Rapport sur l'avancement des travaux concernant la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022

État au premier trimestre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Table des matières

1 Avant-propos

Il y a un an, j'ai pris mes fonctions de délégué fédéral à la cybersécurité. Depuis, j'ai beaucoup appris sur les compétences et les processus existants. J'ai également rencontré des femmes et des hommes motivés qui travaillent ensemble de manière constructive, à travers toutes les structures organisationnelles. La collaboration et les échanges, tant à l'intérieur qu'à l'extérieur de l'administration fédérale, sont en effet essentiels. Ils le sont en particulier pour la mise en œuvre coordonnée de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022. Cette stratégie fixe les objectifs en matière de protection contre les cyberrisques dans tous les champs d'action. Sa mise en œuvre repose aussi en grande partie sur les acteurs cantonaux, les milieux économiques, les hautes écoles et la société. Cette collaboration fonctionne bien, comme le montrent l'avancement des travaux et les mesures visant à améliorer la coordination.

Depuis l'adoption de la SNPC 2018-2022, le Conseil fédéral a défini et mis à exécution la nouvelle organisation de la Confédération dans le domaine des cyberrisques. En vigueur depuis le 1er juillet 2020, l'ordonnance sur les cyberrisques constitue la base légale nécessaire à la réorganisation et règle la collaboration au sein de l'administration fédérale et avec les cantons, les milieux économiques et scientifiques. Le Centre national pour la cybersécurité (NCSC) est opérationnel. Le Groupe Cyber et le comité de pilotage de la SNPC sont les organes interdépartementaux qui permettent d'assurer une coordination étroite de tous les acteurs.

La situation progresse bien dans les différents champs d'action de la SNPC. En ce qui concerne la promotion de la recherche et de la formation, des étapes importantes ont été franchies. Par exemple, un nouvel examen professionnel de spécialiste en cybersécurité a été lancé et le Campus cyberdéfence ouvert dans les deux écoles polytechniques fédérales et à Thoune. Par ailleurs, les petites et moyennes entreprises (PME) bénéficient d'un soutien toujours plus grand dans la protection contre les cyberrisques. Ainsi, le nouveau label cyber-safe.ch permet aux PME d'indiquer de façon transparente et uniforme leur niveau de sécurité informatique. En outre, la coordination de la lutte contre la cybercriminalité a été améliorée par la mise sur pied du Cyberboard, qui réunit les principaux acteurs de la poursuite pénale dans ce domaine. Enfin, la cyberdiplomatie gagne toujours plus en importance dans la politique extérieure numérique de la Suisse: un premier dialogue a pu être mené dernièrement avec les États-Unis, et le Dialogue de Genève sur le comportement responsable dans le cyberespace se poursuit.

Nous sommes dans la bonne voie. L'état d'avancement des travaux liés à la SNPC montre cependant aussi qu'il reste encore beaucoup à faire. Je constate notamment que l'administration fédérale doit rattraper son retard dans le domaine de la protection de base et dans la sensibilisation et la formation continue du personnel. Il me semble par ailleurs crucial que les résultats en matière de cybersécurité puissent être évalués de manière objective. Nous voulons donc qu'ils soient mesurables, pour permettre une critique nuancée. À cette fin, nous devons définir des critères de mesure clairs et les appliquer uniformément. Enfin, une décision majeure doit encore être prise: le Conseil fédéral entend se prononcer, d'ici à la fin de l'année 2020, sur une éventuelle instauration d'une obligation de déclarer les cyberincidents.
En fin de compte, la cybersécurité reste un processus. Nous sommes en plein milieu de ce processus et, selon moi, une chose est sûre: plus la collaboration de tous les acteurs est efficace, plus la Suisse sera protégée contre les cyberrisques.

Florian Schütz

2 Aperçu de l'avancement des travaux

Dans le plan de mise en œuvre de la SNPC, 247 étapes ont été définies dans les 29 mesures que comporte la stratégie. Jusqu'au premier trimestre 2020, 72 étapes ont été réalisées, 23 ont été retardées et trois n'ont pas pu être atteintes. 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.

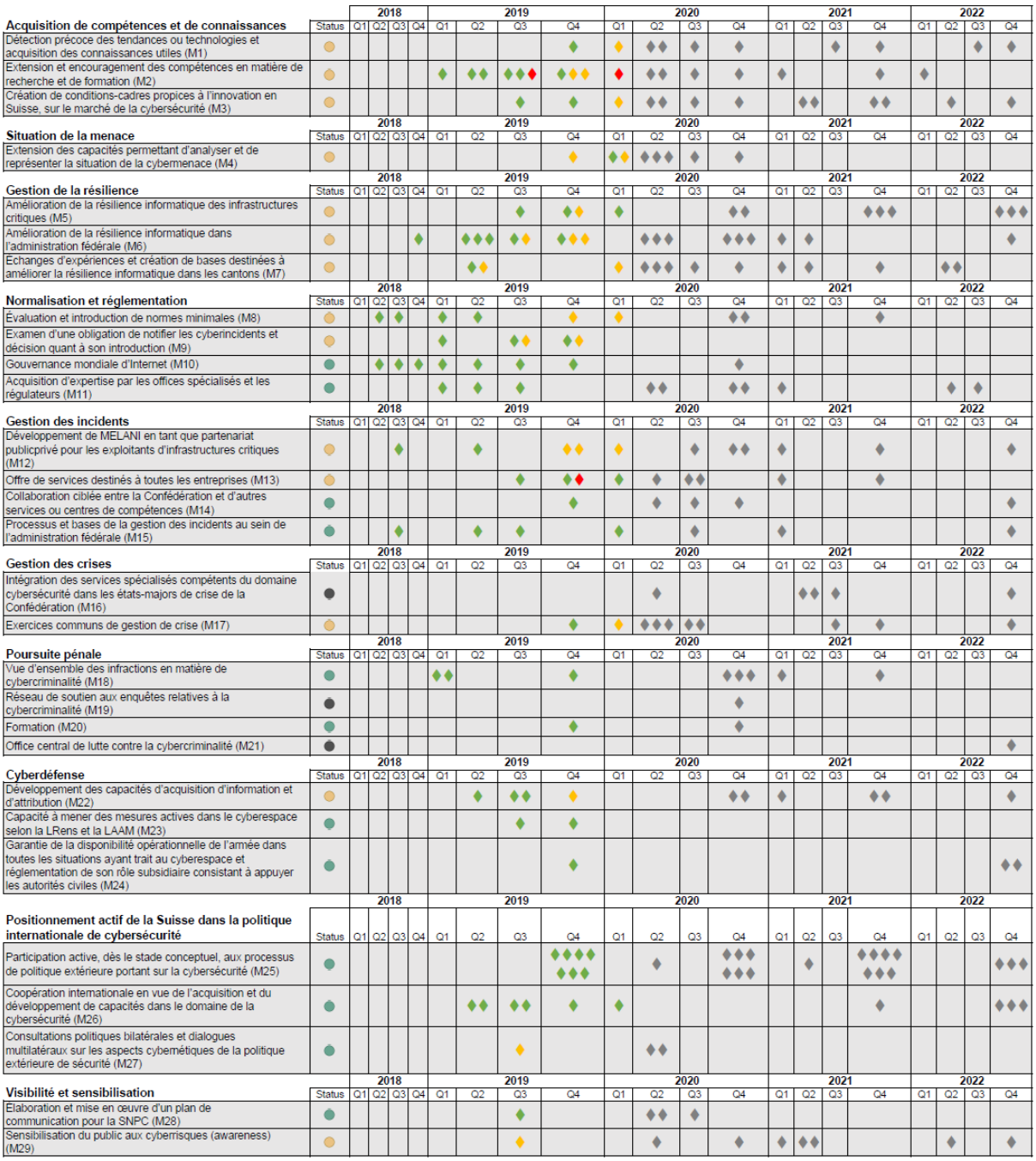


Illustration 1: Aperçu de l'avancement des travaux

3 Organisation de mise en œuvre

L'organisation de la Confédération dans le domaine des cyberrisques a été redéfinie progressivement ces deux dernières années. Le présent chapitre répertorie les décisions prises par le Conseil fédéral et expose l'état d'avancement de l'organisation.

3.1 Aperçu des décisions du Conseil fédéral

Après avoir adopté la SNPC 2018-2022 en avril 2018, le Conseil fédéral a pris plusieurs décisions concernant sa mise en œuvre et l'organisation de la Confédération. Ces décisions sont récapitulées dans l'illustration 2.

