Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Berne, le 27 novembre 2019

Rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques

Rapport du Conseil fédéral en réponse aux postulats 16.4073 Golay du 15 décembre 2016 et 18.3003 CPS-CN du 22 janvier 2018 et à la motion 17.3508 Eder du 15 juin 2017

Table des matières

1 Introduction

La cybersécurité a pris une importance considérable à tous les niveaux ces dernières années. Elle joue un rôle grandissant dans la politique étrangère et de sécurité nationale et internationale, c'est un facteur de plus en plus important pour la place économique suisse, et une personne sur sept a déjà subi une cyberattaque directe[1].
Face à cette tendance, le Conseil fédéral a pris plusieurs décisions pour renforcer les activités de la Confédération dans le domaine de la cybersécurité. En avril 2018, il a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022; en juillet 2018, il a pris des décisions de principe concernant l'organisation de la Confédération dans le domaine des cyberrisques, des décisions qui se sont concrétisées en janvier 2019 par la création d'un Centre de compétences pour la cybersécurité placé sous la conduite du délégué à la cybersécurité (une fonction également créée); en mai 2019, enfin, il a adopté le plan de mise en œuvre et approuvé la première tranche de financement des ressources nécessaires.
En prenant ces décisions, le Conseil fédéral a aussi donné suite à plusieurs interventions parlementaires. Le présent rapport destiné au Parlement présente l'état de la mise en œuvre de la motion 17.3508 Eder, et répond aux questions soulevées par le postulat 16.4073, déposé par Roger Golay, et par le postulat 18.3003, déposé par la Commission de la politique de sécurité du Conseil national (CPS-CN).

1.1 Mandat

Les postulats 16.4073 Golay et 18.3003 CPS-CN demandent que le Conseil fédéral publie un rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). La motion 17.3508 Eder charge le Conseil fédéral de créer un centre de compétences fédéral pour la cybersécurité. Les interventions parlementaires transmises au Conseil fédéral demandent que la Confédération prenne les mesures suivantes:

Postulat 16.4073 Golay «Cyberrisques. Pour une protection globale, indépendante et efficace»: Le Conseil fédéral est prié de remettre un rapport sur l'application de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), dont les effets ne sont pas perceptibles pour la population et l'économie. Le rapport traitera notamment des questions et risques relatifs à la division entre le Département fédéral des finances (DFF) et le Département fédéral de la défense, de la protection de la population et des sports (DDPS), de la compétence dans ce domaine, de la conduite de crises majeures et d'ampleur nationale, des questions et risques relatifs à une dépendance à l'égard de prestataires à l'étranger ou en mains étrangères, du maintien d'un savoir-faire de pointe en Suisse ainsi que de l'intensification des collaborations entre le monde académique, l'industrie et la Confédération.

Postulat 18.3003 CPS-CN «Stratégie globale claire de la Confédération pour la protection contre les cyberrisques»: Le Conseil fédéral est chargé de présenter, d'ici à la fin 2018, un concept global clair de protection et de défense du cyberespace civil et militaire. Ce faisant, il tiendra compte des travaux menés actuellement dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). Ce concept global, qui ne doit pas consister en une simple fusion des concepts (plans d'action) que les différents départements ont déjà élaborés ou sont en train d'établir (un plus un doit donner davantage que deux), contiendra au moins les éléments suivants:
- une définition claire de la mission de l'armée dans le domaine de la cyberdéfense;
- une définition claire de la mission des autorités civiles compétentes en matière de cyberdéfense;

[1] Étude «Sicherheit im Internet – Repräsentative der Deutsch- und Westschweizer Bevölkerung», gfs-zürich, 2019.

- une délimitation et une visualisation des compétences (organigramme avec tous les organes impliqués dans le domaine de la protection contre les cyberrisques, y c. le cahier des charges de la Confédération) découlant des points précédents;
- un modèle de financement (englobant les éventuelles acquisitions et les coûts d’exploitation subséquents) et un plan de recrutement de personnel réaliste pour la défense et les autorités civiles compétentes en matière de cyberdéfense;
- une comparaison internationale – entre la Suisse et des pays pertinents en termes de structure, de volume et d’approche – en ce qui concerne les ressources et les moyens financiers alloués au domaine cybernétique, à la fois sur les plans militaires et civils.

Le rapport mentionnera a) l’appui subsidiaire apporté aux autorités civiles et b) les éventuelles situations de crise et de défense dans lesquelles le Conseil fédéral engage certaines unités de l’armée comme réserve stratégique.

Le Conseil fédéral est chargé de présenter un concept global clair de protection et de défense du cyberespace civil et militaire. Le concept global définira clairement les mandats de l’armée et des autorités civiles, qui seront réunis dans un organigramme. Il clarifiera également la question du financement et du recrutement du personnel, ainsi que la façon dont l’armée peut fournir un appui subsidiaire aux autorités civiles et son rôle dans les situations de défense. Enfin, une comparaison internationale exposera comment des pays comparables à la Suisse protègent leur cyberespace civil et militaire.

