Plan de mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018–2022

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Table des matières

1 Introduction

Le 18 avril 2018, le Conseil fédéral a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022. Cette stratégie repose sur la première SNPC, qui portait sur les années 2012 à 2017, qu'elle développe et complète par de nouvelles mesures. Elle tient ainsi compte de la situation de la menace, qui a connu un net regain d'intensité.
La stratégie doit contribuer à ce que tout en saisissant les chances offertes par le numérique, la Suisse soit protégée de façon appropriée contre les cyberrisques, et résiliente en cas de cyberincident. À partir de cette vision, la SNPC a identifié sept objectifs stratégiques et formulé au total, pour les atteindre, 29 mesures à prendre dans dix champs d'action. La fig. 1 représente synthétiquement le contenu de la SNPC:

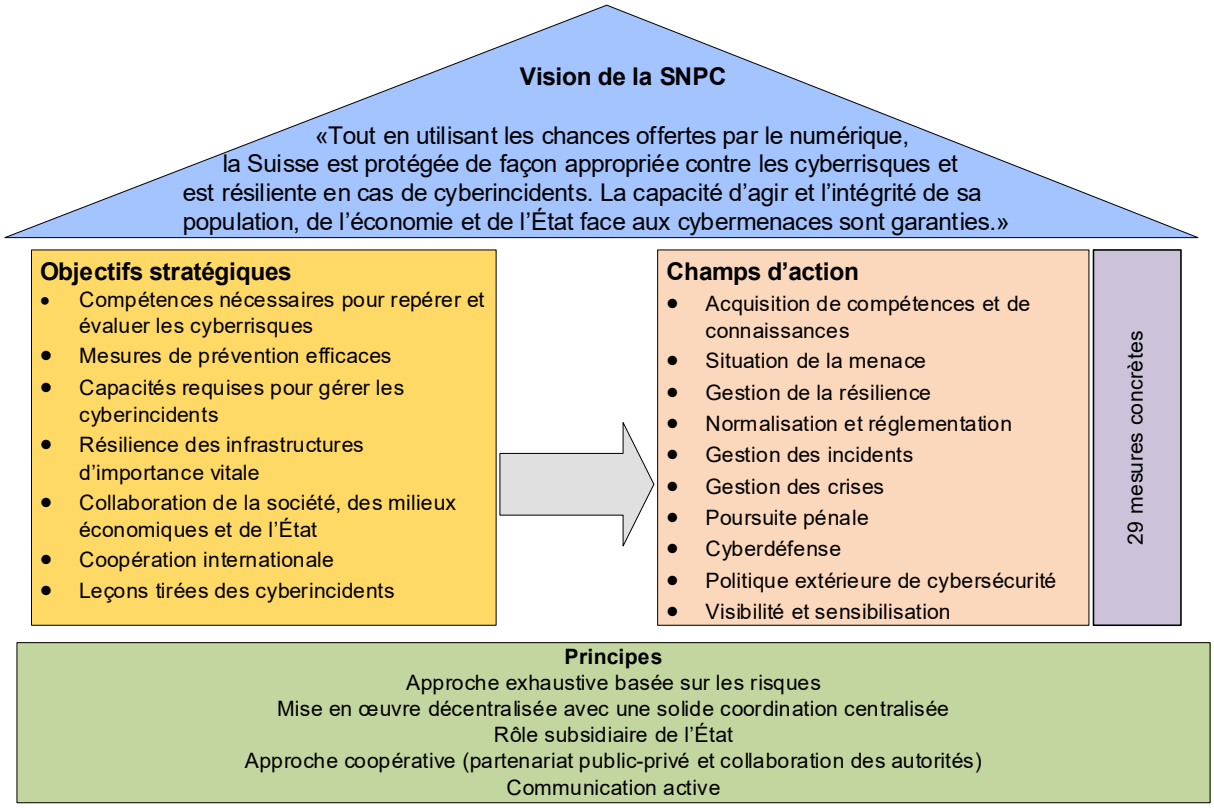


Figure 1: contenu de la SNPC

Le présent plan de mise en œuvre définit des projets concrets pour les 29 mesures de la SNPC, fixant à chaque fois les responsabilités, les objectifs de prestations à atteindre ainsi que les étapes à franchir.
Véritable œuvre collective, il a été conçu entre la fin de 2018 et le début de 2019 avec les services fédéraux compétents, les cantons, les milieux économiques et les hautes écoles, et doté d'une structure qui reprend les champs d'action de la SNPC. Grâce à cette large participation à son élaboration, ce plan de mise en œuvre n'expose pas seulement les activités projetées par les services fédéraux impliqués, mais englobe également les principales activités que d'autres acteurs déploient dans le champ de la SNPC. Par conséquent, il peut servir aussi bien de base pour la planification des travaux puis pour le contrôle de gestion stratégique portant sur l'avancement des travaux, que d'instrument de coordination entre tous les acteurs concernés.
Le présent document reflète l'état actuel de la planification de la mise en œuvre de la SNPC. Des adaptations doivent rester en tout temps possibles, au vu du contexte dynamique dans lequel évoluent les cyberrisques. Les divers comités décrits au chapitre suivant ont par conséquent reçu la compétence d'adapter en cas de besoin le plan de mise en œuvre.