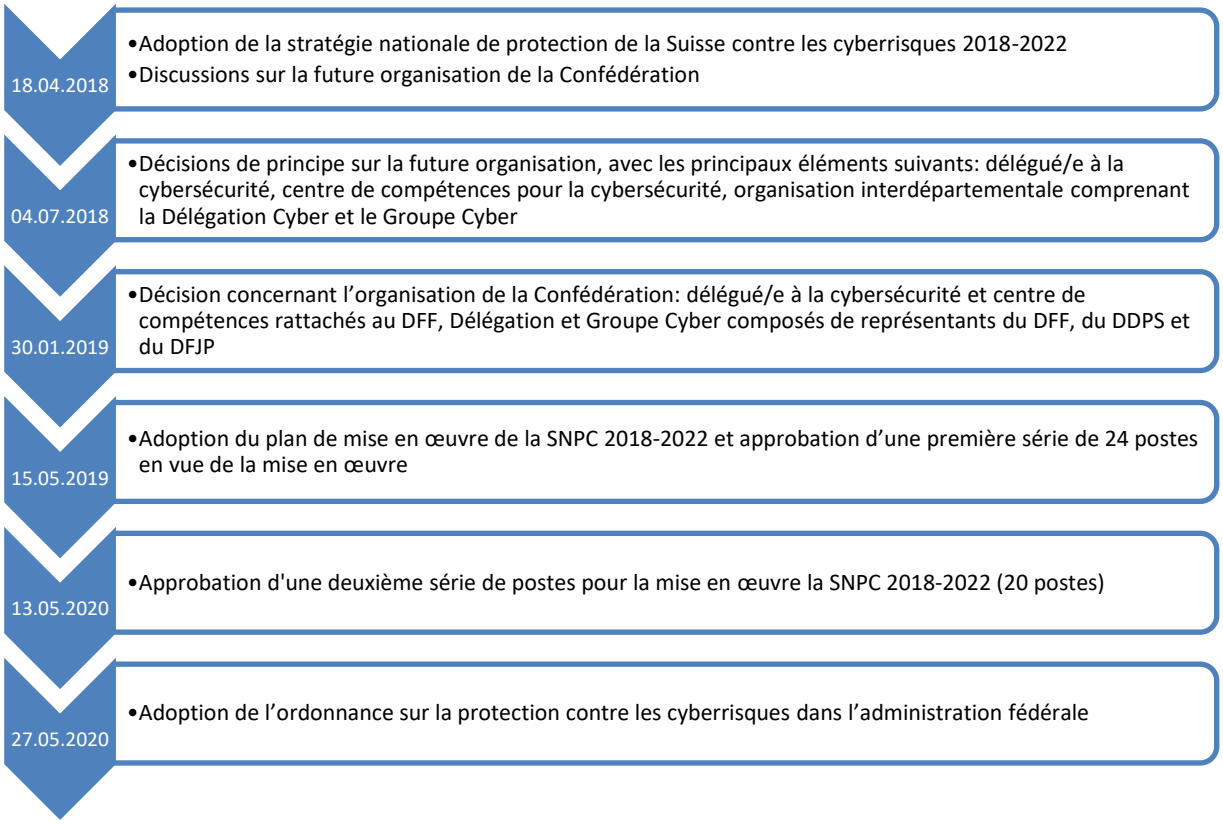


Illustration 2: Aperçu des décisions du Conseil fédéral

En outre, le Conseil fédéral a adopté les rapports suivants en réponse aux postulats qui ont été transmis sur des sujets concernant la cybersécurité:

- 27.11.2019: Rapport sur l'organisation de la Confédération pour la mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques. Rapport du Conseil fédéral en réponse aux postulats 16.4073 Golay du 15 décembre 2016 et 18.3003 CPS-CN du 22 janvier 2018 et à la motion 17.3508 Eder du 15 juin 2017
- 13.12.2019: Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques: solutions possibles. Rapport du Conseil fédéral en réponse au postulat 17.3475 Graf-Litscher du 15 juin 2017
- 29.04.2020: Normes de sécurité pour les appareils connectés à Internet (Internet des objets). Rapport du Conseil fédéral en réponse aux postulats Glättli 17.4295 du 15 décembre 2017 et Reynard 19.3199 du 21 mars 2019

3.2 État d'avancement de l'organisation

L'organisation de la Confédération consacrée à la protection contre les cyberrisques comprend les principaux éléments suivants: trois organes interdépartementaux (Délégation Cyber du Conseil fédéral, Groupe Cyber, comité de pilotage de la SNPC), le délégué à la cybersécurité comme interlocuteur de référence de la Confédération et le Centre national pour la cybersécurité (NCSC) en tant que centre de compétences de la Confédération. Cette section présente les activités des organes interdépartementaux et du délégué ainsi que l'avancement de la mise en place du NCSC.

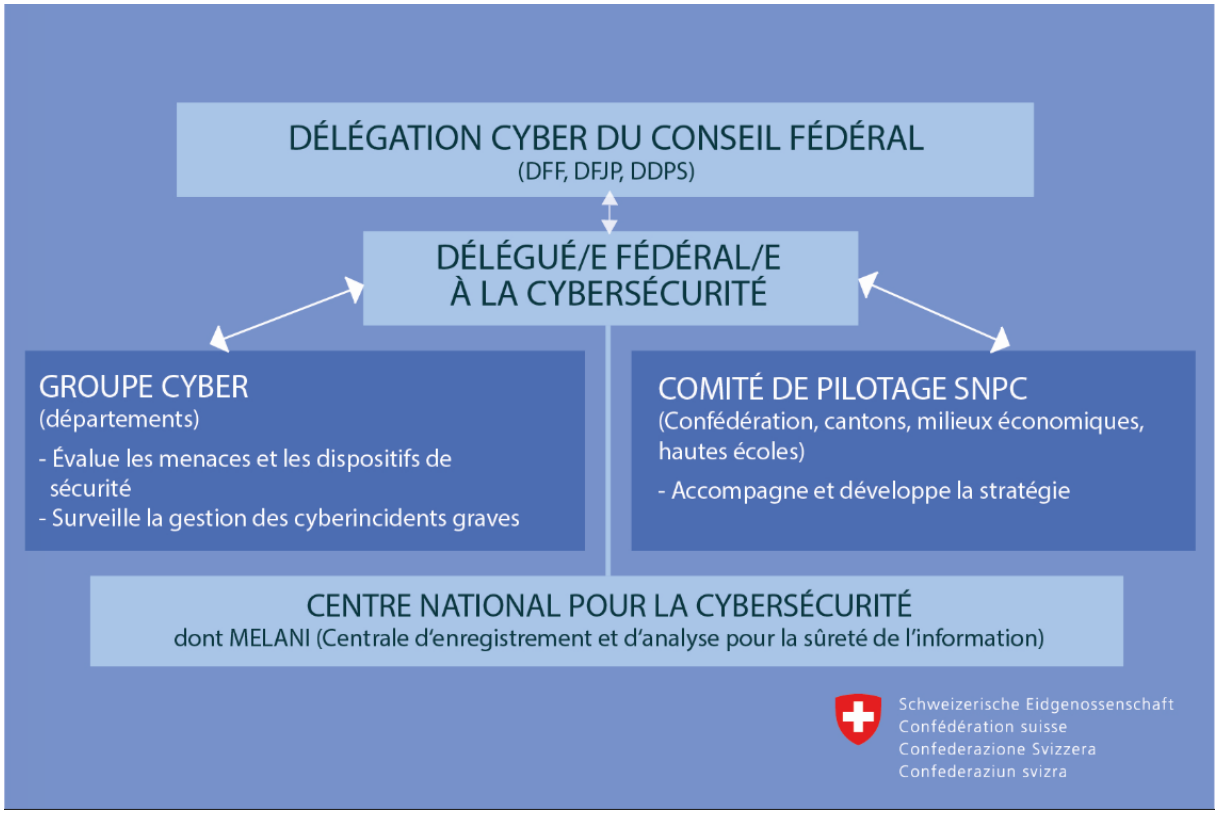


Illustration 3: Organisation de la Confédération dans le domaine des cyberrisques

3.2.1 Délégation Cyber du Conseil fédéral

La Délégation Cyber du Conseil fédéral a siégé trois fois jusqu'en juin 2020, sous la présidence du chef du Département fédéral des finances (DFF). En plus des chefs du DFF, du Département fédéral de justice et police (DFJP) et du Département fédéral de la défense, de la protection de la population et des sports (DDPS), le président de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) et le délégué fédéral à la cybersécurité assistent aux réunions. La Délégation Cyber s'informe des menaces actuelles et discute des affaires du Conseil fédéral en relation avec la cybersécurité ainsi que des questions politico-stratégiques.

