. Le DDPS entend cependant clarifier ce point d'ici fin 2016;
- mesure 6: les échanges sont informels. Par nature, l'évaluation de la situation militaire se concentre sur d'autres aspects que ceux examinés par les policiers;
- autres mesures: l'armée est partiellement informée, mais elle n'y participe pas directement. Bien qu'elle constitue un important fournisseur de prestations, elle n'a pas été invitée à rejoindre le CP SNPC; le problème se situe toutefois au sein du DDPS.

- **Échange d'informations entre la SNPC et le centre de compétence Cyber Defence de l'armée:** établi depuis plusieurs années, l'échange d'informations entre l'armée et la SNPC est informel sur le plan opérationnel. L'armée est généralement informée du contenu et du degré de réalisation de la SNPC et, à l'inverse, les offices participants connaissent les capacités de l'armée. Il est regrettable que cet échange se limite au niveau opérationnel. Sur le plan stratégique, les échanges ne sont ni structurés ni réguliers. L'armée encourage la définition des rôles en cas de guerre ou de conflit à travers des exercices (par ex. Cyber Coalition, Cyber Pakt et Locked Shield).

Outcome: objectifs partiellement atteints

La participation de l'armée à différentes mesures de la SNPC a permis d'exploiter des synergies. En revanche, son rôle subsidiaire reste à définir: on ignore quelles sont ses compétences en cas d'aggravation d'une cybercrise et quand elle devrait être alertée. En l'absence de définitions claires, le soutien subsidiaire de l'armée en cas de crise n'est pas réalisable, en particulier si ses ressources sont engagées en priorité pour sa propre protection et qu'aucun moyen n'est disponible pour des tâches extérieures.

- **Exploitation des synergies existantes:** actuellement, l'armée fournit des prestations pour les mesures susmentionnées. Les synergies y sont bien exploitées. La collaboration passe principalement par des contacts personnels et moins par des processus formels (à l'exception de la convention de prestations entre le BAC-COE et le SRC). Une bonne collaboration s'est établie entre les CERT, mais les compétences doivent être définies plus précisément. La participation du RM à l'élaboration du tableau de la situation pourrait être intensifiée.
- **Clarification du rôle subsidiaire de l'armée:** le soutien subsidiaire n'est pas réglementé. La SNPC ne donne aucune indication précise à ce sujet. De plus, l'armée ne dispose pas actuellement des ressources nécessaires à un mandat de soutien subsidiaire pour l'ensemble des mesures. La protection de ses propres systèmes a donc la priorité.

  En particulier, la responsabilité de conduite doit encore être clarifiée si une cybercrise devait s'aggraver et devenir un conflit cybernétique. Pour ce faire, une révision de la SNPC doit fournir des indications plus précises. De même, il serait important

de considérer ces cas dans les exercices regroupant tous les participants afin d'évaluer si les bonnes personnes sont alertées au bon moment et si la résilience est suffisante. Un soutien subsidiaire est uniquement possible si l'on définit clairement les prestations de l'armée qui sont attendues à un moment précis au cours d'une crise.

Impact: actuellement non évaluable

Seule une version révisée de la SNPC permettra d'évaluer si la collaboration entre l'armée et la SNPC a été renforcée de telle sorte qu'une approche globale de gestion des cyberrisques soit effective à l'avenir. Il faudra alors définir plus précisément le rôle de l'armée en matière de cyberrisques.

5. Questions interdisciplinaires

Après l'évaluation des différentes mesures, le présent chapitre se penche sur l'appréciation des points suivants:

- **Ressources:** dans l'ensemble, les ressources personnelles et financières allouées à la SNPC présentent-elles un volume adéquat?
- **Contenu de la SNPC:** les objectifs de la stratégie étaient-ils appropriés et sont-ils encore valables? Le portefeuille de mesures est-il complet?
- **Organisation:** la mise en œuvre décentralisée de la SNPC a-t-elle fait ses preuves? Dans quelle mesure le CP SNPC et l'OC SNPC ont-ils correctement assumé leur rôle respectif?
- **Communication:** la communication interne et externe était-elle suffisante?

L'évaluation de ces questions s'appuie sur les réponses apportées par les responsables des mesures interrogés et par les autres participants. Lors de chaque entretien, la personne interviewée avait également la possibilité de s'exprimer sur ces aspects interdisciplinaires. Tous n'ont pas pu ou voulu prendre position sur le sujet, mais les réponses obtenues et l'analyse des documents dressent un tableau suffisamment précis pour pouvoir évaluer les questions susmentionnées.

5.1. Planification des ressources (*input*)

✓ **La planification des ressources était majoritairement correcte**

Dans l'ensemble, un nombre tout juste suffisant de postes a été prévu pour la mise en œuvre des mesures. Comme la plupart des unités d'organisation participantes travaillaient déjà sur des sujets similaires, le savoir-faire existant a été exploité. Les mesures ont dès lors pu être appliquées avec peu de ressources en personnel. Les unités d'organisation ont parfois eu des difficultés à pourvoir les postes, car seuls des contrats de travail à durée déterminée étaient proposés. La SNPC n'ayant pas son propre budget, la marge de manœuvre décisionnelle du CP SNPC était limitée.

- **Planification des ressources pour la mise en œuvre des mesures:** sur les 30 postes alloués au total à la SNPC, 28 ont été créés directement dans les unités d'organisation chargées d'appliquer les mesures. Le chapitre 3 précisait déjà les ressources utilisées pour chaque mesure. Dans l'ensemble, on peut affirmer que le besoin de ressources a été estimé de manière réaliste. Bien qu'elles soient plutôt très limitées, les ressources disponibles pour la plupart des mesures sont suffisantes. En revanche, le besoin de ressources pour la mise en œuvre de la mesure 3 a été sous-estimé. Le poste du SCOCI concernant la mesure 6 n'a pas été pourvu (ou ne l'a été que brièvement).

  Plusieurs personnes interrogées ont souligné que la durée limitée des postes pouvait entraver le recrutement. Des postes à durée déterminée sont en effet moins intéressants pour les collaborateurs potentiels et tendent donc à influer négativement sur le nombre et la qualité des candidats.