Motion 17.3508 Eder «Création d’un centre de compétence fédéral pour la cybersécurité»: Dans le cadre de la révision de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), le Conseil fédéral est chargé de prendre les mesures nécessaires en vue de créer un centre de compétence fédéral pour la cybersécurité. Cette entité supradépartementale aura la tâche de renforcer et de coordonner au niveau fédéral les compétences nécessaires pour garantir la cybersécurité. Elle pourra en particulier donner des instructions aux différents offices. Elle collaborera avec des représentants des milieux académiques (universités, HES), avec les entreprises actives dans le domaine de l’informatique et avec les exploitants de grosses infrastructures (par ex. énergie et transport).

1.2 Contexte

Les trois interventions parlementaires ont été transmises avant l’adoption de la SNPC 2018-2022, le 18 avril 2018. La première SNPC 2012-2017, qui était alors en vigueur, ne traitait explicitement que des mesures des acteurs civils et ne formulait aucune directive dans le domaine de la cyberdéfense. L’évaluation de la SNPC 2012-2017 a mis en lumière les problèmes de délimitation causés par cette séparation. Pour y répondre, le Conseil fédéral a décidé d’intégrer le domaine de la cyberdéfense dans la SNPC et d’en faire la stratégie globale pour l’ensemble des activités de protection de la Suisse contre les cyberrisques.

Après avoir adopté la SNPC en avril 2018, le Conseil fédéral a pris d’autres décisions pour satisfaire aux exigences formulées dans les postulats. Le tableau 1 ci-dessous synthétise les décisions du Conseil fédéral qui se rapportent aux postulats:

Date	Décision du Conseil fédéral	Contenu
18 avril 2018	Adoption de la SNPC 2018-2022	Adoption de la SNPC, qui contient 29 mesures dans dix champs d'action. Sur le plan organisationnel, la SNPC distingue trois domaines: la cybersécurité, la cyberdéfense et la poursuite pénale.
4 juillet 2018	Décisions de principe concernant la future organisation de la Confédération dans le domaine des cyberrisques	Détermination des entités essentielles de l'organisation: • Délégation Cyber du Conseil fédéral (DFF, DDPS, DFJP) • Groupe Cyber assurant la coordination entre le DFF, le DDPS et le DFJP (avec la participation des autres départements et des cantons si nécessaire) • Centre de compétences pour la cybersécurité au sein du DFF, sous la conduite d'un délégué de la Confédération à la cybersécurité
30 janvier 2019	Adoption de l'organisation de la Confédération dans le domaine des cyberrisques	Adoption de l'organisation élaborée conformément aux décisions de principe
30 janvier 2019	Ordonnance sur la cyberdéfense militaire	L'ordonnance définit les compétences et les responsabilités de la cyberdéfense militaire.
15 mai 2019	Adoption du plan de mise en œuvre de la SNPC 2018-2022	Définition des compétences et du calendrier de mise en œuvre de la SNPC. Création de 24 postes au total à partir de 2020.

Tableau 1 Décisions prises par le Conseil fédéral depuis 2018 en matière de cybersécurité

Grâce aux décisions qui ont été prises, l'organisation de la Confédération est aujourd'hui bien mieux structurée qu'au moment de la transmission des postulats. Le Conseil fédéral est toutefois conscient que de nouvelles mesures seront nécessaires pour que l'organisation ait l'impact escompté. L'évolution dynamique des cyberrisques nécessite des examens réguliers pour s'assurer que les structures créées et les moyens disponibles sont à la hauteur de ces défis. Les organes créés, notamment la Délégation Cyber du Conseil fédéral et le Centre de compétences pour la cybersécurité, garantissent que les analyses nécessaires seront effectuées.

1.3 Structure du rapport

Le rapport est structuré ainsi:

- Le chapitre «Plan global de protection de la Suisse contre les cyberrisques» présente et illustre la structure organisationnelle de la Confédération, les tâches des différents comités et organisations, et les compétences dans les différents domaines, conformément au plan de mise en œuvre de la stratégie. Il détaille également la collaboration entre la Confédération et les cantons, les milieux économiques et les hautes écoles.
- Le chapitre «Répartition des tâches et interfaces entre les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale» traite spécifiquement de la répartition des tâches entre les départements, de la collaboration entre les acteurs civils et militaires, ainsi que des principes qui régissent la gestion des crises et l'appui subsidiaire apporté aux autorités civiles.
- Le chapitre «Réduction de la dépendance à l'égard des pays étrangers grâce au renforcement des compétences en Suisse» décrit les mesures qui visent à réduire cette dépendance par le développement de compétences en Suisse.

- Le chapitre «Financement et recrutement du personnel» détaille les moyens alloués à la mise en œuvre de la SNPC.
- Le dernier chapitre, «Comparaison internationale», présente des informations sur l’organisation et les structures d’autres pays dans le domaine de la cybersécurité, sur la base d’une étude de l’EPF de Zurich, et compare l’approche de la Suisse et ces structures.

2 Plan global de protection de la Suisse contre les cyberrisques

Avec l’adoption de la SNPC 2018-2022, les décisions concernant la structure organisationnelle de la Confédération et l’adoption du plan de mise en œuvre, tous les éléments du plan global de protection de la Suisse contre les cyberrisques sont connus depuis le printemps 2019. La SNPC énonce les objectifs stratégiques en matière de protection contre les cyberrisques dans tous les domaines (cybersécurité, cyberdéfense et poursuite pénale), la structure organisationnelle de la Confédération précise la répartition fondamentale des tâches et détermine sous quelle forme la Confédération entend collaborer avec les cantons, les milieux économiques et les hautes écoles, tandis que le plan de mise en œuvre de la SNPC définit les compétences des services concernés.