2 Organisation de mise en œuvre

Le succès de la mise en œuvre de la SNPC dépendra largement de l'allocation optimale des ressources disponibles à l'heure actuelle, et aussi de leur renforcement coordonné au fil du temps. Les tâches décrites dans le présent plan de mise en œuvre sont contraignantes pour les offices fédéraux. Ils auront toutefois besoin du concours de tiers pour s'en acquitter, en raison tant de la complexité des tâches que de leurs ressources restreintes et des limites juridiques de leurs compétences. L'organisation des travaux devra en tenir compte. Aussi les sous-chapitres qui suivent décrivent-ils d'abord la manière dont la Confédération s'est organisée dans le domaine des cyberrisques, puis les futures modalités de la collaboration entre la Confédération, les cantons, les milieux économiques et les hautes écoles pour mettre en œuvre la SNPC, et enfin l'organisation du contrôle de gestion et des rapports prévus.

2.1 Organisation de la Confédération dans le domaine des cyberrisques

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

- Cybersécurité: ensemble des mesures visant à prévenir et à traiter les incidents ainsi qu'à améliorer la résilience face aux cyberrisques en renforçant la coopération internationale. La Confédération prend les mesures nécessaires pour renforcer sa propre cybersécurité et participe à l'amélioration de la cybersécurité des entreprises et de la société conformément au principe de subsidiarité, tout en accordant une attention particulière au rôle central que jouent les infrastructures critiques. À ces mesures s'ajoute la promotion de la collaboration internationale dans le domaine de la cybersécurité.
- Cyberdéfense: ensemble des mesures concernant les services de renseignement civils et l'armée et servant à protéger les systèmes critiques, à se défendre contre des attaques dans le cyberespace, à garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace; enfin, elles ont pour but de développer les capacités et les compétences de l'armée afin que celle-ci puisse apporter subsidiairement un soutien aux autorités civiles. Ce domaine prend notamment des mesures actives pour identifier les menaces et les attaquants ainsi que pour entraver et bloquer les attaques.
- Poursuites contre la cybercriminalité: toutes les mesures adoptées par les forces de police et les ministères publics de la Confédération et des cantons, dans leur lutte contre la cybercriminalité.

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

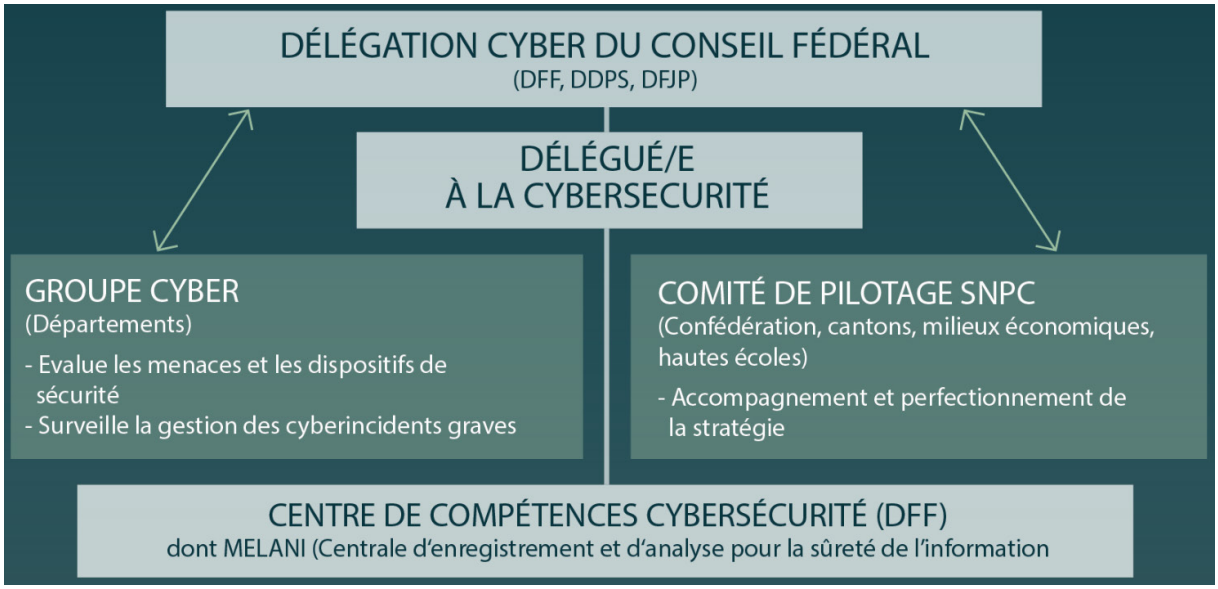


Figure 2: organisation de la Confédération dans le domaine des cyberrisques

Le partage des tâches entre ces comités ou fonctions créés dans le cadre de la SNPC a été défini de la façon suivante:

- La **Délégation Cyber, composée des chefs du DFF, du DFJP et du DDPS**, a pour tâche de surveiller la mise en œuvre de la SNPC.
- Le **Centre de compétences de la Confédération pour la cybersécurité, implanté au DFF**, sert de guichet unique national pour les questions relatives à la cybersécurité et assure, avec son bureau, la coordination de la mise en œuvre de la SNPC.
- Le **délégué à la cybersécurité** exerce à l'échelon de la Confédération la direction stratégique de la cybersécurité, préside les comités créés par la Confédération, et représente cette dernière dans d'autres comités.
- Le **Groupe Cyber** renforce la coordination entre les trois domaines de la sécurité, de la défense et de la poursuite pénale, veille à leur évaluation conjointe de la menace et supervise la gestion par les services fédéraux des incidents graves et impliquant plusieurs départements.
- Le **comité de pilotage de la SNPC** assure la mise en œuvre coordonnée et ciblée des mesures de la SNPC et formule des propositions visant à son développement ultérieur.

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

La collaboration entre la Confédération, les cantons, les milieux économiques et les hautes écoles doit être assurée à tous les échelons. Cela suppose au niveau stratégique et politique que les décisions soient dûment coordonnées entre elles, et que des échanges directs interviennent à intervalles réguliers. Une gestion commune des projets ou des portefeuilles de projets est également importante pour la bonne mise en œuvre de la SNPC par tous les acteurs, et il faut enfin prévoir des échanges réguliers au niveau opérationnel.

2.2.1 Collaboration à l'échelon politico-stratégique

La collaboration à l'échelon politico-stratégique revêt une importance majeure, notamment pour la répartition des tâches entre les cantons et la Confédération. Il est crucial pour la mise en œuvre de la SNPC de définir clairement quel niveau étatique assume quelle tâche. La Délégation Cyber du Conseil fédéral se concerte régulièrement sur de telles questions avec les conférences des gouvernements cantonaux compétents en la matière, notamment avec la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP) et, dans les domaines de l'armée et de la protection civile, avec la Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers (CG MPS). En outre, le Réseau national de sécurité (RNS) est une plateforme politique qui offre la possibilité d'approfondir davantage les thèmes de cybersécurité.
Le délégué à la cybersécurité joue également un rôle-clé dans la collaboration à l'échelon politico-stratégique. Il incarne la politique de cybersécurité de la Confédération, recueille les demandes en la matière et les soumet à la Délégation Cyber du Conseil fédéral.

2.2.2 Le comité de pilotage de la SNPC, organe chargé de la gestion commune des projets

Comme la SNPC a besoin, en tant que projet commun, du soutien de toutes les parties prenantes, cette collaboration directe n'est pas suffisante et il a fallu instituer un comité servant à la prise de décision collective. Cette fonction revient au comité de pilotage de la SNPC, où siégeront des représentants des principaux partenaires de sa mise en œuvre. Cet organe veille à la mise en œuvre coordonnée et ciblée des mesures de la SNPC, avec la participation de tous les acteurs concernés, vérifie régulièrement l'état d'avancement des travaux, adopte en cas de besoin des mesures spéciales, fixe les priorités, veille à ce que des rapports sur la SNPC soient établis à l'intention des milieux politiques et du grand public, et œuvre au développement de la stratégie. Les acteurs suivants sont représentés au comité de pilotage:

- services fédéraux concernés par les mesures de la SNPC[1];
- cantons et organes de coordination entre la Confédération et les cantons, représentés par le secrétariat général de la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP), par le Réseau national de sécurité (RNS) et par le Cyberboard des autorités de poursuite pénale;
- milieux économiques (deux représentants de différentes branches économiques pertinentes pour la SNPC);
- hautes écoles (deux représentants).

Le comité de pilotage de la SNPC est dirigé par le délégué du Conseil fédéral à la cybersécurité. Son secrétariat est assuré par le bureau Cybersécurité du délégué.

2.2.3 Coopération directe au niveau opérationnel

La coopération, pour la mise en œuvre des mesures, des diverses unités engagées sur le plan opérationnel constitue la forme de collaboration la plus directe. Elle se base sur les compétences et les participations définies dans le présent plan de mise en œuvre, mais peut être facilement adaptée et élargie. Le Centre de compétences de la Confédération pour la cybersécurité, placé sous la conduite stratégique du délégué à la cybersécurité, sert de guichet unique national pour tous les services s'occupant de cyberrisques.

[1] Les départements et la ChF disposent d'au moins un représentant chacun.