3.2.2 Délégué fédéral à la cybersécurité

Florian Schütz[1] a pris ses fonctions de délégué fédéral à la cybersécurité en août 2019. Directement subordonné au chef du DFF, il dirige les organes interdépartementaux afin d'améliorer la coordination des travaux relatifs aux

[1] Florian Schütz est titulaire d'un master en sciences informatiques et d'un Master of Advanced Studies en politique de sécurité et gestion de crise de l'École polytechnique fédérale de Zurich (EPFZ). Il bénéficie de plus de dix ans d'expérience dans le domaine de la sécurité informatique dans le secteur privé.

cyberrisques. De plus, il assume la direction stratégique du nouveau NCSC qui, en tant que centre de compétences de la Confédération en matière de cybersécurité, est le premier interlocuteur des milieux économiques, de l'administration, des établissements d'enseignement et de la population pour toute question en la matière.

3.2.3 Groupe Cyber

Par analogie avec la Délégation Cyber du Conseil fédéral, le Groupe Cyber comprend des représentants du DFF (SG), du DFJP (fedpol) et du DDPS (SG) ainsi que le président de la Conférence des commandants des polices cantonales (CCPCS). Présidé par le délégué fédéral à la cybersécurité, il a siégé neuf fois en 2019. Il prépare les séances de la Délégation Cyber et veille en outre à assurer la meilleure coordination possible en matière de cyberrisques. À cette fin, le Groupe Cyber convie à ses réunions d'autres acteurs importants dans le domaine lorsque celles-ci ne portent pas directement sur la préparation des séances de la Délégation Cyber. Le Département fédéral des affaires étrangères (DFAE; Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace) est représenté de façon permanente dans le Groupe Cyber étendu; le délégué invite d'autres acteurs en cas de besoins et en fonction des thèmes.

3.2.4 Comité de pilotage de la SNPC

Le comité de pilotage de la SNPC veille à la cohérence stratégique lors de la mise en œuvre des mesures de la SNPC, coordonne les acteurs et évalue en permanence l'état d'avancement au moyen d'un contrôle de gestion stratégique. Il a siégé pour la première fois en novembre 2019. Y sont représentées les organisations qui sont directement chargées de mettre en œuvre les mesures de la SNPC, à savoir:

- des unités administratives de la Confédération: NCSC, armasuisse Sciences et technologies (S+T), Office fédéral de protection de la population (OFPP), Office fédéral de la communication (OFCOM), Chancellerie fédérale (ChF), Office fédéral pour l'approvisionnement économique du pays (OFAE), Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité commune relative au cyberspace (au sein du DFAE), Office fédéral de la police (fedpol), Secrétariat général du Département fédéral de l'intérieur (DFI), Secrétariat général du DDPS, Service de renseignement de la Confédération (SRC), Base d'aide au commandement (BAC);
- les cantons: CCDJP, Réseau national de sécurité (RNS), Cyberboard;
- les milieux économiques: ICTswitzerland, Switch, Swiss Cyber Experts, Association suisse pour le label de cybersécurité (Cyber-Safe);
- des hautes écoles: EPFZ, EPF Lausanne (EPFL).

3.2.5 Centre national pour la cybersécurité

Le NCSC a été créé en août 2019 en tant qu'unité autonome au sein du Secrétariat général du DFF. Il s'appuie principalement sur la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), qui est transférée dans le NCSC. Celui-ci a été développé comme suit en 2019:

- guichet unique suisse pour déclarer des incidents et poser des questions sur les cyberrisques: opérationnel depuis le 1er janvier 2020, il reçoit en moyenne 200 annonces par semaine. Il en effectue une première analyse, puis les transmet si nécessaire aux services compétents;
- renforcement de l'effectif de la GovCERT en tant qu'équipe nationale d'intervention en cas d'urgence informatique;
- expansion du bureau du NCSC.

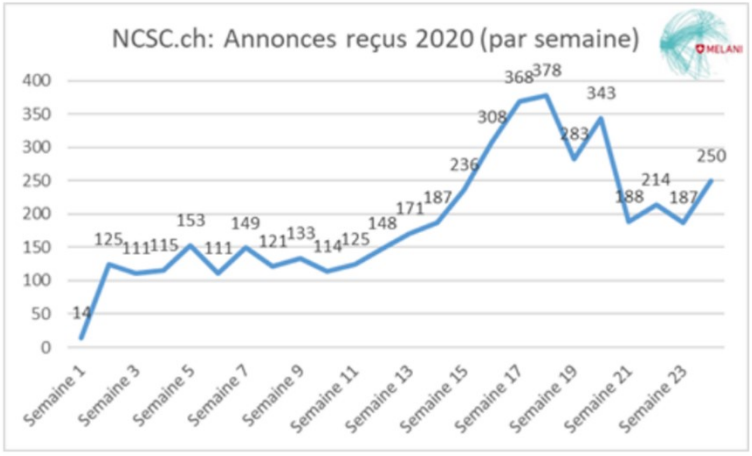


Illustration 4: Nombre d'annonces par semaine (état: mai 2020)

Un pool d'experts est mis sur pied au sein du NCSC dès 2020. Il soutient les offices spécialisés lors de projets spécifiques à la cybersécurité et contribue à renforcer la sensibilisation du public.

4 Grands axes de la mise en œuvre de la SNPC

La SNPC est mise en œuvre parallèlement à la réorganisation de la Confédération en matière de cyberrisques. 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.

4.1 Soutien des PME dans la protection contre les cyberrisques

Les petites et moyennes entreprises (PME) ne faisaient pas partie du groupe cible de la première SNPC 2012-2017. Par conséquent, peu de mesures coordonnées à l'échelle nationale les soutenaient auparavant dans ce domaine. La mise en œuvre de la SNPC 2018-2022 englobe des projets qui amélioreront cette situation dans différents champs d'action.

4.1.1 Test rapide pour PME, guide et boîte à outils de cybersécurité

Un test rapide de cybersécurité pour les PME a été élaboré en 2018 dans le cadre d'une vaste initiative[2] qui visait à proposer un instrument d'auto-évaluation notamment aux plus petites entreprises. Grâce à ce test[3], une entreprise ayant peu de connaissances approfondies en informatique et en sécurité informatique peut déterminer facilement et rapidement si ses mesures techniques, organisationnelles et humaines suffisent à la protéger contre les cyberrisques.
Lors de la publication du test, les PME ont indiqué qu'elles avaient besoin d'instructions claires pour améliorer leur cybersécurité. ICTswitzerland et l'Académie suisse des sciences techniques (SATW) ont donc rédigé, avec la participation d'experts de la Confédération et des milieux économiques, un guide[4] conçu pour aider les PME à atteindre un niveau minimal de cybersécurité. De plus, un accord a été conclu avec la Global Cyber Alliance (GCA) afin que les contenus (outils concrets et gratuits, y c. un guide)[5] soient traduits et mis à la disposition des PME suisses.

Illustration 5: Global Cyber Alliance

[2] L'initiative est portée par ICTswitzerland, l'Information Security Society Switzerland (ISS), l'Académie suisse des sciences techniques (SATW), l'Association Suisse de Normalisation (SNV), l'Association Suisse pour Systèmes de Qualité et de Management (SQS), l'Association Suisse d'Assurances (ASA) et des représentants de la Confédération.

[3] Disponible sous: www.cybersecurity-check.ch

[4] Disponible sous: https://ictswitzerland.ch/content/uploads/2020/04/Leitfaden_Cybersecurity_Schnelltest_F.pdf

[5] Disponibles sous: https://gcatoolkit.org/fr/petites-entreprises/

4.1.2 Label de cybersécurité

L'absence de normes ou des normes trop complexes empêchent les PME d'évaluer de façon transparente leur niveau de cybersécurité et de l'indiquer à des tiers. Le label de cybersécurité élaboré par l'Association suisse pour le label de cybersécurité (ASLaC) entend remédier à cette situation. Initiative privée développée en étroite collaboration avec des représentants des PME[6], ce label a été lancé le 18 décembre 2019 et contribue fortement à la mise en œuvre de la SNPC. Toutes les informations le concernant sont disponibles à l'adresse www.cyber-safe.ch.

