EBP

econcept
Forschung / Beratung / Evaluation

Centre national pour la cybersécurité (NCSC)

Évaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022

Rapport final
28 mars 2022

Élaboré par
econcept AG, Gerechtigkeitsgasse 20, 8002 Zurich
www.econcept.ch / + 41 44 286 75 75

EBP Suisse SA, Mühlebachstrasse 11, 8032 Zurich
www.ebp.ch / +41 44 395 16 16

Auteurs
Benjamin Buser, Dr. sc. ETH, dipl. Geogr., Executive MBA HSG
Jasmin Gisiger, MA ETH UZH in Comparative and International Studies
Christof Egli, Dipl. Ing. EPF Zurich, CAS en protection des données et sécurité de l'information

Table des matières

Liste des abréviations

Abréviation	Signification
CYD	*Cyber-Defence Campus* (Campus cyberdéfense)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
EPF Zurich	École polytechnique fédérale de Zurich
EPFL	École polytechnique fédérale de Lausanne
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information -> MELANI a été intégrée dans le Centre national pour la cybersécurité (voir plus loin)
NCSC	Centre national pour la cybersécurité
NEDIK	Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique
NTC	*Nationales Testinstitut für Cyber-Sicherheit* (institut national de test pour la cybersécurité)
OCDE	Organisation de coopération et de développement économiques
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCOM	Office fédéral de la communication
OFEN	Office fédéral de l'énergie
OFPP	Office fédéral de la protection de la population
OPCy	Ordonnance sur les cyberrisques
PME	Petites et moyennes entreprises
RDS	Réseau de données sécurisé
RS	Recueil systématique du droit fédéral
SNPC	Stratégie nationale de protection de la Suisse contre les cyberrisques
SRC	Service de renseignement de la Confédération
SSCC	*Swiss Support Center for Cybersecurity*
TI	Technologies de l'information
TNI	Transformation numérique et gouvernance de l'informatique
UPIC	Unité de pilotage informatique de la Confédération -> l'UPIC a été intégrée dans le secteur TNI (voir plus haut)

Résumé

Mandat d'évaluation de l'efficacité

La transformation numérique de la Suisse comporte aussi bien des chances que des risques pour l'État, le monde politique, la société et l'économie. En réponse aux menaces potentielles, le Conseil fédéral a conçu dès 2012 la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC). À l'occasion de sa deuxième période de mise en œuvre, qui couvre les années 2018 à 2022, le Conseil fédéral a réagi aux nouvelles menaces en adoptant des mesures supplémentaires pour quatre groupes cibles. La nouvelle stratégie comporte sept objectifs stratégiques, axés sur les capacités de prévention et de gestion des cyberincidents et sur la collaboration entre les acteurs étatiques, civils ou militaires. Son plan de mise en œuvre est formé de dix champs d'action et prévoit toute une série de mesures avec des projets concrets à réaliser.

Dans l'optique du développement ultérieur de la SNPC, le Conseil fédéral a chargé le Centre national pour la cybersécurité (NCSC) d'évaluer l'efficacité de la stratégie en vigueur. La présente évaluation réalisée en externe répond à quatre questions:

Approche globale / Réalisation des objectifs: la SNPC 2018-2022 a-t-elle atteint les objectifs stratégiques définis?

Efficience / Ressources: comment se présente le rapport entre les moyens engagés et les prestations fournies?

Efficacité / Impact: dans quelle mesure les effets recherchés ont-ils été obtenus?

Développement / Recommandations: à l'heure de la refonte de la stratégie, quelles sont les recommandations qui s'imposent pour l'utilisation future des ressources?

L'évaluation de l'efficacité de la SNPC repose sur un modèle d'effets à plusieurs niveaux (*income, input, implementation, output, outcome, impact*).

Utilité et adéquation de la SNPC 2018-2022

L'efficacité de la SNPC dépend de sa conception initiale, de l'accent mis sur les défis rencontrés ainsi que de la mise en œuvre concrète. Les appréciations portant sur la conception de la SNPC éclairent les effets imputables au contexte national ou international (*income*), aux bases, objectifs et ressources (*input*) ainsi qu'aux structures et processus (*implementation*), et peuvent être résumés en sept constats:

— La SNPC repose, en ce qui concerne les **cybermenaces et les défis**, sur des bases actuelles et se concentre sur les défis centraux et les développements permettant de renforcer la cybersécurité nationale.

— Les **bases légales et stratégiques** sont dûment prises en compte dans la SNPC. Il y aurait toutefois un potentiel d'amélioration, au niveau de la coordination de la SNPC et des autres stratégies de numérisation et de protection de la Confédération.

— Les services responsables de la mise en œuvre accomplissent leurs tâches de base avec les **ressources à disposition**. Des ajustements au niveau de la collaboration entre les services impliqués permettraient d'optimiser l'utilisation faite des moyens à disposition. De même, il faudrait prévoir des capacités supplémentaires en personnel pour les travaux de mise en œuvre de la SNPC.

— La structure du réseau se prête à la mise en œuvre de la SNPC, mais il faudrait encore mieux exploiter les potentiels de synergie de ce réseau. Cela vaut aussi pour les liens avec les stratégies supérieures ou apparentées. La **gouvernance** perfectionnée de la SNPC favorise ici la **collaboration**.

— Les bases, le besoin d'agir identifié et les défis ont été dûment pris en compte dans les **objectifs stratégiques** de la SNPC. Le parti pris de se concentrer sur l'administration fédérale, sans penser aux chances qu'offrirait en Suisse un «écosystème de la cybersécurité», est toutefois discutable.

— Avec les **quatre groupes cibles** distingués, la SNPC prend en compte un très grand nombre d'acteurs. Elle accorde un degré d'attention plus ou moins grand aux divers groupes d'acteurs faisant partie de ces champs d'action.

— Les **champs d'action et les mesures** s'intègrent bien dans la stratégie. Le plan de mise en œuvre est un instrument-clé adéquat, et les champs d'action ainsi que les mesures définies tiennent dûment compte de l'ampleur des défis existants.

Prestations et effets des champs d'action

La SNPC vise à déployer ses effets grâce aux mesures ou projets de mise en œuvre répartis entre ses dix champs d'action. La présente évaluation de l'efficacité passe en revue les champs d'action et les mesures formulées à la lumière des prestations réalisées (*outputs*) et des effets à court et moyen terme (*outcomes*). Les conclusions suivantes peuvent être tirées à propos des champs d'action de la SNPC.

— La majorité des projets de mise en œuvre ont abouti, et donc les prestations essentielles ont été fournies, dans le champ d'action **Acquisition de compétences et de connaissances**; les structures souhaitées ont été créées et le réseau de connaissances est en place. Les effets visés ont été obtenus et ont un impact sur les autres champs d'action.

— Les projets de mise en œuvre réalisés ont abouti à créer dans le champ d'action **Situation de la menace** une solide base, qui permet aux services compétents d'obtenir des résultats. D'autres progrès seraient souhaitables dans l'évaluation matérielle de la situation de la menace. Un des défis tient à la pénurie d'experts sur le marché.

— Dans le champ d'action **Gestion de la résilience**, les mesures visant à améliorer la résilience informatique des infrastructures critiques et de l'administration fédérale ont été sensiblement développées. Or s'il y a bien eu des efforts considérables et une prise de conscience, les effets sur le groupe cible ne sont pas encore satisfaisants.

— Des bases ont été créées dans le champ d'action **Normalisation et réglementation,** mais restent sous-exploitées, du fait de leur faible diffusion et de leur caractère avant tout volontaire. Les projets de réglementation réalisés ont abouti à des conditions-cadres propices à l'essor de la normalisation. Autrement dit, même si les effets visés et l'impact restent très limités à l'heure actuelle, les conditions sont réunies pour obtenir à l'avenir des effets accrus.

— Dans le champ d'action **Gestion des incidents**, les compétences acquises, les processus définis et les capacités accrues de gestion des incidents ont renforcé à des degrés divers la résilience des groupes cibles. Aucun effet préventif n'est constatable à ce jour.

— Les capacités de réaction et d'intervention de l'administration fédérale ont été renforcées dans le champ d'action **Gestion des crises**, tandis que la réglementation des responsabilités et les exercices effectués garantissent une meilleure collaboration transversale des autorités et de l'administration. Il reste toutefois très compliqué d'intervenir rapidement.

— Dans le champ d'action **Poursuite pénale**, les poursuites contre la cybercriminalité sont devenues plus performantes et efficaces, grâce à la coordination et au renforcement de la collaboration intercantonale. À l'heure actuelle, les différences de nature technique, juridique et procédurale notamment entre les autorités de poursuite pénale cantonales et fédérales, ainsi que les ressources limitées en personnel ne permettent pas d'obtenir les effets et l'impact visés. Les mesures visant à renforcer les capacités à disposition sont en chantier.

— Les projets de mise en œuvre réalisés dans le champ d'action **Cyberdéfense** ont abouti à un net renforcement des capacités de l'armée et du Service de renseignement de la Confédération, ainsi que de leur disponibilité opérationnelle dans le cyberespace. D'autres mesures figurant dans la «stratégie cyber du DDPS» sont encore venues s'ajouter dans ce champ d'action. Une extension de l'offre de formation destinée aux tiers se fait encore attendre, afin d'accroître l'interopérabilité au sein du Réseau national de sécurité et d'en améliorer l'impact.

— Le champ d'action **Politique extérieure de cybersécurité** a un impact indirect sur la protection des groupes cibles. Les autorités suisses et d'autres acteurs centraux ont fait entendre leur voix dans les discussions internationales sur la cybergouvernance (p. ex. dans le cadre du Dialogue de Genève).

— Les cyberrisques ont gagné en visibilité grâce à la communication renforcée. Les grandes entreprises et les multinationales notamment, ainsi que les exploitants d'infrastructures critiques y sont devenus sensibles. Mais bien souvent, le champ d'action **Visibilité et sensibilisation** n'atteint pas encore suffisamment la population et les PME. Il faudrait encore améliorer la coordination des activités de communication entre les différents acteurs. L'impact s'avère ici indirect.

Effets sur les groupes cibles

La SNPC vise à améliorer chez ses quatre groupes cibles – administration et autorités; exploitants d'infrastructures critiques; population; économie – la résilience face aux cybermenaces, de façon à garantir leur capacité d'agir et leur intégrité. L'évaluation de l'efficacité a examiné dans quelle mesure la SNPC est fructueuse dans ces groupes cibles.

— La mise en œuvre de la stratégie est solidement ancrée dans l'**administration et les autorités**. Les champs d'action et les mesures forment un ensemble cohérent, d'autant plus que le découpage de la stratégie et les mesures proposées s'appuient fortement sur les structures administratives. La SNPC permet d'améliorer la collaboration entre la Confédération et les cantons.

— Les exploitants d'**infrastructures critiques** sont bien sensibilisés et étroitement associés aux mesures ou aux projets de mise en œuvre. On constate que les échanges sont intenses et l'engagement accru, du moins dans les branches comptant des acteurs de poids. Ce n'est guère le cas à ce jour dans les branches caractérisées par une structure morcelée et un très grand nombre d'acteurs, où la conscience du problème est moins prononcée. À l'heure actuelle, les prestations fournies au titre de la stratégie ne suffisent pas à protéger correctement toutes les branches comportant des infrastructures critiques.

— La **population** s'intéresse davantage depuis quelques années à la sécurité du cyberespace; la SNPC ne lui offre toutefois ni sensibilisation plus poussée ni cyberformation de base. Par conséquent, les mesures prévues dans la SNPC atteignent ponctuellement la population, mais la sensibilisation aux enjeux de sécurité du cyberespace n'a pas d'impact à grande échelle.

— Dans le groupe cible de l'**économie**, les grandes entreprises internationales se protègent de façon adéquate contre les cyberrisques. Les PME par contre ne sont pas assez conscientes des menaces du cyberespace et sont peu protégées. La SNPC n'encourage guère les entreprises à agir pour mieux se protéger.

Bilan de l'efficacité de la SNPC

La SNPC 2018-2022 constitue une stratégie cohérente. Son plan de mise en œuvre concrétise judicieusement les objectifs stratégiques. La mise en œuvre respecte le calendrier et produit les effets visés, soit assurer la **réalisation des objectifs stratégiques**. Or les résultats varient entre les groupes cibles. Moyennant des interventions ciblées, comme une mesure d'impact ou un pilotage stratégique renforcé, les responsables pourraient rendre la mise en œuvre de la SNPC encore plus efficace.

Les responsables de la mise en œuvre de la SNPC ont à ce jour **rempli efficacement leur mission de base** avec les ressources disponibles. L'allocation des ressources pourrait toutefois être davantage axée sur les objectifs d'impact. Les ressources en personnel supplémentaires prévues jusqu'à l'échéance de la stratégie à la fin de 2022 ainsi que pour la pérennisation des activités paraissent justifiées.

Les effets de la SNPC sont notamment constatables à ce jour au niveau des infrastructures critiques, des autorités ou institutions tant nationales que cantonales, ainsi que des grandes entreprises. Mais il n'est pas possible d'en apporter la démonstration empirique dans le cadre de la SNPC en cours. En outre, il apparaît clairement que la SNPC n'atteint pas comme il le faudrait les PME, les villes et les communes ainsi que la population. La cyberprotection demeure insuffisante au sein de ces groupes cibles.

Perspectives et recommandations

Les possibilités concrètes d'améliorer la conception de la SNPC pour en accroître l'efficience et en maximiser l'impact sont les suivantes, au vu de la présente évaluation de l'efficacité.

— Il faudra exploiter de manière ciblée le **processus d'élaboration participatif** lors des futurs développements de la SNPC, soit pour les activités postérieures à 2022. Un processus efficient et géré de manière rigoureuse motiverait les divers dépositaires du savoir à collaborer dans ce contexte.

— Il convient de renforcer la **gouvernance** de la SNPC, en réduisant la taille de son comité de pilotage, afin d'augmenter ses possibilités de conduite stratégique. Il faudrait encore encourager de nouvelles possibilités de réseautage. Il s'agira d'examiner comment on pourrait davantage intégrer les PME et l'échelon communal dans la gouvernance de la SNPC.

— Les **objectifs stratégiques** seront formulés le plus concrètement possible et avec un maximum d'indépendance à tous les échelons stratégiques, y compris dans les projets de mise en œuvre, pour faciliter une meilleure concentration et un regroupement plus efficace des activités et des ressources. L'approche SMART (spécifique, mesurable, accepté, réaliste, temporellement défini) peut être utile ici.

— Les **efforts de communication** doivent être intensifiés, concentrés et coordonnés. Il faudra examiner s'il y a lieu d'ajouter un nouvel objectif stratégique intitulé «Transfert et communication».

— La SNPC déploie d'autant mieux ses effets qu'elle adopte le ton juste avec ses **groupes cibles** et les associe directement à la planification et à la mise en œuvre des mesures. Les mesures de la SNPC devront autant que possible répondre directement aux besoins des groupes cibles. En outre, il convient d'examiner si la SNPC devrait créer des «projets passerelles» couvrant les trois échelons de la Confédération, des cantons ainsi que des villes et communes.

— Le **plan de mise en œuvre** s'est avéré un instrument-clé afin de pouvoir rapidement lancer des activités et suivre les objectifs stratégiques. Il faudrait toutefois assouplir encore les modalités de conception et d'exécution du plan de mise en œuvre, en prévoyant le cas échéant des cycles stratégiques plus longs. En outre, il convient d'insister davantage sur la mesure d'impact et sur le contrôle de gestion.

— Il existe une large palette de **mesures**, offrant une grande diversité thématique. Une classification différente, par type de mesures serait souhaitable ici («mesures immédiates», «bonnes pratiques», «projets de réglementation», «projets transversaux de base» et «projets pilotes»). En outre, il faudrait expressément traiter les thèmes des «risques liés à la chaîne d'approvisionnement», de la «formation» et de l'«écosystème de la cybersécurité» pour bien cerner les chances. Et pour soutenir le pilotage stratégique et l'allocation des ressources de la SNPC, il serait nécessaire à l'avenir de prendre en compte l'instrument de la mesure d'impact dans la planification stratégique et la planification des mesures.

— Il a bien fallu jusqu'ici remplir les missions de la SNPC avec les **ressources** à disposition. Le manque de ressources se fait toutefois sentir et des vœux de hausse ciblée de la dotation en personnel ont été émis. Concrètement, un réexamen critique des processus de planification et de budgétisation s'impose afin que les ressources puissent plus aisément être utilisées là où le besoin se fait sentir. Il faudrait notamment vérifier si le Groupe Cyber ou le comité de pilotage devraient davantage s'impliquer dans la gestion des ressources ou des budgets de projet, pour simplifier l'allocation des ressources. De l'avis général, la pénurie d'experts techniques reste bien réelle, dans tous les groupes cibles et à tous les niveaux. Des mesures ciblées de formation et de perfectionnement permettraient de renforcer le pool d'experts.

1 Mandat d'évaluation de l'efficacité

1.1 Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) pour les années 2018 à 2022

Protection dans le cyberespace

La transformation numérique de la Suisse comporte aussi bien des chances que des risques, pour l'État comme pour le monde politique, la société et l'économie. Aujourd'hui déjà, les technologies de l'information et de la communication et les réseaux numériques mondiaux font l'objet d'une utilisation intensive. Or les activités illégales du cyberespace, qui mettent en péril l'intégrité, la confidentialité et la disponibilité des systèmes informatiques et des données[1], se développent au même rythme que la numérisation. À partir du moment où l'on veut garantir à l'avenir la capacité d'agir et l'intégrité des acteurs tant étatiques que privés face aux cybermenaces, des mesures ciblées doivent être prises pour en assurer la protection.

Stratégie du Conseil fédéral

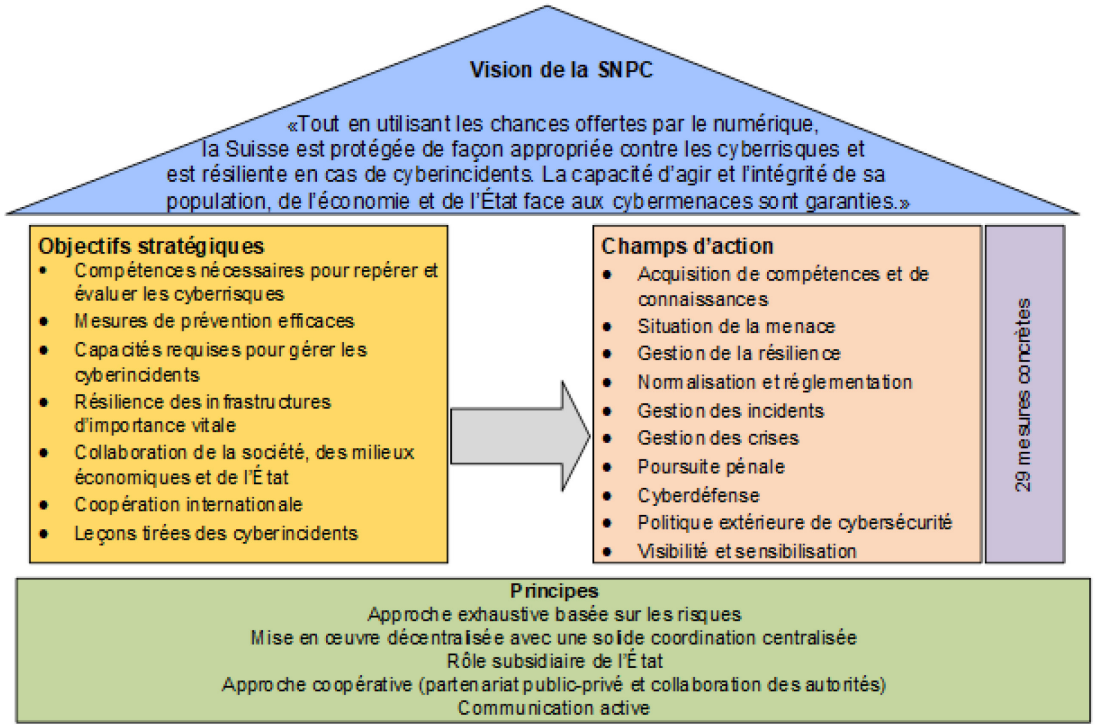
Le Conseil a déjà réagi à de telles menaces dans sa stratégie nationale de protection de la Suisse contre les cyberrisques (Conseil fédéral, 2018). À l'occasion de la deuxième période de mise en œuvre de la SNPC, couvrant les années 2018 à 2022, le Conseil fédéral a réagi aux nouvelles menaces en adoptant des mesures supplémentaires.

La SNPC 2018-2022 est une refonte de la première stratégie, à la lumière des expériences réalisées et des objectifs atteints, compte tenu aussi des menaces ou développements actuels dans le cyberespace. Une cinquantaine d'organisations étatiques ou non ont été associés au processus stratégique, sous la direction de l'ex-Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de l'Unité de pilotage informatique de la Confédération (UPIC). La stratégie a été conçue selon un processus à plusieurs niveaux et adoptée le 18 avril 2018 par le Conseil fédéral, qui l'a mise en vigueur. L'arrêté du Conseil fédéral prévoit des rapports annuels sur la mise en œuvre, ainsi qu'un réexamen global de la stratégie d'ici la fin de l'année 2022.