- **Planification des ressources pour les tâches générales:** deux postes de l'OC SNPC ont été créés à l'UPIC pour les tâches interdisciplinaires relatives à la coordination, au contrôle de gestion et à l'établissement des rapports. En l'espèce, force est de constater que ce nombre de postes était, lui aussi, à peine suffisant au regard du travail à accomplir.

La SNPC n'a pas de budget propre. Les tâches générales (conférence sur les cyberrisques en Suisse, évaluation de l'efficacité) sont financées par l'UPIC. En l'absence de budget spécifique, le CP SNPC a une marge de manœuvre très faible pour lancer ses propres projets et pour fixer des priorités quant au financement du soutien externe requis par certaines mesures.

5.2. Évaluation du contenu de la SNPC

Le contenu de la SNPC a fait ses preuves

Les objectifs stratégiques de la SNPC ont fait leurs preuves et restent judicieux. Les mesures qui en découlent couvrent bien la vaste palette d'activités nécessaires pour lutter contre les cyberrisques, mais le portefeuille de mesures pourrait être davantage rationnalisé.

Le plan de mise en œuvre a fixé des objectifs pour les mesures, mais aucune unité de référence pour déterminer la réussite de l'application. Cela tient au fait que de nombreuses mesures nécessitaient en premier lieu d'acquérir des connaissances et de mettre en place des structures et que des valeurs théoriques précises semblaient peu opportunes. L'instauration du contrôle de gestion stratégique a permis de vérifier l'avancement de la mise en œuvre. Dans l'ensemble, cette procédure était appropriée.

Les remarques suivantes peuvent être formulées sur les différents aspects du contenu de la SNPC:

- **Validité des objectifs suprêmes:** la plupart des personnes interrogées considèrent que les objectifs suprêmes de la SNPC, à savoir la détection précoce des menaces et des dangers dans le cyberespace, l'augmentation de la capacité de résistance des infrastructures critiques et la réduction des cyberrisques, restent d'actualité. Les objectifs ont fait leurs preuves en tant que directives stratégiques générales.
- **Conditions-cadres et interfaces:** la SNPC répertorie les principales stratégies et les principaux projets de la Confédération qui ont un lien avec elle. Le cyberespace étant un thème transversal, ces interfaces revêtent une grande importance. Si la SNPC devait se poursuivre, il faudrait tenir compte des évolutions de ces stratégies et de ces projets.
- **Exhaustivité du portefeuille de mesures:** le portefeuille de mesures de la SNPC a lui aussi fait des preuves. Les mesures élaborées couvraient bien les principaux aspects. Les responsables des mesures ont cependant conscience d'avoir surtout effectué un travail de mise en place jusqu'à présent. Les structures ainsi établies doivent désormais servir à franchir les prochaines étapes. Tous les participants estiment qu'il est primordial d'assurer la continuité du travail accompli.

  Concernant le portefeuille proprement dit, certaines mesures sont étroitement liées sur le fond. Il aurait parfois été possible de les regrouper dès le plan de mise en œuvre (par ex. les mesures 7 et 8 auraient pu n'en former qu'une seule). Pour assurer une meilleure vue d'ensemble, il serait utile de rationaliser le portefeuille (réduction du nombre de mesures). Cette idée devrait être envisagée à l'avenir.

  Les personnes interrogées ont identifié les principaux sujets suivants parmi ceux qui n'ont pas encore été abordés par la SNPC et qui pourraient l'être à l'avenir:
  - importance et conséquences de la directive européenne sur la sécurité des réseaux et de l'information (SRI) pour la Suisse;

  - introduction éventuelle d'une obligation de déclarer les cyberincidents relatifs à la sécurité pour les exploitants d'infrastructures critiques (cette question est désormais plus pertinente dans le sillage de la directive SRI);
  - engagement de la Suisse en faveur des initiatives visant à accroître les capacités des pays en développement.

- **Concrétisation des objectifs des mesures dans le plan de mise en œuvre:** les objectifs formulés par la SNPC pour les différentes mesures sont concrétisés dans le plan de mise en œuvre de la SNPC. Des objectifs ont été définis pour chacune d'entre elles, mais aucune unité de référence n'a été fournie pour déterminer la réussite de la mise en œuvre. En collaboration avec l'OC SNPC, les responsables des mesures ont planifié les étapes et défini les résultats à fournir. Pour réaliser le contrôle de gestion et démontrer l'efficacité des mesures, il aurait été souhaitable que ces critères soient choisis dès le plan de mise en œuvre. De plus, certains responsables des mesures interrogés auraient aimé bénéficier de telles directives.

  Cependant, plusieurs responsables des mesures ont indiqué que la planification des étapes avait dû être modifiée pendant la mise en œuvre en raison de nouveaux enseignements ou d'événements. De nombreuses mesures portant sur l'acquisition de connaissances et la mise en place de structures, il n'aurait guère été possible de fixer des critères de mesure adéquats avant le début des travaux. Plusieurs personnes interrogées ont donc affirmé qu'une certaine flexibilité était indispensable à la réussite de la mise en œuvre et que des objectifs de mesure plutôt généraux étaient préférables à des directives strictes.

  L'exigence de critères prédéfinis pour la réalisation des objectifs et la mesurabilité, d'une part, et le souhait de flexibilité, d'autre part, sont parfois antinomiques. Le plan de mise en œuvre laissait aux responsables des mesures une marge de manœuvre suffisante, car il ne comportait aucun objectif directement quantifiable. Le contrôle de gestion stratégique mis en place par l'OC SNPC a permis de compenser cela. On a ainsi trouvé un compromis acceptable, qui fixait certes une ligne directrice, mais accordait suffisamment de liberté aux responsables des mesures.

5.3. Organisation de la SNPC

L'organisation de la SNPC était en grande partie adéquate

La mise en œuvre décentralisée de la SNPC (responsabilité déléguée aux offices chargés des mesures) s'est révélée parfaitement adéquate. Cette approche est appropriée pour gérer le thème transversal des cyberrisques. Le succès de cette solution repose sur le bon fonctionnement des organes de coordination. Le CP SNPC et l'OC SNPC ont fait leurs preuves en la matière. La composition du CP SNPC devrait cependant être légèrement modifiée afin que des représentants des principales interfaces puissent y siéger. Le rattachement de l'OC SNPC à MELANI n'est pas judicieux, car l'OC SNPC devrait être indépendant vis-à-vis des responsables des mesures (qui font partie de MELANI) pour pouvoir, si nécessaire, arbitrer en toute neutralité entre différents intérêts et exécuter efficacement le contrôle de gestion stratégique.