2.1 Objectifs stratégiques de la SNPC 2018-2022

L’objectif suprême de la SNPC est de contribuer à ce que, tout en saisissant les chances offertes par le numérique, la Suisse soit protégée de façon appropriée contre les cyberrisques, et résiliente en cas de cyberincident. À partir de cette vision, la SNPC a identifié sept objectifs stratégiques et formulé au total, pour les atteindre, 29 mesures à prendre dans dix champs d’action. La figure 1 représente synthétiquement le contenu de la SNPC:

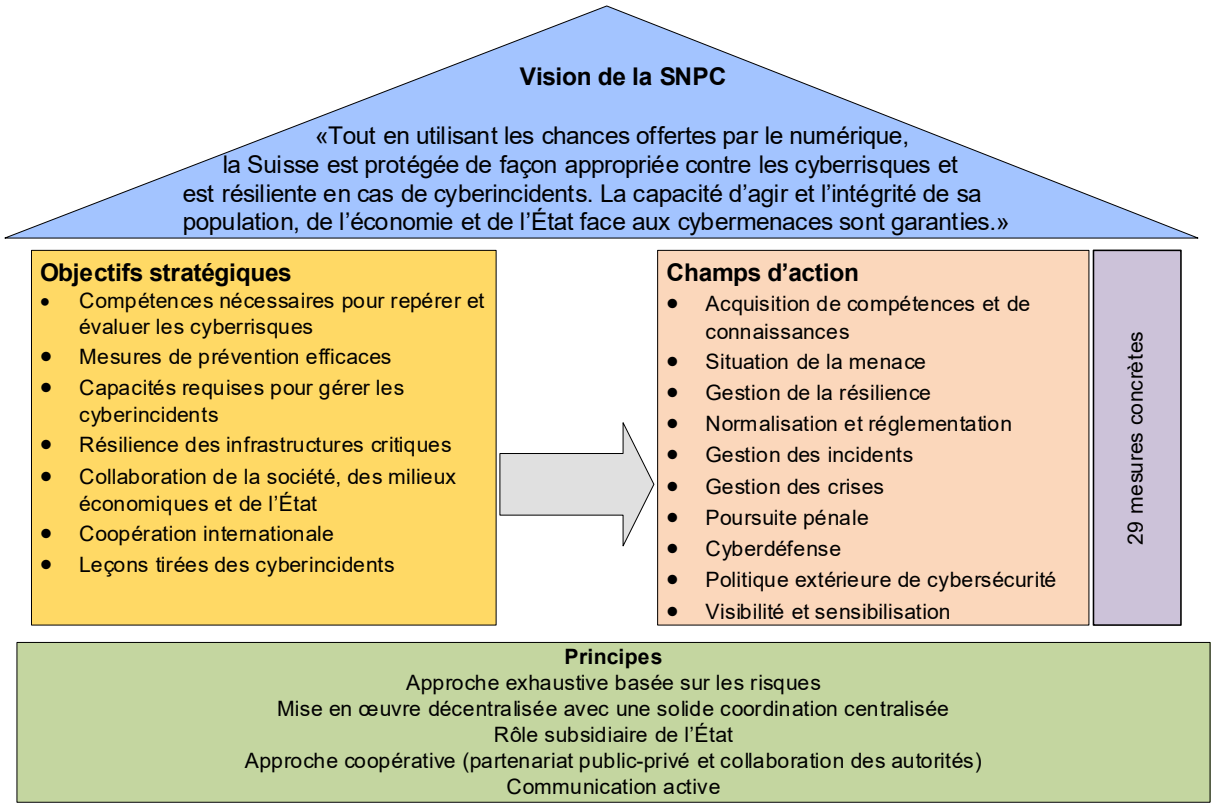

Figure 1 Aperçu du contenu de la SNPC

2.2 Organisation de la mise en œuvre de la SNPC

La SNPC se contente d'énoncer des objectifs et des mesures stratégiques. Elle ne traite pas des questions d'organisation. Après l'adoption de la stratégie, le Conseil fédéral a donc chargé les départements d'élaborer une structure organisationnelle qui tienne compte de la transversalité des tâches dans le domaine des cyberrisques, tout en garantissant que la mise en œuvre soit conduite de manière centralisée et coordonnée et en favorisant la collaboration entre les cantons, les milieux économiques et les hautes écoles. Le Conseil fédéral a défini la structure organisationnelle dans ses décisions du 30 janvier 2019.