La SNPC 2018-2022 a pour vision de protéger la Suisse de façon adéquate face aux cyberrisques et d'accroître sa résilience en la matière. La capacité d'agir et l'intégrité de la population, de l'économie et de l'État face aux cybermenaces sont garanties. À cet effet, le Conseil fédéral a fixé sept objectifs stratégiques, axés sur les capacités de prévention et de gestion des cyberincidents et sur la collaboration entre les acteurs étatiques, civils et militaires (voir figure 1). De nombreux offices fédéraux, les cantons et les milieux économiques sont impliqués dans la mise en œuvre de la stratégie.

[1] Voir la triade «Confidentiality», «Integrity» et «Availability» (CIA).

Représentation schématique de la SNPC 2018 à 2022



Source: Conseil fédéral, 2018

Figure 1: Structure et teneur de la SNPC 2018-2022

La stratégie comporte un plan de mise en œuvre, qui définit des projets concrets de mise en œuvre pour chacune des mesures prévues. Ce plan de mise en œuvre sert de plan de travail et fixe les responsabilités et les étapes. Le comité de pilotage de la SNPC peut le compléter par de nouveaux projets de mise en œuvre, ce qui est arrivé plusieurs fois entre 2019 et 2021. L'annexe A-5 contient un aperçu des champs d'action, avec leurs mesures respectives et les projets de mise en œuvre prévus.

Groupes cibles

Les mesures de la SNPC 2018-2022 s'adressent à différents groupes-cibles, qui forment quatre groupes.

Groupe cible	Description
Infrastructures critiques	Il s'agit du principal groupe cible des mesures, lesquelles ont pour but de garantir en tout temps la disponibilité des biens et services essentiels.
Autorités	Les autorités de la Confédération, des cantons et des communes sont responsables des prestations de services qui, par leurs particularités aussi bien que par leurs besoins de résilience accrue, peuvent être assimilées aux infrastructures critiques.
Population	La SNPC vise à protéger la population, qui doit être spécifiquement protégée face à la cybercriminalité. La population doit pouvoir utiliser l'informatique en toute sécurité et avec confiance, en étant informée des risques existants.
Économie	La sécurité du cyberespace et un approvisionnement stable en biens et services s'avèrent essentiels pour l'intégrité des processus d'affaires. Les entreprises suisses doivent bénéficier ici de conditions-cadres optimales et d'un climat de sécurité.

Tableau 1: Groupes cibles de la SNPC 2018-2022

Les mesures précisent encore à chaque fois les groupes cibles, le cas échéant.

Compétences

La mise en œuvre de la SNPC 2018-2022 relève depuis 2019 de la compétence du délégué du Conseil fédéral à la cybersécurité, qui dirige par ailleurs le Centre national pour la cybersécurité (NCSC). Rattaché au Secrétariat général du Département fédéral des finances (DFF), le NCSC constitue en tant que centre de compétences de la Confédération le premier interlocuteur des milieux économiques, de l'administration, des établissements d'enseignement et des autorités pour toute question liée à la cybersécurité.

Le délégué du Conseil fédéral assure le pilotage stratégique de la SNPC 2018-2022 avec un comité de pilotage. Fort de 23 membres, ce comité implique des unités administratives de tous les départements, de l'armée, des cantons (via la Conférence des directrices et directeurs cantonaux des départements de justice et police), ainsi que des représentants de l'économie et des hautes écoles, afin d'assurer une conduite cohérente de la SNPC 2018-2022. Le comité de pilotage se réunit quatre fois par an.

La structure de conduite actuelle se présente sous cette forme depuis 2018. Auparavant, l'ex-Unité de pilotage informatique de la Confédération (UPIC) était responsable de la SNPC, dont MELANI assurait la mise en œuvre. Les compétences sont réglées depuis mai 2020 dans l'ordonnance sur les cyberrisques (OPCy; RS *120.73*).

1.2 Objectifs et questions inhérentes à l'évaluation de l'efficacité

Le Conseil fédéral a chargé le DFF d'évaluer la SNPC en cours d'ici la fin de l'année 2022 et de la remanier le cas échéant. Le comité de pilotage de la SNPC a décidé d'en faire analyser l'efficacité à l'externe. Le présent rapport sur l'efficacité servira de base aux travaux à entreprendre. Par conséquent, outre un bilan de la SNPC 2018-2022, cette évaluation de l'efficacité renferme des indications utiles pour l'adaptation et l'optimisation de la SNPC dans le cadre de son remaniement et de son développement prévus.

Le présent rapport résume les résultats de l'évaluation de l'efficacité menée entre juillet 2021 et janvier 2022, qui répondait à quatre grandes questions.

Approche globale / Réalisation des objectifs: dans quelle mesure la SNPC 2018-2022 permet-elle d'atteindre les objectifs stratégiques définis? (évaluation sommative)

Efficience / Ressources: quel est le rapport entre les moyens engagés et les prestations fournies lors de la mise en œuvre de la stratégie? (évaluation sommative)

Efficacité / Impact: dans quelle mesure les prestations fournies ont-elles permis d'obtenir les effets recherchés? (évaluation sommative)

Développement / Recommandations: quelles sont les recommandations qui s'imposent pour la refonte de la stratégie, d'une part, et pour l'utilisation future des ressources financières et humaines, d'autre part? (évaluation formative)

L'évaluation de la SNPC 2018-2022 a conduit à examiner et à affiner son modèle d'effets. Sur la base de la «théorie du changement», ce modèle d'effets peut être représenté selon la figure 2. Il sert de cadre d'orientation complet pour la présente évaluation de l'efficacité.

Modèle d'effets

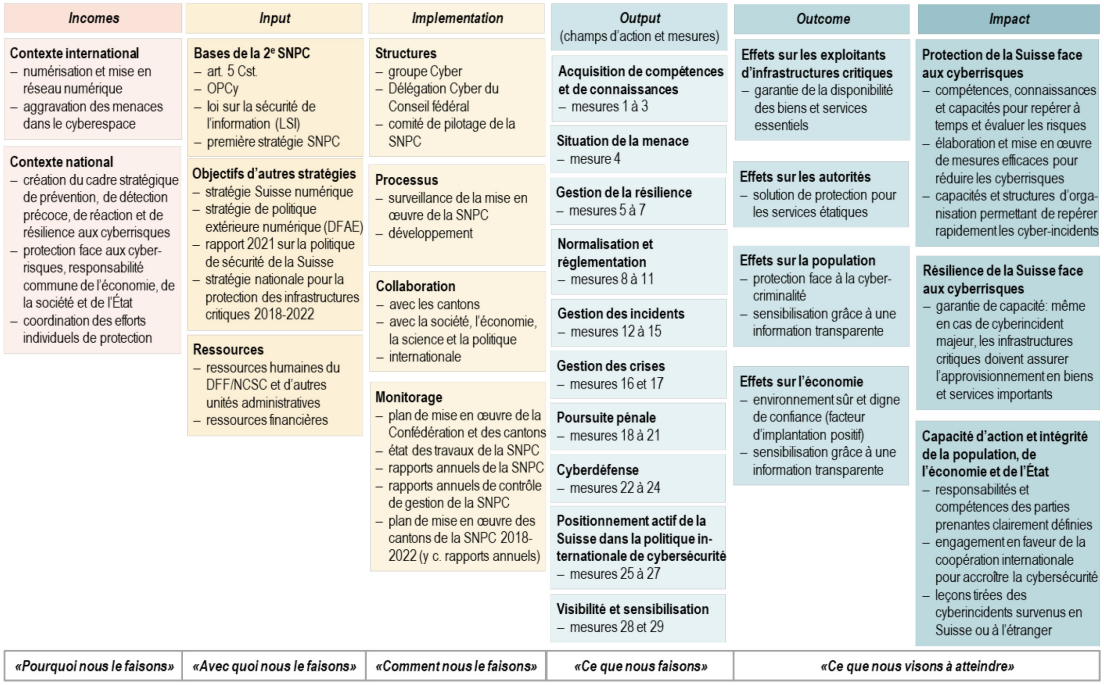


Figure 2: Modèle d'effets de la SNPC 2018-2022. La présente évaluation de l'efficacité se concentre sur trois éléments-clés (*output, outcome, impact*).

Ce modèle d'effets appelle les explications suivantes:

— *Incomes*: contexte mondial ou national dans lequel a été développée la SNPC 2018-2022. Ce contexte est marqué par la transformation numérique croissante au niveau mondial, avec les chances et risques qui s'ensuivent et les efforts de protection entrepris au niveau national.

— *Input*: cette notion recouvre les objectifs de la SNPC 2018-2022, tels qu'ils figurent dans les bases légales, dans la première SNPC et dans les objectifs d'autres stratégies de la Confédération. Les ressources dont la Confédération dispose pour fournir ses prestations dans le cadre de la SNPC 2018-2022 en font aussi partie.

— *Implementation*: structures et processus d'exécution créés par la Confédération, conjointement avec les autres acteurs nationaux ou internationaux. Le monitorage, qui s'appuie sur les plans de mise en œuvre et les rapports, en fait partie.

— *Output*: prestations d'exécution de la SNPC 2018-2022 fournies par tous les acteurs impliqués; il s'agit ici des activités et projets concrets figurant dans les champs d'action définis par la stratégie 2018-2022. Les produits à réaliser sont décrits de manière exhaustive au moyen de 29 mesures comportant au total 246 étapes (voir annexe A-5).

— *Outcome*: effets directs à court ou moyen terme de la SNPC 2018-2022 sur ses groupes cibles, soit les exploitants d'infrastructures critiques, les autorités, la population ainsi que l'économie (voir annexe A-5). Outre les effets recherchés, il peut y avoir des effets non voulus.

— *Impact*: effets à long terme de la SNPC 2018-2022, à un niveau global qui touche l'ensemble de la société. Là encore, il faut s'attendre en plus des effets recherchés à des effets non voulus (voir annexe A-5).

Pour répondre aux quatre grandes questions de recherche, il a fallu examiner les questions détaillées ci-après (tableau 2).

Questions		Niveau d'effets
1	**Contexte**: dans quelle mesure la SNPC 2018-2022 prend-elle en compte les défis ou développements pertinents au niveau national ou mondial, ainsi que les prescriptions légales?	*Incomes*
2	**Bases**: dans quelle mesure les objectifs de la SNPC 2018-2022 reposent-ils sur les bases légales, stratégiques ou autres le cas échéant?	*Input*
3	**Ressources**: dans quelle mesure les ressources allouées à la mise en œuvre de la SNPC 2018-2022 sont-elles jugées adéquates?[2]	*Input*
4	**Structures/Processus**: dans quelle mesure les structures et processus d'implémentation de la SNPC 2018-2022 sont-ils jugés efficaces?	*Implementation*
5	**Champs d'action**: dans quelle mesure les champs d'action définis permettent-ils d'affronter les défis annoncés dans le domaine des cyberrisques?	*Output*
6	**Mesures**: jusqu'à quel point les diverses mesures avec leurs étapes permettent-elles d'atteindre les objectifs de la SNPC 2018-2022 (par ex. des mesures supplémentaires sont-elles indiquées? Y a-t-il lieu d'étendre certaines mesures? Ou faudrait-il en réduire d'autres?)	*Output*
7	**Cohérence**: dans quelle mesure les champs d'action et les mesures de la SNPC 2018-2022 sont-ils cohérents?	*Output*
8	**Utilité**: les mesures de la SNPC atteignent-elles les groupes cibles dans la mesure souhaitée? (par ex. les groupes cibles utilisent-ils les mesures ou les structures et processus établis, de même que les produits, les services, les réseaux et les méthodes mis en place, etc.?)	*Output*
9a	**Effets visés sur les groupes cibles**: dans quelle mesure les effets visés par la SNPC 2018-2022 (aptitudes des acteurs, résilience, etc.) ont-ils été atteints pour ses quatre groupes cibles (infrastructures critiques, autorités, économie, population)?	*Outcome*
9b	**Autres effets sur les groupes cibles**: y a-t-il au niveau des groupes cibles d'autres effets non voulus? Comment faut-il les interpréter?	*Outcome*
9c	**Effets sur d'autres acteurs**: dans quelle mesure des effets (non voulus) apparaissent-ils sur d'autres acteurs et comment faut-il les interpréter?	*Outcome*
10	**Effets sur l'ensemble de la société**: dans quelle mesure les effets visés par la SNPC 2018-2022 sont-ils atteints? – Protection de la Suisse face aux cyberrisques; – Résilience de la Suisse aux cyberrisques; – Garantie de la capacité d'agir et de l'intégrité de la population, de l'économie et de l'État. Y a-t-il des effets non voulus? Comment faut-il les interpréter?	*Impact*
11	**Recommandations**: quelles recommandations et quel potentiel d'optimisation peut-on en déduire en ce qui concerne… – la SNPC pour les années 2023 à 2027; – l'utilisation à venir des ressources humaines et financières?	Tous les niveaux du modèle d'effets

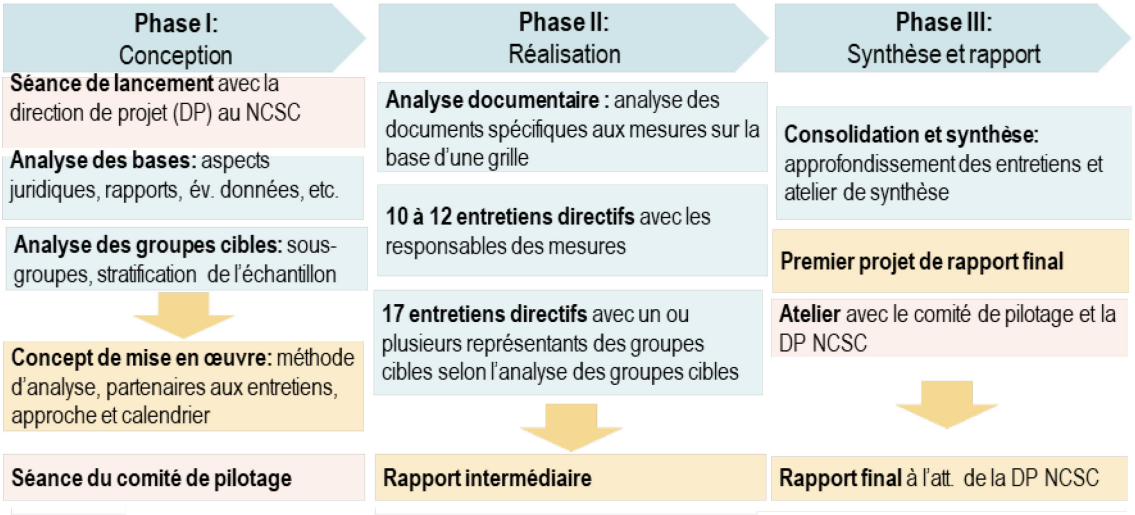
2 Le NCSC prévoyait de mener d'ici l'automne 2021 sa propre étude quantitative des ressources par mesure.

Tableau 2: Questions détaillées de l'évaluation de l'efficacité de la SNPC 2018-2022.

1.3 Marche à suivre et rapport

Différentes méthodes ont été choisies pour l'évaluation de l'efficacité: analyse des documents internes et/ou pertinents pour la mise en œuvre, analyse de la littérature nationale ou internationale, analyse des acteurs ou des groupes cibles impliqués, ou encore entretiens directifs (voir guides de l'annexe A-2) et *focus groups* formés tant de responsables des mesures et de protagonistes de la SNPC 2018-2022 que de représentants des groupes cibles (voir annexe A-3 et annexe A-4). Une telle approche permet de combiner, pour l'évaluation de la SNPC 2018-2022, sa perception de l'intérieur et de l'extérieur. L'analyse a été découpée en trois phases (voir figure 3), et le comité de pilotage de la SNPC était impliqué dans les phases I et II.

Conception du projet en trois phases



econcept et EBP, 2021

Figure 3: Conception du projet d'évaluation de l'efficacité, avec les méthodes, l'interaction avec le NCSC et le calendrier. La phase I s'achève à l'adoption du concept de mise en œuvre.

D'autres détails sur la marche à suivre figurent à l'annexe A-1. Les données ont été traitées entre juillet 2021 et janvier 2022. Le présent rapport résume les résultats de l'évaluation de l'efficacité de la manière suivante:

— Le chapitre 2 procède à une évaluation globale de la SNPC 2018-2022, en indiquant si et dans quelle mesure elle peut être considérée comme opportune et adéquate pour accroître la protection de la Suisse face aux cyberrisques.

— Le chapitre 3 examine quelles prestations ont été fournies jusqu'ici dans les dix champs d'action et quels effets (*outcomes*) peuvent leur être attribués.

— Le chapitre 4 se concentre sur les quatre groupes cibles pour déterminer si et en quoi leur intégrité et leur capacité d'agir face aux cybermenaces se sont renforcées.

— Le chapitre 5 sert à une évaluation globale de l'efficacité. Il répond aux grandes questions de l'enquête ayant une valeur d'évaluation sommative (voir chap. 1.2).

— Enfin, le chapitre 6 examine quelles recommandations peuvent être formulées en vue de la refonte de la SNPC, afin d'en accroître l'efficacité (voir aussi la quatrième grande question du chap. 1.2).

La présente évaluation de l'efficacité reflète l'opinion que ses auteurs se sont forgée au cours de leur approche systématique, qui repose sur plusieurs méthodes et adopte différentes perspectives. Ils saisissent l'occasion pour remercier tous les participants à l'enquête de leur attitude d'ouverture et de leur bonne volonté.

2 Utilité et adéquation de la SNPC 2018-2022

L'efficacité de la SNPC 2018-2022 dépend de différents facteurs, soit sa conception et l'accent mis sur les défis pertinents, d'une part, et les activités de mise en œuvre déployées, d'autre part. Le présent chapitre porte sur la conception de la SNPC 2018-2022. Trois niveaux d'effets y sont principalement analysés: *income* (contexte national et international), *input* (bases, objectifs et ressources) et *implementation* (structures et processus). Les champs d'action de la SNPC (*output*) sont jugés quant à leur adéquation pour atteindre les objectifs. Une évaluation des effets portant sur les divers champs d'action suit au chapitre 3.

Les pages qui suivent présentent les questions détaillées auxquelles il a été répondu à partir de l'analyse des documents et d'entretiens avec les responsables des mesures et avec des représentants des groupes cibles.

2.1 Cybermenaces et défis

Contexte: dans quelle mesure la SNPC 2018-2022 prend-elle en compte les défis ou développements pertinents au niveau national ou mondial, ainsi que les prescriptions légales?

La stratégie actuelle aborde tout d'abord les principales menaces et les cyberrisques majeurs que connaît la Suisse et identifie les défis se posant pour sa capacité de résistance. Elle distingue ici entre les actes illicites intentionnels – soit les cyberattaques, dont relèvent la cybercriminalité, le cyberespionnage, le cybersabotage et le terrorisme, la désinformation et la propagande, de même que la cyberdéfense en cas de conflit – et les incidents volontaires notamment dus à l'erreur humaine (par ex. fraude à la carte de crédit, etc.), ainsi que les pannes techniques.

Des développements stratégiques ont été amorcés dans cinq domaines, au vu de la situation de menace identifiée et des expériences de la SNPC 2013-2017. La stratégie élaborée mise sur la protection face aux menaces et sur une infrastructure résiliente, afin que la Suisse garde intacte sa capacité d'agir. Ces priorités supposent un pilotage stratégique plus ferme et la mise en œuvre de mesures supplémentaires, un renforcement des capacités et des connaissances, un soutien plus large dans la mesure où les groupes cibles sont plus nombreux, ainsi qu'un renforcement de la collaboration. L'accent est clairement mis ici sur le renforcement des structures organisationnelles.

De l'avis des personnes interrogées, les bonnes leçons ont été tirées de la première stratégie et la SNPC 2018-2022 constitue un cadre adéquat pour bien gérer les cybermenaces. Le contexte de la stratégie, avec le rapport de 2016 sur la politique de sécurité, la stratégie «Suisse numérique» du Conseil fédéral et la stratégie nationale de protection des infrastructures critiques, indiquait clairement où il fallait agir. Les personnes

ayant répondu à l'enquête ont notamment salué l'extension de la SNPC à de nouveaux groupes cibles et le renforcement de la collaboration.

Une étude de l'EPF Zurich (CSS, 2019), qui a procédé à des comparaisons internationales entre la SNPC 2013-2017 et la SNPC 2018-2022 et d'autres stratégies nationales, conforte les appréciations qui précèdent. La SNPC répond aujourd'hui à huit grands défis que l'on peut identifier au niveau international, dans diverses analyses du contexte et dans les stratégies correspondantes.

Bilan: la SNPC 2018-2022 repose sur des bases actuelles. En outre, elle est axée sur les défis et les développements centraux pour renforcer la cybersécurité nationale.

2.2 Contexte institutionnel de la stratégie

Bases: dans quelle mesure les objectifs de la SNPC 2018-2022 reposent-ils sur les bases légales, stratégiques ou autres le cas échéant?

La SNPC 2018-2022 repose sur les activités en amont liées à la SNPC 2012-2017 et sur les leçons tirées dans ce contexte. Aux dires des personnes interrogées, le processus défini pour les années 2018 à 2022 a su intégrer de manière rigoureuse et complète ces bases ou expériences avec des études actuelles et avec les évaluations des parties prenantes. De l'avis général, les défis actuels ont été correctement appréhendés (voir chap. 2.1). Le cadre juridique en vigueur a été pris en compte, et la stratégie a anticipé les chantiers de l'OPCy et de la loi fédérale sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI; RS 126).

