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

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Table des matières

Avant-propos

Il s'est écoulé un peu plus d'un an depuis le dernier rapport sur les travaux de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022. «Nous sommes sur la bonne voie», avais-je constaté/conclu à l'époque. Cela reste vrai – même si j'aurais souhaité que les travaux aillent parfois plus vite. Entre-temps, plus des deux tiers du temps imparti sont derrière nous, et près de 60 % des étapes ont été réalisées. J'aurais préféré – d'un point de vue strictement mathématique – que deux tiers des travaux soient déjà réalisés. Mais le bouclement des étapes encore en cours est prévu cette année ou d'ici la fin de 2022, soit quand la SNPC prendra fin.

Plus un projet est hétérogène, plus sa coordination et la cohérence de ses structures comptent. La création par la Confédération de structures organisationnelles adéquates était donc prioritaire pour le succès de la SNPC. Depuis l'entrée en vigueur de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale au milieu de l'année 2020, le cadre et les compétences sont connus et les modalités de la collaboration réglées, tant au sein de l'administration fédérale qu'avec les cantons, les milieux économiques et scientifiques.

Selon moi, la mise en œuvre de la SNPC s'est sensiblement accélérée entre le deuxième trimestre 2020, date du dernier rapport, et le deuxième trimestre 2021. De grands progrès ont été réalisés, d'un point de vue stratégique et organisationnel, dans les domaines de la cybersécurité, de la cyberdéfense et de la poursuite pénale de la cybercriminalité.

Le Centre national pour la cybersécurité (NCSC) a poursuivi son développement et de nouveaux services sont apparus. La mise en place d'une gestion des vulnérabilités est en cours. Un fructueux essai pilote a été mené à ce titre pour repérer, avec l'aide de pirates éthiques, les éventuelles vulnérabilités des systèmes de l'administration fédérale. D'autres programmes de primes aux bogues (*bug bounty*) devraient être menés dans l'ensemble de l'administration fédérale. Dans le cadre de l'application SwissCovid et du certificat COVID, le NCSC a mené deux tests publics de sécurité, faisant bénéficier de son expertise toute l'administration fédérale. Lors des tests privés du certificat COVID réalisés en amont, le NCSC avait collaboré pour la première fois avec l'Institut national de test pour la cybersécurité (NTC), créé à l'initiative du canton de Zoug.

Pour sa part, le Département fédéral de la défense, de la protection de la population et des sports (DDPS) a fixé dans la Stratégie cyber du DDPS les axes qu'il compte suivre en matière de cyberdéfense. Ce document indique comment le DDPS s'engagera dans la SNPC. Le nouveau commandement Cyber de l'armée sera notamment appelé à jouer un rôle important dans la cyberdéfense. Le DDPS a encore participé à divers cyberexercices et en a lui-même réalisé. L'accent a été résolument mis dans ce contexte sur la coopération.

Sur le plan des poursuites pénales, une convention administrative a été conclue en vue de l'organisation et du financement d'un réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK). Ce réseau fédère les ressources spéciales au niveau national, de façon à combattre efficacement la cybercriminalité, et apporte en outre une importante contribution à la prévention. Le Cyberboard, la plateforme de dialogue stratégique du Ministère public de la Confédération, de fedpol et des autorités cantonales de sécurité, revêt une importance croissante afin d'aligner de façon optimale les poursuites pénales sur les besoins de demain.

Il nous reste encore un an et demi pour mettre en œuvre la SNPC. Il y a encore fort à faire, mais j'ai bon espoir que nous accomplirons rapidement de nouveaux progrès au profit de la population, des autorités et des milieux économiques et scientifiques. Il est bien clair que les défis et les travaux liés à la cybersécurité se poursuivront au-delà de la SNPC 2018-2022. Les clarifications et préparatifs nécessaires à la stratégie subséquente ont déjà débuté.

1 Aperçu de l'avancement des travaux

Dans le plan de mise en œuvre de la SNPC, 275 étapes ont été définies dans les 29 mesures que comporte la stratégie. Jusqu'au deuxième trimestre 2021, 154 étapes ont été réalisées et huit n'ont pas pu être atteintes. Six mesures sur 29 sont ainsi entièrement achevées. Le chapitre 5 expose l'état détaillé de la mise en œuvre de la stratégie. L'illustration ci-dessous donne un aperçu de l'avancement des travaux et des étapes planifiées.