Sur la base des entretiens réalisés et des documents analysés, l'organisation de la SNPC peut être évaluée de la manière suivante:

- **Organisation décentralisée:** de manière générale, l'organisation décentralisée de la SNPC constitue le pilier de la mise en œuvre réussie de la SNPC. Elle correspond au caractère interdisciplinaire des cyberrisques et convient au système fédéraliste de la Suisse. La participation de tous les acteurs pertinents est l'un des défis d'une

mise en œuvre décentralisée. Les régulateurs n'ont pas tous pu contribuer aux travaux comme il l'aurait fallu. Ces efforts devraient être renforcés à l'avenir. Une représentation unique et clairement identifiable vis-à-vis de l'extérieur est un défi plus difficile à relever, car plusieurs acteurs participent à la mise en œuvre. Le chapitre 5.4 Communication interne et externe contient de plus amples détails sur la question.

- **Rôle et composition du CP SNPC:** le comité de pilotage de la SNPC a assumé sa fonction d'organe de surveillance en approuvant un contrôle de gestion stratégique semestriel. L'adoption d'une mesure particulière concernant la mesure 3 a montré que le CP SNPC était également prêt à corriger la mise en œuvre de la SNPC.

  La représentation directe de toutes les unités d'organisation participantes a fait ses preuves. Il convient également de saluer le rôle d'observateur d'economiesuisse. En revanche, l'armée et l'OFPP ne sont pas représentés dans le CP SNPC, ce qui a eu tendance à compliquer la coordination entre l'unité Cyber Defence de l'armée, la stratégie nationale pour la protection des infrastructures critiques et la SNPC.

  Le CP SNPC est dirigé par le délégué de l'UPIC. La conduite assurée par l'UPIC est opportune de manière générale, mais elle n'est pas impérative. Organe de pilotage adéquat pour mener une stratégie, l'UPIC s'occupe depuis longtemps des cyberrisques à travers MELANI et la section Sécurité informatique de l'UPIC. Elle ne doit toutefois pas obligatoirement conduire le projet, car un thème transversal comme la SNPC pourrait être dirigé par différentes organisations. Certains acteurs estiment que la conduite assurée par l'UPIC pose problème, car elle se traduit par d'éventuels objectifs contradictoires avec d'autres tâches principales de l'UPIC.

- **Rôle de l'OC SNPC:** l'OC SNPC participe directement à la mise en œuvre de plusieurs mesures, effectue des tâches administratives pour le CP SNPC, organise la conférence annuelle sur les cyberrisques en Suisse, rédige les rapports annuels sur la SNPC et exécute le contrôle de gestion stratégique. Les participants considèrent que ces tâches sont essentielles. Compte tenu de la mise en œuvre décentralisée, il est primordial qu'un organe assure la coordination.

  Certaines personnes interrogées se sont montrées critiques envers le rattachement organisationnel de l'OC SNPC à MELANI. L'OC SNPC réalisant le contrôle de gestion stratégique pour le CP SNPC, il ne devrait pas être subordonné à une unité qu'il doit également auditer. Si la SNPC devait se poursuivre, il faudrait renforcer l'indépendance de l'OC SNPC en ne l'affectant pas à MELANI.

5.4. Communication interne et externe

✖ **Les tâches de communication ne sont réalisées que partiellement**

La réussite de la mise en œuvre décentralisée de la stratégie repose de manière déterminante sur une très bonne communication entre les participants ainsi que sur une bonne communication externe (comment la stratégie est-elle appliquée et par qui?). La communication interne était appropriée; les participants disposaient en temps opportun des informations nécessaires.

En revanche, les objectifs poursuivis par la SNPC, leur réalisation concrète et l'état d'avancement de la mise en œuvre ont trop peu été communiqués à l'extérieur. Par conséquent, les actions de la Confédération en manière de cyberrisques et les limites de ses compétences selon sa propre opinion ne sont guère connues.

Dans le cadre de l'évaluation de l'efficacité, les participants ont été invités à juger la communication interne et externe sur la SNPC. Il en ressort les appréciations suivantes:

- **Communication interne:** les personnes interrogées sont satisfaites du niveau de la communication interne. De nombreux responsables des mesures ont des échanges réguliers avec l'OC SNPC et d'autres participants. L'avancement de la mise en œuvre de la stratégie est toujours présenté lors des séances du CP SNPC. De manière générale, on reconnaît que la SNPC a fortement amélioré, voire établi dans certains cas, la communication entre les acteurs concernés par les cyberrisques. La participation active de nombreux responsables des mesures à la mise en œuvre d'autres mesures et la très bonne compréhension mutuelle qui en découle facilitent grandement la communication.
- **Communication externe:** la communication interne est saluée, alors que des actions sont nécessaires au niveau de la communication externe. Compte tenu de la structure décentralisée, les personnes extérieures à la stratégie ignorent souvent qui est effectivement responsable de la mise en œuvre de la SNPC en général ou d'une mesure spécifique. Le rapport annuel et la conférence annuelle sur les cyberrisques en Suisse sont autant d'outils de communication pour s'adresser à un plus large public. De plus, l'OC SNPC et les responsables des mesures participent régulièrement à des manifestations pour présenter la SNPC ou certaines mesures. Il est néanmoins apparu que ces canaux de communication étaient insuffisants. Les feed-back des milieux économiques et de la population ainsi que la couverture médiatique consécutive à des cyberincidents d'envergure ont montré que les attentes vis-à-vis de la SNPC étaient en partie erronées. On a trop peu précisé que la sécurité des entreprises ne relevait pas de la SNPC, mais continuait d'incomber aux entreprises elles-mêmes. Il est donc nécessaire de consolider le profil de la SNPC vis-à-vis de l'extérieur et de le communiquer plus clairement.