Illustration 6: Cyber-safe.ch

4.2 Promotion de la recherche et de la formation

D'importants progrès ont été réalisés dans le champ d'action 1 «Acquisition de compétences et de connaissances». Le diplôme qui sanctionne le nouvel examen professionnel de spécialiste de la cybersécurité aidera à pallier le manque de main-d'œuvre qualifiée. Encouragé par l'armée dans le cadre de la création de sa propre instruction dans le domaine cybernétique, ce projet illustre parfaitement la collaboration constructive entre les services civils et militaires.
L'ouverture du Campus cyberdéfense (Campus CYD) dans les deux EPF et à Thoune constitue également une étape majeure. En tant que centre de compétences scientifique et technique, celui-ci améliorera le transfert de savoir entre les autorités et les milieux universitaires et contribuera à développer en Suisse un écosystème économique consacré à la cybersécurité. En cours de création, le nouveau «Swiss Support Centre for Cyber-Security» (SSCC) des deux EPF y contribuera également et jouera un rôle de coordination en servant de point de contact pour la Confédération et les cantons.

4.2.1 Examen professionnel de spécialiste en cybersécurité

Le 11 novembre 2019, l'organisation nationale du monde du travail ICT Formation professionnelle Suisse a lancé l'examen professionnel de spécialiste en cybersécurité[7].
L'examen professionnel mène au brevet fédéral, qui est le premier diplôme du degré tertiaire de la formation professionnelle. Sont admis à cet examen professionnel les candidats qui ont terminé une formation professionnelle sanctionnée par un certificat fédéral de capacité (CFC) et justifient d'une expérience professionnelle d'au moins deux ans dans le domaine des technologies de l'information et de la communication.
L'élaboration de l'examen professionnel a été cofinancée par l'armée et devrait inciter davantage de soldats à postuler pour l'instruction militaire dans le domaine cybernétique. Les personnes ayant suivi cette filière avec succès sont admises à l'examen professionnel si elles disposent d'au moins un an d'expérience professionnelle dans le domaine de la sécurité de l'information ou de la cybersécurité.

[6] Les PME étaient représentées par la Fédération des Entreprises Romandes Neuchâtel (FER Neuchâtel), la Chambre de commerce, d'industrie et des services de Genève (CCIG), la Fédération Patronale et Économique Fribourg (FPE-CIGA), la Chambre vaudoise du commerce et de l'industrie (CVCI), la Chambre valaisanne de commerce et d'industrie, l'Association suisse des cadres (ASC), l'Association Femmes PME Suisse romande et le Groupement Suisse de l'Industrie Mécanique (GIM-CH).
En outre, la société civile (ICON), les hautes écoles et les EPF (HEIG-VD, HES-SO Valais, EPFL C4DT) et les communes (Union des Communes Vaudoises) étaient aussi représentées.

[7] De plus amples informations sont disponibles sous: https://www.ict-berufsbildung.ch/fr/formation-professionnelle/formation-superieure-ict/brevet-federal-de-cyber-security-specialist/.

4.2.2 Campus CYD

Le Campus cyberdéfense (CYD) a été inauguré en janvier 2019 par armasuisse S+T pour anticiper autant que possible les développements dans le cyberespace, élaborer et étudier des cybertechnologies ainsi que former et perfectionner des cyberspécialistes. Il sert de lien entre les autorités, l'industrie et les milieux scientifiques en matière de recherche, de développement et de formation à la cyberdéfense. Après le site de Thoune, ceux de l'EPFL et de l'EPFZ ont été inaugurés respectivement en septembre et novembre 2019.
Le Campus CYD organise régulièrement des conférences sur des sujets liés à la cyberdéfense et, en collaboration avec l'EPFL, accorde des bourses de recherche dans ce domaine.

4.2.3 «Swiss Support Centre for Cyber-Security» et master des deux EPF

Les deux EPF se sont engagées conjointement à créer un «Swiss Support Centre for Cyber-Security» (SSCC). Ce centre vise à promouvoir les échanges entre les chercheurs des EPF et les autorités et à contribuer à l'amélioration aussi directe que possible de la cybersécurité en Suisse grâce à la recherche de pointe des deux hautes écoles. Son financement est défini, et les deux premiers collaborateurs sont entrés en fonction. Le centre sera encore développé et apportera ses différentes contributions à la SNPC, conformément au plan de mise en œuvre.
Par ailleurs, les deux EPF proposent depuis l'année universitaire 2019/2020 un master commun en cybersécurité. Les cours portent sur la cryptographie, la sécurité du matériel, des logiciels et des réseaux ainsi que sur les méthodes destinées à garantir la sécurité des systèmes et la confiance des utilisateurs. Comportant des éléments pratiques, ce cursus ne se limite pas aux aspects techniques de la cybersécurité, mais couvre également les questions éthiques, juridiques et opérationnelles dans ce domaine spécialisé.

4.3 Résilience des infrastructures critiques

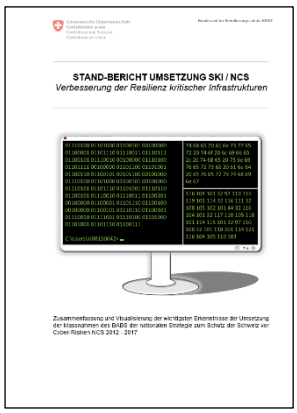

STAND-BERICHT UMSETZUNG SKI / NCS
Verbesserung der Resilienz kritischer Infrastrukturen

Illustration 7: Rapport sur la mise en œuvre de la résilience des infrastructures critiques

En se basant sur les analyses des risques et des vulnérabilités réalisées entre 2012 et 2017, l'OFPP a rédigé un rapport sur le niveau de résilience des infrastructures critiques en Suisse. Ce rapport présente une vue d'ensemble des risques estimés et des mesures prises pour améliorer la résilience durant une période donnée. Ces informations permettent de mieux classer les cyberrisques en fonction de la menace générale qu'ils représentent pour les infrastructures critiques. Le recoupement des informations permet également d'identifier les problèmes globaux et donc de mieux exploiter les synergies pour les traiter.
Les enseignements tirés fournissent aux décideurs une base pour établir l'ordre de priorité des différentes mesures de résilience possibles dans les secteurs partiels critiques.

Coordonnées par l'OFPP, toutes les analyses des risques et des vulnérabilités existantes seront actualisées dans le cadre de la mise en œuvre de la deuxième SNPC (2018-2022) et, si nécessaire, de nouvelles mesures de résilience seront prises. Les mesures de résilience adoptées et appliquées durant la période de la première SNPC seront poursuivies conformément aux responsabilités convenues.

4.4 Normalisation

Dans le champ d'action «Normalisation et réglementation», un rapport sur les normes de sécurité pour les appareils connectés à Internet (Internet des objets) a été publié et des normes minimales supplémentaires ont été définies pour les secteurs critiques.

4.4.1 Normes de sécurité pour les appareils connectés à Internet

Le rapport «Normes de sécurité pour les appareils connectés à Internet (Internet des objets)» présente les défis propres à la sécurité des systèmes ayant des composants reliés à Internet, les normes internationales applicables et les bases légales en vigueur en Suisse. Il a été rédigé en réponse aux postulats 17.4295 Glättli et 19.3199 Reynard[8] et sert de base aux autres travaux dans ce domaine.

4.4.2 Normes informatiques minimales

Une norme informatique minimale fait office de recommandation et d'éventuelle ligne directrice pour améliorer la résilience informatique des entreprises. Elle s'adresse en particulier aux exploitants des infrastructures critiques, mais est librement accessible[9] à toute entreprise ou organisation, qui peut l'appliquer.

Des normes spécifiques aux branches sont définies par les associations sectorielles, en collaboration avec l'OFAE, pour faciliter l'application d'une norme minimale dans les secteurs critiques. Il en existe déjà dans les secteurs de l'électricité, de l'alimentaire, de l'approvisionnement en eau et dans le traitement des eaux usées.