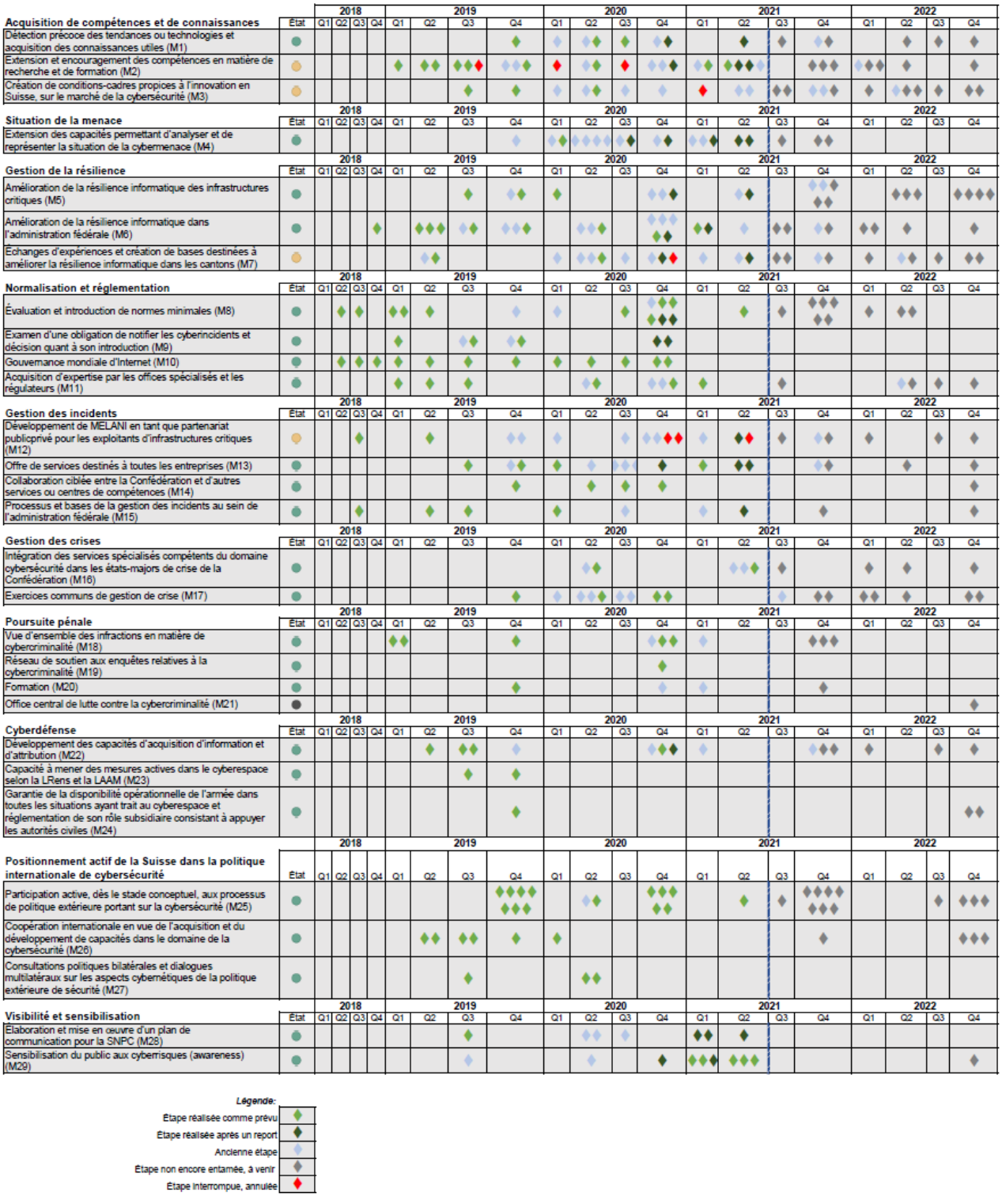


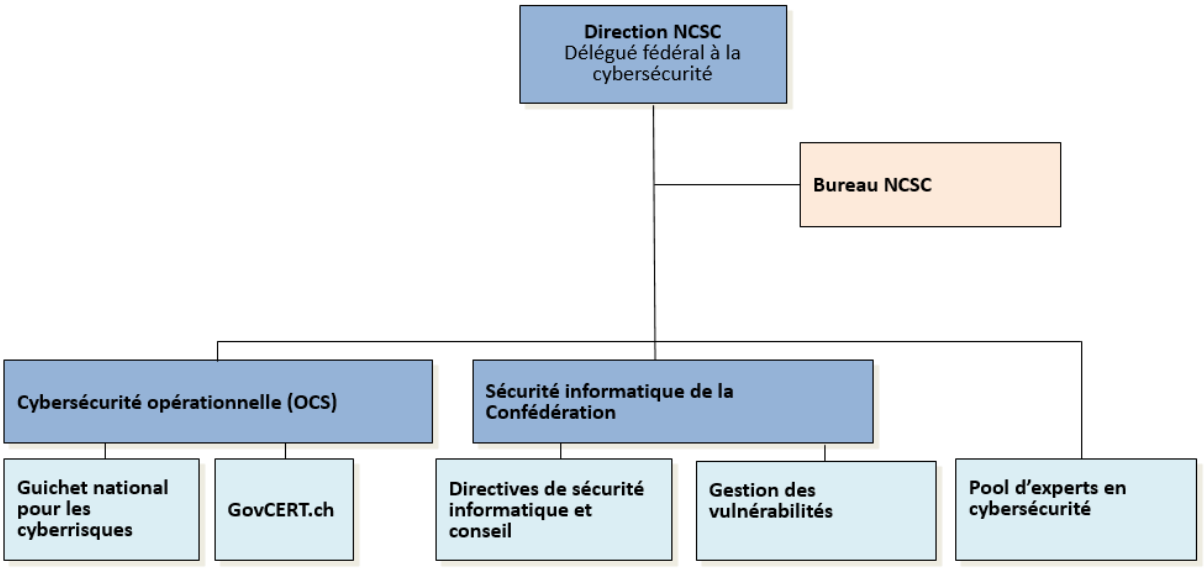
Illustration 1: Aperçu de l'avancement des travaux

2 Organisation et stratégies partielles de mise en œuvre de la SNPC

La mise en œuvre de la SNPC comprend la création de structures organisationnelles au niveau de la Confédération. Le rapport sur l'avancement des travaux de 2020 a décrit les organes assurant la coordination au niveau interdépartemental (Délégation Cyber du Conseil fédéral, Groupe Cyber et comité de pilotage de la SNPC). Ces organes ont poursuivi leur travail et se sont réunis régulièrement. Le présent chapitre passe en revue les principaux développements d'ordre organisationnel ou stratégique en matière de cybersécurité, de cyberdéfense et de poursuite pénale de la cybercriminalité.

2.1 État d'avancement de la mise en place du NCSC

La mise en place du Centre national pour la cybersécurité (NCSC) s'est poursuivie. Le 13 mai 2020, le Conseil fédéral a approuvé à cet effet onze postes supplémentaires. À l'heure actuelle (mai 2021), le NCSC emploie 32 personnes et 13 postes encore vacants seront attribués d'ici la fin de l'année. La figure 1 présente l'organisation du NCSC.



Le NCSC exploite depuis le 1er janvier 2020 un guichet unique national en matière de cyberrisques. En 2020, quelque 10 834 annonces lui sont parvenues d'entreprises ou de particuliers. Parmi les cas relevant clairement de la cybercriminalité, 5924 (55 %) consistaient en tentatives de fraude, 416 (4 %) concernaient des maliciels, 165 (2 %) étaient dus au piratage et 24 (<1 %) provenaient de fuites de données.
L'équipe d'analyse technique du NCSC est le GovCERT (Computer Emergency Response Team). En 2020, il a fermé avec ses partenaires 7500 pages de phishing, enregistré 4500 incidents dus à des maliciels, signalant au passage 90 000 adresses IP infectées, et fourni à 177 exploitants d'infrastructures critiques des informations liées aux menaces.
Au niveau des prescriptions légales, les directives du Conseil fédéral concernant la sécurité informatique dans l'administration fédérale ont été intégrées au 1er avril 2021 dans l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy). Cette mesure a permis de simplifier les directives à suivre, tout en renforçant le rôle du délégué à la cybersécurité. Il peut désormais donner des instructions directes sur le processus et la documentation des procédures de sécurité.[1]

[1] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/cyrv-vorgaben.html

2.2 Stratégie cyber du DDPS

La Stratégie cyber du DDPS, approuvée au printemps 2021 par la cheffe du département, trace l'axe stratégique à suivre en matière de cyberdéfense pour les années 2021 à 2024[2]. Elle indique de quelle manière le DDPS participe à la SNPC, dans le cadre de la stratégie départementale en la matière, comment il contribue à la protection de la Suisse, la défend dans le cyberespace et augmente sensiblement la liberté d'action du pays. Elle contient l'ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la sécurité du pays, 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.
La mise en œuvre obéit au principe suivant: tous les acteurs du DDPS ayant des tâches cyber se coordonnent activement dans le cadre de la Stratégie cyber. Ils collaborent étroitement pour identifier les risques et les chances et pour les maîtriser ensemble. Cela implique que le département axe son développement sur les défis de la cybersécurité – pour ce qui est de ses tâches, du matériel, de ses processus et de son personnel. Dès lors, il est notamment essentiel de former et de perfectionner tout le personnel du DDPS et les militaires de carrière et de milice.
En outre, les responsables cyber du DDPS collaborent avec leurs partenaires pour mettre en œuvre les mesures. En plus du NCSC, il s'agit des cantons, des communes, des milieux scientifiques, de l'économie privée, de certains pays et d'organisations internationales.

2.3 Convention administrative pour le NEDIK

La Conférence des directrices et directeurs cantonaux de justice et police (CCDJP) a approuvé le 12 novembre 2020, lors de son assemblée d'automne, les termes d'une convention administrative conclue avec la Conférence des commandants des polices cantonales de Suisse (CCPCS) en vue de régler l'organisation et le financement d'un réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK).[3] La convention est entrée en vigueur le 1er janvier 2021.
La CCPCS a fondé le NEDIK en 2018 déjà, afin de concentrer les ressources spécialisées et donc de combattre plus efficacement la cybercriminalité. La convention administrative règle les questions d'organisation et de financement du NEDIK.
En tant que réseau, le NEDIK a notamment pour fonction d'assurer le transfert de connaissances, d'établir un aperçu national des cas et de permettre la classification des cas à caractère intercantonal. Le NEDIK contribue également à la prévention et collabore avec la Prévention Suisse de la Criminalité et le Centre national pour la cybersécurité (NCSC).
Au sein du NEDIK, fedpol assume le rôle de coordination supracantonale et transnationale, en particulier dans le cadre de la collaboration avec les autorités partenaires à l'étranger. Fedpol établit des rapports d'analyse et représente la Suisse dans les groupes d'experts internationaux.