6. Conclusion

En décidant de mettre en œuvre la SNPC, le Conseil fédéral a montré sa volonté de lutter contre les cyberrisques à travers des mesures dans différents domaines. Les seize mesures du plan de mise en œuvre indiquent ce que les unités d'organisation doivent accomplir jusqu'à fin 2017 pour réaliser les objectifs stratégiques de la SNPC, à savoir la détection précoce des dangers et des menaces dans le cyberespace, l'augmentation de la capacité de résistance des infrastructures critiques et la réduction des cyberrisques. En prenant cette décision, le Conseil fédéral avait conscience de la complexité et de l'évolution très rapide de la thématique des cyberrisques. C'est la raison pour laquelle il a souhaité qu'une évaluation de l'efficacité soit présentée cinq ans après l'adoption de la stratégie afin de déterminer si les mesures pouvaient être appliquées comme prévu et si elles étaient appropriées pour atteindre les objectifs fixés. Le présent rapport répond à ce mandat et permet de tirer des conclusions sur l'efficacité de la SNPC.

Il convient de préciser dans un premier temps que la mise en œuvre des mesures est bien avancée. L'évaluation de l'efficacité a révélé que les structures organisationnelles et les processus prévus dans le plan de mise en œuvre avaient majoritairement été mis en place et que différents produits (rapports et concepts) avaient été fournis dans les délais. Ce résultat est le fruit du grand engagement des services responsables, qui ont travaillé avec de modestes ressources supplémentaires.

L'*output* obtenu s'est déjà traduit par un *outcome* notable. Les structures, les processus et les produits qui ont été réalisés ont indéniablement contribué à renforcer les capacités, à développer les connaissances et à assurer une meilleure coordination dans les différents domaines. L'évaluation de l'*outcome* n'est pas toujours simple selon la mesure. Force est de constater que tous les objectifs n'ont pas été atteints comme prévu pour trois des seize mesures. Dans l'ensemble, on peut cependant noter que les travaux donnent les résultats souhaités et que les capacités de gestion des cyberrisques se sont sensiblement améliorées par rapport à la situation antérieure à la SNPC.

L'impact des travaux accomplis sur les objectifs stratégiques est le plus difficile à mesurer. Dans le contexte dynamique et complexe des cyberrisques, il n'est guère possible de mettre en évidence le lien de causalité entre les mesures prises et leur impact sur les objectifs de la SNPC. De plus, l'évaluation de l'efficacité a été réalisée trop tôt. En général, les mesures adoptées déploient leurs effets après un certain laps de temps. Par conséquent, l'impact sur au moins l'un des trois objectifs stratégiques n'a pu être quantifié que pour trois mesures. Cela ne signifie pas pour autant que les autres mesures n'auront aucun effet. Les modèles d'efficacité élaborés pour toutes les mesures dans le cadre de l'évaluation indiquent l'impact concret qui peut être escompté au regard des résultats obtenus jusqu'à présent.

L'évaluation de l'efficacité ne s'est cependant pas limitée à l'appréciation des différentes mesures. Elle a également examiné si les interfaces de la SNPC avec les travaux des cantons et avec l'armée avaient été suffisamment prises en compte. Si l'on peut répondre par l'affirmative pour les cantons, des questions importantes restent à clarifier pour l'interface avec l'armée. La délimitation entre les tâches civiles de la SNPC et la conduite par l'armée en cas de conflit ainsi que les compétences correspondantes ne sont pas définies de manière exhaustive. De même, on ignore comment l'armée peut apporter un soutien subsidiaire aux autorités civiles en matière de cyberrisques.

Enfin, les aspects interdisciplinaires ont également été contrôlés: les objectifs de la SNPC ont-ils été choisis correctement? Des ressources suffisantes ont-elles été allouées? L'organisation décentralisée a-t-elle fait ses preuves? La communication a-t-elle fonctionné? De manière générale, le bilan correspondant est positif. Les contenus ont porté leurs fruits, les ressources étaient à peine suffisantes et l'organisation décentralisée

a rencontré un accueil favo. Seule la communication externe était lacunaire et doit être renforcée de l’avis de plusieurs personnes interrogées.

En conclusion, on peut affirmer que la SNPC est une réussite au niveau tant des mesures que des interfaces et des aspects interdisciplinaires. Il convient néanmoins de souligner que les mesures mises en œuvre ne constituent qu’une première étape. Celle-ci a certes été franchie, mais il est indéniablement trop tôt pour s’en contenter. De plus, cela serait plutôt présomptueux, car les cyberrisques se développent extrêmement rapidement. Toute stagnation se traduirait donc par un recul. Il ressort également de l’évaluation de l’efficacité que les travaux accomplis devraient impérativement se poursuivre. Seuls des efforts permanents permettront de protéger la Suisse du mieux possible contre les cyberrisques.

A. Entretiens et questionnaires

A.1. Liste des entretiens effectués

Chaque entretien porte une cote composée d'un «I» et d'un chiffre compris entre 1 et 14. Dans le document, les cotes indiquées sont des liens hypertextes renvoyant aux entretiens ci-dessous.

N°	Date	Mesure	Responsable de la mesure	Heure et lieu
I 1	26 février 2016	M1, M7, M8	Blaise Roulet (délégué de domaine spécialisé au SEFRI) Manuel Suter (coordinateur de la SNPC à l'UPIC)	14 h 00-16 h 00 AWK, Laupenstrasse 4, Berne
I 2	4 mars 2016	M4, M14	Philipp Kronig Marc Henauer (responsable de l'OIC MELANI au SRC) Mauro Vignati (responsable de l'unité Cyber SRC du SRC) Pascal Lamia (responsable de MELANI à l'UPIC)	10 h 00-12 h 00 P20, Berne
I 3	15 mars 2016	M2, M12	Ruedi Rytz (responsable de la section Domaines infrastructure de l'OFAE) Daniel Caduff (collaborateur scientifique à l'OFAE) Dario Walder (collaborateur scientifique à l'OFAE)	10 h 00-12 h 00 AWK, Laupenstrasse 4, Berne
I 4	15 mars 2016	M10	Michele Coduri (responsable de la DPS du DFAE) Laura Crespo (collaboratrice scientifique à la DPS du DFAE)	14 h 00-16 h 00 DPS/DFAE, Bernastrasse, Berne
I 5	22 mars 2016	M6	Adrian Lobsiger (directeur suppléant de fedpol) Tobias Bolliger (responsable par intérim du commissariat du SCOCI au DFJP)	10 h 00-12 h 00 AWK, Laupenstrasse 4, Berne
I 6	5 avril 2016	M9, M11	Rene Dönni (vice-directeur, responsable des services de télécommunication et poste de l'OFCOM) Nicolas Rollier (collaborateur scientifique à l'OFCOM) Matthias Ziehl, (ingénieur en télécommunication à l'OFCOM)	M9, M11 10 h 00-12 h 00 AWK, Laupenstrasse 4, Berne
I 7	5 avril 2016	M3	Marcel Frauenknecht (responsable de la section Sécurité informatique de l'UPIC) Rolf Oppliger (UPIC)	14 h 00-16 h 00 AWK, Laupenstrasse 4, Berne
I 8	12 avril 2016	M2, M12	Stefan Brem (chef de la section Analyse des risques et coordination de la recherche de l'OFPP) Angelika Bischof (collaboratrice scientifique à l'OFPP) Giorgio Ravioli (collaborateur scientifique à l'OFPP)	14 h 00-16 h 00 AWK, Laupenstrasse 4, Berne