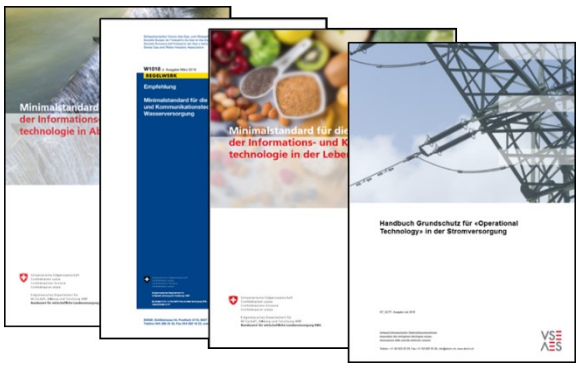


Illustration 8: Normes informatiques minimales

4.5 Examen d'une obligation de déclarer les cyberincidents

En décembre 2019, le Conseil fédéral a adopté le rapport «Obligation de déclarer les incidents graves affectant la sécurité des infrastructures critiques: solutions possibles»[10] en réponse au postulat 17.3475 Graf-Litscher. Ce rapport présente plusieurs solutions permettant d'introduire des obligations de déclarer. Ces solutions se fondent sur les obligations existantes de signaler les incidents de sécurité, sur les constatations issues des entretiens menés avec des experts et sur l'analyse des obligations de déclarer mises en place dans d'autres pays. En l'espèce, il est essentiel de clarifier si les cyberincidents doivent être annoncés à un point de contact distinct ou s'il faut compléter les points de contact sectoriels qui existent déjà en partie pour le signalement des incidents de sécurité. En lien avec cette structure organisationnelle, il convient d'évaluer le seuil à partir duquel les

[8] https://www.ncsc.admin.ch/melani/fr/home/documentation/rapports.html

[9] https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

[10] https://www.ncsc.admin.ch/melani/fr/home/documentation/rapports.html

incidents doivent être déclarés et dans quelles conditions ils doivent l'être, les délais à respecter pour les déclarations, la possibilité de faire des déclarations anonymes et celle de définir des sanctions en cas de non-respect de l'obligation. Le Conseil fédéral a chargé le NCSC et l'OFPP d'examiner ces questions en collaboration avec les autorités concernées des cantons et de la Confédération ainsi qu'avec les milieux économiques. Dans ce contexte, il s'agira également d'étudier si les obligations générales de déclarer les défaillances concernant les infrastructures critiques doivent être étendues. Le Conseil fédéral entend prendre d'ici à fin 2020 des décisions de principe sur la mise en place d'obligations de déclarer.

4.6 Meilleure coordination dans la lutte contre le cybercrime

En collaboration avec les autorités partenaires, les autorités de poursuite pénale ont établi à travers le Cyberboard une méthode de travail nationale destinée au transfert de savoir et à la coordination stratégique et opérationnelle en matière de lutte contre le cybercrime. Le Cyberboard se compose d'un organe de pilotage stratégique, Cyber-STRAT, et d'un domaine opérationnel, qui comprend une unité centrale chargée des tâches de coordination, Cyber-CORE, et deux autres unités, Cyber-CASE (vue d'ensemble des infractions) et Cyber-STATE (tableau de la situation). En 2019, le Cyberboard a régulièrement réuni les principaux acteurs de la poursuite pénale de la cybercriminalité, notamment le réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), renforçant ainsi la collaboration sur cette période. Il a permis d'éviter des conflits de for, notamment lorsque les questions de compétences n'étaient pas tranchées, et de trouver des solutions rapides et consensuelles, ce qui a bénéficié à la lutte contre le cybercrime.
De plus, chaque ministère public a nommé un interlocuteur unique dans le domaine de la cybercriminalité en tant que base de la collaboration opérationnelle. Dans le cadre de cette dernière, les autorités de poursuite pénale ont amélioré la coordination nationale lors de phénomènes de cybercriminalité tels que des fausses annonces immobilières ou des attaques contre les entreprises à l'aide de rançongiciels. La collaboration policière est encouragée au sein du NEDIK. Ce réseau bien établi est en cours de développement. Un groupe de cantons romands a élaboré la plateforme d'information de la criminalité sérielle en ligne (PICSEL) permettant de saisir de manière systématique et structurée les cas de cybercriminalité. Cette plateforme est en phase de test.

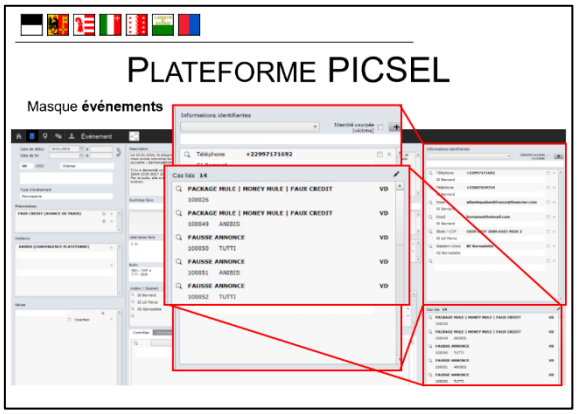


Illustration 9: Plateforme PICSEL

Les autorités de poursuite pénale disposent donc de bases adéquates pour développer régulièrement les capacités de lutte contre le cybercrime au sens d'une tâche commune et mettre en œuvre les mesures de la SNPC.

4.7 Collaboration accrue avec les cantons

Lorsque le Conseil fédéral a décidé de mettre sur pied le NCSC, plusieurs cantons ont exprimé leur intérêt et offert leur soutien. Les premiers entretiens avec les cantons intéressés ont eu lieu en 2019. Ils ont permis de déterminer dans quelle mesure les compétences cantonales en matière de cybersécurité pourraient être mieux intégrées aux

travaux de la Confédération.
En mars 2020, la plateforme politique du RNS a demandé à ses délégués de recenser les compétences et projets cantonaux pour obtenir une vue d'ensemble et jeter les bases d'une collaboration structurée entre le NCSC et les cantons.

4.8 Renouvellement du partenariat public-privé «Swiss Cyber Experts»

Le nouveau contrat de coopération entre la Confédération et l'association Swiss Cyber Experts (SCE), qui comprend une option de prolongation de cinq ans, a été signé au premier trimestre 2020. L'association soutiendra le NCSC dans l'analyse des incidents, contribuera à déterminer la situation de la Confédération et, le cas échéant, exécutera d'autres travaux de soutien pour la cybersécurité de la Suisse.

Illustration 10: Logo de Swiss Cyber Experts

4.9 Geneva Dialogue on Responsible Behaviour in Cyberspace

Dans la stratégie de politique extérieure 2020-2023[11], le Conseil fédéral a défini la numérisation comme une nouvelle priorité thématique de la politique extérieure suisse. La cyberdiplomatie, qui vise à défendre les intérêts du pays dans le cyberespace (ou dans un espace numérique), y est présentée comme un élément central de la politique extérieure numérique. À cet égard, la Suisse entend renforcer son engagement international et développer son rôle dans la cyberdiplomatie.
Le Geneva Dialogue on Responsible Behaviour in Cyberspace (Dialogue de Genève sur le comportement responsable dans le cyberespace) fait partie intégrante de ces activités. Lancé fin 2018 avec DiploFoundation, United Nations Institute for Disarmament Research (UNIDIR), l'EPFZ et l'Université de Lausanne, il est entré dans sa deuxième phase en mai 2020. Celle-ci met l'accent sur les échanges relatifs aux meilleures pratiques entre les entreprises internationales dans le but d'accroître la sécurité des produits dans le cyberespace. Parmi les participants, on trouve des entreprises suisses telles qu'UBS et SwissRe ainsi que Microsoft (États-Unis), Cisco (États-Unis), Kaspersky (Russie), Sberbank (Russie), Huawei (Chine), Siemens (Allemagne), FireEye (États-Unis) et VU Security (Argentine). Ce projet est réalisé par le DFAE, en collaboration avec le Forum économique mondial, l'EPFZ et la Swiss Digital Initiative.

[11] https://www.eda.admin.ch/eda/fr/dfae/dfae/mise-oeuvre-politique-exterieure/aussenpolitischestrategie.html

5 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 premier trimestre 2020. Celles-ci sont brièvement décrites pour une meilleure compréhension de leur contribution à la SNPC.
Sur les 247 étapes définies dans le plan de mise en œuvre de la SNPC, 72 ont été réalisées, 23 ont été retardées et trois n'ont pas été atteintes[12]. Un peu moins d'un tiers des étapes ont donc été réalisées après neuf trimestres (sur les 20 de la durée totale de la SNPC). On peut dès lors affirmer de manière générale que la mise en œuvre de la SNPC suit le cap défini, même si une grande partie des travaux doivent encore être exécutés dans la plupart des mesures. L'illustration 11 montre l'état de la mise en œuvre, toutes étapes confondues.