Outre la SNPC, on trouve la stratégie «Suisse numérique»[3], dont répond depuis 2021 à la Chancellerie fédérale le délégué du Conseil fédéral pour la transformation numérique et la gouvernance de l'informatique (TNI) (elle relevait jusque-là de l'Office fédéral de la communication [OFCOM]). Par ailleurs, le DFAE s'est doté d'une «stratégie de politique extérieure numérique 2021-2024»[4] et le DDPS a adopté la «stratégie Cyber du DDPS 2021-2024»[5]. Un examen matériel révèle la cohérence de ces trois stratégies, qui s'emboîtent l'une dans l'autre. Ainsi le champ d'action Politique extérieure de cybersécurité de la SNPC fait le lien entre les activités déployées à l'échelon national et international. Les personnes interrogées signalent cependant qu'il y aurait un potentiel d'amélioration dans la coordination des différentes stratégies avec la SNPC 2018-2022. Car leurs comités respectifs de conduite stratégique ne se concertent pas suffisamment.

Bilan: la SNPC 2018-2022 tient compte de manière adéquate des bases légales ou stratégiques. On constate toutefois des incohérences institutionnelles.

---

3 https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/strategie-suisse-numerique/digitale-schweiz.html, visite le 7 janvier 2022

4 https://www.eda.admin.ch/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf, visite le 7 janvier 2022

5 https://www.newsd.admin.ch/newsd/message/attachments/66203.pdf; visite le 22 janvier 2022.

2.3 Ressources

Ressources: dans quelle mesure les ressources allouées à la mise en œuvre de la SNPC 2018-2022 sont-elles jugées adéquates?

L'EPF Zurich a constaté, dans une étude comparative internationale de 2019, que les acteurs politiques d'autres pays acceptent de consacrer des ressources substantielles à une approche stratégique de la cybersécurité nationale (CSS, 2019). Or les dépenses consenties par la Suisse sur ce terrain sont plutôt faibles en comparaison.

Les ressources en personnel de la SNPC ont augmenté à plusieurs reprises depuis 2018. En automne 2021, le NCSC a procédé à une réévaluation des ressources et des besoins des services s'occupant de la SNPC (NCSC, 2021c). Une majorité des offices y font part du besoin de renforcer leurs capacités en personnel destinées à la mise en œuvre des mesures de la SNPC 2018-2022.

Suite à cette évaluation de l'efficacité, les responsables des mesures ont précisé qu'à ce jour, les ressources en personnel à disposition leur avaient permis d'exécuter les éléments centraux et les tâches essentielles liées aux 29 mesures. Le besoin de renforts de personnel a été justifié de la façon suivante:

- *Double charge*: de nombreux projets sont réalisés par des personnes ayant déjà une fonction hiérarchique dans leur organisation. D'où une mise en concurrence des ressources et une double charge qui dans bien des cas, est ressentie comme un surcroît de travail. La mise à disposition de ressources supplémentaires doit permettre d'accomplir les tâches courantes dans les fonctions hiérarchiques.
- *Postes vacants*: diverses unités administratives ont des postes vacants. La cause serait imputable tant au parti pris d'attendre encore de certaines directions d'office qu'aux difficultés à trouver des personnes ayant le profil exigé.
- *Besoins de formation continue*: la forte dynamique de développement du cyberespace exige une activité soutenue de perfectionnement et réduit d'autant les capacités pouvant être engagées. Une augmentation des ressources aurait pour effet d'assurer tant une capacité d'action continue qu'une activité intense de formation continue.
- *Croissance des tâches*: la SNPC 2018-2022 comprend des mesures venant renforcer les activités opérationnelles (vue d'ensemble des infractions, etc.). La recrudescence des cyberattaques rend la gestion opérationnelle toujours plus lourde, et donc des ressources supplémentaires semblent nécessaires. Il faudrait viser à pérenniser les mesures opérationnelles à un niveau élevé, ce qui suppose d'accorder les ressources prévues à long terme.

Selon différents partenaires interrogés, les ressources allouées à la gouvernance et aux processus de mise en œuvre auraient pu déployer davantage d'effets. La SNPC se serait concentrée sur les objectifs et les effets visés, sans toujours s'interroger sur l'allocation des ressources. Or il aurait été possible de procéder à un meilleur partage, au profit notamment des secteurs des poursuites contre la cybercriminalité, de la cybersécurité et

de la cyberdéfense. À cet effet, divers acteurs réclament depuis longtemps un pool commun d'experts suffisamment doté en ressources pour renforcer substantiellement la collaboration transversale. Il s'agira de respecter en tout temps les principes de l'État de droit et donc les bases juridiques, qui prévoient une délimitation ciblée des ressources allouées aux divers domaines.

Bilan: les ressources disponibles à ce jour permettent d'assumer les tâches essentielles liées à la mise en œuvre des mesures de la SNPC 2018-2022. Il serait toutefois possible d'en rationaliser l'allocation, en misant sur la transversalité et/ou en adaptant la collaboration (par ex. à l'aide d'un pool d'experts). Il existe par ailleurs un besoin justifié d'accroître les capacités en personnel prévues pour la mise en œuvre de la SNPC.

2.4 Gouvernance et collaboration

Structures/Processus: dans quelle mesure les structures et processus d'implémentation de la SNPC 2018-2022 sont-ils jugés efficaces?

La mise en œuvre de la SNPC repose sur une approche décentralisée, où divers offices fédéraux réalisent directement les projets leur ayant été confiés (voir Conseil fédéral, 2018). Le NCSC veille ici à la coordination entre offices, voire se charge lui-même des projets de mise en œuvre. Cette approche décentralisée du pilotage et de la mise en œuvre correspond à la structure en réseau prônée par la SNPC. Elle est caractérisée par un organe commun de coordination ainsi que par des concertations peu formalisées, que ce soit entre les domaines «Cyberdéfense», «Cybersécurité» et «Poursuites contre la cybercriminalité» ou entre les différents champs d'action.

Les personnes ayant répondu à l'enquête jugent cette structure en réseau tout à fait opportune. D'abord, elle a permis de démarrer rapidement les activités et d'intégrer grâce aux structures établies les compétences existantes, lors de l'introduction de la SNPC 2018-2022. Ensuite, une telle structure garantit constamment une grande agilité et une bonne capacité de réaction, ce qui permet d'intégrer rapidement et à valeur égale des acteurs supplémentaires. La collaboration au sein du réseau est jugée empreinte de confiance, efficiente et axée sur des solutions. Ce constat vaut tant pour la mise en œuvre des mesures opérationnelles qu'au niveau de la conduite stratégique. Le cadre donné et les orientations matérielles de la SNPC y contribuent. A contrario, le processus d'élaboration de la SNPC 2018-2022 a été ponctuellement jugé laborieux, en raison du grand degré de liberté matérielle consenti et du nombre élevé de parties prenantes.

Les synergies matérielles rendues possibles par le réseau n'ont toutefois été que partiellement exploitées. Il a été dit à ce sujet que la mise en réseau s'était quasiment limitée à trois grands domaines de l'administration fédérale («cyberdéfense», «cybersécurité» et «poursuite pénale et cybercriminalité»). Les activités latérales, mettant à contribution d'autres champs d'action voire tous, laissaient à désirer. On peut citer ici, comme exemples de pertes de synergies, les analyses des menaces, les mesures de renforcement de la résilience et les formations, qui ne sont pas entièrement coordonnées

entre la défense et la sécurité, de même qu'entre les autorités civiles et les éléments militaires. Il est vrai que selon certains acteurs, une harmonisation complète entre les volets «Defence» et «Security» est impossible. Des réserves liées à l'État de droit ainsi que des lois concrètes s'y opposent, par exemple pour des échanges d'informations à propos des vulnérabilités identifiées. Il serait par contre souhaitable d'acquérir des compétences en commun. La formation de Cyber Security Specialist avec brevet fédéral (BF), que proposent tant l'Armée suisse que des organisations civiles, constitue une offre importante dans cette optique.

Au-delà des activités du comité de pilotage, il n'y a guère d'occasions d'étendre les réseaux en place et d'entrer directement en contact avec d'autres acteurs.

La gouvernance de la SNPC 2018-2022 a reçu un ancrage institutionnel supplémentaire avec le poste de délégué du Conseil fédéral à la cybersécurité et la création du Centre national pour la cybersécurité (NCSC). Ces mesures relevant de la gouvernance ainsi que la collaboration avec le personnel du NCSC sont jugées tout à fait positives.

La SNPC 2018-2022 a jeté les bases d'une consolidation des diverses activités du Centre national pour la cybersécurité. Ce dernier a eu depuis lors des effets positifs sur la stratégie, en renforçant la conduite stratégique et en augmentant la capacité de réaction. Selon la plupart des responsables des mesures qui ont été interrogés, les publications régulières du NCSC ainsi que les interventions du Délégué ont accru la visibilité et la notoriété de la SNPC. On le voit à la recrudescence dans les médias des comptes rendus de cyberrisques avec mention du délégué et des services compétents de la Confédération (à commencer par le NCSC). Les personnes interrogées ont souvent mentionné que le délégué du Conseil fédéral à la cybersécurité devait essentiellement posséder des compétences techniques et stratégiques ainsi qu'une personnalité rassembleuse.

Quelques participants à l'enquête jugent insuffisants, en termes d'efficience et d'efficacité de la gouvernance et des processus, les liens établis entre la SNPC et les autres stratégies de l'administration fédérale (Suisse numérique, stratégie cyber, protection contre les cyberrisques). En effet, toutes les unités administratives impliquées dans ces diverses stratégies ne font pas partie du Groupe Cyber. En pareil cas, la gouvernance de la SNPC ne tient pas suffisamment compte de leurs activités opérationnelles.

Bilan: la structure du réseau est jugée propice à la mise en œuvre de la SNPC 2018-2022. La mise en œuvre opérationnelle n'en exploite toutefois pas pleinement les avantages, même si l'évolution constatable depuis 2018 au niveau de la gouvernance de la SNPC semble bénéfique à ce point de vue. Il faudrait encore améliorer les liens structurels ou procéduraux avec les stratégies supérieures ou apparentées.

2.5 Objectifs stratégiques

Bases: dans quelle mesure les objectifs de la SNPC 2018-2022 reposent-ils sur les bases légales, stratégiques ou autres le cas échéant?

Les partenaires des entretiens considèrent que le processus d'élaboration de la stratégie a largement contribué à tisser de bonne heure des liens entre les dépositaires du savoir et à renforcer leur collaboration. Cet engagement commun a été expressément salué. L'Agence européenne chargée de la sécurité des réseaux et de l'information recommande elle aussi, dans son guide pratique (ENISA, 2016), d'associer de bonne heure les parties prenantes à la conception d'une stratégie. Les objectifs identifiés pour la stratégie peuvent être considérés comme justes dans l'optique d'alors. Ils reposent sur les connaissances pertinentes de tous les acteurs et sur un consensus entre eux. Ils ont par conséquent accepté de s'engager afin de réaliser les objectifs fixés.

Selon les personnes interrogées, les sept objectifs stratégiques supérieurs et les principes d'action définissent avec une précision suffisante ce qui doit être fait pour concrétiser la vision de la SNPC afin que la Suisse soit correctement protégée face aux cyberrisques et que la capacité d'agir et l'intégrité de la population, de l'économie et de l'État restent garanties face aux cybermenaces. La structuration en trois volets (cybersécurité, poursuite pénale et cyberdéfense) est également jugée pertinente. L'approche ouverte utilisée, qui associe aussi les cantons et d'autres institutions, est considérée comme importante pour faire accepter les objectifs fixés. Quelques interlocuteurs reprochent toutefois à cette approche fédéraliste et décentralisée d'empêcher un déploiement rapide des effets au quotidien.

Il a été dit à diverses reprises que la stratégie reste fortement axée sur la Confédération ou l'administration fédérale. Aux yeux des personnes interrogées, le plan de mise en œuvre cantonal a permis de fixer ici d'autres priorités. Il devrait être possible à l'avenir de tenir encore mieux compte des préoccupations des cantons.

Il a été ponctuellement signalé que les chances offertes par le numérique, dont il est question au sous-chapitre «Vision» de la stratégie, n'apparaissent pas dans les objectifs stratégiques. Aucune mesure spécifique n'a été définie à ce sujet. Les objectifs stratégiques se concentrent exclusivement sur la gestion des cyberrisques. D'autres avis individuels soulignent que le but principal de la SNPC doit être de protéger la Suisse en se concentrant sur les risques. Il convient d'aborder ailleurs, comme dans la stratégie «Suisse numérique» du Conseil fédéral (Confédération suisse, 2020a), les chances offertes par une cyberprotection avancée de la Suisse, caractérisée par sa grande capacité d'agir et son intégrité face aux cybermenaces.

Bilan: les bases actuelles, le besoin d'agir identifié et les défis ont été dûment pris en compte dans les objectifs de la SNPC 2018-2022. La forte concentration sur l'administration fédérale et la non-prise en compte des chances possibles font parfois l'objet de remarques critiques.

2.6 Groupes cibles

Bases: dans quelle mesure les objectifs de la SNPC 2018-2022 reposent-ils sur les bases légales, stratégiques ou autres le cas échéant?

Utilité: les mesures de la SNPC atteignent-elles les groupes cibles dans la mesure souhaitée?

La conception efficace de la SNPC 2018-2022 doit beaucoup à l'accent mis sur les groupes cibles (voir au chap. 1.2 la notion d'«*outcome*» du modèle d'effets). La SNPC 2018-2022 procède à une répartition fortement agrégée en quatre groupes cibles, soit les infrastructures critiques, les autorités, la population et l'économie. Les responsables des mesures jugent en principe appropriée cette agrégation, qui offre la possibilité de subdivisions supplémentaires durant la mise en œuvre des mesures. La difficulté de la SNPC 2018-2022 tient plutôt à ce que ses mesures ne permettent pas d'atteindre autant que souhaité ses quatre groupes cibles, auxquels elles s'adressent différemment.

Les différences dans la manière de prendre contact avec les groupes cibles tiennent notamment au vide juridique. Ainsi, la Confédération doit en premier lieu se protéger elle-même face aux cyberrisques[6]. Les mesures de protection des infrastructures critiques figurant dans la SNPC reposent sur les bases légales applicables aux services concernés (par ex. SRC, OFPP, OFAE, OFCOM). En outre, le Parlement a adopté pendant la mise en œuvre de la SNPC la loi sur la sécurité de l'information (LSI), qui charge expressément la Confédération de soutenir les exploitants d'infrastructures critiques sur le terrain de la cybersécurité.

Il n'existe pas de bases légales suffisantes pour les activités visant à protéger la population ou par exemple les PME.

Le fort accent mis sur le groupe cible «Infrastructures critiques» est jugé tout à fait correct, au vu des objectifs d'impact de la SNPC. Les difficultés surgissent au stade de la délimitation concrète des acteurs de ce groupe cible. Les personnes interrogées déplorent encore que les risques inhérents à la chaîne d'approvisionnement, soit aux composants ou services destinés aux infrastructures critiques, ne soient pas pris assez au sérieux et que la SNPC ne s'y attaque pas systématiquement. Le même constat vaut, au niveau communal, pour l'exploitation des infrastructures par les villes et communes.

Un autre facteur d'incertitude inhérent à la SNPC était dû à l'absence d'unité de doctrine: au départ, l'Office fédéral de la protection de la population (OFPP), l'Office fédéral de l'approvisionnement économique (OFAE) et les offices responsables d'un secteur spécifique portaient tous un regard différent sur les infrastructures critiques et n'avaient pas les mêmes exigences envers elles. Le transfert à l'OFPP de la responsabilité globale de coordonner la gestion de la résilience garantit entre-temps une analyse uniforme et une carte des dangers consolidée. L'OFAE a en contrepartie la responsabilité générale d'élaborer les normes minimales de protection des infrastructures critiques. Selon

6 OPCy

certaines personnes interrogées, il reste nécessaire d'adopter une définition exhaustive des infrastructures critiques, applicable à toute l'administration fédérale.

Dans le cas du groupe cible «Autorités», les responsables des mesures et les représentants des groupes cibles s'accordent à dire qu'au début de la SNPC 2018-2022, les communes étaient laissées pour compte. Entre-temps, le projet de mise en œuvre d'un label de cybersécurité destiné aux communes et aux PME (Cyber-Safe) a tenté de combler cette lacune. La collaboration entre la Confédération et les communes est peu répandue, aujourd'hui où règne le principe de subsidiarité, avec pour effet que la Confédération et les communes ne sont guère sensibilisées aux offres et à la collaboration possibles. Il est vrai que la collaboration avec les cantons s'est bien développée pendant la SNPC 2018-2022. Mais les cantons ne tissent des liens avec les communes qu'à l'échelon local.

Il a été signalé de divers côtés que la SNPC n'implique pas de la même manière tous les acteurs importants. C'est ainsi que des offices importants du Département fédéral de l'environnement, des transports, de l'énergie et de la communication ne sont pas pris en compte de façon adéquate. L'Office fédéral de l'aviation civile, l'Office fédéral des transports, l'Office fédéral des routes et l'Office fédéral de l'énergie (OFEN) ont beau être responsables d'infrastructures critiques, ils n'ont pas voix au chapitre dans les organes de la SNPC. Ces offices ont parfois créé eux-mêmes des postes dédiés à cette tâche, afin de mettre en œuvre leurs tâches dans le contexte de la SNPC.

Le groupe cible «Économie» n'est pas couvert de manière équilibrée aux yeux d'une majorité des personnes ayant répondu à l'enquête. On peut y distinguer trois sous-groupes, qui diffèrent par leurs structures ou défis, par leurs normes de protection actuelles face aux cyberrisques ainsi que par leurs réglementations:

- *Exploitants d'infrastructures critiques*: ils constituent un groupe cible de la SNPC 2018-2022, alors qu'il existe des différences significatives entre ces entreprises, qu'il s'agisse de leur taille ou du champ de leurs activités.
- *Entreprises actives au niveau international*: les entreprises suisses actives à l'étranger déploient souvent des ressources considérables pour garantir l'intégrité de leurs processus d'affaires et pour respecter différentes réglementations nationales en matière de sécurité et de protection des données. Il en va de même des multinationales étrangères ayant un établissement en Suisse. Elles assurent de manière autonome leur cybersécurité et peu d'entre elles ont des contacts réguliers avec la SNPC. Le NCSC a élargi ces dernières années le cercle fermé de ses clients pour y intégrer toujours plus les PME.
- *PME*: tant les personnes responsables des mesures que les représentants de l'économie voient dans le maillage serré des PME un facteur de vulnérabilité. Il y aurait notamment un problème de sensibilisation aux cyberrisques (*awareness*), dû à ce que la SNPC 2018-2022 n'a pas suffisamment pris en compte ce groupe cible.

Pour beaucoup d'acteurs, la population est le maillon faible de la chaîne de protection contre les cyberrisques. C'est néanmoins le groupe cible avec lequel la SNPC 2018-2022

établit le moins de contacts directs. Les personnes ayant répondu à l'enquête ont des avis différents sur le rôle de la population, selon que l'objectif est de réduire les cyberrisques et les dommages subis par les ménages privés ou qu'il est question de la population active, qui doit au moins avoir été sensibilisée à la cybersécurité et disposer de connaissances de base en la matière pour son activité professionnelle.

Bilan: avec ses quatre groupes cibles, la SNPC 2018-2022 s'adresse à une large palette d'acteurs. Il existe toutefois de grandes disparités et des lacunes, au niveau des mesures concrètes destinées aux divers segments de ces groupes cibles.

2.7 Champs d'action et mesures définis dans la stratégie

Cohérence: dans quelle mesure les champs d'action et les mesures de la SNPC 2018-2022 sont-ils cohérents?

Afin d'atteindre les objectifs stratégiques, la SNPC 2018-2022 définit dix champs d'action, portant sur divers aspects des cyberrisques. Au total, 29 mesures sont formulées dans ces champs d'action.

Tous les participants aux entretiens estiment que la structure de la SNPC 2018-2022 est appropriée et cohérente. L'ampleur, la structure et le degré de détails sont adéquats et permettent de se faire rapidement une bonne idée de la manière dont la Suisse gère les cyberrisques.

La direction prise par les activités inscrites dans les champs d'action est jugée adéquate pour atteindre les sept objectifs stratégiques. Le large spectre couvert par les dix champs d'action de la SNPC 2018-2022 semble approprié, compte tenu du degré de maturité actuel de la Suisse face aux cyberrisques. Il crée les conditions requises par un grand nombre de groupes cibles ou de défis, avec un risque toutefois de dispersion. Aussi est-il parfois recommandé d'envisager un recentrement des activités, quand des progrès auront été réalisés. Les champs d'action servent en premier lieu, dans la SNPC 2018-2022, à structurer l'approche définie. Le plan de mise en œuvre de la stratégie constitue l'instrument clé, de l'avis des partenaires interrogés. Il se réfère aux champs d'action de la stratégie et reflète par ailleurs l'ampleur du secteur administratif et des groupes cibles impliqués, avec une forte logique organisationnelle. La subdivision hiérarchique en champs d'action --> mesures --> projets de mise en œuvre est en outre ressentie comme trop complexe et rigide. De l'avis de quelques personnes interrogées, cela a freiné la mise en réseau des contenus, et des synergies potentielles sont restées en friche. Il a encore été dit que les champs d'action et les mesures sont fortement calqués sur l'administration fédérale. Selon quelques participants, il n'y aurait pas encore d'approche satisfaisante pour juger de l'efficacité des mesures et effectuer les contrôles utiles.

Faute d'approche concrète pour mesurer l'efficacité obtenue, le controlling des mesures est jugé formaliste à l'excès et pauvre en contenu. Mieux vaudrait opter pour une structure

plus flexible, qui se prête à une différenciation plus poussée en fonction du genre d'activité, selon qu'il s'agit d'une mesure immédiate, d'un projet ou d'une nouvelle tâche courante.