3 Bases juridiques

Le droit est la base et la limite de l'activité de l'État, selon l'art. 5 de la Constitution fédérale. Les activités des autorités décrites dans le plan de mise en œuvre doivent par conséquent reposer sur des bases juridiques. Les unités administratives mentionnées ci-après disposent – à moins que les bases légales manquantes ne soient expressément signalées – des compétences juridiques nécessaires à la mise en œuvre des mesures prévues. Autrement dit, c'est dans le cadre de leurs activités définies dans le droit en vigueur qu'elles accomplissent certaines tâches liées à la SNPC. Ces tâches ne sont pas nouvelles d'un point de vue matériel; leur champ d'application est simplement élargi aux cyberrisques. Les services compétents veilleront à ne pas outrepasser leurs compétences juridiques dans la mise en œuvre de la SNPC.
Il faudra par contre légiférer sur les tâches du Centre de compétences pour la cybersécurité, étant donné que cette unité administrative nouvellement créée ne peut s'appuyer sur le droit en vigueur et qu'elle assumera des tâches pour lesquelles il n'existe pas encore de base juridique. Les descriptions faites ci-après des mesures précisent à chaque fois où il faudra créer de nouvelles bases juridiques.

4 Contrôle de gestion stratégique et rapports

Le comité de pilotage de la SNPC examine régulièrement l'état des travaux, à l'occasion d'un contrôle de gestion stratégique, et conçoit des stratégies d'adaptation ou remanie le plan de mise en œuvre, si les facteurs déterminants pour la réalisation des objectifs s'écartent des prévisions. Les rapports du contrôle de gestion stratégique sont par ailleurs un gage de transparence pour tous les acteurs.
Le contrôle de gestion inclut une évaluation des étapes atteintes dans chaque projet, ainsi qu'une analyse de la planification ultérieure sur le plan du contenu, des délais et des ressources. Outre ces vérifications, le bureau du Centre de compétences pour la cybersécurité dresse un état des lieux des mesures de mise en œuvre dans un bref rapport semestriel au comité de pilotage de la cybersécurité, qui l'adopte et le transmet pour information à la Délégation Cyber du Conseil fédéral. Chaque année, le comité de pilotage de la SNPC soumet au Conseil fédéral un rapport sur la mise en œuvre de la SNPC. Par ailleurs, l'efficacité de la SNPC sera évaluée d'ici 2022, ce qui permettra de déterminer les autres mesures nécessaires.

5 Systématique du plan de mise en œuvre

Le plan de mise en œuvre définit les projets conçus pour chacune des 29 mesures. Il reprend la structure de la SNPC et regroupe les mesures de chaque champ d'action dans dix sous-chapitres. La figure 3 indique la systématique du plan de mise en œuvre.