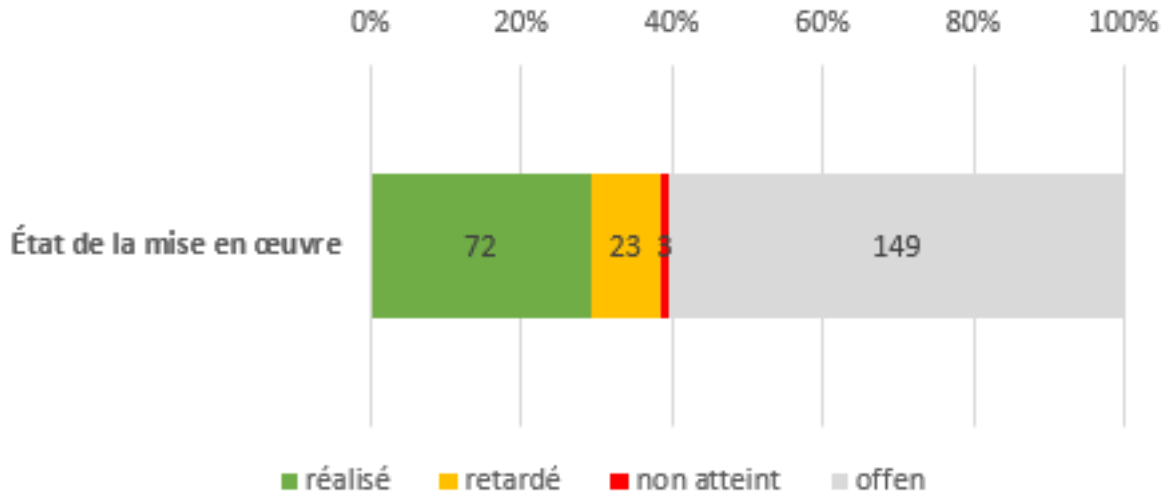


Illustration 11: État de mise en œuvre de l'ensemble des étapes de la SNPC

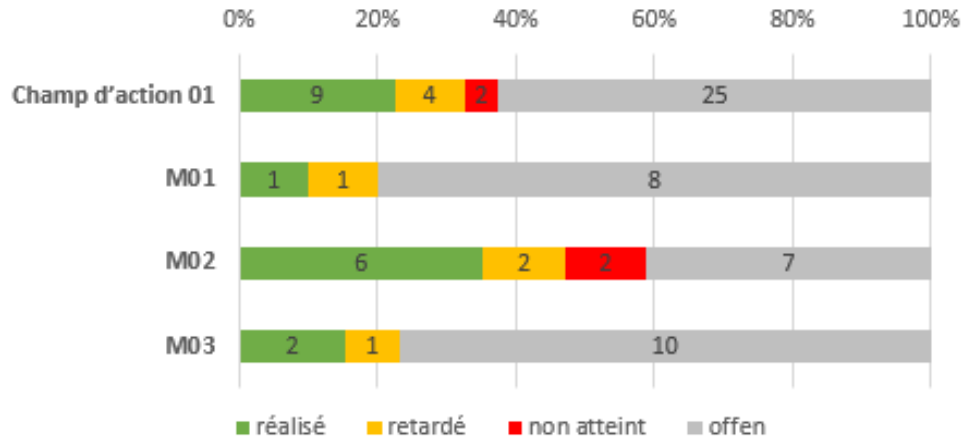
[12] On parle de retard lorsque l'étape n'a pas pu être atteinte en temps opportun, mais que les responsables de la mise en œuvre ont démontré de manière plausible que la réalisation n'était pas menacée.

5.1 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 premier trimestre 2020

	Étape	Statut
M1	Monitorage des technologies: définition des prestations du Campus CYD pour le monitorage destiné au NCSC	Réalisé
	Analyse des tendances: élaboration d'un plan relatif au public cible, aux contenus et à la diffusion des rapports	Retardé
M2	Analyse des besoins de formation: réalisation de l'analyse et définition des groupes cibles	Retardé
	Centre de recherche et d'assistance des deux EPF: élaboration du projet de centre	Réalisé
	Centre de recherche et d'assistance des deux EPF: règlement du financement et choix du site	Réalisé
	Début des activités du Campus CYD sur le site de Thoune	Réalisé
	Début des activités du Campus CYD sur le site de l'EPFL	Réalisé
	Début des activités du Campus CYD sur le site de l'EPFZ	Réalisé
	Identification des principaux instituts de recherche sur les cyberrisques	Retardé
	Identification des événements existants dans le domaine du piratage éthique	Réalisé
	Conception des instruments d'encouragement; si nécessaire, demande de moyens financiers, et mise à disposition des subventions	Non atteint. Mesure: modification du projet. Un financement fédéral ne convient pas à l'encouragement des événements dans le domaine du piratage éthique.
M3	Écosystème de la cybersécurité: identification des principaux instituts de recherche sur les cyberrisques des hautes écoles suisses	Retardé

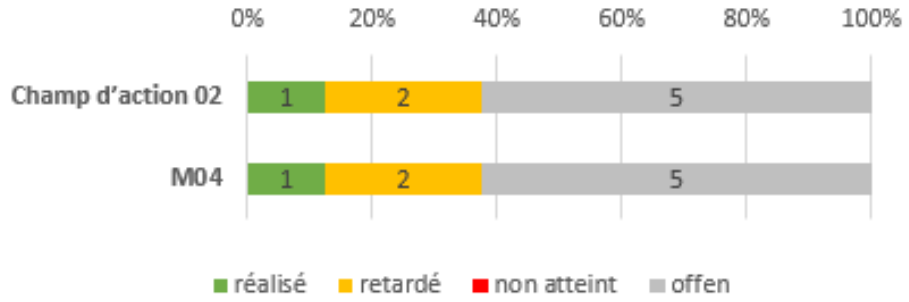
	Laboratoire d'idées: élaboration du projet de centre de recherche et d'assistance des deux EPF	Réalisé
	Laboratoire d'idées: règlement du financement et choix du site du centre de recherche et d'assistance des deux EPF	Réalisé

5.2 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 premier trimestre 2020

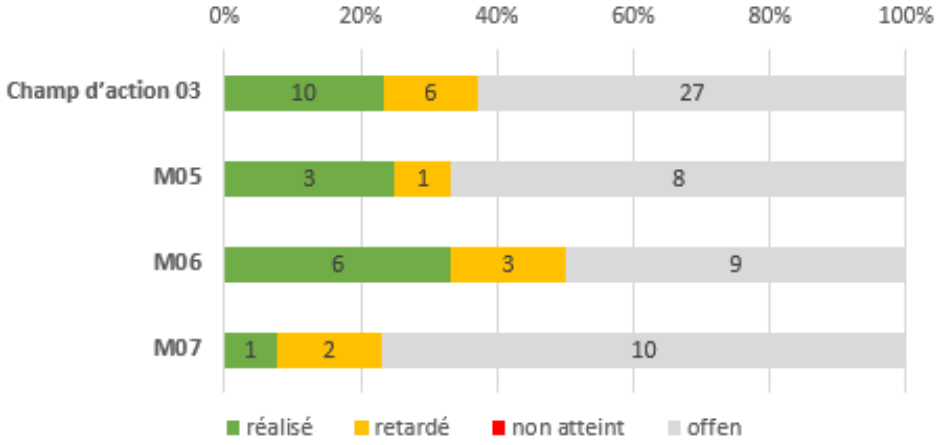
	Étape	**Statut**
M4	Analyse des besoins et définition des groupes cibles	Réalisé
	Catalogue de prestations: délimitation des compétences respectives de la Confédération et des milieux économiques	Retardé
	Sources: liste des sources supplémentaires nécessaires	Réalisé

5.3 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[13])

État de la mise en œuvre:



Étapes entre 2018 et le premier trimestre 2020

	Étapes	Statut
M5	État des lieux des projets déjà réalisés ou encore à réaliser selon les rapports sur les mesures	Réalisé
	Définition des responsabilités pour la mise en œuvre	Réalisé
	Feuille de route/planification des mesures actuelles ou à venir	Réalisé
	Établissement d'un groupe de travail universitaire pour la cybersécurité	Retardé
M6	Directives de sécurité: analyse des tâches liées à la sécurité prescrites dans les méthodes de projet, avec leurs résultats	Retardé
	Première ébauche de la campagne de sensibilisation portant sur la sécurité informatique dans l'administration fédérale (T4/2018)	Réalisé
	Début de la campagne de sensibilisation portant sur la sécurité informatique dans l'administration fédérale	Réalisé
	Coordination avec d'autres acteurs pour une transformation en campagne nationale (voir M29 «Sensibilisation du public aux cyberrisques»)	Retardé
	Élaboration d'un nouveau plan de mesures pour les années 2021/2022	Retardé
	SCION: déclaration d'intention des services intéressés et des utilisateurs pilotes	Réalisé
	SOC: projet et plan de mise en œuvre	Réalisé
	SOC: fin des travaux	Retardé