Bilan: les champs d'action et les mesures s'intègrent bien dans la stratégie. Sa structure est globalement jugée adéquate et son plan de mise en œuvre est perçu comme un instrument-clé adéquat. Les champs d'action et les mesures couvrent l'ensemble des défis et possèdent un lien logique pour des tiers avec les objectifs de la stratégie.

3 Prestations et effets obtenus dans les champs d'action

La SNPC 2018-2022 est conçue pour déployer ses effets à travers les mesures définies dans ses dix champs d'action. Les champs d'action et les mesures adoptées se situent globalement au niveau des *outputs* de la stratégie. Il faut par contre distinguer, à propos des champs d'action et de leurs mesures, entre les prestations qui ont été réalisées (*outputs*) et les effets visés à court et moyen terme (*outcomes*). Les explications ci-après se réfèrent à ces deux niveaux et tirent un bilan global des champs d'action. Ils répondent pour chacun des champs d'action aux questions suivantes:

Champs d'action: dans quelle mesure les champs d'action définis permettent-ils d'affronter les défis annoncés dans le domaine des cyberrisques?

Mesures: jusqu'à quel point les diverses mesures avec leurs étapes permettent-elles d'atteindre les objectifs de la SNPC 2018-2022 (par ex. des mesures supplémentaires sont-elles indiquées? Y a-t-il lieu d'étendre certaines mesures? Ou faudrait-il en réduire d'autres?)

3.1 Acquisition de compétences et de connaissances

N°	Mesure	Projets de mise en œuvre	Statut
1	Détection précoce des tendances ou technologies et acquisition des connaissances utiles	Monitorage des technologies	Réalisé
		Analyse des tendances	Réalisé
2	Extension et encouragement des compétences en matière de recherche et de formation	Analyse des besoins d'offres en matière de formation	Réalisé
		Centre de recherche et d'assistance créé par les deux EPF	Réalisé
		Cyber Defence Campus	Réalisé
		Recherche et formation interdisciplinaires sur la cybersécurité	Réalisé
		Encouragement du piratage éthique (*ethical hacking*)	Réalisé
		Réalisation du programme pilote de chasse aux bogues (*Bug Bounty*)	Réalisé
3	Création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité	Création de centres d'innovation	Suspendu
		Laboratoire d'idées pour la cybersécurité	Réalisé

Tableau 3: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Acquisition de compétences et de connaissances». Source: Conseil fédéral, 2021

Mesures et objectif: le champ d'action «Acquisition de compétences et de connaissances» comprend les mesures M1 à M3, qui visent à créer des conditions propices aux activités ultérieures.

Évaluation des prestations: d'importants projets de mise en œuvre ont été réalisés pour toutes les mesures, sauf deux où ils ont été suspendus. Les prestations essentielles (*outputs*) ont été fournies dans le champ d'action «Acquisition de compétences et de connaissances» et le Swiss Support Center for Cybersecurity (SSCC) a permis de réaliser la mise en réseau souhaitée entre les hautes écoles, l'administration, l'industrie et la société civile. La collaboration entre les EPF et le DDPS a également été renforcée, au niveau surtout de la formation en cybersécurité. Plusieurs projets concrets ou de mise en œuvre ont été traités ou sont en cours dans d'autres champs d'action (*outcome*).

Évaluation des effets: les partenaires interrogés signalent la grande importance de ce champ d'action, censé créer les conditions requises pour gérer de façon adéquate les cyberrisques. Il convient de mentionner en particulier le rapport du Campus cyberdéfense (CYD) d'armasuisse sur l'évolution technologique, ainsi que les conférences coorganisées par le CYD et les hautes écoles; ou encore les ateliers du SSCC, l'initiative commune des deux EPF, ainsi que l'aperçu des offres de formation des hautes écoles. Ce champ d'action a des effets pouvant être qualifiés d'indirectement perceptibles. Ils sont attestés par une étude de l'Université d'Oxford, qui attribue une note de 4,5 (sur une échelle de maturité allant d'un à cinq) au cadre suisse pour la formation professionnelle (University of Oxford, 2020, voir aussi l'annexe A-5).

Bilan: les prestations essentielles ont été fournies, grâce à la réalisation de la majorité des projets de mise en œuvre de ce champ d'action; les structures souhaitées ont été créées et le réseau de connaissances est en place. Les effets visés sont atteints, et l'impact est perceptible dans les autres champs d'action.

3.2 Situation sur le plan des cybermenaces

N°	Mesure	Projets de mise en œuvre	Statut
4	Extension des capacités permettant d'analyser et de représenter la situation sur le plan des cybermenaces	Identification des groupes cibles et de leurs besoins	Réalisé
		Définition d'un catalogue de produits par groupe cible (catalogue de prestations)	Réalisé
		Acquisition des sources et des ressources de production nécessaires	Réalisé

Tableau 4: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Situation de la menace». Source: Conseil fédéral, 2021

Mesure et objectif: le champ d'action «Situation de la menace» comprend la mesure M4, qui vise à soutenir une prévention efficace, axée sur les menaces réelles, en livrant une vue d'ensemble aussi complète que possible de la situation sur le plan des cybermenaces.

Évaluation des prestations: la mesure a été largement réalisée. Selon les entretiens menés, les bons projets de mise en œuvre ont été menés. Ils permettront d'informer la Confédération et les autres «clients» en fonction des besoins de ces groupes cibles.

Évaluation des effets: il a notamment été question ici du radar de la situation, qui fait régulièrement l'objet de mises à jour systématiques afin d'informer au sujet des cybermenaces la Délégation Cyber du Conseil fédéral et le Groupe Cyber. Autre point positif souligné, le NCSC ainsi que les programmes de prévention et de sensibilisation du Service de renseignement de la Confédération font parvenir au grand public des informations sur les menaces actuelles.

Durant les entretiens, les responsables des mesures ont signalé les exigences spéciales liées à la situation de la menace: elle peut changer d'un moment à l'autre, ce qui constitue un sérieux défi pour les compétences requises du personnel. La difficulté tient à ce qu'il faut disposer de ressources adéquates pour obtenir l'efficacité voulue. Les capacités à disposition doivent suffire tant pour venir à bout des tâches opérationnelles prévues que pour réagir à des situations inédites et pour assurer la formation continue permanente. À l'avenir, il faudra encore davantage veiller à la qualité de la formation des experts en cybermenaces. Il s'agit d'un réel défi alors qu'au niveau des infrastructures, de fructueux efforts ont déjà été consentis pour renforcer les capacités ainsi que les compétences.

Bilan: les projets de mise en œuvre réalisés ont créé une solide base pour permettre aux services compétents (à commencer par le SRC et le NCSC) d'obtenir des résultats. D'autres progrès seraient souhaitables au niveau de l'analyse matérielle de la situation sur le plan des cybermenaces. Le manque d'experts sur le marché est toutefois considéré ici comme un obstacle de taille.

3.3 Gestion de la résilience

N°	Mesure	Projets de mise en œuvre	Statut
5	Amélioration de la résilience informatique des infrastructures critiques (OFPP en collaboration avec les offices spécialisés dans les secteurs réglementés)	Mise en œuvre des projets prévus ou en cours destinés à renforcer la résilience des sous-secteurs critiques	Réalisé
		Établissement d'un groupe de travail universitaire pour la cybersécurité	Réalisé
6	Amélioration de la résilience informatique dans l'administration fédérale [7]	Élaboration de directives de sécurité relatives aux méthodes de projet agiles	Réalisé
		Campagne de sensibilisation dans l'administration fédérale	Réalisé
		Transmission sécurisée des données	Réalisé
		Security Operations Center de l'OFIT	Réalisé
		Création d'une interface avec le domaine des EPF	Réalisé
7		Échange permanent entre cantons	Suspendu
		Organisation de la Cyberlandsgemeinde	Réalisé

7 Le Conseil fédéral a déjà confié en 2015 la réalisation d'un projet de réseau de données sécurisé (RDS) sur le plan suisse (Conseil fédéral, 2015). Même s'il ne s'agit pas d'un projet de mise en œuvre de la SNPC, ce mandat est étroitement lié à la mesure n° 6 de la SNPC 2018 à 2022.

N°	Mesure	Projets de mise en œuvre	Statut
	Échange d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons	Création dans le domaine des EPF d'une interface avec les cantons	Réalisé

Tableau 5: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Gestion de la résilience». Source: Conseil fédéral, 2021

Mesures et objectifs: les infrastructures critiques et les autorités doivent mettre en œuvre des mesures permettant de limiter les dégâts et de réduire les temps d'arrêt en cas de panne. Les mesures M5 à M7 servent à l'identification et à la mise en œuvre d'activités susceptibles de renforcer la résilience informatique.

Évaluation des prestations: les travaux liés à ces mesures sont déjà bien avancés. D'importants progrès ont été réalisés grâce à l'accent mis sur le renforcement de la résilience des infrastructures critiques, sur les exigences propres à l'administration fédérale et sur les échanges entre cantons. Dans le cas de la mesure M7 notamment, l'engagement des cantons joue un rôle important, car ils améliorent encore la cybersécurité avec leur propre plan de mise en œuvre. Entre autres prestations réalisées (*outputs*), on peut citer l'actualisation des analyses des risques et de la vulnérabilité dans différents secteurs, le renforcement de la résilience de l'administration fédérale grâce à l'ordonnance sur les cyberrisques (OPCy), ainsi que l'organisation de la Cyberlandsgemeinde et la création de l'Institut national de test pour la cybersécurité à Zoug. Il a été ponctuellement souligné que le champ d'action doit absolument être poursuivi lors du prochain cycle stratégique.

Évaluation des effets: il ressort des entretiens avec les responsables des mesures que les mesures choisies sont pertinentes et correctes et qu'il y a lieu de les poursuivre. Dans le cas des infrastructures critiques, les mesures débouchent sur des activités (*outcome*) qui soutiennent la protection face aux cyberrisques; elles couvrent à l'heure actuelle 27 sous-secteurs, selon la stratégie nationale pour la protection des infrastructures critiques du Conseil fédéral (stratégie PIC, Conseil fédéral, 2017). L'Agence européenne chargée de la sécurité des réseaux et de l'information avait déjà qualifié d'exemplaire l'approche basée sur les risques retenue pour la SNPC 2012-2017 (ENISA, 2016). La Suisse a ainsi atteint un stade de maturité de trois (stade établi) sur cinq (stade dynamique) dans la mise en œuvre de la cybersécurité (University of Oxford, 2020). Tout en disposant d'un niveau de connaissances élevé et de stratégies adéquates, il lui manque encore la capacité de déployer rapidement et à grande échelle son savoir-faire et ses stratégies de protection.

L'approche suivie, qui mise fortement sur la responsabilité individuelle des exploitants, atteint toutefois à ses limites. Elle laisse en effet une grande liberté aux acteurs, qui décident eux-mêmes de l'ampleur des activités à réaliser (*outcome*).

La plupart des participants à l'enquête aimeraient que les activités aient un caractère plus contraignant, avec par exemple des exigences formulées au niveau de branche ou une approche réglementaire renforcée (voir ci-après chap. 3.4). Un examen externe de la

cybersécurité était parvenu aux mêmes conclusions en 2020 (University of Oxford, 2020). Une étude de l'EPF Zurich (CSS, 2016) suggère ici d'examiner d'autres modèles. Quelques voix soulignent toutefois l'importance de la responsabilité individuelle et se disent sceptiques à propos d'un durcissement réglementaire. Il ne faut pas oublier non plus que les sous-secteurs critiques sont plus ou moins fortement réglementés.

Bilan: les mesures visant à améliorer la résilience informatique ont été fortement développées, au profit tant des infrastructures critiques que de l'administration fédérale. Bien que beaucoup de prestations aient été réalisées (*output*) et que la conscience du problème soit aiguisée, l'effet sur le groupe cible n'est pas encore satisfaisant. Aucune norme minimale n'a pu être imposée à ce jour.

3.4 Normalisation et réglementation

N°	Mesure	Projets de mise en œuvre	Statut
8	Définition et introduction de normes minimales	Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique Développement et implantation d'outils destinés aux PME	Réalisé
		Label Cyber-Safe destiné aux communes	Réalisé
		Label pour prestataires informatiques	Réalisé
9	Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction	Étude de modèles de base d'obligations de notifier	Réalisé
		Débat de fond avec l'économie et les autorités	Réalisé
10	Gouvernance mondiale d'Internet	Rencontres du groupe de haut niveau du Secrétaire général de l'ONU	Réalisé
		Plateformes d'échange multi-acteurs pour la coordination au niveau national	Réalisé
11	Acquisition d'expertise sur les questions de normalisation dans le domaine de la cybersécurité	Renforcement des projets de normalisation par le soutien apporté aux hautes écoles	Réalisé
		Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale	Réalisé

Tableau 6: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Normalisation et réglementation». Source: Conseil fédéral, 2021

Mesures et objectifs: les mesures M8 à M11 de la SNPC 2018-2022, portant sur la normalisation et la réglementation, se concentrent sur la création de bases dans ce domaine. Trois labels ont été créés pour garantir la cybersécurité des communes et des PME (Cyber-Safe), des prestataires de services informatiques (Cyberseal) ainsi que des entreprises technologiques (Digital Trust). Un projet de réglementation a par ailleurs abouti, en vertu duquel certains «émetteurs radio», à l'instar des téléphones mobiles, des tablettes et d'autres appareils permettant de communiquer par Internet et comportant des applications pour l'Internet des objets, sont soumis depuis 2022 à certaines exigences de

cybersécurité. Ces nouvelles dispositions entendent contribuer à une protection accrue des réseaux de télécommunication, à une meilleure protection de la sphère privée des consommateurs et à une réduction des risques de fraude financière. En outre, les projets relatifs à l'obligation de déclarer les cyberincidents et à la révision de l'ordonnance sur les services de télécommunication ont été mis en consultation et les Chambres fédérales ont adopté la LSI.

Évaluation des prestations: les mesures ont été mises en œuvre selon le calendrier prévu. Pour chacune d'elles, les offices compétents ont réalisé les projets de mise en œuvre, qui préparent les bases techniques et qui renferment des propositions concrètes. Il a été signalé qu'à côté de ces projets de mise en œuvre, les découvertes techniques des hautes écoles sont souvent directement intégrées dans les normes (par ex. élimination des faiblesses liées à la technologie 5G).

Les acteurs interrogés signalent les difficultés de faire respecter les normes. Les causes en sont les suivantes:

— *Caractère facultatif*: les mesures visant à rehausser la protection face aux cyberrisques ont un caractère facultatif pour des pans entiers de l'économie, de la population et des autorités. Les meilleures pratiques doivent être considérées comme des offres et font partie intégrante des dispositifs de soutien. C'est essentiellement au niveau des infrastructures critiques qu'il faudrait aller plus loin pour faire appliquer les normes.

— *Processus législatif*: La SNPC 2018-2022 est une stratégie factuelle du Conseil fédéral. Elle peut tout au plus stimuler des processus législatifs et les soutenir sur le plan matériel. Il appartient aux décideurs politiques de déterminer si de tels processus doivent être réalisés, et le cas échéant comment.

— *Mise en réseau et structures décentralisées*: il n'est pas possible d'imposer unilatéralement des normes ou exigences de gouvernance spécifiques dans les structures décentralisées d'Internet. Il faut qu'un grand nombre d'acteurs (étatiques, semi-étatiques ou privés) soutiennent de tels efforts. La Suisse peut exercer une influence dans les organes internationaux compétents, en formulant des propositions solides et en participant aux discussions menées.

Les personnes interrogées concluent en résumé que les prestations fournies au titre des mesures (*outputs*) ont jeté les bases nécessaires pour soutenir la normalisation et une éventuelle réglementation future. Mais il n'a pas été possible d'en renforcer sensiblement la mise en œuvre et la diffusion dans le cadre de la SNPC 2018-2022 et parmi les acteurs du réseau de la SNPC.

Évaluation des effets: les effets des projets de mise en œuvre exécutés sont jugés encore faibles à l'heure actuelle. À titre de mesure «indirecte», il faudrait créer une offre à la demande pour le groupe cible. Tout indique qu'avec les avancées réglementaires, la demande serait stimulée et que les effets seraient d'autant plus grands.

L'effet potentiel des normes élaborées est par ailleurs d'autant moindre que les entreprises ont le choix entre différentes normes émanant de divers acteurs ou institutions. Il faudrait vérifier ici si lors du prochain cycle stratégique, en lieu et place de normes élaborées par la Suisse, il serait possible de s'appuyer davantage sur les normes ou cadres de référence établis au niveau international.

Bilan: des bases ont été créées à des fins de normalisation mais sont sous-utilisées à ce jour, en raison de leur faible diffusion et de leur caractère généralement facultatif. Les projets de réglementation instaurent des conditions cadres propices à la diffusion de telles bases. Les effets à court terme et l'impact à plus long terme sont jugés très restreints à l'heure actuelle, mais les conditions sont toutefois réunies pour qu'à l'avenir, les effets des mesures augmentent.

3.5 Gestion des incidents

N°	Mesure	Projets de mise en œuvre	Statut
12	Développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques	Élargissement ciblé du cercle fermé	Réalisé
		Développement des services et des produits	Réalisé
		Développement de la plateforme d'échange existante	Réalisé
13	Offre de services destinés à toutes les entreprises	Création d'un guichet unique national Cyber	Réalisé
		Information très rapide en cas d'incident au moyen de l'application Alertswiss	Réalisé
14	Collaboration ciblée entre la Confédération et d'autres services ou centres de compétences	Aperçu des CERT et des SOC opérationnels, et des interlocuteurs de référence	Réalisé
		Échange d'informations avec les CERT et les SOC	Réalisé
15	Processus et bases de la gestion des incidents au sein de l'administration fédérale	Élaboration de l'ordonnance sur la cybersécurité	Réalisé
		Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale	Réalisé

Tableau 7: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Gestion des incidents». Source: Conseil fédéral, 2021

Mesures et objectifs: les quatre mesures de gestion des incidents M12 à M15 visent à créer les conditions juridiques, organisationnelles, procédurales et matérielles nécessaires pour venir à bout rapidement et efficacement des cyberincidents.

Évaluation des prestations: les projets de mise en œuvre des quatre mesures ont été pratiquement entièrement réalisés et les prestations correspondantes sont en place (*outputs*). Les personnes interrogées ont notamment signalé le NCSC comme guichet unique et l'OPCy, qui règle les compétences liées à la gestion des incidents au sein de l'administration fédérale. Le NCSC a reçu et examiné en 2021 plus de 21 400 annonces

de cyberincidents (www.ncsc.admin.ch, visite le 31.01.2022). Les cercles fermés des clients ont été agrandis, et le guichet unique a été renforcé dans le cadre d'un partenariat privé-public.

Évaluation des effets: une distinction s'impose, dans l'évaluation des effets, entre l'examen des incidents au cas par cas et l'effet global de protection face aux cyberrisques.

À propos de l'examen des cas d'espèce, les personnes interrogées jugent efficaces les structures, les compétences et les processus destinés à la gestion des incidents. Le NCSC dispose des capacités requises et de structures qui garantissent sa réactivité. En outre, le processus de gestion des incidents fait l'objet de contrôles permanents et il est adapté là où il le faut sur la base des incidents traités. L'OPCy a précisé le cadre légal de la gestion des incidents au sein de l'administration fédérale, tandis que l'obligation de déclarer les cyberincidents actuellement en consultation vise à augmenter la marge de manœuvre du NCSC dans le domaine civil. L'armée s'est dotée en parallèle de capacités opérationnelles destinées à la gestion des incidents du domaine militaire. D'où des structures et des processus opérationnels jugés à même de garantir la capacité d'action et l'intégrité des autorités, de l'économie, des infrastructures critiques et de la population.

Les procédures applicables à la gestion des incidents ont été précisées dès 2018 pour l'administration fédérale, et l'ordonnance sur les cyberrisques (OPCy) a fixé les compétences en la matière. Le NCSC a été désigné responsable de la gestion des incidents, ce qui constitue de l'avis général une étape importante vers une gestion agile et efficace des incidents. Aucun incident grave n'étant survenu depuis la mise en place de ce système, on manque d'expériences directes de la pertinence et de l'efficacité immédiate de la procédure définie.

Une gestion efficiente des incidents peut avoir un effet préventif et empêcher des cyberattaques potentielles. Or les acteurs interrogés ne constatent pas un tel effet. Le NCSC continue de recevoir toujours plus d'annonces d'attaques dans le cyberespace.

Bilan: les compétences, les processus et les capacités de gestion des incidents renforcent potentiellement la résilience au sein du groupe cible, mais de différentes manières. Aucun effet préventif n'a toutefois été constaté.

3.6 Gestion des crises

N°	Mesure	Projets de mise en œuvre	Statut
16	Intégration du centre de compétence fédéral pour la cybersécurité dans les états-majors de crise de la Confédération	Élargissement du glossaire de la cybersécurité	Réalisé
17	Exercices communs de gestion de crise	Création de bases pour des exercices de crise comportant des aspects cybernétiques	Réalisé
		Réalisation d'exercices sectoriels	Réalisé
		Intégration d'aspects cybernétiques dans les exercices généraux	Réalisé

Tableau 8: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Gestion des crises». Source: Conseil fédéral, 2021

Mesures et objectifs: la Confédération développe et entraîne avec les mesures M16 et M17 ses propres aptitudes à la gestion des crises. Elle fait part de ses connaissances et propose des formations notamment au groupe cible des infrastructures critiques.