N°	Date	Mesure	Responsable de la mesure	Heure et lieu
I 9	15 avril 2016	M15, RNS	André Duvillard (délégué au RNS) Melanie Friedli (collaboratrice scientifique au RNS) Nicolas Mueller (responsable de l'unité Formation à la gestion des crises à la ChF)	10 h 00-11 h 30 AWK, Laupenstrasse 4, Berne
I 10	25 avril 2016	M5	Pascal Lamia (responsable de MELANI à l'UPIC) Reto Inversini (analyste du GovCERT)	10 h 00-12 h 00 AWK, Laupenstrasse 4, Berne
I 11	3 mai 2016	Interface avec l'armée, M4, M14	AF_CYD RM Gérald Vernez AF_BAC COE (CNO) Riccardo Sibilia	10 h 00-12 h 00 P20
I 12	3 mai 2016	M13	Stefanie Frey (coordinatrice de la SNPC à l'UPIC) Ronja Tschümperlin (analyste de l'OIC MELANI au SRC) Manuel Suter (coordinateur de la SNPC à l'UPIC)	14 h 00-16 h 00 P20
I 13	24 mai 2016	M16	Stefanie Frey	Questionnaire rempli à la main
I 14	3 juin 2016	M2, M12	OFEN Marc Kenzelmann, vice-directeur et responsable de la division Surveillance et sécurité de l'OFEN Hans-Peter Binder, responsable de la gestion des risques et surveillance du transport par conduites Christian Holzner, spécialiste en gestion des risques	10 h 00-12 h 00 AWK, Laupenstrasse 4, Berne

A.2. Liste des questionnaires envoyés

Une enquête a été effectuée dans certains secteurs partiels de l'infrastructure critique au moyen d'un questionnaire portant sur les mesures M2 et M12. Ici aussi, les questionnaires sont assortis d'une cote composée d'un «f» et d'un chiffre compris entre 1 et 6. Dans le document, les cotes indiquées sont des liens hypertextes renvoyant aux questionnaires ci-dessous.

N°	Domaine	Responsables des mesures
F 1	Approvisionnement en gaz naturel	• Andre Martin, Gasverbund Mittelland, andre.martin@gvm-ag.ch • Jens Harenberg, Swissgas harenberg@swissgas.ch
F 2	Trafic de ligne	• Peter Frey, Aéroport de Zurich, peter.frei@zurich-airport.com • Reto Gasser, reto.gasser@2assistu.ch
F 3	Santé	Secteur laboratoires • Samuel Roulin, Office fédéral de la santé publique OFSP samuel.roulin@bag.admin.ch • Martin Risch, président de l'USML (Union Suisse de Médecine de Laboratoire) et suppléant du président du conseil d'administration du centre des laboratoires médicaux Dr. Risch martin.risch@risch.ch Secteur soins médicaux et hôpitaux • Philipp Stoll, représentant de H+ philipp.stoll@ukbb.ch
F 4	Banques	• Yves Obrist, FINMA Yves.Obrist@finma.ch • Michael Brügger, FINMA Michael.Bruegger@finma.ch • Thomas Rhomberg, SIX Group Services AG Thomas.Rhomberg@six-group.com
F 5	Médias	• Andreas Schneider, Société suisse de radiodiffusion et télévision SSR, andreas.schneider@srgssr.ch • René Wehrlin, Office fédéral de la communication OFCOM rene.wehrlin@bakom.admin.ch
F 6	Approvisionnement en électricité	• Reto Bondolfi, EWZ reto.bondolfi@ewz.ch • Daniel Schelbert, Elektrizitätswerk des Bezirks Schwyz [centrale électrique du district de Schwyz] d.schelbert@ebs-strom.ch • Beat Schüpbach, Swissgrid beat.schuepbach@swissgrid.ch (n'a pas répondu malgré nos nombreux rappels)

B. Documents référencés

Titre		Auteur / éditeur	Date
[1]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)	Département fédéral de la défense, de la protection de la population et des sports DDPS	19.06.2012
[2]	Plan de mise en œuvre	Département fédéral des finances DFF, Unité de pilotage informatique de la Confédération UPIC	13.05.2013
[3]	Concept détaillé pour l'évaluation de l'efficacité de la SNPC	ECOPLAN	28.07.2015
[4]	Description «Demande d'offres pour l'évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques»	Département fédéral des finances DFF, Unité de pilotage informatique de la Confédération UPIC	16.11.2015
[5]	Offre de prestations de conseiller et d'ingénieur pour l'évaluation de l'efficacité de la SNPC	AWK	22.10.2015
[6]	Feuille de route SNPC	UPIC	13.07.2015
[7]	Programme de la conférence «Les cyberrisques en Suisse»	UPIC	02.11.2015
[8]	Mandat du comité de pilotage de la SNPC et de l'organe de coordination de la SNPC	UPIC	15.05.2013
[9]	Contrôle de gestion stratégique effectué par le comité de pilotage de la SNPC quant à l'état d'avancement de la mise en œuvre au 1er janvier 2015	OC SNPC	27.05.2015
[10]	Procès-verbal de la 1re séance du comité de pilotage de la SNPC	OC SNPC	30.10.2013
[11]	Procès-verbal de la 2e séance du comité de pilotage de la SNPC	OC SNPC	11.02.2014
[12]	Procès-verbal de la 3e séance du comité de pilotage de la SNPC	OC SNPC	19.08.2014
[13]	Procès-verbal de la 4e séance du comité de pilotage de la SNPC	OC SNPC	10.02.2015
[14]	Procès-verbal de la 5e séance du comité de pilotage de la SNPC	OC SNPC	20.08.2015
[15]	Procès-verbal de la 6e séance du comité de pilotage de la SNPC	OC SNPC	25.02.2016
Recherche M1, aperçu de la formation M7 et M8			
[16]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 1: identification des cyberrisques par la recherche, étape 1.1: organisation et description des processus	OC SNPC	30.07.2015
[17]	Procès-verbal CoPIRFCyber	Département fédéral des finances DFF	11.09.2015
[18]	Procès-verbal CoPIRFCyber	Département fédéral des finances DFF	18.12.2015
[19]	Procès-verbal CoPIRFCyber	Département fédéral des finances DFF	22.05.2015
[20]	Programme provisoire	Swiss Cyber Risk Research Conference 2016	24.11.2015
[21]	Groupe d'experts «Recherche et formation relatives aux cyberrisques»	Département fédéral des finances DFF	novembre 2015