[2] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-83160.html

[3] https://www.kkjpd.ch/newsreader-fr/renforcement-des-efforts-cantonaux-contre-la-cybercri-minalit%C3%A9-et-la-p%C3%A9docriminalit%C3%A9.html

2.4 Stratégie de politique extérieure numérique

Le Conseil fédéral a adopté la stratégie de politique extérieure numérique en novembre 2020[4]. La stratégie souligne à propos de la cybersécurité que la Suisse entend développer la promotion de la paix partout où c'est possible. Dans le cyberespace, il s'agit concrètement de renforcer les structures et de favoriser les forums de dialogue qui contribuent à faire respecter le droit international, y compris son volet humanitaire. La Suisse reconnaît la validité des normes en vigueur et œuvre pour qu'elles soient appliquées dans la lutte contre toutes les formes de cyberattaque. En cela, la cybersécurité englobe un ensemble d'acteurs, allant des États à la société civile, en passant par les acteurs de l'économie privée. L'approche multipartite est une constante dans la définition stratégique de la politique extérieure de la Suisse, de même que sa longue tradition de bons offices.

[4] https://www.eda.admin.ch/dam/eda/fr/documents/publications/SchweizerischeAussenpolitik/20201104-strategie-digitalaussenpolitik_FR.pdf

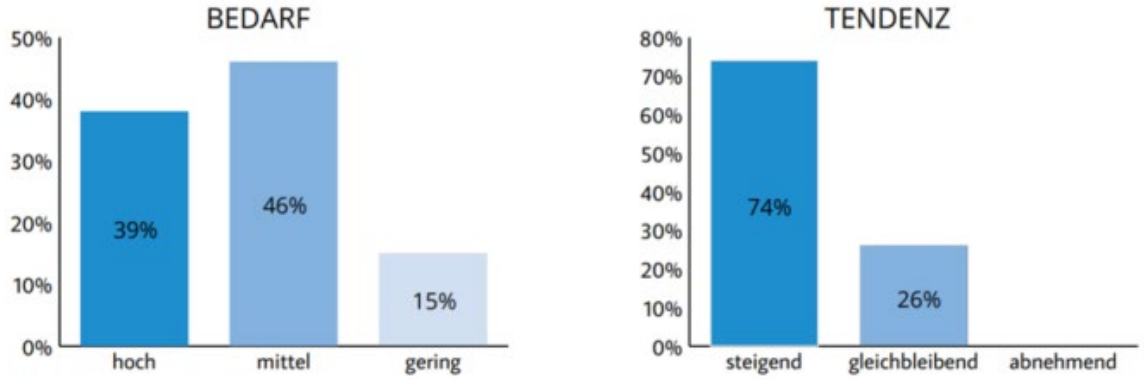
3 Thèmes principaux de la mise en œuvre de la SNPC

Les travaux de mise en œuvre de la SNPC se poursuivent en parallèle au développement de l'organisation de la Confédération en matière de cybersécurité. Les travaux concernés ne sont pas réalisés uniquement par l'administration fédérale, mais reposent en grande partie sur les acteurs cantonaux, les milieux économiques, les hautes écoles et la société. Le chapitre 5 indique quelles étapes ont été franchies dans tous les champs d'action, tandis que le présent chapitre est consacré aux projets-clés des travaux en cours.

3.1 Mise en place de l'Institut national de test pour la cybersécurité (NTC)

La sécurité des produits informatiques revêt une importance majeure pour la cybersécurité. En cas de failles de sécurité, la menace est d'autant plus grave lorsque ces produits sont utilisés par des infrastructures critiques, car cela peut causer des préjudices considérables à l'économie et à la société. À ce jour, la Suisse n'est pas dotée de capacités suffisantes pour traquer les vulnérabilités de tels produits.
Un institut national de test pour la cybersécurité (NTC) a par conséquent été créé, à l'initiative du canton de Zoug. Dans le cadre de ce projet, un sondage a été mené en octobre 2020 auprès d'exploitants d'infrastructures critiques pour savoir si un tel institut de test répondait à un besoin. Les résultats sont clairs: 85 % des sondés aimeraient faire tester des produits et seraient prêts à confier cette tâche au NTC. En outre, 75 % des sondés pensent que le besoin de tests de cybersécurité va encore augmenter au cours des prochaines années, alors que personne ne s'attend à ce qu'il diminue.

«Selon vous, quelle sera l'ampleur du besoin de tests de cybersécurité que votre organisation serait prête à confier à un institut national de test pour la cybersécurité ces cinq prochaines années?»
N=64



L'association «Institut national de test pour la cybersécurité NTC» a été fondée en novembre 2020. Promotrice du projet, elle prendra la responsabilité de l'exploitation de l'institut lorsque celui-ci aura abouti. La Confédération accompagne déjà l'initiative sur le plan technique.
Dans une intervention parlementaire de décembre 2020, le conseiller national Franz Grüter a demandé à ce que celle-ci participe à la création et au fonctionnement du NTC (20.4495).
Le NTC réalise depuis 2021 les premiers processus d'audit pilotes, développe son modèle d'affaires et de gouvernance dans l'optique de sa mise en œuvre opérationnelle.

3.2 Labelcyber-safe.ch pour les communes suisses

Les technologies de l'information jouent aujourd'hui un rôle-clé dans les communes, de la gestion des stations d'épuration à la cyberadministration, en passant par les systèmes de chauffage urbains. Plus aucune commune ne peut se permettre d'ignorer les enjeux de cybersécurité, indépendamment de sa taille et de ses moyens financiers. Depuis le milieu de l'année 2020, dans le cadre d'un projet pilote lancé avec le soutien de la SNPC, du Réseau national de sécurité (RNS) et de l'Association des communes suisses (ACS), une quinzaine de communes ont pu faire évaluer leur sécurité informatique au moyen du label cyber-safe.ch, être informées sur les mesures à prendre et, le cas échéant, se voir décerner le label – à l'image de Bussigny (VD) ou Jonen (AG).
Ce projet pilote doit permettre au NCSC de juger du bien-fondé d'un label de cybersécurité pour les communes et les administrations publiques, et d'en tirer les leçons utiles pour la mise en œuvre de mesures futures.

3.3 Label pour prestataires de services informatiques

Avec les progrès croissants de la numérisation, les petites et moyennes entreprises (PME) sont toujours plus exposées aux menaces provenant du cyberespace. En outre, les PME suisses recourent toujours plus souvent à des prestataires externes de services informatiques: deux tiers des PME collaborent aujourd'hui avec de tels fournisseurs. Ceux-ci ayant un impact direct sur la cyberrésilience des PME, il est indispensable qu'ils possèdent des compétences techniques et organisationnelles en matière de cybersécurité et de sécurité de l'information.
Au quatrième trimestre 2020, des partenaires de la Confédération et des acteurs du secteur privé ont pris ensemble l'initiative de créer un label de qualité indépendant pour prestataires de services informatiques. Ce label de qualité désignera des fournisseurs de services informatiques ayant adopté des mesures techniques et organisationnelles leur permettant de garantir à leurs clients un niveau de protection adéquat. La diffusion de ce label aura une influence positive sur la cyberrésilience des PME, elle rehaussera le niveau de qualité des activités de transformation numérique et renforcera ainsi la confiance accordée à la Suisse sur le terrain de la sécurité numérique.
Le concept du label de qualité a été défini et créé en décembre 2020. De janvier à mars 2021, un essai pilote a été mené avec quatre prestataires de services informatiques. Entre mai et juillet 2021, une phase de test élargie a été réalisée avec dix fournisseurs. En parallèle, un concept de mise sur le marché a été lancé en mai 2021 (site Internet, communication, marketing, réseau d'auditeurs, processus commerciaux et opérationnels). L'entrée sur le marché, avec le passage en phase d'exploitation de l'association nouvellement créée, est prévue pour septembre 2021.