Évaluation des prestations: la gestion des crises prévue dans le cadre des mesures M16 et M17 a été développée. Les processus de formation et le mode opératoire des états-majors de crise sont définis, si bien qu'une activité opérationnelle peut rapidement démarrer. Des exercices de crise ont été réalisés conjointement avec les secteurs des finances et de la santé. Le délégué du Conseil fédéral à la cybersécurité fait partie de l'État-major fédéral Protection de la population (EMFP).

Évaluation des effets: les protagonistes partent du principe que des délais de réaction rapides et une durée d'intervention suffisante (*outcome*) renforcent la résilience de l'administration fédérale. La capacité d'action s'avère d'autant plus grande que les temps d'arrêt ont tendance à être plus brefs en cas d'incident.

On voit généralement bien comment les cibles ont été déterminées et les attaques planifiées. Chaque crise est suivie d'une réunion bilan, et des efforts sont entrepris pour intégrer aux processus et structures les enseignements à tirer des incidents. Les personnes interrogées ont de la peine à évaluer si et dans quelle mesure cette approche a un effet préventif. Les états-majors de crise participent sans doute à des formations ciblées et à des exercices visant à tester leur capacité d'agir. Mais les effets à long terme des exercices réalisés à ce jour restent peu clairs.

Bilan: les capacités de réaction et d'intervention de l'administration fédérale ont été renforcées, et la réglementation des responsabilités ainsi que des formations ciblées garantissent une meilleure capacité d'agir transversale aux autorités et à l'administration. Une intervention rapide demeure une opération complexe. Les événements futurs montreront le cas échéant les effets des mesures adoptées.

3.7 Poursuites pénales

N°	Mesure	Projets de mise en œuvre	Statut
18	Vue d'ensemble des infractions en matière de cybercriminalité (fedpol et CCPCS en collaboration avec le NEDIK)	Vue d'ensemble des infractions en matière de cybercriminalité (plateforme PICSEL)	Phase de test en cours
		Élaboration d'une vue d'ensemble judiciaire des infractions	Réalisé
		Présentation de l'évolution en matière de cybercriminalité et de ses conséquences	Réalisé
19	Réseau de soutien aux enquêtes relatives à la cybercriminalité (fedpol dans le cadre de la CCPCS)	Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons	Réalisé
20	Formation (CCPCS y c. fedpol, CPS et MPC)	Mise en œuvre des programmes de formation	Réalisé
21	Office central de lutte contre la cybercriminalité (fedpol)	Aucune étape jusqu'au 2e trimestre 2021	

Tableau 9: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Poursuite pénale». Source: Conseil fédéral, 2021

Mesures et objectifs: la Confédération est chargée de favoriser la collaboration intercantonale et a des compétences directes dans la lutte contre la cybercriminalité. Le Tribunal fédéral l'a confirmé à plusieurs reprises, à propos notamment d'affaires de crime organisé et de criminalité économique tirant parti du cyberespace. La lutte est menée en commun avec les cantons, sur la plateforme Cyberboard (Cyber-STRAT et Cyber-CASE). Depuis 2018, les échanges d'informations et de connaissances se sont intensifiés au sein du Réseau national de soutien aux enquêtes dans la lutte contre la cybercriminalité (NEDIK). Il faut y intégrer 26 organisations cantonales autonomes avec leurs propres processus, leurs systèmes informatiques, leurs prestations préalables, etc. L'Office fédéral de la police (fedpol) accomplit avec les mesures M18 à M21 le travail de fond, il encourage la formation et soutient la coordination.

Évaluation des prestations: les mesures M18 à M21 progressent globalement selon le calendrier prévu, et leur mise en œuvre opérationnelle avec les cantons s'effectue par étapes. La vue d'ensemble des infractions PICSEL est en phase de test. Un réseau de soutien aux enquêtes est en place avec le NEDIK, et une filière de formation a vu le jour. La mise en réseau des cantons est donc une réalité, même si leurs contributions au NEDIK varient d'un cas à l'autre. Toutes les mesures en matière de poursuite pénale ne sont pas encore achevées. Le tableau incomplet de la situation (projet de mise en œuvre de la vue d'ensemble des infractions PICSEL) reste un sérieux défi. Il a récemment été question d'adapter les activités de projet en 2022, mais rien n'a encore été décidé.

Évaluation des effets: des progrès significatifs ont été réalisés, avec le NEDIK notamment, dans la lutte coordonnée sur le plan suisse contre la cybercriminalité. Il est trop tôt toutefois pour constater les résultats (*outcome*) ou prouver les effets du NEDIK et des autres projets de mise en œuvre récemment achevés.

Tous les acteurs interrogés soulignent la grande importance d'un tableau policier complet et à jour de la situation. Les mesures de la SNPC misent sur la prévention et sont de nature avant tout policière. Il manque à ce jour à la SNPC une dimension judiciaire. Les «représentants des utilisateurs» interrogés dans les cantons relèvent encore toute une série d'obstacles imputables à l'organisation, au droit cantonal ou à la répartition des tâches entre les autorités d'enquête et celles de poursuite pénale. Il faudrait en venir à bout pour pleinement exploiter les possibilités créées.

Les acteurs interrogés jugent nécessaire, pour les clarifications juridiques à venir sur la cybercriminalité, que le législateur se détache davantage des aspects matériels. À l'heure des supports de stockage accessibles de partout de façon décentralisée, la «triade CIA»[8] doit s'appliquer aux connexions en temps réel. Les autorités de poursuite pénale disposent ici de diverses approches, à l'instar du «principe de continuité» (développement du droit), pour s'assurer des preuves et les collecter là où elles se trouvent, ou encore d'un «Swiss CLOUD-Act» (application de la loi) obligeant toutes les entreprises internationales ayant un établissement en Suisse à remettre leurs données selon le droit suisse. Dans le passé, des motions dans ce sens ont été déposées auprès des deux Chambres fédérales.

Bilan: moyennant une coordination et un renforcement de la collaboration intercantonale, les poursuites contre la cybercriminalité pourraient gagner en efficacité et accroître leur effet préventif. À l'heure actuelle, leurs effets à court ou long terme sont amoindris tant par les différences techniques, juridiques, procédurales et autres entre les diverses autorités de poursuite pénale organisées au niveau fédéral que par les capacités limitées à disposition. Les mesures visant à renforcer les capacités sont en cours. Il existe par ailleurs des lacunes judiciaires au niveau de la mise en œuvre procédurale des poursuites contre la cybercriminalité.

3.8 Cyberdéfense

N°	Mesure	Projets de mise en œuvre	Statut
22	Développement des capacités d'acquisition d'information et d'attribution	Capacités d'acquisition d'information et d'attribution	Réalisé
		Réalisation d'une formation spécifique en cyberdéfense (armée)	Réalisé
23	Capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM	Utilisation des capacités développées par le COE de la BAC dans le contexte de la LRens	Réalisé
24	Garantie de la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et réglementation de son rôle subsidiaire consistant à appuyer les autorités civiles	Fin du projet de développement de la cyberdéfense	Réalisé

Tableau 10: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Cyberdéfense». Source: Conseil fédéral, 2021

[8] Triade: «Confidentiality», «Integrity» et «Availability» (CIA)

Mesures et objectifs: l'art. 6b de l'ordonnance sur les cyberrisques définit le domaine de la cyberdéfense comme l'«ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles; ce domaine inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques». Les trois mesures M22 à M24 visent à mettre en place les aptitudes et les capacités en personnel nécessaires dans le vaste secteur d'activité de la cyberdéfense.

Évaluation des prestations: les mesures M22 et M23 ont été entièrement réalisées et la mesure M24 en bonne partie. Les étapes importantes mentionnées ici comprennent la décision du Conseil fédéral de transformer la Base d'aide au commandement (BAC) de l'armée en commandement Cyber ainsi que la nouvelle stratégie Cyber du DDPS 2021-2024 (DDPS, 2021), qui sert de boussole à ce département dans le domaine de la cyberdéfense. L'armée a la capacité de lancer des mesures actives dans le cyberespace. Sa disponibilité opérationnelle dans le cyberespace est garantie dans toutes les situations. La cyberformation des militaires est également assurée; la création du Cyber Training Center, dont l'offre sera également accessible aux tiers, a toutefois été différée jusque vers 2026.

Évaluation des effets: de l'avis des participants aux entretiens, les prestations fournies dans ce champ d'action ont obtenu des effets tangibles et le thème de la cyberdéfense est clairement perçu comme un des trois piliers de la stratégie. Le SRC et l'armée ont connu un important développement durant la période stratégique étudiée et ont fortement accru leurs propres capacités. Les bases sont ainsi en place pour générer les résultats nécessaires (*outcomes*).

Bilan: les projets de mise en œuvre réalisés ont nettement renforcé tant les capacités de l'armée et du Service de renseignement de la Confédération que leur disponibilité opérationnelle dans le cyberespace. La stratégie Cyber du DDPS y contribue encore avec ses propres mesures. Il reste encore à étendre l'offre de formation destinée aux tiers. Cette nouvelle étape vise à accroître l'interopérabilité au sein du Réseau national de sécurité et à en améliorer l'impact.

3.9 Politique extérieure de cybersécurité

N°	Mesure	Projets de mise en œuvre	Statut
25	Participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité	Participation à des processus de l'ONU	Réalisé
		Défense des intérêts dans le cadre de l'OSCE (renforcement de la confiance entre États)	Réalisé
		Élaboration et établissement du Dialogue de Genève sur le comportement responsable	Réalisé

N°	Mesure	Projets de mise en œuvre	Statut
		Suivi des développements dans l'UE (en particulier au sein du Service européen pour l'action extérieure et de l'ENISA)	Réalisé
		Engagement en faveur d'un cyberespace ouvert et libre	Réalisé
26	Coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité	Réalisation d'ateliers avec des organisations régionales	Réalisé
		Ateliers sur la mise en place d'institutions et de structures de cybersécurité extérieure	Réalisé
27	Consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité	Cyber dialogue sino-européen (*Sino-European Cyber Dialogue*, SECD)	Réalisé
		MENA Cybersecurity Forum	Réalisé

Tableau 11: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Politique extérieure de cybersécurité». Source: Conseil fédéral, 2021

Mesures et objectifs: les mesures relevant de la politique extérieure de cybersécurité (M25 à M27) doivent permettre un positionnement actif de la Suisse sur le terrain de la politique extérieure de cybersécurité. Elles relèvent de la politique étrangère et ne cherchent pas à déployer d'effets immédiats pour leurs groupes cibles.

Évaluation des prestations: les responsables des mesures ont procédé à divers ajustements depuis 2018, afin de se concentrer sur les mesures apportant une contribution tangible à la stratégie. Il s'agit de jeter un pont entre les acteurs internationaux et la Suisse. Dans le cadre des mesures M26 et M27, un processus de dialogue a été établi ou est en préparation avec la Suède, les Pays-Bas, l'Autriche, la Grande-Bretagne, le Japon, les États-Unis, Israël et la Chine, sans oublier le dialogue multilatéral avec l'ASEAN. Des ateliers de renforcement des capacités ont par ailleurs été réalisés en collaboration avec la Mission permanente de la République du Kenya auprès de l'Office des Nations Unies (ONU) et d'autres États ou organisations africains (source: compilation du DFAE du 26 janvier 2022).

Évaluation des effets: il est apparu que les contributions aux débats des organismes multilatéraux ont davantage retenu l'attention que les échanges bilatéraux entre États. L'OCDE a ainsi constitué, contrairement à la première impression donnée, un cadre de travail adéquat débouchant sur des effets concrets. En outre, le délégué de la Confédération à la cybersécurité préside depuis le 1er janvier 2022 le groupe de travail sur la sécurité dans l'économie numérique (SEN) de l'OCDE. La SNPC 2018-2022 a encore apporté une contribution significative à la création du Dialogue de Genève sur le comportement responsable dans le cyberespace[9].

Lors d'un récent sondage effectué dans la population (SOTOMO, 2022), 56 % des personnes ayant répondu à l'enquête ont déclaré que la Confédération est à même de bien

[9] www.genevadialogue.ch, visite le 10 janvier 2022

représenter les intérêts de la Suisse dans les débats sur la réglementation multilatérale du cyberespace.

La participation active et stratégique de la Suisse à un dialogue international complète bien les contacts internationaux établis dans les autres champs d'application pratiques (à propos de la situation de la menace, lors de poursuites pénales ou à des fins de cyberdéfense), tout en renforçant les bases de collaboration. Ce résultat (*outcome*) aide d'autres champs d'action à atteindre leurs effets à court sinon à long terme.

Bilan: la politique extérieure de cybersécurité contribue indirectement à la protection des groupes cibles. Les autorités suisses et d'autres acteurs centraux ont pris position (dans le cadre du Dialogue de Genève) dans le sens de la SNPC 2018-2022, lors de discussions internationales sur la cybergouvernance.

3.10 Visibilité et sensibilisation

N°	Mesure	Projets de mise en œuvre	Statut
28	Élaboration et mise en œuvre d'un concept de communication pour la SNPC	Élaboration d'un plan de communication sur la SNPC	Réalisé
29	Sensibilisation du public aux cyberrisques	Développement et exécution d'une campagne nationale de sensibilisation	Réalisé
		Plateforme d'information sur les cyberrisques	Réalisé

Tableau 12: Mesures et étapes, avec leur degré de réalisation, dans le champ d'action «Visibilité et sensibilisation». Source: Conseil fédéral, 2021

Mesures et objectifs: les mesures M28 et M29 constituent le champ d'action «Visibilité et sensibilisation». Elles sont dirigées vers l'extérieur et servent à informer tant la population que l'économie sur la SNPC et sa mise en œuvre, d'une part, et sur les développements ou incidents actuels, d'autre part.

Évaluation des prestations: plusieurs campagnes de sensibilisation, basées sur le concept de communication et sur divers projets de mise en œuvre, ont été réalisées depuis 2018 à l'intérieur comme à l'extérieur de l'administration fédérale, en collaboration aussi avec la Prévention suisse de la criminalité (PSC). En parallèle, les informations publiées sur le site ont été structurées par groupe cible (population, entreprises, spécialistes et autorités) et les rapports semestriels ont été étoffés, tout comme les rapports hebdomadaires.

Les projets de mise en œuvre des deux mesures ont été en bonne partie réalisés. Il a fallu se limiter à quelques priorités pour la communication, compte tenu des ressources à disposition. Selon les axes de communication définis pour la mise en œuvre de la SNPC, la Confédération recherche non seulement le contact direct avec ses groupes cibles, mais collabore encore avec différents partenaires et tire parti d'autres organismes existants ou de plateformes tierces déjà en place. Les projets de mise en œuvre réalisés ont beau livrer

des idées et des concepts utiles pour poursuivre et pérenniser la sensibilisation, il manque à ce jour les ressources nécessaires.

Évaluation des effets: les personnes interrogées relèvent une bien meilleure visibilité, qu'elles attribuent aux activités régulières de communication du NCSC, aux campagnes de sensibilisation et aux enquêtes soutenues par ses partenaires, ainsi qu'à la communication spécifique sur des projets choisis. Les analyses basées sur l'équivalence publicitaire et le nombre d'accès, sur la durée des visites et le taux de rebond attestent d'une couverture nationale et d'une bonne approche de divers segments des groupes cibles. Les graves incidents des derniers mois ont également aidé à attirer l'attention des groupes cibles sur cet enjeu.

Il reste beaucoup à faire au sein de la population et dans les PME. Le hic réside dans la passivité d'une partie de ces groupes cibles, qui ne réfléchissent à ces thèmes qu'en cas d'incident.

On constate ponctuellement un déficit d'information sur les compétences; dans l'administration fédérale comme au Parlement, bien des gens ignorent à qui incombe telle ou telle tâche, en particulier si elle relève du NCSC ou du secteur Transformation numérique et gouvernance de l'informatique (TNI) de la Chancellerie fédérale.

Par ailleurs, d'autres services de communication de l'administration fédérale se lancent dans toutes sortes d'activités liées à la protection contre les cyberrisques, souvent sans concertation préalable avec le NCSC. Il faudrait chercher ici à améliorer la coordination, dans une approche axée sur les résultats (*outcome*), pour parvenir en définitive à l'effet visé auprès des groupes cibles.

Bilan: la SNPC jouit d'une bien meilleure visibilité, grâce à l'accent mis sur la communication, notamment dans les groupes cibles de l'économie et des infrastructures critiques. La population et les PME ne sont pas encore assez bien atteints. De même, la coordination laisse à désirer entre les activités de communication des différents acteurs. Ce champ d'action n'a qu'un impact indirect.

4 Effets sur les groupes cibles

La SNPC 2018-2022 vise à promouvoir la résilience de la population, de l'économie et de l'État face aux cybermenaces, de façon à garantir leur capacité d'agir et leur intégrité. L'évaluation de l'efficacité a examiné si et comment de tels effets étaient constatables pour ces groupes cibles. Les considérations et évaluations qui suivent se rapportent surtout au niveau des résultats (*outcome*) de la stratégie.

Concrètement, les questions suivantes ont été analysées:

Utilité: les mesures de la SNPC atteignent-elles les groupes cibles dans la mesure souhaitée? (par ex. les groupes cibles utilisent-ils les mesures ou les structures et processus établis, de même que les produits, les services, les réseaux et les méthodes mis en place, etc.?)

Effets visés pour les groupes cibles: dans quelle mesure les effets visés par la SNPC 2018-2022 (aptitudes des acteurs, résilience, etc.) ont-ils été atteints pour ses quatre groupes cibles (infrastructures critiques, autorités, économie, population)?

Effets sur d'autres acteurs: y a-t-il au niveau des groupes cibles d'autres effets non voulus? Comment faut-il les interpréter?

4.1 Autorités

Les activités de développement et de mise en œuvre de la stratégie ont bénéficié, selon les personnes interrogées, d'un solide ancrage dans l'administration et les autorités. Les champs d'action et les mesures formaient un ensemble cohérent, ce qui n'est guère surprenant sachant que sa structure et ses mesures se réfèrent directement aux structures de l'administration. Il a également été souligné que la SNPC a permis d'améliorer la collaboration entre la Confédération et les cantons.

Partout où les acteurs ou les groupes cibles ont été étroitement associés à la SNPC, on observe un effet positif, dans le cas des autorités notamment. La stratégie a largement œuvré à la sensibilisation. Elle produit également son effet là où la répartition des tâches est clairement définie. Dans les cas où elle se contente de sensibiliser, la stratégie a au mieux un effet à court terme.

Il a été signalé que d'autres autorités, au niveau cantonal notamment, ont repris la stratégie nationale afin de lancer leurs propres projets de gestion des cyberrisques. Les personnes interrogées réservent par contre leur jugement à propos des villes et les grandes communes. La population est elle aussi consciente de la nécessité d'agir, dont les médias se sont fait l'écho au cours des derniers mois. Seules 28 % des personnes questionnées à propos de la cybersécurité de l'administration et des infrastructures critiques la jugent suffisante (Sotomo, 2022).

Toujours à propos des autorités, l'importance d'une mise en réseau horizontale a été soulignée. Elle est encore jugée insuffisante; les personnes s'occupant des mêmes thèmes dans différents domaines devraient avoir la possibilité de davantage se concerter.

Bilan: les autorités tant fédérales que cantonales sont bien impliquées dans la stratégie et ses projets de mise en œuvre. Les prestations réalisées (*output*) contribuent à la sensibilisation. Elles produisent des effets, pour autant que les compétences et responsabilités aient été dûment précisées.

4.2 Infrastructures critiques

De l'avis d'une majorité des participants aux entretiens, il y a eu de nouvelles avancées sur le plan de la sensibilisation. Les exploitants d'infrastructures critiques ont été largement impliqués, branche par branche, par le biais du projet de protection des infrastructures critiques (PIC) de l'Office fédéral pour la protection de la population (OFPP) ainsi que des mesures en la matière prévues dans le Plan de mise en œuvre des cantons de la SNPC élaboré par le Réseau national de sécurité (RNS).

Les exploitants d'infrastructures critiques prennent bien davantage au sérieux que dans le passé la protection face aux cyberrisques. Dans les branches comptant des acteurs de poids, un rapprochement a eu lieu, les échanges sont plus intenses et on constate un engagement accru. Ce n'est guère le cas à ce jour dans les branches caractérisées par une structure morcelée et par un très grand nombre d'acteurs, où la conscience du problème est moins prononcée.

Différentes études, analyses et enquêtes confirment cette impression d'un degré de conscience variable et parfois insuffisant du problème. C'est ainsi qu'une étude consacrée par l'OFEN au secteur suisse de l'approvisionnement électrique fustige le manque de maturité des acteurs de la branche pour mettre en œuvre les mesures recommandées (OFEN, 2021). Dans son rapport semestriel 2020/2, le NCSC s'est penché sur les menaces pesant sur le secteur de la santé et a recommandé la mise en œuvre de diverses mesures de protection supplémentaires (NCSC, 2021a). En automne 2021, un sondage réalisé outre-Sarine auprès de 1254 personnes (Sotomo, 2022) a encore montré qu'aux yeux de 72 % des personnes ayant répondu à l'enquête la protection des infrastructures critiques et des autorités face aux cyberrisques est insuffisante en Suisse.