[13] Vous trouverez des informations sur d'autres projets du plan de mise en œuvre des 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

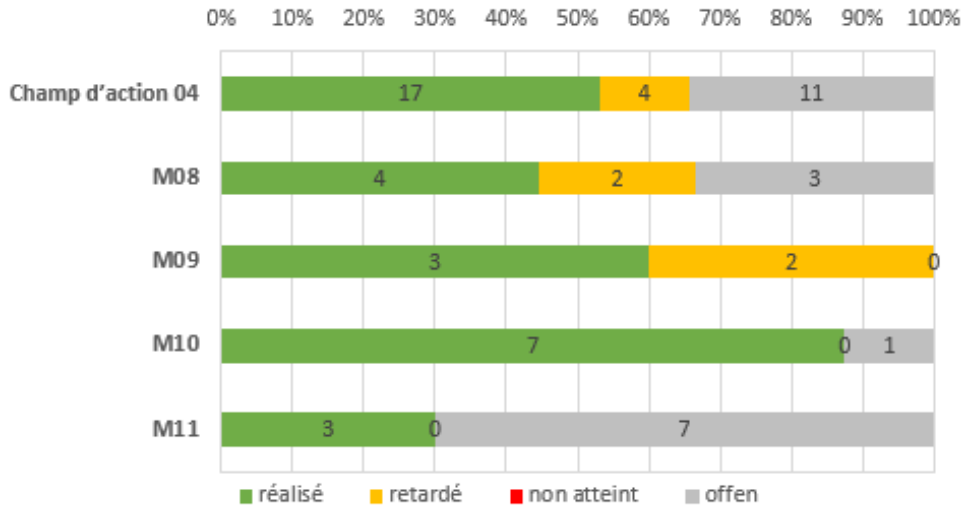
	Interface avec les EPF: coordination avec le délégué à la cybersécurité	Réalisé
M7	Échange avec les cantons: Évaluation des besoins liés aux postes de travail du NCSC	Retardé
	Organisation de la Cyberlandsgemeinde	Réalisé
	Interface entre les EPF et les cantons: coordination avec le RNS	Retardé

5.4 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 premier trimestre 2020

	Étapes	**Statut**
M8	Publication de la norme minimale et d'un outil d'évaluation	Réalisé
	Norme minimale «Manuel Protection de base» de l'Association des entreprises électriques suisses (AES)	Réalisé
	Norme sectorielle sur l'eau potable et les denrées alimentaires	Réalisé
	Norme sectorielle sur le gaz naturel	Retardé
	Norme sectorielle sur les transports publics	Retardé
	Publication du test rapide sur la cybersécurité pour les PME (SATW) [T3/2018]	Réalisé
	Analyse du besoin d'autres outils spécifiques aux PME (outils techniques, labels, guides et instructions)	Réalisé
M9	Appel d'offres et rédaction d'une étude de base	Réalisé
	Rapport (réponse au postulat)	Réalisé
	Débat de fond avec les milieux économiques et politiques	Retardé
	Base décisionnelle sur l'obligation de déclarer	Retardé
M10	Réunion du groupe de haut niveau du Secrétaire général des Nations Unies (New York, Genève, Helsinki)	Réalisé

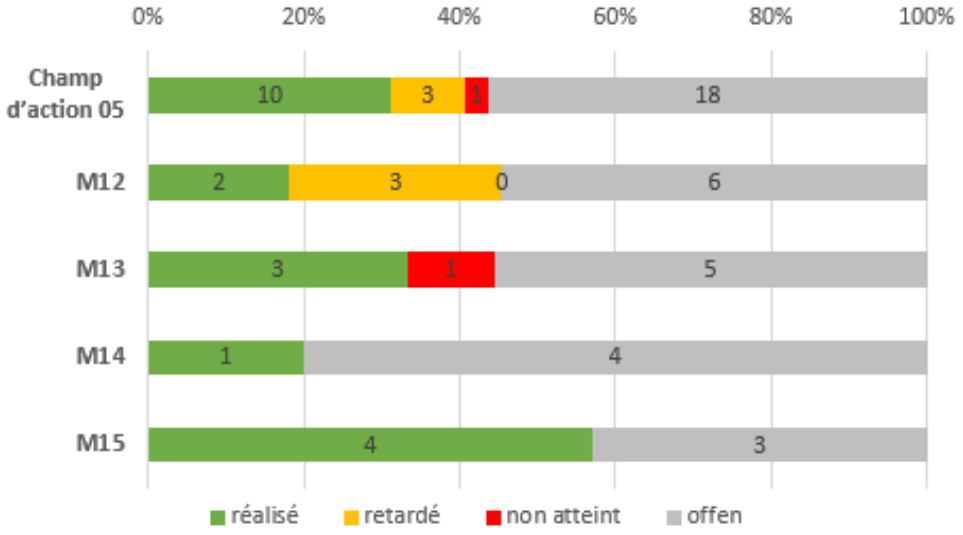
	Rapport du groupe	Réalisé
	Évaluation des possibilités de mise en œuvre	Réalisé
M11	Pool d'experts: identification des besoins	Réalisé
	Pool d'experts: création de postes pour le pool	Réalisé
	Élaboration du projet de centre de recherche et d'assistance commun EPFL-EPFZ	Réalisé

5.5 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 premier trimestre 2020

	Étapes	**Statut**
M12	Cercle fermé de MELANI: état des lieux de l'utilisation de MELANI par les différents secteurs critiques	Retardé
	Réalisation de l'étude avec recommandation d'une solution pour MELANI-NET 2.0 (T3/2018)	Réalisé
	Réalisation de la preuve du concept (*proof of concept*) pour la solution recommandée	Réalisé
	Plan pour MELANI-NET 2.0	Retardé
	MELANI-NET 2.0 productif	Retardé
M13	Guichet unique national: élaboration d'un projet sommaire de portail en ligne pour la déclaration de cyberincidents	Réalisé
	Analyse de la situation et des besoins concernant les éventuelles «meilleures pratiques» pour la gestion des cyberincidents	Non atteint. Mesure: modification de la planification du projet. Intégration de partenaires supplémentaires

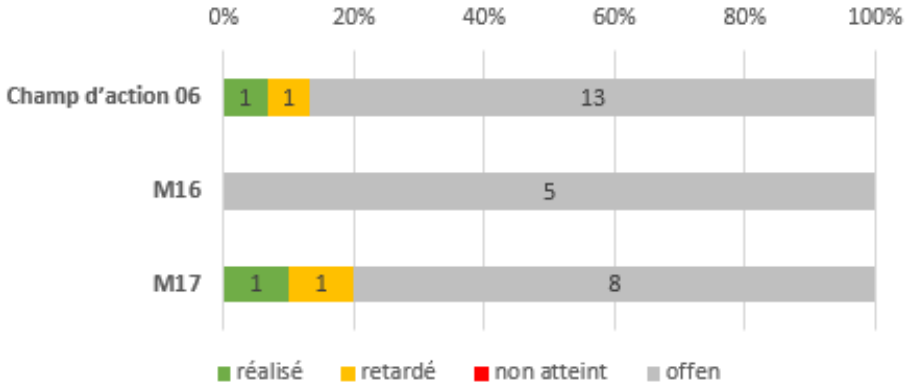
	Détermination des exigences concernant l'alerte, l'avertissements et l'information du public en cas de cyberincident -> application Alertswiss	Réalisé
	Établissement du plan d'intégration des cyberinformations dans l'application Alertswiss	Réalisé
M14	Exécution et documentation du recensement des CERT et des SOC opérationnels et des interlocuteurs de référence	Réalisé
M15	Élaboration d'une ordonnance sur la cybersécurité	Réalisé
	Adoption de l'ordonnance par le Conseil fédéral	Réalisé
	Détermination de l'entrée en vigueur de l'ordonnance	Réalisé
	Premier projet de processus de gestion des incidents de sécurité dans l'administration fédérale, discussion avec les fournisseurs de prestations et les services concernés	Réalisé