3.4 Campagne nationale de sensibilisation

La première campagne nationale de sensibilisation à la cybersécurité a été menée du 3 au 7 mai 2021, sous la forme d'une semaine d'action. Son comité d'organisation comptait, outre le NCSC, la Prévention Suisse de la Criminalité (PSC), la Haute école de Lucerne (HSLU) et la Swiss Internet Security Alliance (SISA) avec sa plateforme iBarry. Divers partenaires ont en outre relayé la campagne sur leurs propres canaux. Il convient de citer Digitalswitzerland et Digital Liechtenstein, les membres de la SISA comme Swisscom, UPC-Sunrise, SWITCH et la Mobilière, près de 100 banques partenaires de la plateforme «eBanking – en toute sécurité!», ainsi que tous les corps de police cantonaux ou municipaux.

Pendant cinq jours, un thème différent a été présenté quotidiennement afin de sensibiliser la population et de lui donner les moyens d'agir de manière responsable dans le cyberespace. Ces thèmes comprenaient la sauvegarde des données, les mots de passe, les mises à jour de sécurité, la protection contre les virus et la vigilance dans le cyberespace. Les contenus étaient principalement diffusés en ligne, et la campagne focalisée sur les médias sociaux.

3.5 Projet pilote avec «Bug Bounty Switzerland»

Le NCSC a décidé de mener avec la société Bug Bounty Switzerland un projet pilote dans le cadre duquel des pirates éthiques étaient chargés de repérer les failles de sécurité (bogues) des systèmes de l'administration fédérale. Chaque bogue découvert donnait lieu à une prime, dont le montant était fixé en fonction de la gravité de la faille détectée.
L'essai pilote a débuté le 10 mai 2021 et s'est déroulé sur onze jours. Quinze pirates ont passé au peigne fin six systèmes informatiques du Département fédéral des affaires étrangères (DFAE) et des Services du Parlement. Dix failles en tout ont été signalées au NCSC. Ce nombre est relativement faible pour un projet réalisé en collaboration avec des pirates éthiques et démontre que tous les systèmes informatiques testés jouissent d'une sécurité élevée et ne constituent pas des cibles faciles. Or malgré toutes les mesures de sécurité adoptées dans les systèmes accessibles en ligne au public, de tels environnements comportent encore des failles de sécurité et révèlent bien la nécessité d'un programme de chasse aux bogues. Aussi le NCSC compte-t-il lancer dans l'administration fédérale de nouveaux programmes de ce type, en tirant parti des expériences réalisées.[5]

3.6 Élaboration d'un projet destiné à la consultation sur l'obligation de signaler les cyberattaques

Le 11 décembre 2020, le Conseil fédéral a chargé le Département fédéral des finances (NCSC) de préparer d'ici la fin de l'année 2021, en concertation avec les services compétents de tous les départements, un projet destiné à la consultation concernant l'introduction d'une obligation de signaler les cyberattaques pour les exploitants d'infrastructures critiques. Il s'agit de désigner une centrale qui analyse les annonces pour améliorer la détection précoce des cyberrisques et qui tienne des statistiques des cyberincidents. La nouvelle obligation devra être harmonisée avec les obligations de déclarer existantes (notamment avec celles prévues par le droit sur la protection des données).
Le NCSC a réalisé en avril 2021, auprès desexploitants d'infrastructures critiques et des autorités, une enquête concernant l'obligation de signaler les cyberincidents. L'accueil est en principe favorable, pour autant qu'il n'en résulte que peu de formalités administratives. L'illustration 2 montre dans quelle mesure les personnes interrogées (n=400) adhéraient à cette obligation, l'échelle allant de 1 «pas du tout d'accord avec l'introduction de l'obligation de déclarer» à 5 «tout à fait d'accord avec l'introduction de l'obligation de déclarer». Les résultats de l'enquête serviront à fixer, cette année encore, les modalités pour le projet destiné à la consultation.

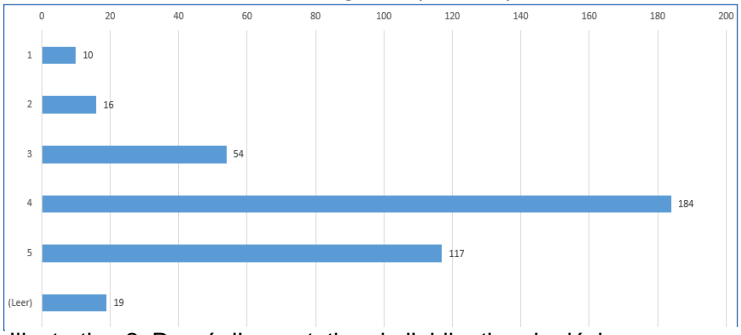


Illustration 2: Degré d'acceptation de l'obligation de déclarer

[5] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-84304.html

4 État détaillé de la mise en œuvre

Ce chapitre présente l'état de la mise en œuvre de la SNPC en se basant sur la planification des étapes. Pour chaque mesure, il indique quelles étapes ont été atteintes ou non jusqu'au deuxième trimestre 2021. Celles-ci sont brièvement décrites pour une meilleure compréhension de leur contribution à la SNPC.
Sur les 275 étapes définies dans le plan de mise en œuvre de la SNPC, 154 ont été réalisées, et huit n'ont pas encore été atteintes. Six des 29 mesures ont été menées à terme. Étant donné qu'un peu moins des deux tiers des étapes ont été réalisées après quatorze trimestres (sur les 20 de sa durée totale), on peut dire que la mise en œuvre de la SNPC suit son cours, et donc que les travaux qui doivent encore être exécutés pourront l'être comme prévu durant les trimestres restants. L'illustration 3 montre l'état de la mise en œuvre, toutes étapes confondues.

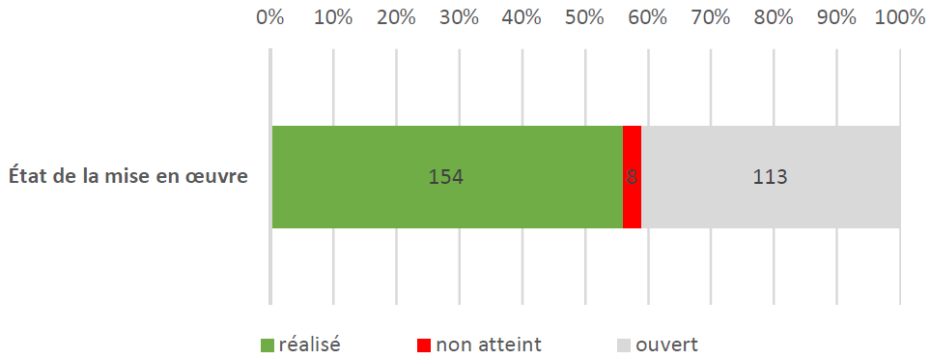


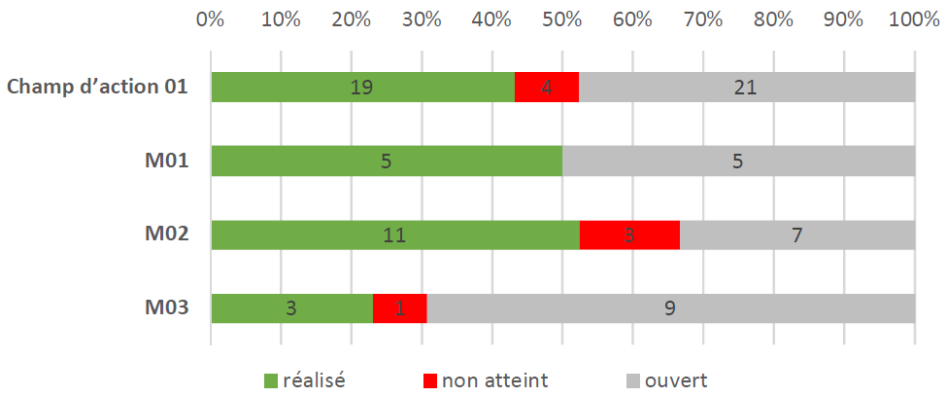
Illustration 3: État de mise en œuvre de l'ensemble des étapes de la SNPC