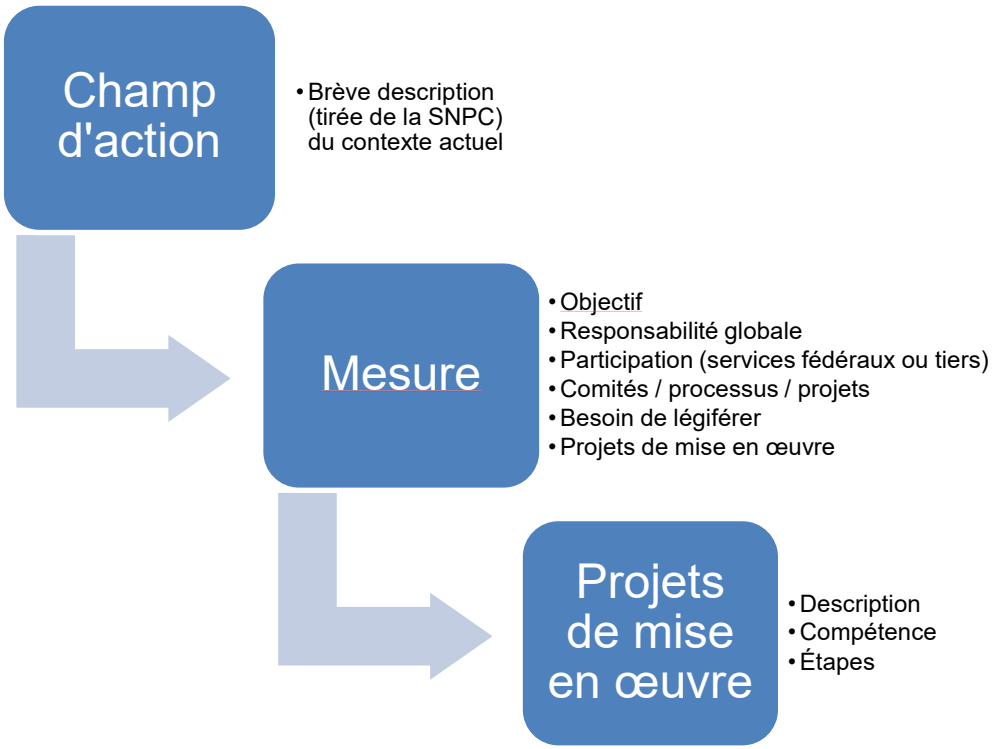


Figure 3: systématique du plan de mise en œuvre

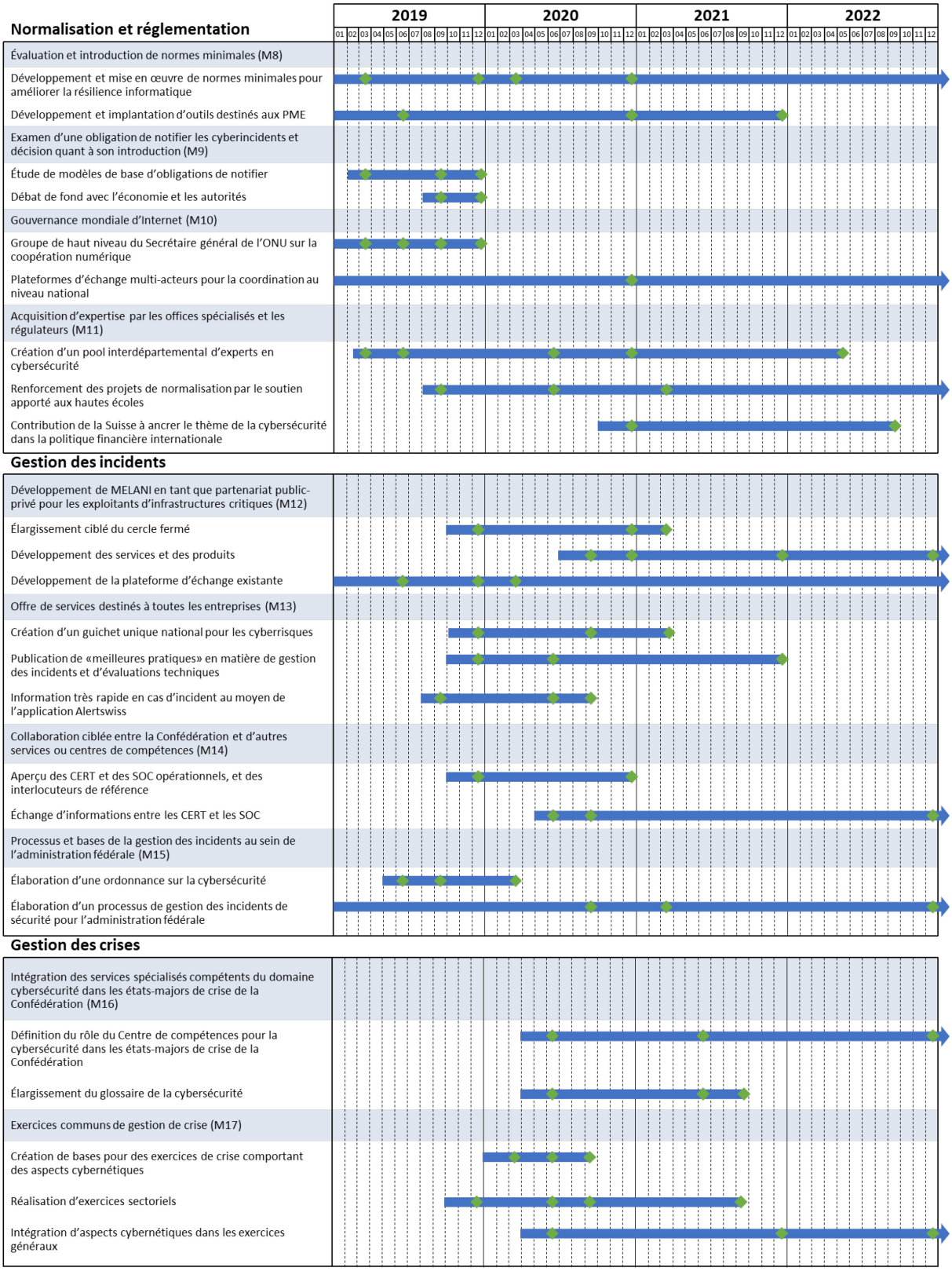
Chaque champ d'action fait l'objet d'une brève introduction rappelant le contexte des projets de mise en œuvre. À cette présentation vient s'ajouter l'extrait correspondant de la feuille de route pour la mise en œuvre.
Pour chaque mesure, un tableau synoptique aborde en introduction les points suivants:

- Objectifs: découlant directement de la SNPC, les objectifs indiquent concrètement ce que la mesure vise à atteindre.
- Responsabilité globale: service(s) compétent(s) pour la mise en œuvre de la mesure complète et devant rendre au comité de pilotage de la SNPC des comptes sur l'état des travaux.
- Participation de services fédéraux ou de tiers: organisations de l'administration fédérale ou services externes s'étant engagés, dans le cadre du plan de mise en œuvre, à collaborer aux travaux. La liste n'a pas un caractère exhaustif: d'autres services peuvent en tout temps participer à la mise en œuvre des mesures.
- Comités / processus / projets: présentation de la base déjà en place pour la mise en œuvre de la mesure; description de la situation présente.
- Nécessité de légiférer: indication, le cas échéant, des nouvelles bases légales à créer ou de celles qui doivent être adaptées (voir chapitre 3).
- Projets de mise en œuvre: aperçu des projets définis.