Les personnes interrogées sont pleinement conscientes du conflit d'objectifs entre l'attitude responsable attendue des exploitants d'infrastructures critiques et le caractère non contraignant des mesures de protection. Le potentiel d'impact est encore loin d'être épuisé. Il faudrait examiner ici d'autres approches pour encourager la mise en œuvre des mesures. Un tour de vis réglementaire est évoqué, allant du recours au principe de précaution jusqu'au respect d'une norme minimale fixée dans la loi, en passant par une obligation de révision (similaire à celle de tenir une comptabilité). Une autre approche consisterait à mener des analyses plus poussées des événements dangereux, de leurs causes et raisons profondes, afin de prévenir de futurs incidents ou situations à risque. La

procédure de consultation en cours sur l'introduction d'une obligation de notifier les cyberincidents qui incomberait aux exploitants d'infrastructures critiques indique une piste possible.

Bilan: les exploitants d'infrastructures critiques sont sensibilisés et étroitement associés aux mesures ou projets de mise en œuvre; on constate toutefois de nettes différences entre les secteurs. Aussi les prestations adoptées en vertu de la stratégie ne suffisent-elles pas à protéger de façon adéquate toutes les infrastructures critiques.

4.3 Population

De nombreuses personnes ayant répondu à l'enquête reconnaissent que la population est devenue plus réceptive aux enjeux de la cybersécurité. De l'avis des responsables des mesures, les campagnes de sensibilisation et les activités de relations publiques déployées dans le cadre de la SNPC et par le SCSC ont eu une portée en rapport avec les moyens engagés. Il n'existe toutefois pas d'évidence empirique à ce sujet, ni sur la contribution due aux initiatives et campagnes de sensibilisation menées en parallèle[10].

Le NCSC reçoit toujours plus d'annonces de la population (en 2021, plus de 21 400 annonces ont été reçues au total), même si le lien est peu clair entre la recrudescence des cyberattaques et une sensibilisation accrue permettant de juger d'un incident et de le signaler. Le NCSC sert en partie de guide à la population et joue ainsi un rôle de sensibilisation auprès de certains cercles de la population. Il convient de noter ici que non seulement les compétences numériques diffèrent entre catégories de la population, mais aussi les instruments informatiques à disposition et l'usage qui en est fait (voir par ex. Université de Zurich, 2020). A contrario, la gestion des incidents proposée par le NCSC ne s'adresse que ponctuellement à la population.

À ce jour, la SNPC n'a pas su sensibiliser les jeunes, faute de leur offrir une «cyberformation de base» obligatoire. À en croire notamment les représentants de l'économie interrogés, ce serait le levier le plus puissant et le plus efficace à long terme pour protéger la population face aux cyberrisques. Il est vrai que la SNPC dispose ici de possibilités jugées limitées, d'autant plus que la formation est une prérogative des cantons.

Les lacunes en «cyberformation de base» revenant dans différentes déclarations vont de pair avec une compétence numérique jugée insuffisante (Sotomo, 2022). Lors d'une enquête menée au sein de la population, 60 % des participants ont jugé que le développement des compétences numériques est à la traîne dans la formation.

Bilan: les mesures de la SNPC 2018-2022 n'atteignent que très ponctuellement la population et n'ont pas déployé à ce jour d'effet de sensibilisation à grande échelle.

[10] Il n'existe aucune vue d'ensemble de ce genre d'initiatives et des campagnes de tiers.

4.4 Économie

Lors des entretiens consacrés à la protection de l'économie, tout le monde s'est accordé à dire que les grandes entreprises internationales se protègent mieux face aux cyberrisques. Elles font ponctuellement bénéficier la SNPC de leurs compétences et expériences. Les PME par contre, qui constituent l'épine dorsale de l'économie suisse, ne seraient pas suffisamment protégées et sous-estimeraient les menaces présentes dans le cyberespace. De l'avis des experts, les efforts consentis pour renforcer la protection n'ont pas suivi l'augmentation des cyberattaques. Deux points faibles expliqueraient surtout cette situation:

— *Cibles des attaques*: les entreprises s'imaginent être des cibles «peu intéressantes».

— *Conscience des menaces pesant sur les données*: on tend à se concentrer avant tout sur la protection des données et à négliger la disponibilité et l'intégrité des données (et des processus d'affaires).

Les enquêtes actuelles menées auprès des entreprises confirment que dans bien des cas, elles ne sont pas suffisamment protégées face aux cyberattaques (gfs-Zürich, 2021). C'est ainsi que la part des entreprises attaquées qui ont dû consentir des efforts considérables pour réparer les dommages a bondi de 25 % en 2020 à 33 % à la fin de 2021 (gfs-Zürich, 2021). Le NCSC a également enregistré une augmentation des attaques, qui touchent toujours plus souvent des entreprises internationales connues (NCSC, 2021b). Une extrapolation suggère qu'en Suisse, près de 55 000 entreprises ont déjà subi une attaque lourde de conséquences lancée depuis le cyberespace.

L'enquête de gfs-Zürich (2021) révèle en outre une forte corrélation entre la taille des entreprises et la conscience des cyberrisques. La population aussi a un avis nuancé sur la compétence numérique des entreprises (Sotomo, 2022). Selon un sondage actuel, 78 % des gens jugent élevée la compétence numérique des grandes entreprises. Dans le cas des PME, ils ne sont plus que 45 % à leur attribuer une grande compétence numérique. Quant à la cybersécurité, 87 % des personnes interrogées espèrent un redoublement des efforts étatiques visant à protéger les entreprises des cyberattaques.

On observe qu'à l'heure actuelle, les entreprises investissent beaucoup dans leur protection technique et que le régime de travail à domicile instauré en raison de la pandémie a donné un coup d'accélérateur à cette évolution. Les déficiences organisationnelles n'ont pas pour autant disparu. Les cas d'«arnaque au président» ont même fortement augmenté. Les mesures de la SNPC 2018-2022 ne sont pas assez efficaces pour amener les PME à améliorer systématiquement leurs activités de protection. La SNPC 2018-2022 a créé de bonnes bases, en mettant en place différentes mesures (par ex. dans les champs d'action «Acquisition de compétences et de connaissances», «Normalisation et réglementation» et «Visibilité et sensibilisation»). Il n'y a toutefois pas assez de mesures et de possibilités (financières, organisationnelles, réglementaires, etc.) prévues pour encourager la diffusion à grande échelle et la reprise des bases et des bonnes pratiques.

L’admission des entreprises dans le cercle fermé des clients du NCSC est considérée comme une mesure très efficace pour obtenir leur coopération. Un effet multiplicateur est à prévoir de la part des entreprises impliquées de cette façon. En effet, le battage publicitaire autour des graves incidents subis par des entreprises connues suscite de réelles attentes quant à l’effet de sensibilisation des mesures adoptées. Les médias mentionnent toujours plus souvent dans ce contexte le NCSC, renforcé par la fonction de délégué du Conseil fédéral à la cybersécurité que son directeur exerce depuis 2019.

Bilan: l’économie n’a pas suffisamment amélioré sa protection face aux cyberrisques dans le cadre de la SNPC 2018-2022. En particulier, la SNPC ne parvient guère avec les prestations réalisées (*outputs*) à amener les PME à prévoir des activités pour améliorer leur protection.

5 Bilan de l'efficacité de la SNPC

Les explications qui suivent répondent aux grandes questions inhérentes à l'évaluation de l'efficacité (évaluation sommative).

5.1 Réalisation des objectifs stratégiques

Question: Dans quelle mesure la SNPC 2018-2022 a-t-elle atteint les objectifs stratégiques définis?

Pour réaliser la vision de la SNPC 2018-2022, il s'agissait de poursuivre systématiquement sept objectifs stratégiques (voir figure 1). La SNPC 2018-2022 soutient ces objectifs, en définissant des champs d'action auxquels correspondent à chaque fois des mesures assorties de projets de mise en œuvre. Sa contribution à la réalisation de la vision initiale est la suivante:

— La SNPC 2018-2022 forme un cadre cohérent, axé sur la réalisation des objectifs fixés. Les objectifs et la conception de la stratégie forment une structure logique, tenant compte du contexte institutionnel et thématique. L'accent est résolument mis sur le potentiel de résultats.

— La SNPC 2018-2022 a déjà été mise en œuvre dans une large mesure, et toutes les mesures ont produit des effets pertinents (*outcomes*) avant que la stratégie ne touche à sa fin. Mais il s'est écoulé trop peu de temps entre la mise en œuvre des mesures, avec l'obtention de résultats et l'impact attendu sur la cyberprotection, afin qu'il soit possible de fournir des observations solides ou mesurables.

— Les effets visés au niveau des mesures sont en principe jugés propres à atteindre les objectifs fixés. Les groupes cibles n'ont toutefois pas reçu la même attention. D'une part, les mesures ont été plus ou moins efficaces d'un groupe cible à l'autre et au sein des groupes cibles. D'autre part, l'hétérogénéité des groupes a fait obstacle à la réalisation des objectifs stratégiques de la SNPC 2018-2022.

— La SNPC 2018-2022 présente des déficits au niveau de son pilotage stratégique, de la planification de la mise en œuvre et des ressources disponibles. Ces déficits ont pesé sur ses effets potentiels. Le peu d'importance accordée à la mesure de l'impact, au niveau des champs d'action et des mesures, nuit à sa réactivité et donc aux adaptations des mesures visant à maximiser en permanence les effets obtenus.

— La forte dynamique des cybermenaces (avec notamment une forte recrudescence des attaques) risque de mettre en péril la réalisation des objectifs stratégiques, au cas où les mesures de la SNPC ne parviendraient pas à renforcer dûment la protection de la Suisse et sa capacité d'adaptation dynamique.

Bilan: la SNPC 2018-2022 constitue une stratégie cohérente, avec un plan de mise en œuvre qui soutient la réalisation des objectifs stratégiques. Sa mise en œuvre respecte le

calendrier et aboutit à des résultats pertinents, qui n'atteignent toutefois pas de la même façon tous les groupes cibles. Des interventions ciblées (mesures d'impact et pilotage stratégique notamment) permettraient de renforcer encore l'efficacité de la mise en œuvre de la SNPC.

5.2 Effets

Question: dans quelle les prestations fournies ont-elles permis d'obtenir les effets recherchés?

Les effets de la SNPC 2018-2022, comme impact à long terme sur la société et l'économie helvétiques, ne sont guère mesurables à ce jour et il n'est pas possible non plus de les démontrer empiriquement d'une autre manière. L'estimation consolidée fondée sur des entretiens avec les responsables des mesures ou des représentants des groupes cibles ainsi que sur des études actuelles appelle les commentaires suivants:

— À ce jour, on peut considérer que les infrastructures critiques, les autorités ou institutions nationales, ainsi que les autorités cantonales et les hautes écoles ont été les principaux bénéficiaires des effets des mesures. L'économie et la population n'en ont que peu profité jusqu'ici, voire pas du tout.

— De grandes différences sont observables dans l'économie, en fonction du spectre d'activités et de la taille des entreprises. Alors que les exploitants d'infrastructures critiques et les grandes entreprises internationales ont accru leur cyberprotection, la plupart des PME demeurent insuffisamment protégées.

— Les villes et les communes sont considérées comme insuffisamment protégées. Les mesures de la SNPC 2018-2022 ne les atteignent guère. Les institutions cantonales actives dans le cadre de la SNPC ne parviennent pas à opérer un transfert efficace des mesures réalisées au profit des villes et des communes.

— Dans le cas du groupe cible de la population, la SNPC 2018-2022 n'a pas d'effets directs en termes d'amélioration de la cyberprotection. Les mesures réalisées n'agissent pas directement sur la population.

— De façon générale, la SNPC 2018-2022 manque de canaux ou de capacités pour faire connaître les effets visés des mesures aux groupes cibles et pour les amener à déployer des activités aboutissant à un niveau accru de cyberprotection. Les prestations fournies au titre des mesures réalisées ne déploient dès lors pas tous leurs effets.

Bilan: on peut considérer qu'à ce jour, la SNPC 2018-2022 déploie des effets au profit surtout des infrastructures critiques, des autorités ou institutions nationales et cantonales ainsi que des grandes entreprises. Aucune preuve empirique n'en atteste toutefois dans le cadre de la SNPC 2018-2022. En outre, de clairs indices montrent que les mesures de mise en œuvre de la SNPC n'atteignent pas de façon substantielle les PME, les villes et les communes ainsi que la population, ni ne les aident à renforcer leur cyberprotection.

5.3 Efficacité

Question: comment se présente le rapport entre les moyens engagés et les prestations fournies durant la mise en œuvre de la stratégie?

Les moyens financiers consacrés à la SNPC 2018-2022 sont faibles en comparaison internationale. Si l'on se place dans l'optique des prestations fournies, les conclusions suivantes peuvent être tirées:

- Les ressources allouées étaient suffisantes pour produire jusqu'au moment de l'enquête (automne 2021) les effets prévus dans la mission de base, en déployant les mesures inscrites dans le plan de mise en œuvre. Ces effets visés (*outcomes*) sont nécessaires afin que la SNPC 2018-2022 puisse déployer son impact potentiel.
- L'efficience dans l'allocation des ressources doit être examinée d'un œil critique, sachant que:
  - le nombre élevé de mesures et de projets de mise en œuvre a rendu très difficile la concentration des moyens financiers;
  - une compétition pour les ressources a été parfois constatée entre l'activité de projet et les activités opérationnelles. La capacité d'agir peut en pâtir, tout comme l'intégrité face aux cybermenaces dans les tâches d'exécution courantes;
  - le transfert des prestations produites jusqu'aux groupes cibles n'a pas pu être suffisamment garanti, faute de ressources.
- Les ressources en personnel supplémentaires demandées jusqu'à la fin de la SNPC 2018-2022 sont jugées justifiées et nécessaires pour atteindre une qualité élevée dans l'accomplissement de la mission (sous forme d'activités de projet et d'activités opérationnelles). Des clarifications s'imposent encore sur le montant exact de la dotation supplémentaire. Il est indiqué de distinguer ici entre les activités de projet te les activités pérennes (par ex. aperçu des cas en cours).

Bilan: la SNPC 2018-2022 a rempli jusqu'ici sa mission de base avec les ressources mises à sa disposition. L'allocation des ressources pourrait toutefois être davantage axée sur les objectifs d'impact. L'augmentation des ressources en personnel pour la fin du programme ainsi que pour les activités pérennes paraît justifiée.

6 Perspectives et recommandations

Le cyberespace se caractérise par une très forte dynamique. La cybersécurité doit par conséquent être considérée comme un développement dynamique. Elle vise à garantir en tout temps, compte tenu des conditions-cadres applicables, des possibilités technologiques, des exigences organisationnelles et de la situation concrète de la menace, la capacité d'agir et l'intégrité des entreprises, des organisations ainsi que des collectivités publiques et des ménages. L'amélioration de la protection face aux cyberrisques constitue ainsi une tâche à poursuivre même après 2022. Dans l'optique des prochains cycles stratégiques de la SNPC (par ex. 2023-2027), une grande question a été examinée (évaluation formative):

Question: quelles sont les recommandations pouvant être formulées sur la base de l'évaluation de l'efficacité, en vue de la refonte de la stratégie, d'une part, et pour l'utilisation à venir des ressources humaines et financières, d'autre part?

L'évaluation de l'efficacité signale divers facteurs de succès critiques au niveau tant matériel qu'organisationnel. Ces facteurs de succès sont autant de conditions qui à un niveau donné, revêtent une importance centrale pour la réalisation des objectifs globaux de la SNPC 2018-2022. Si de telles conditions ne sont pas toutes réunies voire si les conditions sont défavorables, de tels déficits peuvent sérieusement entraver l'efficacité de la SNPC (d'après: Gabler Wirtschaftslexikon, www.wirtschaftslexikon.gabler.de, visite le 22 janvier 2022).

Sur la base des facteurs critiques de succès identifiés, des recommandations peuvent être formulées sur la manière d'améliorer la conception adéquate définie pour la SNPC afin d'en accroître l'efficience et l'efficacité et d'obtenir ainsi le meilleur impact possible. Les recommandations ci-après se basent sur la structure de l'actuelle SNPC.

6.1 Processus et acceptation

Un facteur de succès majeur de la SNPC 2018-2022 tient à son processus d'élaboration. Elle a été conçue de manière structurée, avec la participation d'un grand nombre d'acteurs. Une telle approche:

- garantit une large prise en compte des bases, des défis ou des capacités propres aux divers groupes cibles;
- augmente l'acceptation des mesures, comme elles ont été développées en commun;
- crée une base de participation dans la mise en œuvre; la collaboration nécessaire a été dûment établie;
- crée un réseau qui a conduit à la diffusion des prestations réalisées, voire à des activités ayant les effets visés au sein des groupes cibles.

Le processus d'élaboration de la SNPC 2018-2022 a marqué le ton comme «nouveau développement» de la stratégie. Après le lancement de la SNPC 2012-2017, les premières expériences ont été exploitées de manière ciblée afin de renforcer l'approche stratégique et la participation de nombreux acteurs au deuxième cycle stratégique.

Recommandation: les avantages d'un processus d'élaboration participatif doivent être exploités de manière ciblée en vue du développement de la SNPC. Un processus géré de façon stricte et efficiente motivera les divers dépositaires du savoir à bien collaborer.

6.2 Gouvernance

La gouvernance, assurée dans une structure de réseau avec comité de pilotage, est jugée propice à la réalisation de la SNPC. La mise en place du NCSC a en outre renforcé les capacités opérationnelles de coordination ainsi que la gestion opérationnelle des thèmes transversaux. De nombreux participants déplorent toutefois le manque d'efficacité du comité de pilotage. Du fait de sa taille et de son organisation et faute de vue d'ensemble de ses divers membres, il n'a guère été en mesure jusqu'ici d'assurer un pilotage stratégique. Les capacités du comité de pilotage servent essentiellement au contrôle de gestion des mesures, tandis que les discussions globales sur des sujets stratégiques restent peu significatives.

Lors des entretiens menés, la nécessité de réduire la taille du comité et de concentrer ses activités est apparue à diverses reprises. Des possibilités d'échanges tant formels qu'informels entre tous les participants à la mise en œuvre de la SNPC devraient être prévues dans d'autres organes ou structures, toujours selon le principe de l'autogestion.

Recommandation: le comité de pilotage doit être réorganisé dans sa structure (il faudrait en particulier réduire sa taille) comme dans ses fonctions et tâches, pour en renforcer les possibilités de pilotage stratégique. Il faudrait par ailleurs encourager d'autres possibilités de mise en réseau.

L'analyse des effets a montré qu'il existe entre les groupes cibles des différences significatives quant à l'impact obtenu. Des difficultés apparaissent surtout avec les PME, les autorités communales et la population. Comme la Confédération ne dispose que d'accès directs très limités à ces protagonistes, elle a peu d'informations actuelles sur leurs difficultés et leurs besoins concrets. Au niveau opérationnel, il est recommandé de prévoir des «projets passerelle» visant à améliorer la collaboration et le transfert. Le cas échéant, il serait possible d'accroître la pertinence et l'efficacité de tels projets en impliquant davantage à l'échelon stratégique de la SNPC les groupes d'intérêts des PME, les autorités communales ainsi que l'administration.

Recommandation: il faudra étudier de quelle manière les PME et l'échelon communal pourraient être plus étroitement associés à la gouvernance de la SNPC.

6.3 Objectifs stratégiques

Il ressort de l'évaluation de l'efficacité que les objectifs stratégiques de la SNPC sont opportuns et adéquats dans l'ensemble. Ils s'inscrivent dans une structure classique comprenant une vision, des objectifs et des champs d'action pour atteindre les objectifs. La stratégie est complétée par un plan de mise en œuvre qui concrétise les mesures avec des projets de mise en œuvre.

Il a été ponctuellement suggéré d'axer expressément la vision de la SNPC sur un horizon temporel plus long que les cycles stratégiques actuels. Une telle approche fournirait également de précieux repères aux projets à plus long terme. Car un certain nombre de projets de mise en œuvre, avec les mesures correspondantes, ne sauraient être réalisés efficacement dans un seul cycle stratégique.

L'analyse de l'efficacité révèle qu'au stade de la mise en œuvre, les objectifs stratégiques ne bénéficient pas tous du même degré d'attention. Les mesures comportent parfois des objectifs peu concrets et doivent être resituées dans un contexte plus général. Il n'est pas toujours jugé possible de les mettre en œuvre indépendamment les unes des autres. Or des objectifs peu clairs réduisent l'impact des mesures (éparpillement, groupes cibles flous, etc.), et il devient très difficile de mesurer et d'évaluer les effets obtenus. La matrice SMART (spécifique, mesurable, accepté, réaliste, temporellement défini) offre une piste possible pour pouvoir formuler des objectifs précis et en mesurer les effets respectifs.

La fixation d'objectifs simples et compréhensibles à tous les niveaux est jugée importante à la mise en commun efficace des activités et des ressources. Or la SNPC 2018-2022 laisse parfois à désirer à cet égard. Alors que sa vision et ses objectifs stratégiques leur paraissent concrets, les participants jugent insuffisamment concrets les objectifs des divers projets de la SNPC 2018-2022.

Recommandation: les objectifs seront formulés aussi concrètement que possible et en toute indépendance à tous les niveaux de la stratégie, y compris dans les projets de mise en œuvre.

Le transfert des prestations fournies (*outputs*) jusqu'aux groupes cibles est l'un des points faibles de la SNPC 2018-2022. Un concept de communication a certes été élaboré, et la forte augmentation des activités de communication a accru de manière mesurable la visibilité de l'enjeu de la cybersécurité ainsi que du SNPC pour les groupes cibles et le grand public.