4.1 Champ d'action 1 «Acquisition de compétences et de connaissances»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M1: détection précoce des tendances ou technologies et acquisition des connaissances utiles (armasuisse S+T)
- M2: extension et encouragement des compétences en matière de recherche et de formation (NCSC et armasuisse S+T)
- M3: création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

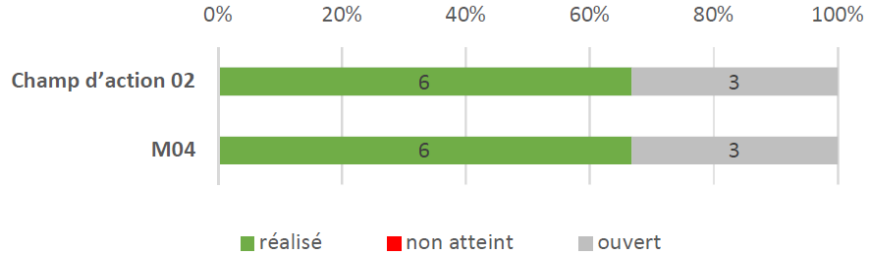
	Étapes	**Statut**
M1	Monitorage des technologies: 1) Définition des prestations du Campus CYD pour le monitorage destiné au NCSC 2) Début des activités de monitorage 3) Première évaluation	réalisé
	Analyse des tendances: 1) Élaboration d'un plan relatif au public cible, aux contenus et à la diffusion des rapports 2) Attribution des mandats d'évaluation	réalisé
M2	Analyse des besoins de formation: 1) Aperçu des offres de formation 2) Analyse des besoins et définition des groupes cibles	réalisé *«Projet achevé plus tôt que prévu: l'aperçu de l'offre montre que le marché s'est entre-temps établi.»*
	Centre de recherche et d'assistance des deux EPF: 1) Projet de centre de recherche et d'assistance 2) Règlement du financement et choix du site 3) Mise en service du centre de recherche, et expansion par étapes en 2021 et 2022	réalisé
	Campus cyberdéfense: 1) Début des activités sur le site de Thoune 2) Début des activités sur le site de l'EPFL 3) Début des activités sur le site de l'EPFZ	réalisé
	Recherche et formation interdisciplinaires en matière de cybersécurité: 1) Identification des principaux instituts de recherche sur les cyberrisques	réalisé
	Encouragement du piratage éthique (*ethical hacking*): 1) Identification des événements existants dans le domaine du piratage éthique 2) Conception des instruments d'encouragement: demande si nécessaire de moyens financiers	réalisé Projet suspendu*: un financement fédéral ne convient pas à la promotion d'événements dans le domaine du piratage éthique. Moyens investis dans Bug Bounty.*
	Réalisation d'un programme pilote de Bug Bounty: 1) Conclusion du contrat entre Bug Bounty Switzerland et le NCSC 2) Réalisation du projet pilote, évaluation et rapport de terrain disponibles	réalisé
M3	Création de centres d'innovation: 1) Proposition pour la création et le financement d'un pôle de cybersécurité national	Projet suspendu: *en raison d'initiatives en cours (comme trust valley, l'initiative zougoise, etc.) et suite aux entretiens menés avec les cantons notamment,le projet est suspendu dans le plan de mise en œuvre et fera l'objet, le cas échéant, d'une nouvelle évaluation dans le cadre de la nouvelle SNPC.*
	Laboratoire d'idées: 1) Élaboration du projet de centre de recherche et d'assistance des deux EPF 2) Règlement du financement et choix du site du centre de recherche et d'assistance des deux EPF 3) Inauguration du centre de recherche avec son laboratoire d'idées; consolidation par étapes en 2021 et en 2022	réalisé

4.2 Champ d'action 2 «Situation de la menace»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M4: extension des capacités permettant d'analyser et de représenter la situation de la cybermenace (SRC)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étapes	Statut
M4	Identification des groupes cibles et de leurs besoins 1) Identification des groupes cibles élargis et de leurs besoins 2) Identification des canaux de communication pour chaque groupe cible	réalisé
	Définition d'un catalogue de produits par groupe cible (catalogue de prestations): 1) Délimitation des compétences respectives de la Confédération et des milieux économiques 2) Définition d'un catalogue de prestations par groupe-cible	réalisé
	Acquisition des sources et des ressources de production nécessaires: 1) Liste des sources supplémentaires nécessaires 2) Projet de mise en place du soutien technique	réalisé

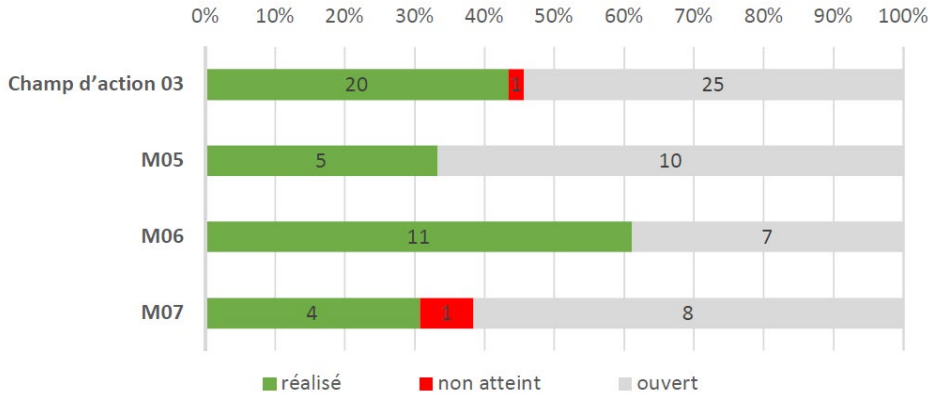
4.3 Champ d'action 3 «Gestion de la résilience»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M5: amélioration de la résilience informatique des infrastructures critiques (OFPP en collaboration avec les offices spécialisés dans les secteurs réglementés)
- M6: amélioration de la résilience informatique dans l'administration fédérale (NCSC)
- M7: échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons (NCSC, RNS)[6]

[6] Vous trouverez des informations sur d'autres projets du plan de mise en œuvre par les cantons de la SNPC 2018–2022 et sur leur état d'avancement sur le site du RNS, sous: www.rns.admin.ch > Thèmes et agenda > Cybersécurité > Plan de mise en œuvre des cantons > Rapport annuel sur l'état d'avancement des projets du plan de mise en œuvre des cantons

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étape	Statut
M5	Mise en œuvre des projets destinés à renforcer la résilience dans les sous-secteurs critiques: 1) État des lieux des projets déjà réalisés ou encore à réaliser selon les rapports sur les mesures 2) Définition des responsabilités pour la mise en œuvre 3) Feuille de route/planification des mesures actuelles ou à venir	réalisé
	Établissement d'un groupe de travail universitaire pour la cybersécurité 1) Bilan des projets et des groupes actifs 2) Institutionnalisation du groupe de travail	réalisé
M6	Développement de prescriptions de sécurité pour méthodes de projet agiles: 1) Analyse des tâches liées à la sécurité prescrites dans les méthodes de projet, avec leurs résultats 2) Identification et description de tâches supplémentaires avec leurs résultats, et des compléments ponctuels à apporter aux directives existantes	réalisé
	Campagne de sensibilisation dans l'administration fédérale 1) Première ébauche de la campagne de sensibilisation portant sur la sécurité informatique dans l'administration fédérale (T4/2018) 2) Début de la campagne de sensibilisation portant sur la sécurité informatique dans l'administration fédérale 3) Coordination avec d'autres acteurs pour une transformation en campagne nationale	réalisé
	Transmission sécurisée des données (SCION) 1) Déclaration d'intention des services intéressés et des utilisateurs pilotes 2) Création et mise en service des applications pilotes	réalisé
	Security Operations Center (SOC) de l'OFIT 1) Projet et plan de mise en œuvre	réalisé
	Création d'une interface avec le domaine des EPF 1) Coordination avec le délégué à la cybersécurité 2) Mise en œuvre de mesures concrètes 3) Coordination commune	réalisé
M7	Échange permanent entre les cantons: 1) Évaluation des besoins liés aux postes de travail au NCSC	Projet suspendu: *suspension en raison notamment de la pandémie; réévaluation prévue au début de 2022, en fonction de l'évolution du NCSC*