Titre		Auteur / éditeur	Date
[22]	Sous-groupe thématique: projet «Recherche et formation relatives aux cyberrisques»	Département fédéral des finances DFF	
[23]	Researsch Capabilities in Switzerland	Bernhard Hämmerli et Solange Ghernaoutie	
[24]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 7: aperçu des offres de formation, étape 7.1: aperçu des offres de formation à la gestion des cyberrisques	Département fédéral des finances DFF	26.06.2014
[25]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 7: aperçu des offres de formation, étape 7.2: bref rapport visant à déterminer les offres de formation de grande qualité rédigé grâce à des recommandations d'experts	Département fédéral des finances DFF	30.06.2014
[26]	Formation à la gestion des cyberrisques (mesure 7 de la SNPC)	International institute for management in technology – IIMT	16.03.2015
[27]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), rapport final concernant la mesure 8: usage accru des offres de formation et comblement des lacunes	Département fédéral des finances DFF	25.02.2016
[28]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 8: usage accru des offres de formation et comblement des lacunes, étape 8.1: structure organisationnelle (mandat et participation de l'unité chargée du pilotage)	Département fédéral des finances DFF	30.07.2015
[29]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 8: usage accru des offres de formation et comblement des lacunes, étape 8.2: projet de concept	Département fédéral des finances DFF	30.07.2015
[30]	Cybersecurity Competence Building Trends	DiploFoundation	novembre 2015
[31]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 8: usage accru des offres de formation et comblement des lacunes, étape 8.4: plan de mise en œuvre	Département fédéral des finances DFF	02.02.2016
[32]	Expert en sécurité informatique, un nouveau profil professionnel	Unité de pilotage informatique de la Confédération UPIC	20.05.2016
[33]	Tableau des ressources pour la SNPC	Unité de pilotage informatique de la Confédération UPIC	10.02.2016
Analyse des secteurs (mesures 2 et 12)			
[34]	Analyse des risques et des vulnérabilités du secteur partiel du trafic aérien	Département fédéral de l'économie, de la formation et de la recherche DEFR	27.11.2015
[35]	Analyse des risques et des vulnérabilités du secteur partiel des médias	Office fédéral de la protection de la population OFPP	03.12.2015
[36]	Analyse des risques et des vulnérabilités du secteur partiel des laboratoires	Office fédéral de la protection de la population OFPP	05.02.2016
[37]	Analyse des risques et des vulnérabilités du secteur partiel de la protection civile	Office fédéral de la protection de la population OFPP	16.02.2016

Titre		Auteur / éditeur	Date
[38]	Analyse des risques et des vulnérabilités du secteur partiel de l'approvisionnement en gaz naturel	Département fédéral de l'économie, de la formation et de la recherche DEFR	26.09.2014
[39]	Analyse des risques et des vulnérabilités du secteur partiel du trafic routier	Département fédéral de l'économie, de la formation et de la recherche DEFR	12.02.2015
[40]	Analyse des risques et des vulnérabilités du secteur partiel de l'approvisionnement électrique	Département fédéral de l'économie, de la formation et de la recherche DEFR	27.11.2015
[41]	Mesures visant à renforcer la résilience informatique	Département fédéral de l'économie, de la formation et de la recherche DEFR	23.02.2016
[42]	Méthode: Analyse des risques et des vulnérabilités des secteurs partiels critiques	Office fédéral de la protection de la population OFPP	26.05.2015
[43]	Analyse des risques et des vulnérabilités du secteur partiel des soins médicaux et des hôpitaux	Office fédéral de la protection de la population OFPP	18.12.2015
[44]	Analyse des risques et des vulnérabilités du secteur partiel des banques	Office fédéral de la protection de la population OFPP	07.03.2016
[45]	Analyse des risques et des vulnérabilités du secteur partiel des services d'urgence	Office fédéral de la protection de la population OFPP	20.05.2016
[46]	Analyse des risques et des vulnérabilités du secteur partiel Parlement, gouvernement, justice, administration	Office fédéral de la protection de la population OFPP	20.05.2016
[47]	Liste de contrôle: vérification des travaux préliminaires en vue de l'analyse des vulnérabilités PIC / SNPC	Office fédéral de la protection de la population OFPP	
[48]	Note de dossier sur la discussion entre l'OFAE et l'OFPP relative à la stratégie PIC et la SNPC	Office fédéral de la protection de la population OFPP	24.03.2014
[49]	Courriel de Daniel Schelbert	Elektrizitätswerk des Bezirks Schwyz AG	21.07.2015
[50]	Courriel de Hansjörg Holenstein	Association des entreprises électriques suisses	19.03.2015
[51]	Collaboration entre MELANI et l'OFAE / comparaison avec les informations de la SNPC	Collaboration MELANI–OFAE	
[52]	Office fédéral de l'aviation civile	Département fédéral de l'économie, de la formation et de la recherche DEFR	20.09.2015
[53]	Analyse des commentaires sur l'approvisionnement électrique	Analyse des commentaires sur l'approvisionnement électrique	???
[54]	Élaboration et réception des analyses des vulnérabilités	Office fédéral pour l'approvisionnement économique du pays OFAE	11.09.2014
[55]	Mesures visant à renforcer la résilience du trafic aérien	Office fédéral pour l'approvisionnement économique du pays OFAE	12.01.2016
[56]	Table des matières commentée de l'analyse des risques et des vulnérabilités dans les secteurs partiels critiques	Office fédéral de la protection de la population OFPP	
[57]	Rapport d'étape 2.1: Analyse des risques et des vulnérabilités SNPC	Office fédéral de la protection de la population OFPP	
[58]	Mise en œuvre de la mesure 2 SNPC et de la mesure 15 Stratégie PIC	Office fédéral de la protection de la population OFPP / Office fédéral pour l'approvisionnement économique du pays OFAE	18.03.2014