Quoi qu'il en soit, de nombreux partenaires interrogés estiment qu'il faudrait renforcer les efforts de communication. La cybersécurité devrait gagner en visibilité et il faudrait prévoir des activités encore mieux profilées et plus percutantes. Les campagnes menées dans le secteur de la santé ont été citées ici comme modèles possibles. Il faudrait encore mieux «vendre» les activités prévues et les étapes franchies, et des projets ou succès spécifiques devraient obtenir un écho médiatique adéquat. En outre, il a été suggéré de davantage regrouper et de coordonner les activités de communication que les divers services fédéraux consacrent à la gestion des cyberrisques. De même, les «acteurs clés», à

commencer par les acteurs économiques, devraient s'engager comme multiplicateurs. L'accent devrait être mis, dans le renforcement des efforts de communication, sur le groupe cible de la population. À cet effet, il faudra utiliser des messages accrocheurs, comme l'ont fait par exemple les campagnes de la Suva ou la campagne d'information de la Confédération sur le coronavirus.

Recommandation: il faudrait renforcer, regrouper et coordonner les activités de communication. Il convient d'examiner s'il y a lieu de prévoir un nouvel objectif stratégique intitulé «Transfert et communication».

6.4 Groupes cibles

La SNPC ne peut déployer d'effets qu'à condition de s'adresser de manière adéquate à ses groupes cibles. Seules les activités réalisées par les groupes cibles permettent d'accroître la protection de la Suisse face aux cyberrisques (voir le modèle d'effets de la figure 2). À cet effet, il est important d'avoir une perception différenciée des groupes cibles et des défis qu'ils rencontrent, ainsi que d'atteindre directement un maximum d'acteurs avec les mesures réalisées.

Les mesures ont un impact maximal là où des représentants des groupes cibles sont directement associés à leur planification et à leur mise en œuvre. Or la SNPC 2018-2022 n'a désigné des représentants directs que pour quelques groupes cibles revêtant une grande importance stratégique. Là où ils n'étaient que des bénéficiaires passifs des mesures, les effets ont eu tendance à être jugés insuffisants (par ex. groupe cible «population», «économie» en partie aussi).

Recommandation: les mesures de la SNPC doivent autant que possible satisfaire directement les besoins des groupes cibles. Ces derniers seront associés sous une forme adéquate (a fortiori la «population») aux projets de mise en œuvre.

Il s'agit d'associer la Confédération, les cantons et les villes et communes à la mise au point et au traitement des mesures concrètes. Par exemple, l'introduction d'un plan de mise en œuvre des cantons de la SNPC, qui avait été élaboré par le Réseau national de sécurité (RNS) et qui incluait un module d'apprentissage en ligne pour sensibiliser les employés cantonaux aux cyberrisques, a facilité la réalisation et la diffusion des projets de mise en œuvre.

Recommandation: il convient d'examiner si la SNPC devrait lancer des «projets passerelles» aux trois échelons étatiques.

6.5 Plan de mise en œuvre

Le plan de mise en œuvre, rédigé en parallèle à la SNPC 2018-2022, a joué un rôle important dans le lancement rapide d'activités et la prise en compte d'objectifs stratégiques. Ce plan est jugé trop rigide de divers côtés. Un tel constat rejoint les

appréciations selon lesquelles la stratégie concrétisant la vision de la SNPC devrait déployer ses effets pendant plus de quatre ans et s'accompagner d'un plan de mise en œuvre évolutif. Un plan de mise en œuvre offrant une plus grande flexibilité est parfois perçu comme plus attrayant dans une optique de collaboration.

Recommandation: il faudrait davantage flexibiliser la conception et le déroulement du plan de mise en œuvre, en prévoyant le cas échéant des cycles stratégiques plus longs.

L'introduction d'un plan de mise en œuvre plus flexible ou évolutif doit s'accompagner du renforcement des mesures d'impact et du contrôle de gestion (voir la recommandation ci-après du chapitre 6.6 et le pilotage stratégique (voir la recommandation du chapitre 6.2).

6.6 Mesures adoptées et mesure de leur impact

Les 29 mesures reflètent la diversité des défis actuels et couvrent dès lors une large palette de thèmes. Ce nombre élevé de mesures pourrait toutefois donner à penser que la SNPC a créé un ensemble disparate de mesures.

Une structuration supplémentaire basée sur une typologie des mesures, telles les mesures-clés ou les mesures d'accompagnement, montrerait les priorités et soulignerait les interactions voulues. On pourrait distinguer par exemple entre les «mesures immédiates», les «bonnes pratiques», les «projets de réglementation», les «projets transversaux de base» et les «projets pilotes». Il faut également songer aux différences entre les projets de durée limitée et ceux prévoyant la mise en place d'une activité opérationnelle ainsi que sa pérennisation. En outre, il serait possible de définir un niveau d'ambition spécifique pour les mesures clés et d'évaluer les mesures d'accompagnement en fonction de leur soutien effectif aux mesures clés.

Recommandation: il faudrait à l'avenir affiner la liste des mesures et de leurs projets de mise en œuvre, avec des critères de tri comme le type de mesure et la nature de l'objectif visé, la durée de l'intervention ou son niveau d'ambition.

Plusieurs partenaires interrogés ont indiqué d'autres thèmes ou questions, en invitant à leur consacrer des mesures spécifiques lors du prochain cycle stratégique:

— *Prise en compte des risques liés à la chaîne d'approvisionnement*: la Suisse est très dépendante de chaînes d'approvisionnement mondialisées. Or la production en flux tendus, la grande complexité des relations commerciales et la réduction au minimum des stocks rendent la chaîne de création de valeur sujette aux dysfonctionnements, aux pannes ou aux cyberattaques. Il faudrait donc examiner systématiquement comme tel le thème des risques liés à la chaîne d'approvisionnement, ou du moins l'ajouter aux autres facteurs affectant les mesures en place. Il en sera également tenu compte dans les processus de politique extérieure et dans le cadre du dialogue multilatéral, en raison de la dimension mondiale des chaînes d'approvisionnement.

— *Renforcer la formation*: comme cela a été souligné à diverses reprises, la capacité qu'ont tous les acteurs des divers groupes cibles de bien gérer les divers cyberrisques s'avère déterminante pour le succès de la stratégie. Le thème de la formation et du perfectionnement devrait donc bénéficier d'une attention encore plus grande qu'aujourd'hui durant le prochain cycle stratégique.

— *Écosystème suisse de la cybersécurité*: les cyberrisques constituent un défi mondial et requièrent des mesures techniques et organisationnelles spécifiques. Une économie nationale considérée comme bien protégée et affichant un niveau élevé d'intégrité et de capacité d'agir face aux cyberincidents jouira d'avantages compétitifs dans la concurrence mondiale entre places économiques. En outre, le développement systématique du savoir dans un écosystème de cybersécurité déjà mature crée de nouveaux débouchés pour l'exportation de technologies et de services à forte intensité de connaissances. L'inscription dans la SNPC du thème d'un écosystème de la cybersécurité soulignerait encore les opportunités résultant de cette stratégie.

Recommandation: la SNPC devrait aborder d'autres thèmes encore dans ses mesures. Les thèmes des risques de la chaîne d'approvisionnement, de la formation et de l'écosystème de la cybersécurité sont jugés prioritaires pour tirer parti des opportunités.

Les mesures de la SNPC 2018-2022 ne comportent pas d'analyse systématique de leurs effets. Le pilotage inhérent à la stratégie repose à ce jour sur un monitorage de sa mise en œuvre. Une analyse des effets s'avère d'autant plus compliquée que pour des raisons compréhensibles, les mesures comportent parfois des objectifs peu concrets, dont le degré d'ambition n'est jamais précisé. Or divers acteurs soulignent à quel point des objectifs mesurables et dont les effets sont régulièrement mesurés sont importants et constituent un facteur de succès. Les activités de mesure d'effets facilitent le pilotage stratégique et l'allocation des ressources de la SNPC. C'est d'ailleurs sur la base de telles analyses, menées au niveau des mesures individuelles, qu'il est possible de juger en tout temps de l'efficacité globale de la SNPC.

Des réflexions ont porté entre-temps sur la manière de mesurer les effets d'une stratégie similaire, soit la cyberstratégie du DDPS, en attribuant un degré de maturité aux activités déployées. Une telle approche a aussi été utilisée lors d'un examen de la cybersécurité consacré à la Suisse (University of Oxford, 2020). De telles approches scientifiques établies peuvent servir à établir des classements internationaux (*benchmarking*).

Recommandation: il faudrait à l'avenir inclure une analyse des effets dans toute activité de planification d'une stratégie et de ses mesures. Il s'agira de tirer parti de manière ciblée, pour l'élaboration de telles mesures d'impact, des avantages du processus d'élaboration participative ainsi que de l'expérience acquise aussi bien par les stratégies «voisines» des départements concernés que par le plan de mise en œuvre des cantons de la SNPC.

6.7 Ressources

Le chapitre 2.3 (Ressources) et le chapitre 5.3 (Efficience) montrent que les ressources engagées pour la mise en œuvre de la SNPC 2018-2022 sont adéquates. Les ressources allouées ont ainsi permis jusqu'ici de remplir la mission de base de la SNPC 2018-2022.

Des pénuries sont toutefois apparues et ont suscité un désir de renforcement ciblé sur le plan des ressources humaines. Pour qu'un tel renforcement soit possible à court terme, il faudrait adapter certaines conditions-cadres en place. D'une part, il faut être au clair sur l'objectif ou le niveau d'ambition que l'on vise à atteindre. Il s'agit de définir ici des objectifs plus clairement mesurables, en ajoutant le cas échéant des indicateurs, afin qu'il soit possible de déterminer la performance des activités réalisées («*key performance indicators*»). On pourra d'autant mieux en déduire les compétences et les qualifications requises pour atteindre l'objectif fixé.

D'autre part, il devrait être possible d'allouer plus facilement qu'aujourd'hui les ressources là où d'importants besoins se font sentir. Or les longs cycles de la planification pluriannuelle et les budgets gérés de manière décentralisée ne se prêtent guère à une allocation flexible et rapide des ressources. Il faudrait donc réexaminer d'un œil critique les processus de planification et de budgétisation de l'administration fédérale, dans le contexte de la structure du réseau de la SNPC. Il s'agit par exemple d'étudier s'il y a lieu de davantage confier au Groupe Cyber ou au comité de pilotage la gestion de ressources essentielles ou de budgets de projet.

Recommandation: il s'agit de formuler des objectifs et des niveaux d'ambition entièrement mesurables, afin que les ressources nécessaires puissent être chiffrées plus précisément. Le Groupe Cyber ou le comité de pilotage s'occuperont davantage de la gestion des budgets de projet, afin de faciliter la répartition des ressources.

Le besoin d'experts techniques supplémentaires se fait sentir dans tous les groupes cibles et à tous les niveaux. La forte dynamique du cyberespace exige des activités constantes de formation continue. Lors du prochain cycle stratégique aussi, il faudra donc clairement mettre l'accent sur le thème de la formation et du perfectionnement ainsi que sur le renforcement des capacités.

Recommandation: des mesures ciblées de formation et de perfectionnement serviront à renforcer le pool d'experts techniques.

Annexe

A-1 Détails sur l'approche suivie

Analyse documentaire et entretiens avec les responsables des mesures

N°	Méthode/étape	Période	Détails	Information/résultats générés
1	Analyses documentaires	septembre à novembre 2021	Emploi d'une grille de questions Regroupement des documents (développement de la stratégie, planification de la mise en œuvre et planification des ressources) Analyse approfondie des documents spécifiques aux mesures	Préparation des brefs entretiens avec les responsables des mesures Opérationnalisation à chaque étape (*output, outcome, impact*) Remarques concernant les questions, par niveau d'impact
Secrétariat du NCSC	*Contrôle de gestion de la mise en œuvre par le secrétariat*	*septembre et octobre 2021*	*Collecte et évaluation à l'att. du comité de pilotage, selon la procédure définie pour le controlling trimestriel*	*Contrôle permanent de la mise en œuvre*
	Collecte des ressources par le secrétariat	*septembre à novembre 2021*	*Relevé des ressources sollicitées, obtenues et utilisées* *Enquête écrite réalisée par le secrétariat du NCSC*	*Aperçu des ressources engagées par mesure*
2	Entretiens directifs	septembre et octobre 2021	Premier contact avec les responsables des mesures, d'entente avec le comité de pilotage Fixation des dates et remise des éventuels documents spécifiques 10 à 12 entretiens téléphoniques / assistés par vidéo (max. 1 h) selon le guide avec les responsables des mesures Procès-verbal à usage interne des entretiens (non remis au NCSC)	Effets de la SNPC perçus, dans une perspective interne Facteurs favorisant ou inhibant les effets Défi lié à la mise en œuvre des mesures Clarification des éventuelles données nécessaires pour le contrôle de gestion de la mise en œuvre
3	*Rapport intermédiaire*	*avant la mi-novembre 2021*	– *Analyse pour le rapport intermédiaire de la perception tant interne qu'externe des mandataires*	*Résultats intermédiaires pour les mandataires* *Esquisse de thèmes possibles pour des ateliers*
4	Retour d'information au NCSC et au comité de pilotage	*fin novembre 2021*	– Rapport au comité de pilotage – Consolidation des réponses par le secrétariat du NCSC – Discussion avec econcept/EBP	Validation des résultats intermédiaires Remarques sur des points à approfondir ou clarifier

Entretiens/*focus groups* formés de représentants des groupes cibles

N°	Méthode	Période	Détails	Information/résultats attendus
1	Analyse des groupes cibles	août 2021	Définition du groupe cible Analyse des acteurs (influence subie ou exercée Sélection des acteurs (voir plus bas)	Sélection d'acteurs assurant une bonne perception extérieure dans différentes perspectives
2	Comité de pilotage (présentation/questions de clarification)	14.9.2021	Premier contact avec le comité de pilotage Explication, discussion et réactions à l'analyse des groupes cible, puis choix des partenaires à interroger Définition de l'aide et prise de contact du comité de pilotage	Acceptation du projet Choix final des représentants des groupes cibles Personnes de contact dans les groupes cibles
3	Entretiens directifs	septembre à novembre 2021	Lettre d'accompagnement du NCSC (projet fourni par econcept/EBP) Premier contact établi avec les interlocuteurs, selon la personne ou le service, par le NCSC ou econcept/EBP Prise de contact pour fixer un rendez-vous par econcept/EBP Envoi de guides d'entretien, adaptés pour chaque acteur Réalisation de l'entretien et procès-verbal (env. 45' par tél./en ligne) Procès-verbal à usage interne des entretiens (non remis au NCSC)	Effets de la SNPC perçus, dans une perspective interne Facteurs favorisant ou inhibant les effets Défi de combiner les mesures de la SNPC avec ses propres activités
4	*Focus group* Comité pour la cybersécurité de digitalswitzerland	novembre 2021	Planification en commun avec digitalswitzerland Guide pour la discussion Réalisation (2h, vidéoconférence) Procès-verbal à usage interne des entretiens (non remis au NCSC)	Effets de la SNPC perçus, dans une perspective externe Facteurs favorisant ou inhibant les effets Défi de combiner les mesures de la SNPC avec ses propres activités
5	*Rapport intermédiaire*	*avant la mi-novembre 2021*	*Analyse pour le rapport intermédiaire de la perception tant interne qu'externe des mandataires*	*Résultats intermédiaires pour les mandataires* *Esquisse de thèmes possibles pour des ateliers*
6	Retour d'information au NCSC et au comité de pilotage	*fin novembre 2021*	– Rapport au comité de pilotage – Consolidation des réponses par le secrétariat du NCSC Discussion avec econcept/EBP	Validation des résultats intermédiaires Remarques sur des points à approfondir ou clarifier

A-2 Guides pour les entretiens

Guide pour les entretiens avec les responsables des mesures

Introduction

Fonction: veuillez pour commencer nous expliquer votre fonction et vos responsabilités dans le contexte de la mise en œuvre de la SNPC 2018-2020.

Appréciation d'ensemble

Stratégie et bases: selon vous, dans quelle mesure la SNPC 2018-2022 est-elle globalement appropriée pour protéger correctement la Suisse face aux cyberrisques? Les bases pertinentes sont-elles suffisamment prises en compte? Y a-t-il à votre avis des lacunes qu'il s'agira à l'avenir de combler?

Mesures en général: jusqu'à quel point jugez-vous les 29 mesures globalement appropriées pour atteindre les objectifs de la stratégie?

Effets auprès des groupes cibles: la SNPC 2018-2022 obtient-elle à votre avis les effets visés auprès des groupes-cibles? Pourquoi (oui / non)?

Autres effets: la SNPC 2018-2022 a-t-elle selon vous d'autres effets (non voulus)?

Mise en œuvre de la SNPC 2018-2022

Mesure(s) relevant de votre responsabilité: que faut-il penser selon vous des aspects indiqués ci-après, compte tenu de l'objectif de protection de la Suisse face aux cyberrisques, soit de leur contribution à la réalisation de cet objectif:

1) projets de mise en œuvre relevant des mesures (voir la planification des mesures)?

2) niveau d'ambition (état souhaité en 2022) des mesures?

Ressources: comment jugez-vous les ressources allouées – pour la mise en œuvre de votre ou vos propres mesures, et le cas échéant dans un contexte plus large?

Structures et processus: dans quelle mesure jugez-vous les structures et/ou les processus efficaces et efficients:

1) mise en œuvre de votre/vos mesure(s)?

2) collaboration au sein de votre service/division

3) collaboration au sein du comité de pilotage/avec le NCSC

4) autres thèmes le cas échéant

Potentiels d'optimisation

Potentiels d'optimisation: où identifiez-vous le cas échéant des potentiels d'optimisation:

1) stratégie SNPC 2018-2022 (par ex. objectifs)

2) champs d’action (par ex. cohérence réciproque)

3) mesures (par ex. adéquation)

4) projets de mise en œuvre (par ex. projets supplémentaires)

Étapes-clés

Autres, le cas échéant

Conclusion

Et pour terminer: avez-vous encore d’autres remarques à nous communiquer ici?

Merci pour cet entretien.

Guide pour les entretiens avec les représentants des groupes cibles

Introduction

1 **Fonction**: veuillez pour commencer nous expliquer brièvement vos responsabilités dans la cybersécurité de votre organisation/entreprise/service.

2 **Risque et vulnérabilité**: comment évaluez-vous les aspects suivants:

2.1 risque lié aux cybermenaces pesant sur votre organisation/entreprise/poste [*représentants d'infrastructures critiques / de l'économie:* ainsi que votre branche/secteur] et

2.2 sa vulnérabilité aux cyberattaques

Comment votre appréciation des risques et de la vulnérabilité a-t-elle évolué depuis 2018?

Risques, vulnérabilité, stratégie

3 **SNPC 2018-2022**: quels sont les effets ou l'influence de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022 sur votre organisation/entreprise/poste [*représentants d'infrastructures critiques / de l'économie:* ainsi que sur votre branche/secteur]? Utilisez-vous la stratégie comme instrument de travail (oui/non)? Et pourquoi?

4 **Exigences**: à quelles exigences une stratégie de protection de la Suisse face aux cyberrisques doit-elle répondre, compte tenu des risques spécifiques et des vulnérabilités existantes? Quels aspects faut-il y régler ou non à vos yeux?

5 **Évaluation de la SNPC 2018-2022**: quel est dans ce contexte votre appréciation globale de la SNPC 2018-2022?

6 **Évaluation des champs d'action et des mesures**: et comment jugez-vous les champs d'action identifiés et les mesures visant à protéger la Suisse face aux cyberrisques? [*représentants d'infrastructures critiques / de l'économie:* jusqu'à quel point ces mesures contribuent-elles selon vous à protéger votre branche/votre secteur?]

Mise en œuvre de la stratégie

7 **Effets de la SNPC 2018-2022**: y a-t-il eu sous l'effet de la stratégie 2018-2022 des changements concrets pour votre organisation/entreprise/poste [*représentants d'infrastructures critiques / de l'économie:* ainsi que sur votre branche/secteur? Si oui, quels sont-ils?

8 **Facteurs d'influence (action stimulante ou inhibante)**: quels sont à votre avis les circonstances ou conditions générales qui soutiennent les effets de la SNPC 2018-2022? Et qu'est-ce qui en freine les effets?

9 **Potentiels d'optimisation**: en résulte-t-il des besoins concrets d'améliorations et voyez-vous un potentiel d'optimisation au niveau de la stratégie elle-même, des processus ou des structures? Si oui, quels sont-ils?

Conclusion

10 **Attentes**: quelles sont de façon générale vos attentes à l'égard d'une stratégie de protection de la Suisse face aux cyberrisques? Quelles sont vos attentes à l'égard des responsables?

11 **Et pour terminer**: avez-vous encore d'autres remarques à nous communiquer ici?

Merci pour cet entretien.