5.6 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 premier trimestre 2020

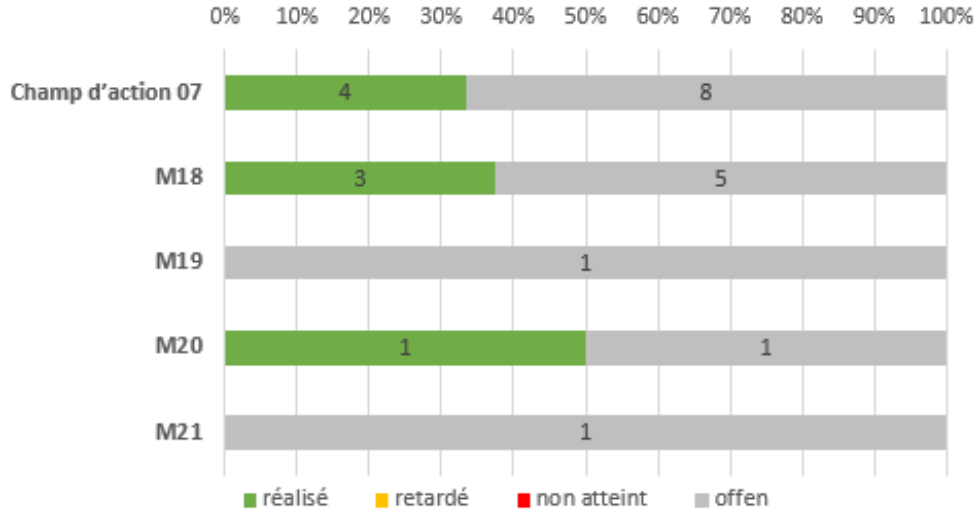
	Étapes	**Statut**
M16	Aucune étape jusqu'au premier trimestre 2020	
M17	Inventaire des exercices de crise nationaux et internationaux qui comportent des aspects cybernétiques et qui existent ou sont prévus	Retardé
	Analyse des besoins relatifs aux exercices de crise sectoriels	Réalisé

5.7 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 premier trimestre 2020

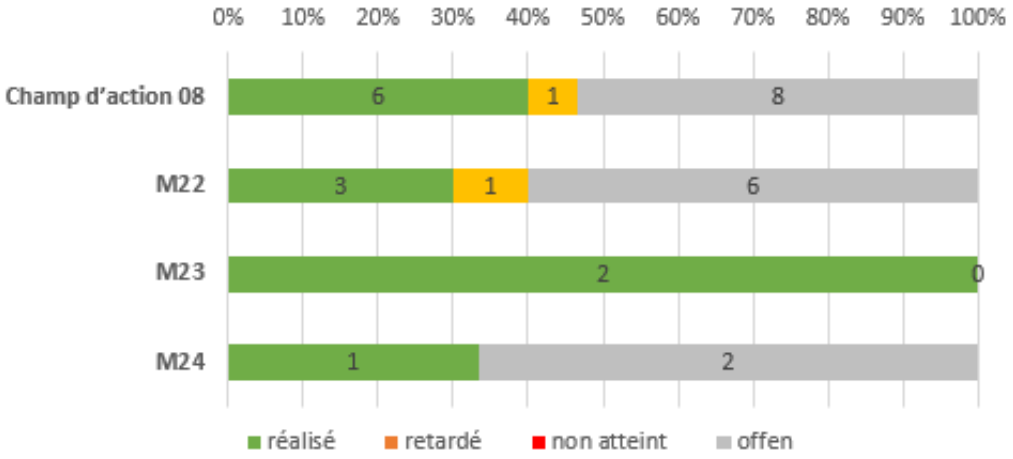
	Étapes	Statut
M18	Vue d'ensemble des infractions en matière de cybercriminalité: début de la phase de test de PICSEL	Réalisé
	Outil Cyber-CASE; liste des infractions pour tous les procureurs qui font office d'interlocuteurs uniques dans le domaine de la cybercriminalité (déjà opérationnelle)	Réalisé
	Bulletin mensuel (de la police) NEDIK	Réalisé
M19	Aucune étape jusqu'au premier trimestre 2020	
M20	Vue d'ensemble des possibilités de formations académiques (policières)	Réalisé
M21	Aucune étape jusqu'au premier trimestre 2020	

5.8 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 premier trimestre 2020

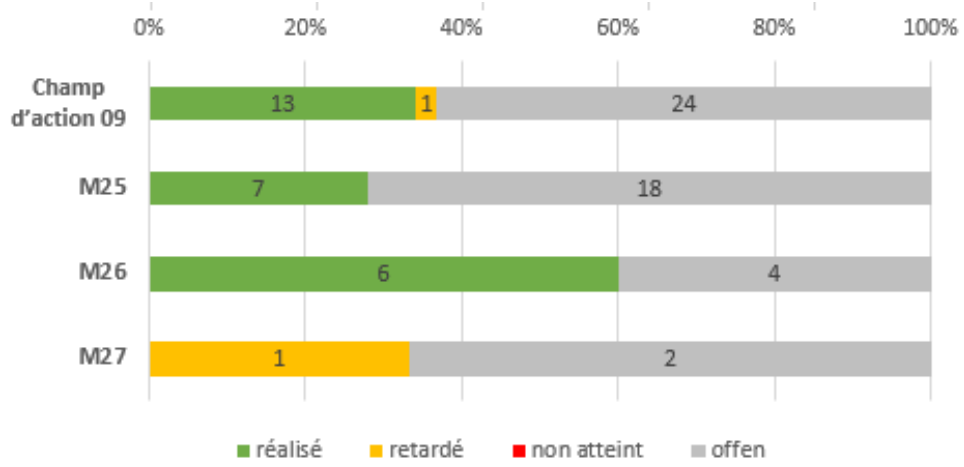
	Étapes	Statut
M22	Capacités d'acquisition d'information et d'attribution: fin de la première étape de développement	Retardé
	Formation: premier entraînement avec la BAC des Forces terrestres	Réalisé
	Lancement du master commun EPFL-EPFZ-DDPS	Réalisé
	Premières formations EPFL-DDPS	Réalisé
M23	Capacités du COE de la BAC: les effets collatéraux des activités prévues ont été envisagés avec les offices spécialisés	Réalisé
	Capacités disponibles	Réalisé
M24	Fin du projet de développement de la cyberdéfense	Réalisé

5.9 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 premier trimestre 2020

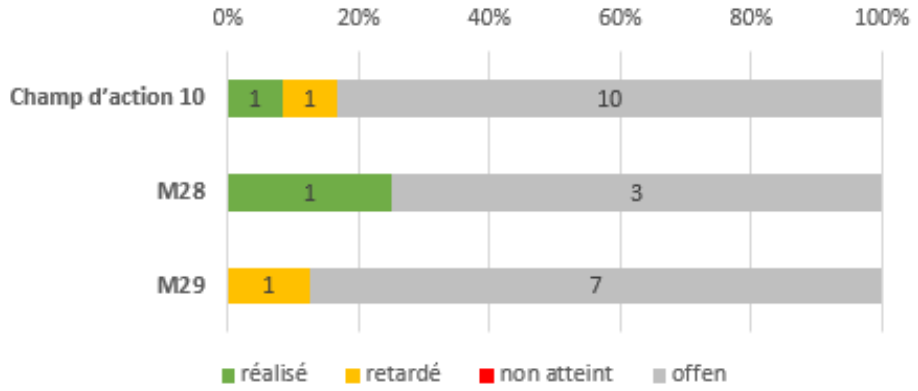
	Étapes	Statut
M25	Participation à des processus de l'ONU: rapport annuel	Réalisé
	OSCE: participation aux négociations, contribution active au processus et rapport annuel	Réalisé
	Plan pour l'établissement du Dialogue de Genève comme plateforme multi-acteurs	Réalisé
	Réalisation de deux à trois dialogues du processus d'experts sur l'application du droit international dans le cyberespace	Réalisé
	Vue d'ensemble des principaux acteurs, processus et mesures de l'UE ainsi que des services qui participent aux processus en Suisse	Réalisé
	État des lieux des principaux processus internationaux et forums en matière de droits de l'homme	Réalisé
M26	Coopération internationale: 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: analyse des besoins, formation, plan, organisation d'un premier atelier	Réalisé
M27	Développement du Sino-European Cyber Dialogue (SECD)	Retardé

5.10 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 premier trimestre 2020

	Étapes	Statut
M28	Concept de communication du NCSC: analyse de la situation	Réalisé
M29	Conception d'une campagne nationale de sensibilisation: coordination avec les acteurs actifs	Retardé