Titre		Auteur / éditeur	Date
[59]	Table des matières commentée des mesures visant à renforcer la résilience des secteurs partiels critiques	Office fédéral de la protection de la population OFPP	
[60]	Rapport d'étape 12.1: Mesure visant à renforcer la résilience de la SNPC	Office fédéral de la protection de la population OFPP / Office fédéral pour l'approvisionnement économique du pays OFAE	
[61]	Note de dossier sur la discussion entre l'OFAE et l'OFPP relative à la stratégie PIC et la SNPC	Office fédéral de la protection de la population OFPP	24.03.2014
[62]	Courriel, autres adresses: stratégie nationale de protection de la Suisse contre les cyberrisques	Hansjörg Holenstein, Association des entreprises électriques suisses AES	19.03.2015
[63]	Analyse des commentaires sur l'approvisionnement électrique		15.03.2016
[64]	Représentation du processus d'établissement et de validation d'analyses des vulnérabilités de la SNPC	Office fédéral pour l'approvisionnement économique du pays OFAE	11.09.2014
Analyse de la vulnérabilité des systèmes informatiques de la Confédération (mesure 3)			
[65]	Demande du 25 février 2016 au CP SNPC: mesure spéciale relative à la mesure 3	Département fédéral des finances DFF	25.02.2016
[66]	Analyse des vulnérabilités pour les composants de processus et de systèmes informatiques		
[67]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 3: analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale à l'aide d'un concept de contrôle, document de base	Département fédéral des finances DFF	11.11.2015
[68]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 3: analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale à l'aide d'un concept de contrôle, étape 3.3: concept de contrôle	Département fédéral des finances DFF	11.11.2015
[69]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 3: analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale à l'aide d'un concept de contrôle, étape 3.2: le concept est au stade de projet et fait l'objet d'améliorations	Département fédéral des finances DFF	04.02.2015
[70]	Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 3: analyse de la vulnérabilité des infrastructures informatiques de l'administration fédérale à l'aide d'un concept de contrôle, étape 3.1: concept sommaire (établissement du concept de contrôle)	Département fédéral des finances DFF	02.09.2014
Tableau de la situation (mesure 4) et identification des agresseurs (mesure 14)			
[71]	Cybermenaces	Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI	

Titre	Auteur / éditeur	Date
[72] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesures 4 et 14 «Tableau de la situation» et «Identification des agresseurs», étapes 4.6 et 14.3: le SRC acquiert des connaissances spéciales et des compétences dans le cyberespace, avec la BAC et le RM comme fournisseurs de prestations	Département fédéral des finances DFF	
[73] Mesure 4 de la SNPC: concept de renforcement de MELANI en tant que plate-forme d'échange d'informations	Département fédéral des finances DFF	20.02.2014
[74] Mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) au SRC, rapport d'étapes 4.2 / 5.1 / 14.1 selon la feuille de route	Département fédéral de la défense, de la protection de la population et des sports DDPS	
[75] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 4 «établissement d'un tableau de la situation et de son évolution», étape 4.3: l'accord de niveau de service (SLA) avec le BAC-COE est modifié.	Département fédéral des finances DFF	
[76] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), mesure 4: établissement du tableau de la situation et de son évolution, étape 4.4: radar de la situation.	Département fédéral des finances DFF	
[77] Plateforme DNS passive	Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI	22.12.2014
[78] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesures 4 et 14 «Tableau de la situation» et «Identification des agresseurs», étapes 4.6 et 14.3: le SRC acquiert des connaissances spéciales et des compétences dans le cyberespace avec la BAC et le RM comme fournisseurs de prestations.	Département fédéral des finances DFF	
[79] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 14 «Mesures actives et identification des agresseurs», étape 14.2: l'accord de niveau de service (SLA) avec le BAC-COE est modifié.	Département fédéral des finances DFF	
Analyse des incidents (mesure 5)		
[80] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 5 «Analyse et suivi des incidents», étape 5.2: structure organisationnelle du GovCERT	Département fédéral des finances DFF	29.04.2014
[81] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 5 «Analyse et suivi des incidents», étape 5.3: accroissement de la résilience du GovCERT	Département fédéral des finances DFF	30.06.2014
[82] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 5 «Analyse et suivi des incidents»", étape 5.4: la plate-forme destinée à l'échange d'informations sur les maliciels (*Malware Information Sharing Platform*, MISP) est établie.	Département fédéral des finances DFF	16.06.2014