A-3 Aperçu des entretiens avec les responsables des mesures

N°	Prénom	Nom	Organisation	1	2	3	4	5	6	7	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29
1	Philipp	Kronig	SRC				X																	X	X						
2	Stefan	Brem	OFPP					X																							
	Giorgio	Ravioli	OFPP																												
3	André	Duvillard	DDPS							X																					
4	Daniel	Caduff	OFAE					X																							
	Christophe	Hauert	Cybersafe																												
5	René	Dönni Kuoni	OFCOM									X																			
	Nicolas	Rollier	OFCOM																												
6	Yanis	Callandret	Fedpol																	X	X	X	X								
	Céline	Aubry	PJF/fedpol																												
7	Roger	Michlig	DDPS																							X					
8	Jonas	Grätz	DFAE																								X	X	X		
	Daniel	Seiler	DFF																												
9	Claudio	Stricker	CCDJP							X											X	X	X								
10	Robert	Flück	Cdmt Cyber																						X	X					
11	Patrick	Schaller	EPFZ		X	X		X	X	X		X	X											X							
	Imad	Aad	EPFL		X	X		X	X	X		X	X											X							
12	Martin	Leuthold	SWITCH													X															
13	Pascal	Lamia	NCSC																												
	Manuel	Sutter	NCSC			X				X	X		X	X	X	X	X	X	X											X	
	Marco	Willisch	NCSC																												
14	Dominique	Trachsel	NCSC						X																						X
15	Monica	Ratte	NCSC							X																					

Tableau 13: Aperçu des entretiens menés avec les responsables des mesures (*encore à mener)

A-4 Aperçu des entretiens menés avec les groupes cibles

N°	Prénom	Nom	Organisation	Statut
1	Christoph	Niederberger	Communes suisses	réalisé
2	Erich	Herzog	economiesuisse	réalisé
	Andreas W.	Kälin	digitalswitzerland	réalisé
	Christian	Grasser	Association suisse des télécommunications, ASUT	réalisé
	Thomas	Holderegger	UBS	réalisé
	Raphael	Reischuk	Zülke	réalisé
2	Markus	Trutmann	Association des hôpitaux H+	réalisé
	Stefan	Trachsel	Service sanitaire coordonné (SSC)	réalisé
4	Andy	Fluetsch	UPC/Salt	réalisé
5	Roger	Schneeberger	CCDJP	réalisé
6	Patric	Graber	Conseil des EPF	réalisé
8	Philippe	Vuilleumier	Swisscom	réalisé
10	Serdar	Cünal Rütsche	Police cantonale zurichoise	réalisé
	Stefan	Walder	Ministère public du canton de Zurich	réalisé
11	Bertrand	Schnetz	Police judiciaire jurassienne	réalisé
12	Gunthard	Niederbäumer	Association suisse d'assurances	réalisé
	Maya	Bundt	SwissRE	réalisé
13	Nicole	Wettstein	SATW	réalisé
	Umberto	Annino	Président de l'Advisory Board Cybersecurity	réalisé
14	Christophe	Hauert	Cyber-Safe	réalisé *
15	Olivier	Crochat	C4DT	réalisé *
	Imad	Aad		
16	Alain	Gut	IBM, président de Swiss Cyber Experts	réalisé

Tableau 14: Liste des organisations d'appartenance des représentants des groupes cibles (*réalisé lors de l'entretien prévu pour les responsables des mesures)

A-5 Activités réalisées (*outputs*) selon les étapes définies

Champ	Mesure	Projets de mise en œuvre (*output*)	Résultats (*outcome*)
Acquisition de compétences et de connaissances	M1: détection précoce des tendances ou technologies et acquisition des connaissances utiles	Mise en place d'un monitorage des technologies et du marché Analyse des tendances: évaluation des développements technologiques, publication de rapports	– Identification précoce des tendances ou des technologies informatiques – Identification précoce des chances et risques qui en découlent – Communication au monde scientifique, aux acteurs politiques et à la société
	M2: extension et encouragement des compétences en matière de recherche et de formation	Actualisation de l'analyse des besoins de formation et comblement des lacunes de l'offre Création par l'EPFZ et l'EPFL d'un centre commun de recherche et d'assistance en cybersécurité Mise en œuvre des projets de recherche du Campus cyberdéfense Encouragement de la recherche et de la formation interdisciplinaires en cybersécurité via la création d'un réseau informel Encouragement du piratage éthique (*ethical hacking*) par le soutien apporté à des événements établis	– Analyse du besoin d'offres de formation aux cyberrisques – Examen de l'intégration du thème des cyberrisques dans les filières de formation des hautes écoles et de l'encouragement des talents dans le piratage éthique (*ethical hacking*) – Renforcement de la recherche fondamentale et appliquée – Indication des possibilités d'encourager la recherche interdisciplinaire – Développement des compétences et des connaissances du DDPS dans le domaine de la cyberdéfense grâce à son CYD Campus
	M3: création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité	Création d'un «écosystème de la cybersécurité» grâce au Centre de compétences pour la cybersécurité Mise à disposition de moyens d'encouragement pour les projets d'innovation Création de centres d'innovation Établissement d'un laboratoire d'idées pour la cybersécurité	– Attrait accru de la Suisse comme site d'implantation des entreprises spécialisées dans la cybersécurité – Intensification des échanges entre l'économie et la recherche – Création d'un climat favorable à l'innovation et aux start-up
Situation sur le plan des cybermenaces	M4: extension des capacités permettant d'analyser et de représenter la situation de la cybermenace	Identification des groupes cibles et de leurs besoins face aux cybermenaces Définition d'un catalogue de produits par groupe cible Identification/acquisition des sources et production	– Création d'un tableau d'ensemble de la situation de la menace, permettant aussi de représenter et de traiter les cybermenaces en fonction des groupes cibles (autorités, exploitants d'infrastructures critiques, entreprises, population) – Mise en place de capacités permettant de recenser de manière systématique et durable les cyberincidents – Déploiement systématique de l'OSINT comme base d'information – Échanges d'informations accrus avec les autorités de poursuite pénale, les experts en cybersécurité, l'armée, le service des renseignements, l'économie et les canton
Gestion de la résilience	M5: amélioration de la résilience informatique des infrastructures critiques	Mise en œuvre des projets prévus ou en cours destinés à renforcer la résilience des sous-secteurs critiques Actualisation des analyses des risques et de la vulnérabilité Établissement d'un groupe de travail universitaire pour la cybersécurité	– Mise en œuvre des mesures destinées à améliorer la résilience informatique des sous-secteurs, avec la participation des autorités de régulation et des offices spécialisés – Actualisation régulière des analyses et des mesures

Champ	Mesure	Projets de mise en œuvre (*output*)	Résultats (*outcome*)
	M6: amélioration de la résilience informatique dans l'administration fédérale	Élaboration de directives de sécurité relatives aux méthodes de projet agiles Campagne de sensibilisation dans l'administration fédérale Transmission sécurisée des données grâce aux nouvelles technologies: phase de test avec SCION Security Operations Center de l'OFIT Création d'une interface avec le domaine des EPF	– Amélioration de la résilience informatique dans l'administration fédérale
	M7: échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons	Échange permanent entre les cantons et le Centre de compétences pour la cybersécurité Organisation annuelle de la Cyberlandsgemeinde Développement et diffusion de directives de sécurité communes à la Confédération et aux cantons Création d'une interface avec le domaine des EPF	– Création d'un réseau ad hoc pour les échanges d'expériences et pour l'élaboration de bases communes destinées à renforcer la résilience informatique dans les cantons – Soutien mutuel des autorités et coordination des efforts entre la Confédération et les cantons.
Normalisation et réglementation	M8: évaluation et introduction de normes minimales	Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique Développement et implantation d'outils destinés aux PME	– Élaboration et introduction de normes minimales et d'un outil d'évaluation – Passage en revue des organisations ou activités pour lesquelles les normes devraient être obligatoires
	M9: examen d'une obligation de notifier les cyberincidents et décision quant à son introduction	Étude de modèles de base d'obligations de notifier Débat de fond avec l'économie et les autorités	– Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction
	M10: gouvernance mondiale d'Internet	Groupe de haut niveau du Secrétaire général de l'ONU sur la coopération numérique Plateformes d'échange multi-acteurs pour la coordination au niveau national	– Déploiement de règles internationales portant sur l'usage d'Internet et son développement, en accord avec la conception suisse de la liberté, de la démocratie et de la responsabilité individuelle, du service public, de l'égalité des chances, de la sécurité, des droits de l'homme et de l'État de droit
	M11: acquisition d'expertise par les offices spécialisés et les régulateurs	Création d'un pool interdépartemental d'experts en cybersécurité à l'appui des offices spécialisés Renforcement des projets de normalisation par le soutien apporté aux hautes écoles Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale	– Renforcement de la cybersécurité – Création d'un pool d'experts chargé d'élaborer des mesures ciblées, y c. au niveau réglementaire
Gestion des incidents	M12: développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques	Élargissement ciblé du cercle fermé Développement des services et des produits Développement de la plateforme d'échange existante	– Développement de MELANI (plateforme d'échange d'informations) – Prise en compte de tous les secteurs dans l'échange d'informations – Préservation de la qualité de l'offre et claire définition des accès autorisés
	M13: offre de services destinés à toutes les entreprises	Création d'un guichet unique national pour les cyberrisques Publication de «meilleures pratiques» en matière de gestion des incidents et d'évaluations techniques	– Soutien offert par MELANI à l'économie suisse – Élargissement du groupe cible de MELANI

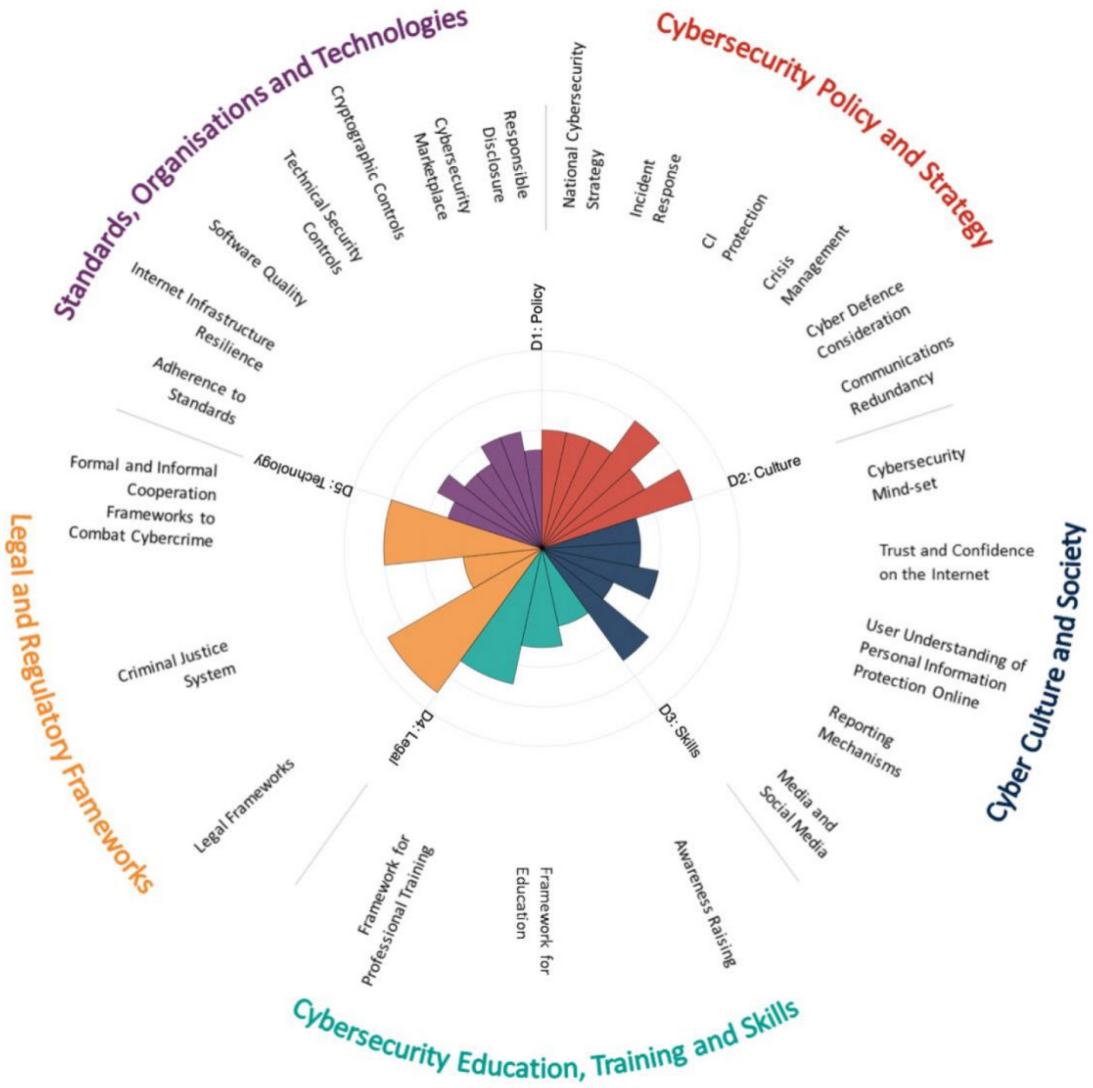
Champ	Mesure	Projets de mise en œuvre (*output*)	Résultats (*outcome*)
		Information très rapide en cas d'incident ☞ application Alertswiss	– Développement d'une offre de services complémentaires axés sur la prévention et la gestion des incidents
	M14: collaboration ciblée entre la Confédération et d'autres services ou centres de compétences	Aperçu des SOC opérationnels et des interlocuteurs de référence Échange d'informations avec les CERT et les SOC	– Renforcement de la collaboration entre les services compétents de la Confédération ou des cantons avec MELANI d'une part, et des échanges entre ces services d'autre part
	M15: processus et bases de la gestion des incidents au sein de l'administration fédérale	Élaboration d'une ordonnance sur la cybersécurité Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale	– Uniformisation de la gestion des incidents dans l'administration fédérale
Gestion des crises	M16: intégration des services spécialisés compétents du domaine cybersécurité dans les états-majors de crise de la Confédération	Définition du rôle du Centre de compétences pour la cybersécurité dans les états-majors de crise de la Confédération Élargissement du glossaire de la cybersécurité	– Sollicitation des états-majors de crise existants pour gérer les cybercrises – Création d'organisations spécifiques aux branches pour gérer les cybercrises frappant l'économie – Mise en réseau des services chargés de la cybersécurité avec les états-majors de crise
	M17: exercices communs de gestion de crise	Création de bases pour des exercices de crise comportant des aspects cybernétiques Réalisation d'exercices sectoriels Intégration d'aspects cybernétiques dans les exercices généraux	– Tests de la gestion des crises – Optimisation des procédures et processus de conduite
Poursuites pénales	M18: vue d'ensemble des infractions en matière de cybercriminalité	Synthèse des données policières cantonales dans une vue d'ensemble des infractions (PICSEL) Élaboration d'une vue d'ensemble judiciaire des infractions Présentation de l'évolution en matière de cybercriminalité et de ses conséquences	– Contrôles et conception du cadre technique nécessaire à l'élaboration d'une vue d'ensemble des infractions en matière de cybercriminalité en Suisse
	M19: réseau de soutien aux enquêtes relatives à la cybercriminalité	Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons	– Élaboration d'un cadre de collaboration et de coordination entre les centres de cybercompétences national et cantonaux dans le cadre du NEDIK
	M20: formation	Mise en œuvre des programmes de formation	– Acquisition durable des compétences nécessaires dans le domaine de la poursuite pénale
	M21: office central de lutte contre la cybercriminalité	Adaptation de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)	– Création d'un office central de lutte contre la cybercriminalité et des bases légales nécessaires en vue de la collaboration avec les cantons dans le domaine de la lutte contre la cybercriminalité

Champ	Mesure	Projets de mise en œuvre (*output*)	Résultats (*outcome*)
Cyberdéfense	M22: développement des capacités d'information et d'attribution	Développement des capacités d'acquisition d'information et d'attribution Réalisation d'une formation spécifique en cyberdéfense (armée)	– Identification précoce par le SRC des nouveaux modes opératoires – Développement des connaissances spécifiques et des compétences du SRC nécessaires à l'acquisition d'informations – Analyses approfondies des acteurs et des environnements – Utilisation et développement des moyens techniques – Traitement systématique des cyberattaques identifiées
	M23: capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM	Utilisation des capacités développées par le COE de la BAC dans le contexte de la LRens	– Présence de compétences adéquates en nombre et en qualité et des capacités nécessaires pour perturber, empêcher ou ralentir des attaques visant les infrastructures critiques
	M24: garantie de la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et réglementation de son rôle subsidiaire consistant à appuyer les autorités civiles	Projet de développement de la cyberdéfense, visant à rendre l'armée capable d'effectuer ses tâches dans le cyberespace Création d'un centre de cyberformation en Suisse Formation des organisations de la conduite à la gestion de cybercrises	– Maîtrise des cybermenaces toujours plus virulentes (fréquence, intensité et complexité des attaques) – Mise en œuvre des volets de la loi sur le renseignement et de la loi sur l'armée touchant au cyberespace – Soutien aux exploitants d'infrastructures critiques victimes de cyberattaques
Positionnement actif de la Suisse dans la politique internationale de cybersécurité	M25: participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité	Participation à des processus de l'ONU axés sur la cybersécurité internationale Défense des intérêts dans le cadre de l'OSCE (renforcement de la confiance entre États) Établissement du Dialogue de Genève sur le comportement responsable Suivi des développements dans l'UE (en particulier au sein du Service européen pour l'action extérieure et de l'ENISA) Engagement en faveur d'un cyberespace ouvert et libre	– Développement et mise en œuvre de normes étatiques ou non réglant le comportement dans le cyberespace – Reconnaissance du droit international et respect des droits de l'homme dans le cyberespace – Instauration dans le cyberespace d'un climat de confiance interétatique – Application des régimes de contrôle des exportations de technologies de surveillance
	M26: coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité	Réalisation d'ateliers avec des organisations régionales Réalisation d'ateliers sur la mise en place d'institutions et de structures de cybersécurité extérieure Soutien au Global Forum on Cyber Expertise	– Échanges internationaux avec des organismes étatiques ou privés, en vue de l'acquisition et du développement de capacités nationales liées aux cyberrisques – Création et renforcement des cybercapacités dans des États tiers – Amélioration de la cybersécurité au niveau mondial
	M27: consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité	Cyberconsultations politiques bilatérales sur la politique extérieure de cybersécurité Sino European Cyber Dialogue – groupe de travail IL, renforcement de la confiance Dialogue MENA: cadre de débat pour la région MENA	– Réalisation de consultations sur la sécurité du cyberespace – Participation aux dialogues multilatéraux

Champ	Mesure	Projets de mise en œuvre (*output*)	Résultats (*outcome*)
Visibilité et sensibilisation	M28: élaboration et mise en œuvre d'un plan de communication pour la SNPC	Élaboration d'un plan de communication sur la SNPC	– Élaboration et mise en œuvre d'un plan de communication pour la SNPC – Fixation des lignes directrices, des compétences et des processus en matière de communication
	M29: sensibilisation du public aux cyberrisques (*awareness*)	Développement et exécution d'une campagne nationale de sensibilisation Plateforme d'information sur les cyberrisques gérée par les interlocuteurs nationaux	– Sensibilisation du public aux cyberrisques – Renforcement de la communication sur les cyberrisques

Tableau 15: Projets de mise en œuvre (*output*) et résultats (*outcome*) pour chaque mesure. Champ = Champ d'action. Source: Plan de mise en œuvre de la SNPC 2018-2022

A-7 Capacité de cybersécurité en Suisse: degré de maturité



Source: University of Oxford, 2020

Figure 4: Présentation générale de la capacité de cybersécurité en Suisse, avec son degré de maturité

Bibliographie

Center for Security Studies (CSS) ETH Zürich (2019): *Nationale Cyber-Sicherheitsstrategien im Vergleich – Herausforderungen für die Schweiz*. Zurich.

Centre de gérontologie de l'Université de Zurich (2020): *Digital Seniors 2020. Utilisation des technologies de l'information et de la communication (TIC) par les personnes de 65 ans et plus en Suisse*. Étude réalisée sur mandat de Pro Senectute Suisse, Zurich.

Centre national pour la cybersécurité (2021a): *Rapport semestriel 2020/2*. Berne.

Centre national pour la cybersécurité (2021b): *Rapport semestriel 2021/1*. Berne.

Centre national pour la cybersécurité (2021c): *Ergebnisse der Ressourcenerhebung zur Umsetzung der NCS 2021*. Interne Auswertung. Berne.

Confédération suisse (2020a): *Stratégie Suisse numérique*. Berne.

Confédération suisse (2020b): *Stratégie de politique extérieure numérique 2021-2024*. Berne.

Conseil fédéral (2015): *Projet de réseau de données sécurisé (RDS)*. Communiqué du 20 mai 2015. Berne.

Conseil fédéral (2017): *Stratégie nationale de protection des infrastructures critiques (PIC) 2018-2022*. Berne.

Conseil fédéral (2018): *Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022*. Berne.

Conseil fédéral (2021): *Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022*. État au deuxième trimestre 2021 Berne.

Département fédéral de la défense, de la protection de la population et des sports (2021): *Strategie Cyber VBS 2021-2024*. Berne.

European Union Agency for Network and Information Security ENISA (November 2016), *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies*. Attiki, Greece.

gfs-Zürich (2021): *Auswirkungen der Corona-Krise auf die Digitalisierung und Cyber-Sicherheit in Schweizer KMU. Befragung von Geschäftsführenden kleiner Unternehmen in der Schweiz*. Studie im Auftrag von: Digitalswitzerland, et al., Zurich.

Office fédéral de l'énergie (2021): *Cyber-Sicherheit und Cyber Resilienz für die Schweizer Stromversorgung*. Rapport du 28 juin 2021. Berne

Sotomo (2022): *Digitaler Staat in der Schweiz*. Studie im Auftrag der Swico, Zurich.

University of Oxford (2020): *Cyber-Security Capacity Review*. Switzerland. June 2020. Study at the invitation of the Swiss Federal Department of Foreign Affairs and the Swiss Federal Department of Finance, Oxford.