Ce tableau synoptique est suivi d'un tableau en trois points par projet de mise en œuvre. Après une brève description du contenu du projet, on y trouve le nom des services compétents, puis les étapes pertinentes pour la feuille de route.

6 Feuille de route pour la mise en œuvre

La feuille de route suivante énumère, pour chacun des champs d'action de la SNPC, toutes les mesures décidées, les projets de mise en œuvre correspondants et leurs calendriers respectifs.


2019
2020
2021
2022
01 02 03 04 05 06 07 08 09 10 11 12
Normalisation et réglementation
Évaluation et introduction de normes minimales (M8)
Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique
Développement et implantation d'outils destinés aux PME
Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction (M9)
Étude de modèles de base d'obligations de notifier
Débat de fond avec l'économie et les autorités
Gouvernance mondiale d'Internet (M10)
Groupe de haut niveau du Secrétaire général de l'ONU sur la coopération numérique
Plateformes d'échange multi-acteurs pour la coordination au niveau national
Acquisition d'expertise par les offices spécialisés et les régulateurs (M11)
Création d'un pool interdépartemental d'experts en cybersécurité
Renforcement des projets de normalisation par le soutien apporté aux hautes écoles
Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale
Gestion des incidents
Développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques (M12)
Élargissement ciblé du cercle fermé
Développement des services et des produits
Développement de la plateforme d'échange existante
Offre de services destinés à toutes les entreprises (M13)
Création d'un guichet unique national pour les cyberrisques
Publication de «meilleures pratiques» en matière de gestion des incidents et d'évaluations techniques
Information très rapide en cas d'incident au moyen de l'application Alertswiss
Collaboration ciblée entre la Confédération et d'autres services ou centres de compétences (M14)
Aperçu des CERT et des SOC opérationnels, et des interlocuteurs de référence
Échange d'informations entre les CERT et les SOC
Processus et bases de la gestion des incidents au sein de l'administration fédérale (M15)
Élaboration d'une ordonnance sur la cybersécurité
Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale
Gestion des crises
Intégration des services spécialisés compétents du domaine cybersécurité dans les états-majors de crise de la Confédération (M16)
Définition du rôle du Centre de compétences pour la cybersécurité dans les états-majors de crise de la Confédération
Élargissement du glossaire de la cybersécurité
Exercices communs de gestion de crise (M17)
Création de bases pour des exercices de crise comportant des aspects cybernétiques
Réalisation d'exercices sectoriels
Intégration d'aspects cybernétiques dans les exercices généraux