2.2.1 Organisation supradépartementale de la Confédération

L'administration fédérale est active dans trois domaines pour protéger le pays face aux cyberrisques:

- Cybersécurité: ce domaine comprend l'ensemble des mesures ayant pour objectif la prévention, la gestion des incidents et l'augmentation de la résilience face aux cyberrisques. La Confédération prend les mesures nécessaires pour renforcer sa propre cybersécurité et participe à l'amélioration de la cybersécurité des entreprises et de la société conformément au principe de subsidiarité, tout en accordant une attention particulière au rôle central que jouent les infrastructures critiques. À ces mesures s'ajoute la promotion de la collaboration internationale dans le domaine de la cybersécurité.
- Cyberdéfense: ce domaine comprend l'ensemble des mesures prises par les services de renseignement civils et l'armée et servant à protéger les systèmes critiques, à se défendre contre des attaques dans le cyberespace, à garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace; enfin, elles ont pour but de développer les capacités et les compétences de l'armée afin que celle-ci puisse apporter subsidiairement un appui aux autorités civiles. Ce domaine renferme notamment des mesures actives pour identifier les menaces et les attaquants ainsi que pour entraver et bloquer les attaques.
- Poursuite pénale de la cybercriminalité: ce domaine comprend l'ensemble des mesures de la

police et des ministères publics de la Confédération et des cantons pour lutter contre la cybercriminalité.

Le 30 janvier 2019, le Conseil fédéral a défini l'organisation générale de la Confédération dans le domaine des cyberrisques sur la base de cette répartition des tâches. La figure 2 montre les éléments essentiels de cette organisation axée sur la mise en œuvre de la SNPC.

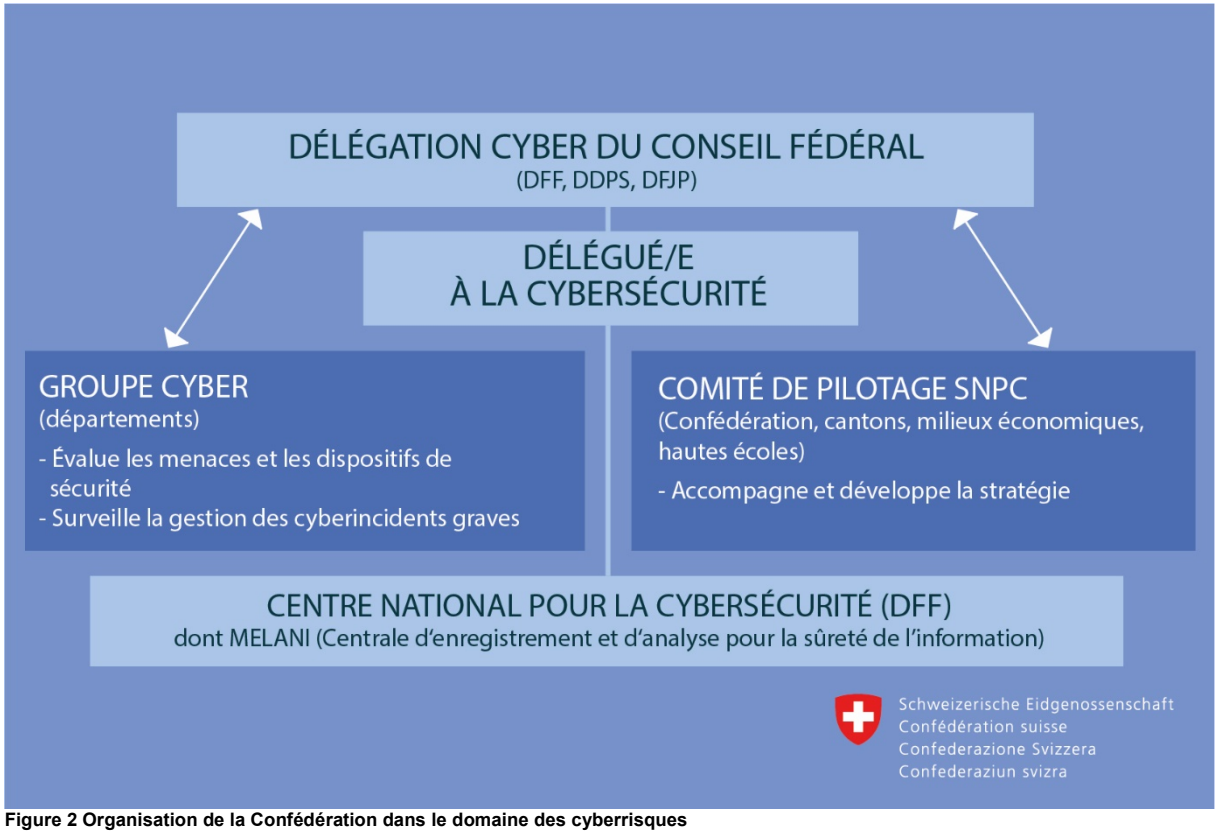

Figure 2 Organisation de la Confédération dans le domaine des cyberrisques

La répartition des tâches entre ces comités ou fonctions créés dans le cadre de la SNPC 2018-2022 a été définie de la façon suivante:

- La **Délégation Cyber du Conseil fédéral**, composée des chefs du Département fédéral des finances (DFF), du Département fédéral de justice et police (DFJP) et du Département fédéral de la défense, de la protection de la population et des sports (DDPS), a pour tâche de surveiller la mise en œuvre de la SNPC.
- Le **délégué de la Confédération à la cybersécurité** exerce à l'échelon de la Confédération la direction stratégique de la cybersécurité, préside les comités interdépartementaux créés par la Confédération (à l'exception de la Délégation Cyber), et représente la Confédération dans d'autres comités.
- Le **Groupe Cyber** renforce la coordination entre les trois domaines de la sécurité, de la défense et de la poursuite pénale, veille à leur évaluation conjointe de la menace et surveille la gestion par les services fédéraux des incidents graves et impliquant plusieurs départements.
- Le **comité de pilotage de la SNPC** assure la mise en œuvre coordonnée et ciblée des mesures de la SNPC et formule des propositions visant à son développement ultérieur.