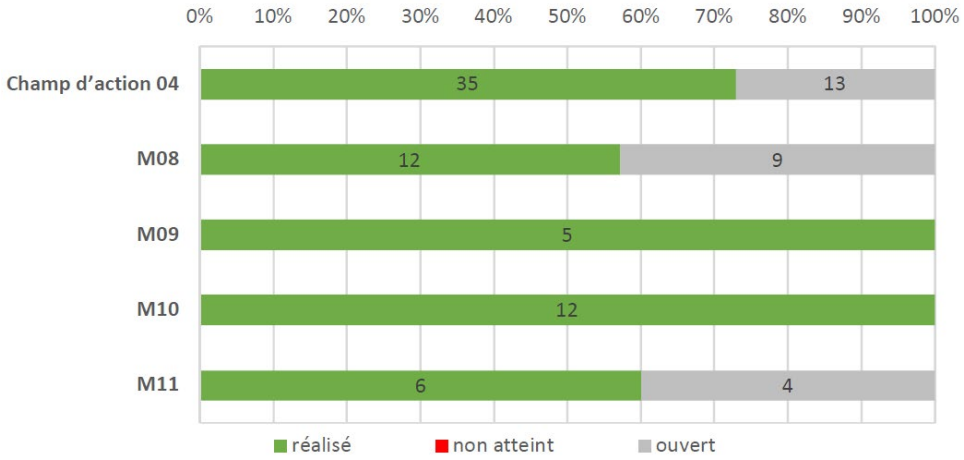
	Organisation de la Cyberlandsgemeinde 1) Exécution de la Cyberlandsgemeinde 2019 2) Exécution de la Cyberlandsgemeinde 2020	réalisé
	Création d'une interface entre les EPF et les cantons: 1) Coordination avec le RNS 2) Réalisation de mesures concrètes	réalisé

4.4 Champ d'action 4 «Normalisation et réglementation»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M8: évaluation et introduction de normes minimales (OFAE)
- M9: examen d'une obligation de notifier les cyberincidents et décision quant à son introduction
- M10: gouvernance mondiale d'Internet (OFCOM)
- M11: acquisition d'expertise sur les questions de normalisation dans le domaine de la cybersécurité (NCSC)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étape	Statut
M8	Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique 1) Publication de la norme minimale et d'un outil d'évaluation 2) Norme minimale «Manuel Protection de base» de l'Association des entreprises électriques suisses (AES) 3) Normes sectorielles sur l'eau potable, les denrées alimentaires, le gaz naturel et les transports publics	réalisé
	Développement et implantation d'outils destinés aux PME 1) Publication du test rapide sur la cybersécurité pour les PME (SATW) [T3/2018] 2) Analyse du besoin d'autres outils spécifiques aux PME (outils techniques, labels, guides et instructions) 3) /Fin de l'examen en vue de l'introduction éventuelle de labels et de normes	réalisé
	Label cyber-safe.ch pour les communes 1) Contrat entre Cyber-Safe et le NCSC, et convention entre le NCSC et l'Association des communes suisses (ACS) 2) Projet de feuille de route et conventions conclues avec les 15 communes pilotes	réalisé
	Label pour prestataires de services informatiques: 1) Signature d'un contrat entre Digitalswitzerland et le NCSC 2) Élaboration des bases du label (manuel d'audit, liste de contrôle, etc.)	réalisé

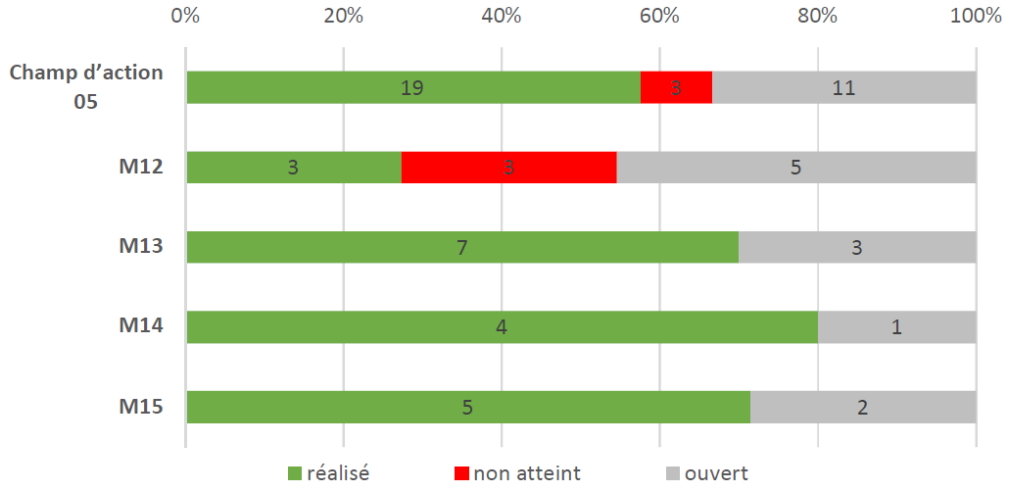
M9	Étude de modèles de base d'obligations de notifier 1) Appel d'offres et rédaction d'une étude de base 2) Compte rendu sur les modèles de base et recommandations les concernant	réalisé
	Débat de fond avec l'économie et les autorités 1) Débat de fond avec les milieux économiques et politiques 2) Base décisionnelle sur l'obligation de déclarer	réalisé
M10	Réunions du groupe de haut niveau du Secrétaire général des Nations Unies: 1) Réunions à New York, Genève et Helsinki 2) Rapport final du groupe 3) Évaluation des possibilités de mise en œuvre	réalisé
	Plateformes d'échange multi-acteurs pour la coordination au niveau national 1) Swiss IGF 2018 (T4/2018) 2) Swiss-IGF 2020	réalisé
M11	Création d'un pool interdépartemental d'experts en cybersécurité 1) Identification des besoins 2) Conception du pool d'experts et détermination des ressources	réalisé
	Renforcement des projets de normalisation par le soutien apporté aux hautes écoles 1) Élaboration du projet de centre de recherche et d'assistance commun EPFL-EPFZ 2) Établissement d'une vue d'ensemble des activités de la Suisse dans ce domaine 3) /Mise en œuvre des activités dans les groupes de travail identifiés comme stratégiques	réalisé
	Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale 1) Premier rapport intermédiaire sur les activités de renforcement des cybercapacités internationales dans le secteur financier	réalisé