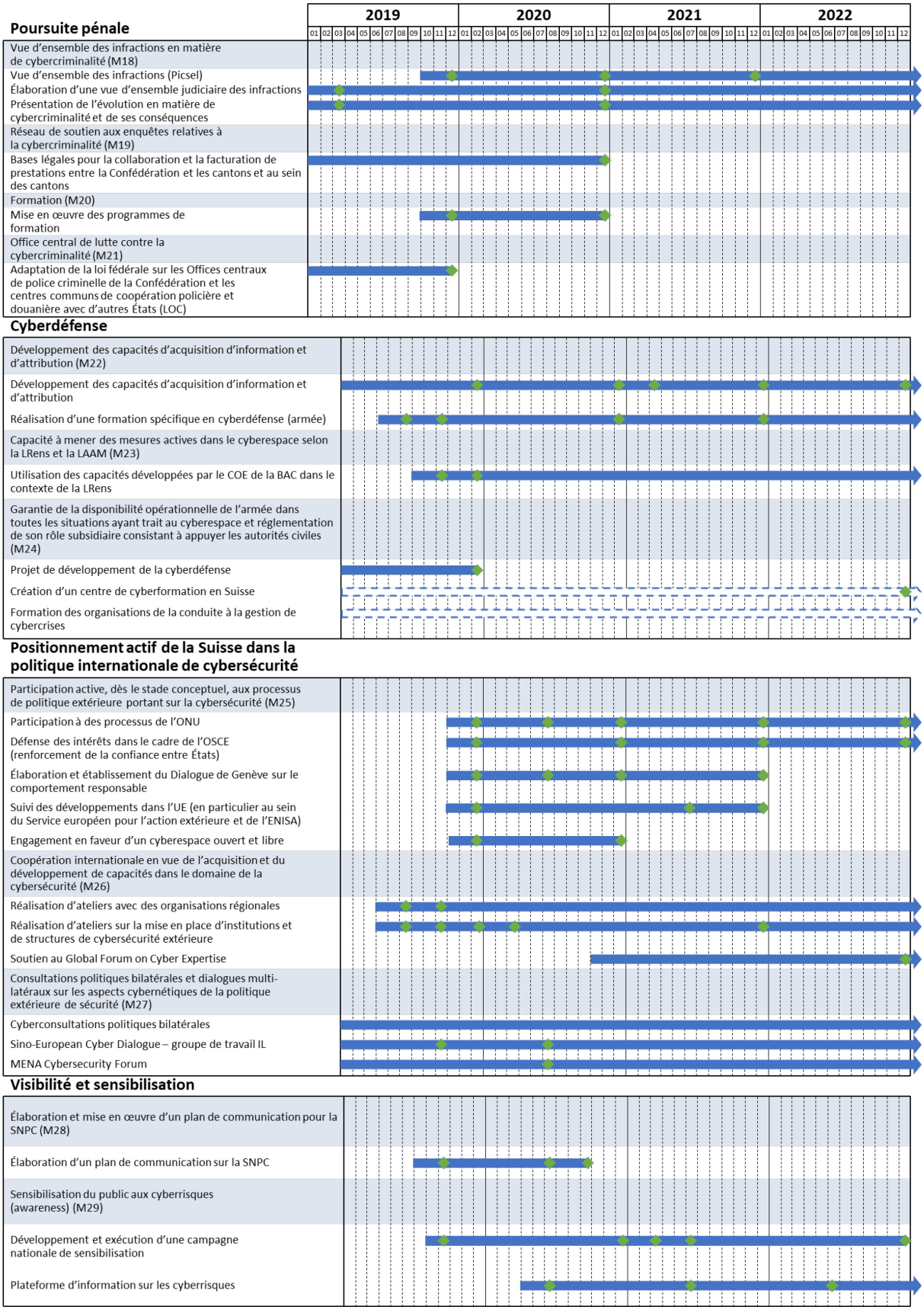


Figure 4: aperçu de la feuille de route

7 Plan de mise en œuvre

7.1 Acquisition de compétences et de connaissances

La détection aussi précoce que possible des cyberrisques ainsi que leur évaluation correcte sont deux conditions nécessaires pour limiter la menace. Les institutions de formation et de recherche doivent privilégier la transversalité dans l'acquisition des compétences correspondantes à ce savoir, dans leur transmission et leur enrichissement. La Suisse dispose à tous les niveaux d'un réseau performant d'institutions de formation et de recherche. Les milieux de la formation et de la recherche en Suisse accorderont aux cyberrisques l'importance que ceux-ci méritent, et fourniront à la société, à l'économie et aux autorités les compétences et les connaissances scientifiques nécessaires. Les travaux de recherche menés dans le domaine de la cybersécurité créent les bases utiles pour atteindre ces objectifs.

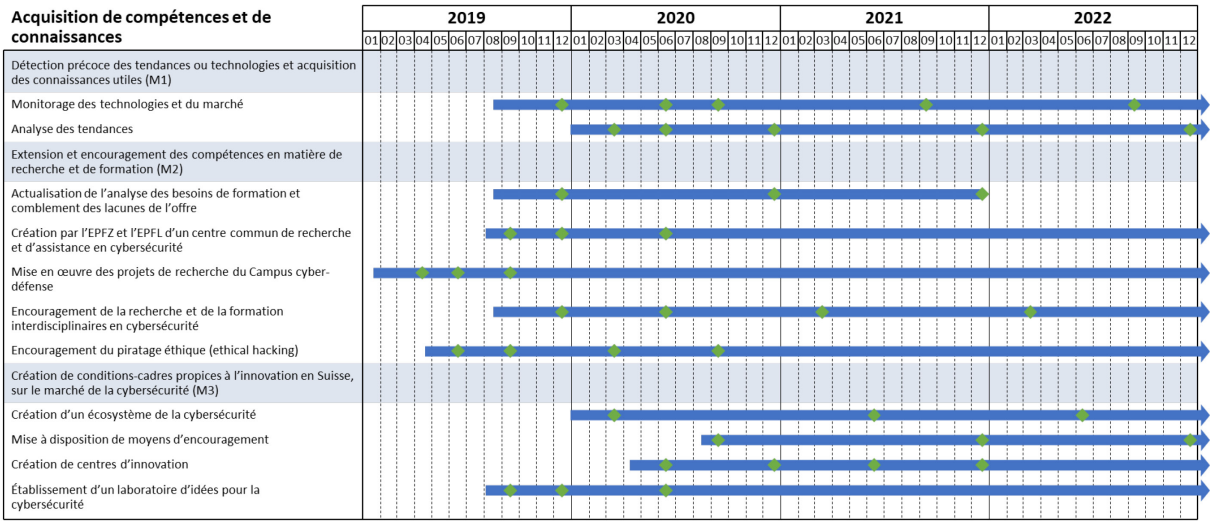


Figure 5: feuille de route «Acquisition de compétences et de connaissances»