2.2.2 Centre de compétences pour la cybersécurité

Le centre de compétences assume, sous la conduite du délégué de la Confédération à la cybersécurité, les quatre tâches suivantes: la direction stratégique de la cybersécurité de la Confédération, la direction du guichet unique national, du service spécialisé de sécurité informatique

de la Confédération et du pool de compétences pour la cybersécurité. La figure 3 précise les tâches concrètes dans ces quatre domaines. Pour accomplir ses tâches, le centre de compétences travaille avec tous les services concernés en Suisse et échange des informations avec des services similaires (centres nationaux pour la cybersécurité) et avec des organisations spécialisées internationales.

L’organisation du centre de compétences doit également tenir compte des exigences de centralisation, tout en s’appuyant sur les compétences et les capacités existantes lorsque cela est possible. Les trois mesures suivantes visent à répondre à ces exigences:

1. Au sein du centre de compétences, il faut donner suffisamment de poids au bureau et au guichet national pour que le centre de compétences produise, par une communication active et des prestations étendues pour les entreprises et la population, un maximum d’effets à l’extérieur et soit réellement perçu comme le guichet unique.
2. Il convient de créer, au sein du centre de compétences, un pool d’experts qui aidera les offices compétents à mettre en œuvre les mesures dans le domaine de la cybersécurité. Il se tiendra à la disposition des offices spécialisés des différents secteurs, notamment, et son expertise en matière de cybersécurité viendra compléter les connaissances sectorielles et les compétences juridiques en fonction des besoins et des projets.
3. Enfin, le centre de compétences doit travailler en étroite collaboration avec les services disposant de l’expertise et des capacités nécessaires pour réaliser certaines tâches dans le domaine de la cybersécurité. Dans le cadre de cette collaboration, on évitera de créer des redondances entre les compétences du centre et celles des autres services, tout en veillant à ce que les services impliqués réalisent leurs tâches de façon coordonnée et en concertation étroite avec le centre de compétences.

Sur la base de ces considérations, le DFF propose d’organiser le centre de compétences de la manière suivante (cf. figure 3):

Rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques

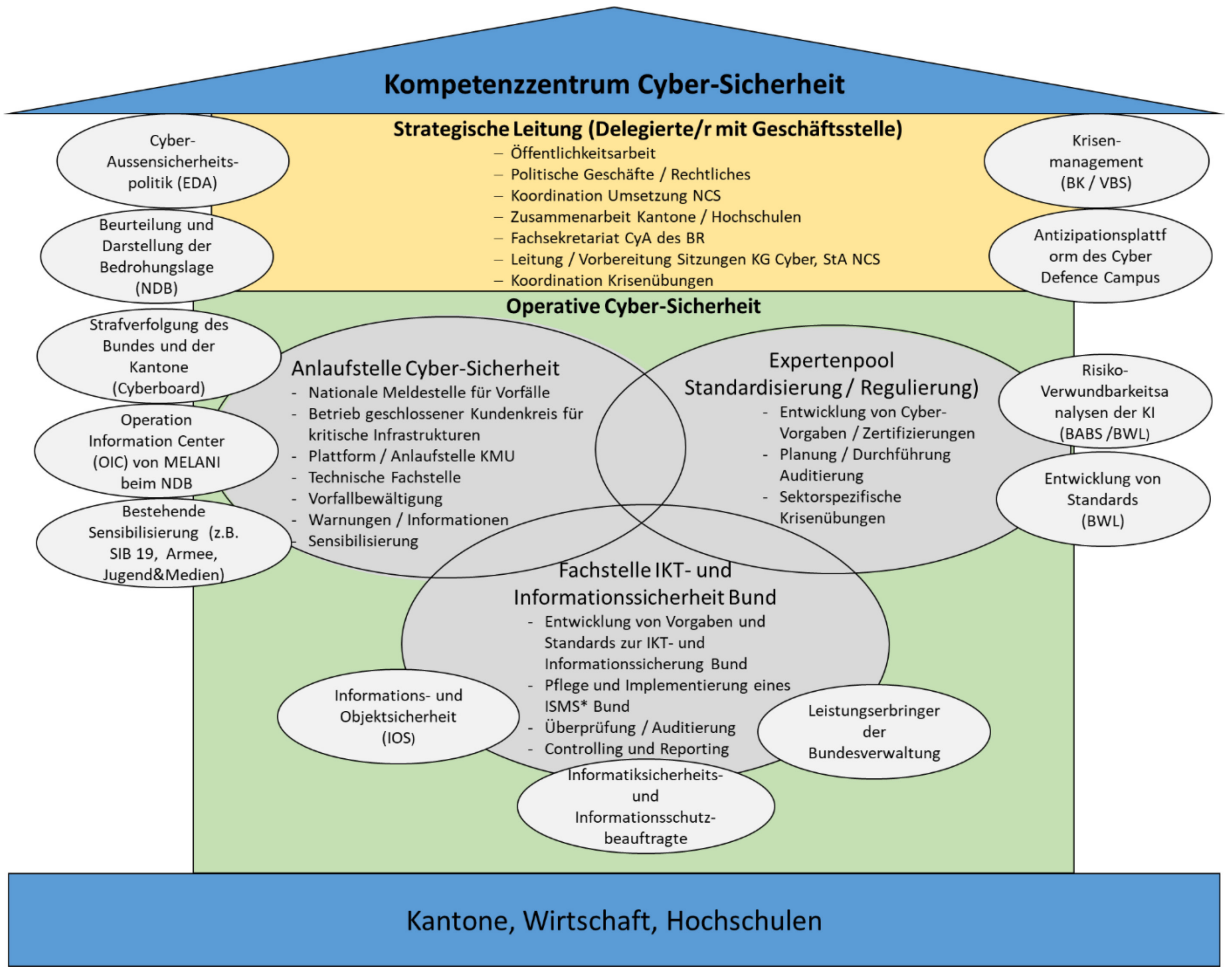

Figure 3 **Organisation et tâches du Centre de compétences pour la cybersécurité, interfaces avec les organisations partenaires de l'administration fédérale**

2.2.3 Collaboration entre la Confédération, les cantons, les milieux économiques et les hautes écoles

La collaboration entre la Confédération, les cantons, les milieux économiques et les hautes écoles doit être garantie à tous les échelons. Concrètement, elle sera assurée par les comités et les mécanismes suivants:

- **Collaboration sur le plan politico-stratégique par une représentation des cantons au sein de la Délégation Cyber du Conseil fédéral**: La collaboration sur le plan politico-stratégique revêt une importance de premier plan, notamment pour la répartition des tâches entre les cantons et la Confédération. Il est crucial pour la mise en œuvre de la SNPC de définir clairement quel niveau étatique assume quelle tâche. Pour débattre de ces questions, la Délégation Cyber échange régulièrement avec les conférences des gouvernements cantonaux pertinentes, et notamment avec la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP).
- **Gestion commune des projets par le comité de pilotage de la SNPC:** Comme la SNPC a besoin, en tant que projet commun, du soutien de toutes les parties prenantes, cette collaboration directe n'est pas suffisante et il a fallu instituer un comité servant à la prise de décision collective. Cette fonction revient au comité de pilotage de la SNPC, où siègent des représentants des principaux partenaires de sa mise en œuvre.
- **Mise en œuvre collective des mesures de la SNPC:** La coopération, pour la mise en œuvre des mesures, des diverses unités engagées sur le plan opérationnel constitue la forme de collaboration la plus directe. Elle se base sur les compétences et les participations définies

dans le plan de mise en œuvre de la SNCP, mais peut être facilement adaptée et élargie. Le Centre de compétences pour la cybersécurité, placé sous la conduite stratégique du délégué de la Confédération à la cybersécurité, sert de guichet unique national pour tous les services s'occupant de cyberrisques.

3 Répartition des tâches et interfaces entre les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale

La distinction établie par la SNPC entre les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale permet de différencier plus clairement les tâches des divers domaines. Le plan de mise en œuvre définit les compétences précises pour la mise en œuvre des mesures de la SNPC. L'organisation de la gestion des crises et l'appui subsidiaire fourni par l'armée aux autorités civiles sont présentés séparément dans ce chapitre.

3.1 Répartition des tâches dans le plan de mise en œuvre

Le plan de mise en œuvre de la SNPC 2018-2022 définit les tâches et les compétences des unités organisationnelles concernées de l'administration fédérale, et précise aussi les projets réalisés par des tiers (cantons, milieux économiques, hautes écoles) dans le cadre de la SNPC. Sur la base du plan de mise en œuvre et des projets qui y sont présentés, la répartition des tâches au sein de l'administration fédérale peut être représentée de la manière suivante:

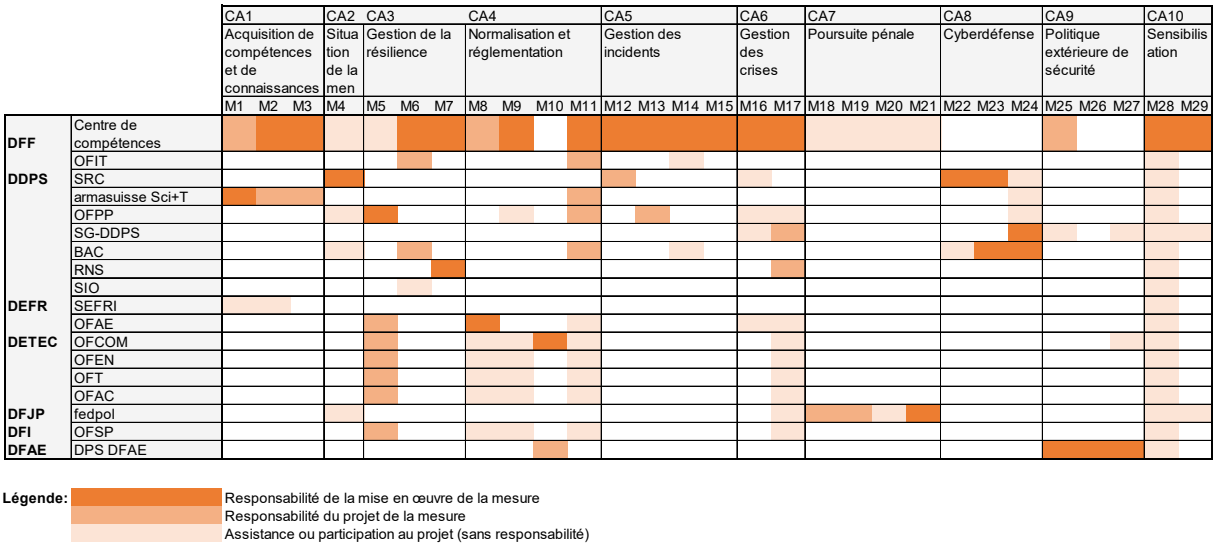

Figure 4 Répartition des tâches pour la mise en œuvre de la SNPC (conformément au plan de mise en œuvre)

La figure montre que le Centre de compétences pour la cybersécurité participe à la mise en œuvre dans tous les champs d'action, et qu'il est responsable d'au moins une mesure dans six des dix champs d'action. Cela étant, on observe que les compétences et les capacités des unités administratives actives dans les différents champs d'actions restent sollicitées. Le plan de mise en œuvre réalise ainsi un équilibre entre la centralisation exigée par le Parlement et les milieux économiques et l'utilisation de toutes les capacités et compétences décentralisées, y compris juridiques, dont dispose l'administration fédérale.

3.2 Gestion des crises

Les cyberincidents peuvent être lourds de conséquences, et s'aggraver au point d'exiger une gestion de crise au niveau national. Les processus de conduite des décideurs ont une importance de premier plan dans la gestion des crises. Ils sont définis dans les instructions du 21 juin 2019 concernant la gestion des crises dans l'administration fédérale[2]. Ces instructions étant valables dans tous les scénarios, elles s'appliquent également aux crises résultant de cyberincidents.
À dessein, les instructions concernant la gestion des crises ne définissent pas les compétences a priori. Il incombe au Conseil fédéral, en tant qu'organe suprême de direction, de déterminer les états-majors chargés de la gestion des crises. Selon la gravité de la crise et les personnes affectées, le Conseil fédéral recourra aux états-majors (interdépartementaux) existants, par exemple l'État-major fédéral Protection de la population ou l'État-major Prises d'otage et chantage (unité d'intervention de fedpol). Cette souplesse est indispensable: c'est le seul moyen de garantir que la responsabilité de gérer une crise sera attribuée au service le plus compétent.
En cas de crises provoquées par des cyberincidents, il est crucial pour la prise de décisions de disposer d'une vue d'ensemble homogène et exhaustive de la situation. Cette responsabilité incombe aux équipes spécialisées du Service de renseignement de la Confédération et à l'équipe d'analyse technique du Centre de compétences pour la cybersécurité. En collaboration avec des experts d'autres services, cette équipe épaule les états-majors et leur offre son expertise en cas de crise.

3.3 Appui subsidiaire de l'armée aux autorités civiles

Les art. 1 et 68 à 75 de la loi sur l'armée définissent les conditions dans lesquelles l'armée apporte son appui aux autorités civiles. Un appui de ce genre est possible pour faire face à une menace grave pesant sur la sécurité intérieure ou à d'autres situations extraordinaires, lorsque les moyens des autorités civiles deviennent insuffisants. Les autorités civiles doivent demander cet appui, que le Conseil fédéral doit en outre approuver.
Le développement des capacités et des compétences de l'armée en matière de cybersécurité rend possibles des engagements subsidiaires de l'armée dans ce domaine. La mesure 24 de la SNPC charge l'armée de former ses cadres et membres en conséquence et de définir avec les autorités civiles de la Confédération et des cantons les conditions-cadres de son soutien subsidiaire en cas de cyberincidents, les tâches dont elle peut assumer la responsabilité et le déroulement concret d'une intervention.

4 Réduction de la dépendance à l'égard des pays étrangers grâce au renforcement des compétences en Suisse

La dépendance à l'égard de prestataires et de fabricants de logiciels et de matériel étrangers ne peut être totalement supprimée par des mesures économiquement supportables et techniquement réalisables. Il n'en demeure pas moins primordial d'identifier ces dépendances, d'analyser minutieusement les risques qui en découlent et de prendre des mesures pour réduire ces risques. Cela implique de prendre des mesures ciblées pour acquérir des compétences et des connaissances en Suisse. La SNPC définit ces mesures dans le champ d'action «Acquisition de compétences et de connaissances». Dans ce champ d'action, la mesure 3 de la SNPC a pour objectif la création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité. Cette mesure sera mise en œuvre grâce aux projets suivants:

[2] https://www.admin.ch/opc/fr/federal-gazette/2019/4415.pdf

- **Développement d'un «écosystème de la cybersécurité»:** Le Centre de compétences pour la cybersécurité fait office d'intermédiaire entre les milieux économiques, les hautes écoles, les autorités et les centres d'innovation existants, afin de promouvoir un écosystème de la cybersécurité novateur en Suisse. Il collabore à cet effet avec le Campus cyberdéfense d'armasuisse S+T, qui représente le pôle de compétences pour la collaboration entre les hautes écoles et les milieux économiques dans le domaine de la cyberdéfense.
- **Moyens d'encouragement:** Des moyens d'encouragement destinés aux projets d'innovation des hautes écoles, des associations et des entreprises dans le domaine de la cybersécurité sont identifiés et indiqués comme tels. Il s'agit de vérifier quels instruments d'encouragement (par ex. réseaux thématiques nationaux, projets d'innovation R&D, programme d'encouragement ad hoc) sont les plus efficaces pour promouvoir l'innovation dans le domaine de la cybersécurité.
- **Développement de centres d'innovation:** On examine les possibilités de former autour du Centre de compétences pour la cybersécurité un pôle de cybersécurité (incluant le centre de recherche de l'EPFZ, avec la participation de l'écosystème de la cybersécurité et du Campus cyberdéfense, ainsi que du réseau de recherche). L'innovation en matière de cybersécurité sera spécialement encouragée dans ce réseau, dans les centres d'innovation régionaux existants ou nouvellement créés.

La Confédération travaille en étroite collaboration avec les hautes écoles, les milieux économiques et les cantons pour mettre en œuvre ces projets.

5 Financement et recrutement du personnel

Les structures et les ressources (financières et humaines) existantes sont utilisées autant que possible pour mettre en œuvre les mesures adoptées. Des ressources supplémentaires sont toutefois nécessaires car la SNPC 2018-2022 élargit l'éventail des tâches des unités administratives existantes dans de nombreux domaines. Cela vaut notamment pour le Centre de compétences pour la cybersécurité, qui, même s'il utilisera les ressources existantes de MELANI, verra son éventail de tâches être considérablement élargi du fait de l'appui offert à la population et aux PME en matière de protection contre les cyberrisques.

Les 30 postes qui avaient été créés en 2013 pour les besoins de la première SNPC, avant d'être reconduits pour une durée indéterminée en 2017, ne suffisent pas pour faire face aux nouvelles tâches plus intensives qui sont décrites dans le plan de mise en œuvre de la SNPC 2018-2022. Sur la base du plan de mise en œuvre, les services fédéraux concernés ont identifié un besoin supplémentaire de 67 postes au total. Ce besoin sera examiné de manière approfondie d'ici au 2^{e} trimestre 2020 et réduit dans la mesure du possible. Il s'agira notamment d'identifier les ressources existantes qui pourront être davantage utilisées et les synergies qui pourront être générées.

Les mesures prioritaires doivent toutefois pouvoir être mises en œuvre sans attendre. Aussi le Conseil fédéral a-t-il annoncé, le 15 mai 2019, la création de 24 postes supplémentaires au total afin de permettre la mise en œuvre de la SNPC. En plus des ressources humaines, les moyens financiers sont également augmentés. En effet, le Centre de compétences pour la cybersécurité bénéficiera d'une dotation annuelle supplémentaire d'un million de francs pour mettre en œuvre la SNPC, établir et exploiter le centre de compétences. Le délégué de la Confédération à la cybersécurité est entré en fonction début août.

L'accroissement progressif des ressources permet d'atténuer les difficultés de recrutement. Il permet de surveiller en continu les besoins de ressources avérés, sans que cela ralentisse des travaux urgents.

6 Comparaison internationale

Les comparaisons portant sur la cybersécurité civile et militaire de différents États peuvent être très instructives, mais doivent être réalisées avec la prudence qui s’impose. Tous les pays créent des dispositifs adaptés à leurs systèmes politiques respectifs. Il existe par exemple des différences de compétence importantes aux différents échelons de l’État, et la question de savoir quelles sont les tâches que l’État doit assumer pour se protéger contre les cyberrisques appelle des réponses différentes selon la culture stratégique et la conception du rôle de l’État des différents pays. Les comparaisons doivent tenir compte de ces différences fondamentales. L’exercice est d’autant plus difficile dans le domaine de la cybersécurité puisque les gouvernements sont peu enclins à communiquer des renseignements sur leurs ressources financières et humaines.
Néanmoins, pour évaluer l’approche de la Confédération dans un contexte international plus large, le DFF a demandé au Center for Security Studies de l’EPF de Zurich de comparer la Suisse avec l’Allemagne, la Finlande, la France, Israël, l’Italie et les Pays-Bas. Il ressort de cette étude que de nombreux pays disposent de structures similaires à celles de la Suisse dans le domaine de la cybersécurité, et que le développement de ces structures est encore inachevé dans nombre de pays. Les défis en matière de cybersécurité, de même que l’approche utilisée pour y faire face, ne diffèrent pas sensiblement de ceux de la Suisse. Aucun des pays étudiés n’a mis en place une organisation unique pour réaliser tous les travaux liés aux cyberrisques. Globalement, la répartition des tâches varie quelque peu entre les services de défense, de sécurité civile et de poursuite pénale des États. Aucun des pays étudiés n’a confié à son armée la responsabilité d’assurer la protection contre les cyberrisques.