4.5 Champ d'action 5 «Gestion des incidents»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M12: développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques (NCSC)
- M13: offre de services destinés à toutes les entreprises (NCSC)
- M14: collaboration ciblée entre la Confédération et d'autres services ou centres de compétences (NCSC)
- M15: processus et bases de la gestion des incidents au sein de l'administration fédérale (NCSC)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étape	Statut
M12	Élargissement ciblé du cercle fermé 1) État des lieux de l'utilisation de MELANI par les différents secteurs critiques	retardé: *report lié aux développements stratégiques; réévaluation et nouvelle planification prévues début 2022*
	Développement des services et des produits 1) Analyse des produits et services MELANI existants et des besoins	réalisé
	Développement de la plateforme d'échange existante 1) Réalisation de l'étude avec recommandation d'une solution pour MELANI-NET 2.0 (T3/2018) 2) Réalisation de la démonstration de faisabilité (*proof of concept*) pour la solution recommandée 3) Plan pour MELANI-NET 2.0 et 4) MELANI-NET 2.0 opérationnel	réalisé réalisé retardé: *report lié aux développements stratégiques des plateformes d'information du NCSC; réévaluation et nouvelle planification prévues début 2022*
M13	Création d'un guichet national pour les cyberrisques: 1) Élaboration d'un projet sommaire de portail en ligne pour la déclaration de cyberincidents 2) Mise à la disposition du public du portail en ligne pour la notification de cyberincidents 3) Intégration dans la plateforme d'information sur les cyberrisques (voir M29)	réalisé
	Information rapide en cas d'incident au moyen de l'application Alertswiss 1) Détermination, par le Centre de compétence et l'OFPP, des exigences concernant l'alerte, la mise en garde et l'information du public en cas de cyberincident 2) Établissement du plan d'intégration des cyberinformations dans l'application Alertswiss 3) Possibilité d'informer le public d'un cyberincident au moyen de l'application Alertswiss 4) Informations sur les nouveaux développements (cyberincidents) publiées dans l'application Alertswiss	réalisé
M14	Aperçu des CERT et des SOC opérationnels, et des interlocuteurs de référence 1) Exécution et documentation du recensement des CERT et des SOC opérationnels et des interlocuteurs de référence 2) Clarification du processus et des responsabilités concernant la mise à jour continue de l'aperçu	réalisé
	Échange d'informations avec les CERT et les SOC 1) Analyse des besoins et des possibilités concernant un échange d'informations systématique 2) Définition et attribution des projets d'établissement d'un échange d'informations	réalisé
M15	Élaboration d'une ordonnance sur la cybersécurité: 1) Élaboration de l'ordonnance 2) Adoption de l'ordonnance par le Conseil fédéral 3) Fixation de l'entrée en vigueur de l'ordonnance	réalisé
	Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale 1) Premier projet de processus, discussion avec les fournisseurs de prestations et les services concernés	réalisé

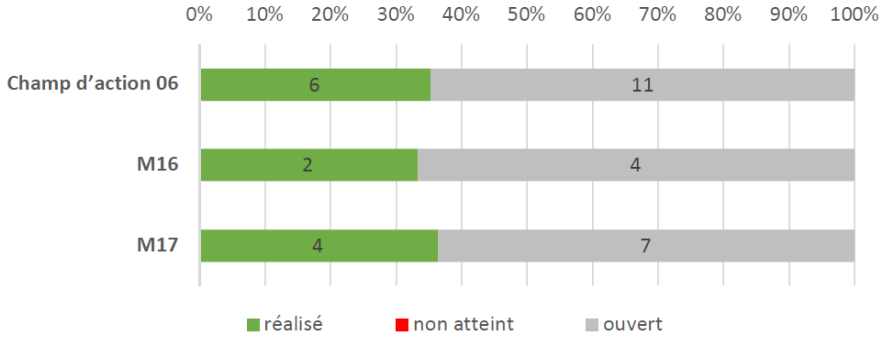
	2) Adaptation du processus à l'ordonnance sur la cybersécurité	

4.6 Champ d'action 6 «Gestion des crises»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M16: intégration des services spécialisés compétents du domaine cybersécurité dans les états-majors de crise de la Confédération (NCSC)
- M17: exercices communs de gestion de crise (NCSC, SG-DDPS)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

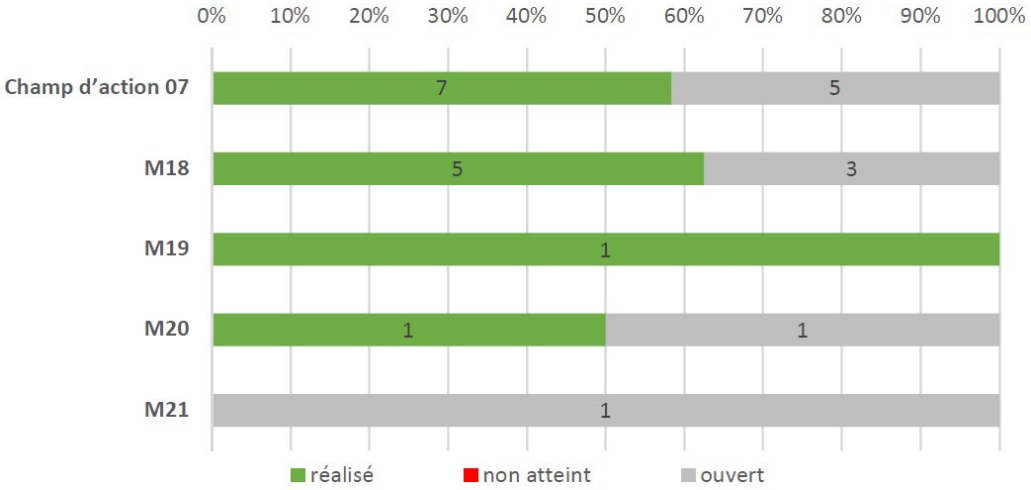
	Étape	Statut
M16	Élargissement du glossaire de la cybersécurité 1) Inventaire des définitions existantes 2) Cyberglossaire établi ou élargi	réalisé
M17	Création de bases pour des exercices de crise comportant des aspects liés à la cybersécurité 1) Inventaire des exercices de crise nationaux et internationaux qui comportent des aspects liés à la cybersécurité et qui existent ou sont prévus 2) Processus d'actualisation et de coordination avec l'aperçu des cyberexercices	réalisé
	Réalisation d'exercices sectoriels 1) Analyse des besoins relatifs aux exercices de crise sectoriels	réalisé
	Intégration d'aspects liés à la cybersécurité dans les exercices généraux 1) Concertation avec les partenaires responsables afin d'intégrer les critères de cybersécurité pertinents dans l'exercice	réalisé

4.7 Champ d'action 7 «Poursuite pénale»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M18: vue d'ensemble des infractions en matière de cybercriminalité (fedpol et CCPCS en collaboration avec le NEDIK)
- M19: réseau de soutien aux enquêtes relatives à la cybercriminalité (fedpol dans le cadre de la CCPCS)
- M20: formation à la lutte contre la cybercriminalité [CCPCS (y c. fedpol), Conférence des procureurs de Suisse (y c. MPC)]
- M21: office central de lutte contre la cybercriminalité (fedpol)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

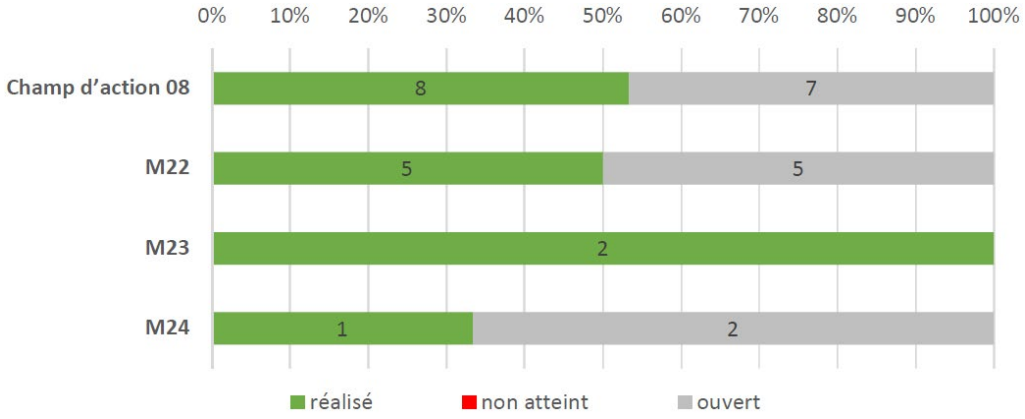
	Étape	Statut
M18	Vue d'ensemble des infractions en matière de cybercriminalité (PICSEL) 1) Lancement de la phase de test de PICSEL	réalisé
	Élaboration d'une vue d'ensemble judiciaire des infractions 1) Outil Cyber-CASE; liste des infractions pour tous les procureurs qui font office d'interlocuteurs uniques dans le domaine de la cybercriminalité (déjà opérationnelle) 2) Outil en ligne pour la vue d'ensemble des procédures en cours	réalisé
	Présentation de l'évolution en matière de cybercriminalité et de ses conséquences 1) Bulletin mensuel (de la police) NEDIK 2) Aperçu des procédures en cours (enquêtes policières ou judiciaires)	réalisé
M19	Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons 1) Convention(s) signée(s) et adoptée(s)	réalisé
M20	Mise en œuvre des programmes de formation 1) Vue d'ensemble des possibilités de formations académiques (policières)	réalisé
M21	Aucune étape jusqu'au deuxième trimestre 2021	