Titre	Auteur / éditeur	Date
[83] Plateforme DNS passive	Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI	18.06.2015
Vue d'ensemble des infractions (mesure 6)		
[84] Phénomènes de cybercriminalité: définitions, mode opératoire et mesures	Département fédéral de justice et police DFJP	28.05.2015
[85] État de la mise en œuvre de la mesure 6 de la SNPC: vue d'ensemble des infractions et coordination des cas intercantonaux complexes	Département fédéral de justice et police DFJP	20.08.2015
[86] Rapport annuel 2014 du Service de coordination de la lutte contre la criminalité sur Internet (SCOCI)	Département fédéral de justice et police DFJP	26.03.2015
[87] Concept pour la mesure 6 de la SNPC: vue d'ensemble nationale des infractions et coordination des cas intercantonaux complexes	Département fédéral de justice et police DFJP	mars 2016
[88] Tableau de structure des catégories de délits et des priorités en la matière		
[89] État de la mise en œuvre de la mesure 6 de la SNPC: vue d'ensemble des infractions et coordination des cas intercantonaux complexes	Département fédéral de justice et police DFJP	20.08.2015
Gouvernance d'Internet (mesure 9) et standardisation internationale (mesure 11)		
[90] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 9 «Gouvernance d'Internet», étape 9.1: aperçu des manifestations ou initiatives prioritaires et des comités internationaux ayant un lien avec la gouvernance d'Internet	Office fédéral de la communication OFCOM	30.05.2014
[91] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 9 «Gouvernance d'Internet», étape 9.2: un aperçu des processus de gouvernance d'Internet ainsi que de la participation active de la Suisse est en place.	Office fédéral de la communication OFCOM	30.05.2014
[92] Étape 9.3 de la SNPC: priorités de la Suisse dans la gouvernance d'Internet et identification des acteurs pertinents	Office fédéral de la communication OFCOM	20.10.2014
[93] Atelier dédié à la mesure 11 de la SNPC	Office fédéral de la communication OFCOM	15.02.2016
[94] Mesure 11 de la SNPC: standardisation internationale et initiatives en matière de sécurité: aperçu des organes s'occupant de la sécurité, de la sûreté et de la standardisation	Office fédéral de la communication OFCOM	10.12.2014
[95] Mesure 11 de la SNPC: standardisation internationale et initiatives en matière de sécurité: aperçu des acteurs concernés en Suisse et de leurs activités	Office fédéral de la communication OFCOM	11.12.2015
[96] Mesure 11 de la SNPC: standardisation internationale et initiatives en matière de sécurité: aperçu des organes s'occupant de la sécurité, de la sûreté et de la standardisation	Office fédéral de la communication OFCOM	11.12.2015
[97] Mesure 11 de la SNPC: standardisation internationale et initiatives en matière de sécurité: aperçu des organes s'occupant de la sécurité, de la sûreté et de la standardisation	Office fédéral de la communication OFCOM	10.12.2014

Titre	Auteur / éditeur	Date
Coopération internationale (mesure 10)		
[98] Aperçu annuel des activités en matière de cyberespace		2014
[99] Aperçu annuel des activités en matière de cyberespace		2015
[100] Liste de questions sur l'évaluation de l'efficacité SNPC – Coopération internationale en matière de cybersécurité visée (mesure 10)	Philipp Grabher, Markus Meier AWK	08.03.2016
[101] Note au Secrétaire d'État: cybercriminalité: positionnement en matière de politique extérieure et champs d'action de la Suisse	Département fédéral des affaires étrangères DFAE	10.02.2015
[102] Note au Secrétaire d'État: cybersécurité: champs d'action de la Suisse pour la promotion de normes étatiques de bonne conduite	Département fédéral des affaires étrangères DFAE	12.08.2015
[103] Concept pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques au sein du DFAE		20.12.2013
[104] Aperçu des activités entreprises en 2014 en matière de politique extérieure relative au cyberespace	Département fédéral des affaires étrangères DFAE	09.04.2015
[105] État de la mise en œuvre de la mesure 6 de la SNPC: vue d'ensemble des infractions et coordination des cas intercantonaux complexes	Département fédéral de justice et police DFJP	20.08.2015
[106] Affaires de politique extérieure relatives au cyberespace: aperçu des activités entreprises en 2015	Département fédéral des affaires étrangères DFAE	04.01.2016
[107] A Geneva Declaration for Cyberspace	Stein Schjolberg, Norvège	janvier 2016
[108] Mandat du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	21.03.2014
[109] Note au Secrétaire d'État: cybercriminalité: positionnement en matière de politique extérieure et champs d'action de la Suisse	Département fédéral des affaires étrangères DFAE	10.02.2015
[110] Note au Secrétaire d'État: cybersécurité: champs d'action de la Suisse pour la promotion de normes étatiques de bonne conduite	Département fédéral des affaires étrangères DFAE	12.08.2015
[111] Note au Secrétaire d'État: gouvernance d'Internet: bases de la politique extérieure et champs d'action du DFAE	Département fédéral des affaires étrangères DFAE	04.03.2015
[112] Assemblée constituante du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	25.10.2013
[113] Procès-verbal du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	21.03.2014
[114] Procès-verbal du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	18.12.2014
[115] Procès-verbal du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	30.06.2015
[116] Procès-verbal du groupe spécialisé Cyber International (GS-CI)	Département fédéral des affaires étrangères DFAE	25.09.2015
Gestion des crises (mesures 13 et 15)		

Titre	Auteur / éditeur	Date
[117] Concept pour la gestion nationale des crises ayant des aspects cybernétiques basé sur la mesure 15 de la SNPC		16.04.2016
[118] Résultats de l'évaluation MELANI	Manuel Suter, OC SNPC	07.01.2016
[119] Questionnaire de l'évaluation MELANI	Manuel Suter, OC SNPC	
[120] Résultats de l'évaluation MELANI	OC SNPC	mars 2016
[121] Rapport sur la première séance de coordination du groupe spécialisé Cyber	Dario Walder, RNS	25.03.2013
[122] Présentation sur la troisième cyber-landsgemeinde		23.04.2015
[123] Séminaire stratégique du 11 juin 2015, rapport succinct		11.06.2015
[124] Mise en œuvre de la mesure 15 de la SNPC: concept pour la gestion des crises cybernétiques	Stéphane Derron	26.09.2013
[125] Mise en œuvre de la mesure 15 de la SNPC: concept pour la gestion des crises cybernétiques (au niveau fédéral)	Stéphane Derron	17.02.2014
[126] Programme de la quatrième cyber-landsgemeinde		06.04.2016
Bases légales (mesure 16)		
[127] Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC): mesure 16 «Nécessité de modifier les bases juridiques» étape 16.1: aperçu de la nécessité urgente de légiférer et de procéder à des révisions dans le domaine de la cybersécurité	Stefanie Frey, OC SNPC	30.06.2014
Interface RNS		
[128] Feuille d'information concernant le groupe spécialisé et les groupes de travail du RNS dédiés au cyberespace	Réseau national de sécurité RNS	25.02.2016
[129] RNS: la SNPC et les interactions avec les cantons	Réseau national de sécurité RNS	20.05.2016
[130] Traitement des informations données par MELANI	Réseau national de sécurité RNS	22.10.2015

C. Résumé des questionnaires issus des entretiens

Tous les questionnaires traités avec les partenaires au cours des entretiens sont réunis dans une annexe séparée. Cette annexe est classifiée «CONFIDENTIEL». Elle peut être consultée auprès de l'OC SNPC.