4.8 Champ d'action 8 «Cyberdéfense»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M22: développement des capacités d'acquisition d'information et d'attribution (SRC)
- M23: capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM (SRC, COE de la BAC)
- 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 (SG-DDPS et BAC)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

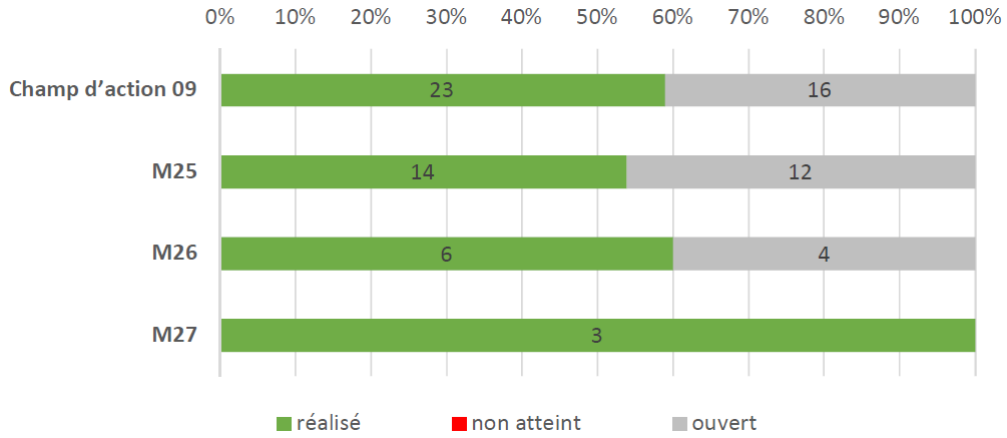
	Étape	Statut
M22	Capacités d'acquisition d'informations et d'attribution: 1) Fin de la première étape du développement	réalisé
	Réalisation d'une formation spécifique en cyberdéfense (armée) 1) Premier entraînement avec la BAC des Forces terrestres 2) Lancement du master commun EPFL-EPFZ-DDPS 3) Premières formations EPFL-DDPS 4) Introduction d'un cursus en cyberdéfense	réalisé
M23	Utilisation des capacités développées par le COE de la BAC dans le contexte de la LRens 1) Les effets collatéraux des activités prévues ont été envisagés avec les offices spécialisés 2) Capacités disponibles	réalisé
M24	Fin du projet de développement de la cyberdéfense	réalisé

4.9 Champ d'action 9 «Positionnement actif de la Suisse dans la politique internationale de cybersécurité»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M25: participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité (DFAE, SECO)
- M26: coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité (DFAE)
- M27: consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité (DFAE)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étape	Statut
M25	Participation à des processus de l'ONU 1) Rapports annuels 2019 et 2020	réalisé
	Défense des intérêts dans le cadre de l'OSCE (renforcement de la confiance entre États) 1) OSCE: participation aux négociations, contribution active au processus et rapport annuel 2019 et 2020	réalisé
	Mise en place et établissement du Dialogue de Genève sur le comportement responsable dans le cyberespace: 1) Plan pour l'établissement du Dialogue de Genève comme plateforme multi-acteurs 2) Réalisation de deux à trois dialogues du processus d'experts sur l'application du droit international dans le cyberespace 3) Intégration des enseignements du processus d'experts dans l'UNGGE et l'OEWG 4) Reflet des intérêts suisses s'agissant de l'application du droit international dans le cyberespace dans les rapports finaux de l'UNGGE et de l'OEWG	réalisé
	Suivi des développements dans l'UE (en particulier au sein du Service européen pour l'action extérieure et de l'ENISA) 1) Vue d'ensemble des principaux acteurs, processus et mesures de l'UE ainsi que des services qui participent aux processus en Suisse 2) Les conséquences possibles des différentes mesures de l'UE pour la Suisse sont analysées	réalisé
	Engagement en faveur d'un cyberespace ouvert et libre 1) État des lieux des principaux processus internationaux et forums en matière de droits de l'homme 2) Évaluation relative à la participation suisse à des processus et forums choisis	réalisé

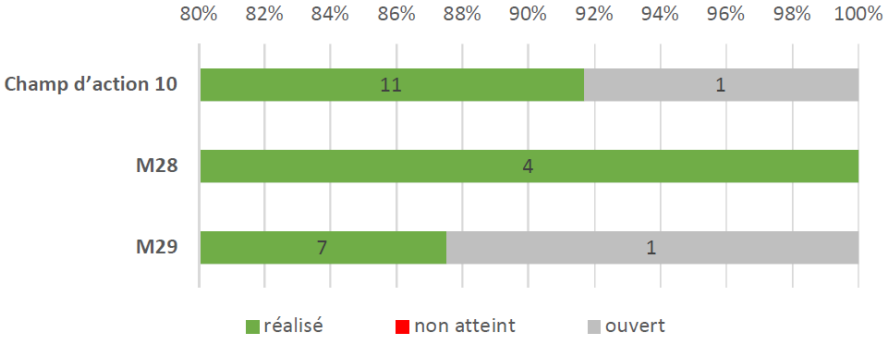
M26	Réalisation d'ateliers avec des organisations régionales 1) Élaboration d'un plan et organisation d'un premier atelier à Genève	réalisé
	Ateliers sur la mise en place d'institutions et de structures de cybersécurité extérieure: 1) Analyse des besoins, formation, plan, organisation d'un premier atelier	réalisé
M27	Sino-European Cyber Dialogue (SECD): 1) Établissement du groupe de travail International Law 2) Développement du SECD	réalisé
	MENA Cybersecurity Forum 1) Développement du MENA Cybersecurity Forum	réalisé

4.10 Champ d'action 10 «Visibilité et sensibilisation»

Aperçu du champ d'action: mesures et responsabilité de la mise en œuvre

- M28: élaboration et mise en œuvre d'un concept de communication pour la SNPC (NCSC)
- M29: sensibilisation du public aux cyberrisques (NCSC)

État de la mise en œuvre:



Étapes entre 2018 et le deuxième trimestre 2021

	Étape	Statut
M28	Élaboration d'un plan de communication sur la SNPC 1) Analyse de la situation 2) Plan de communication sur la SNPC élaboré (objectifs, groupes cibles, messages, poursuite des objectifs [stratégie], instruments/mesures, mesure des résultats et budget) 3) Responsabilités et délais de communication (plan) définis, et coordination à cette fin avec d'autres acteurs de la SNPC réalisée 4) Début de la mise en œuvre du plan de communication	réalisé
M29	Développement et exécution d'une campagne nationale de sensibilisation 1) Conception d'une campagne nationale de sensibilisation: coordination avec les acteurs actifs 2) Formulation du concept de la campagne nationale 3) Plan de mise en œuvre disponible 4) Lancement et production de la campagne nationale	réalisé
	Plateforme d'information sur les cyberrisques: 1) Développement du concept de la plateforme (contenus) 2) Lancement de la plateforme dans le cadre de la campagne de sensibilisation 3) Évaluation de l'utilisation de la plateforme et adaptation des contenus	réalisé