7.1.1 Détection précoce des tendances ou technologies et acquisition des connaissances utiles (M1)

Aperçu de la mesure	
Objectif	Les tendances ou technologies informatiques seront identifiées de bonne heure, avec leurs chances et risques, et communiquées au monde scientifique, aux acteurs politiques ainsi qu'à la société.
Responsabilité globale	armasuisse S+T
Participation de services fédéraux	Centre de compétences pour la cybersécurité, SEFRI
Participation de tiers	Hautes écoles, SATW (analyse des tendances)
Comités / processus / projets	Campus cyberdéfense d'armasuisse S+T: plateforme d'anticipation à des fins de monitorage et de détection précoce des cybertechnologies

	Le Centre de compétences pour la cybersécurité doit être chargé de mener ou de confier à des tiers des analyses des tendances et des technologies dans le domaine civil, ainsi que d'en informer le public.
Projets de mise en œuvre	1. Monitorage des technologies et du marché: mise en place d'un monitorage des développements technologiques 2. Analyse des tendances: évaluation des développements technologiques, publication de rapports

Projets de mise en œuvre

1. Monitorage des technologies et du marché	
Description du projet	Mise en place d'un «radar technologique» automatisé, qui passera au crible les bases de données, les sites Internet et les répertoires afin d'identifier de bonne heure les tendances ou technologies, et d'en évaluer l'importance pour la Suisse.
Compétence	armasuisse S+T
Étapes	***T4/2019*** Définition des prestations fournies par le Campus cyberdéfense d'armasuisse S+T au Centre de compétences pour la cybersécurité, aux fins de son monitorage ***T2/2020*** Début des activités de monitorage ***T3/2020*** Première évaluation ***T3/2021*** Deuxième évaluation ***T3/2022*** Troisième évaluation

2. Analyse des tendances	
Description du projet	Évaluations qualitatives des résultats du monitorage des technologies et du marché; analyses montrant l'importance des tendances ou technologies identifiées pour la Suisse, dans l'optique de sa cybersécurité.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T1/2020*** Élaboration d'un plan relatif au public cible, aux contenus et à la diffusion des rapports ***T2/2020*** Attribution des mandats d'évaluation ***T4/2020*** Publication du premier rapport ***T4/2021*** Publication du deuxième rapport ***T4/2022*** Publication du troisième rapport

7.1.2 Extension et encouragement des compétences en matière de recherche et de formation (M2)

Aperçu de la mesure	
Objectif	Des échanges entre les milieux économiques, les hautes écoles, la Confédération et les cantons serviront à analyser en permanence les besoins dans l'offre de formation aux cyberrisques. Il s'agit de vérifier en particulier comment on pourrait mieux intégrer le thème des cyberrisques dans les filières de formation existantes tout en respectant l'autonomie des hautes écoles, et aussi comment on pourrait encourager les talents dans le domaine du piratage éthique (*ethical hacking*). L'accent est mis sur la recherche fondamentale et appliquée nécessaire à la compréhension des cyberrisques, et sur les possibilités envisageables d'encourager de façon ciblée la recherche interdisciplinaire. Le DDPS développe ses compétences et ses connaissances dans le domaine de la cyberdéfense grâce à son Campus cyberdéfense (CYD-Campus).
Responsabilité	Centre de compétences pour la cybersécurité (pour le domaine de la cybersécurité) et armasuisse S+T en collaboration avec le CYD-Campus (pour le domaine de la cyberdéfense)
Participation de services fédéraux	SEFRI
Participation de tiers	Hautes écoles, ICT Formation professionnelle Suisse, SATW (état de la recherche, identification de lacunes de la recherche), Université de Zurich, représentants des banques (analyse des besoins)
Comités / processus / projets	• Rapport: «Recherche sur les cyberrisques en Suisse: rapport d'experts 2017 sur les thèmes les plus importants pour la recherche» • Programme de recherche du Campus cyberdéfense • Plan d'action Numérisation pour le domaine FRI durant les années 2019 et 2020 • Analyse des besoins: «Offres en matière de formation des compétences en gestion des cyberrisques» (2015) • Collaboration entre la Confédération et les milieux économiques en vue de la création de nouveaux diplômes dans le cadre de l'association ICT Formation professionnelle Suisse • Projet Canvas (UE, H2020) placé sous la conduite de l'Université de Zurich, portant sur les enjeux juridiques et éthiques de la cybersécurité • Swiss Cyber Storm avec «European Cybersecurity Challenge»

Projets de mise en œuvre	1. Actualisation de l'analyse des besoins de formation et comblement des lacunes de l'offre 2. Création d'un centre de recherche et d'assistance en cybersécurité par l'EPFL et l'EPFZ: collaboration avec d'autres hautes écoles 3. Mise en œuvre des projets de recherche du Campus cyberdéfense 4. Encouragement de la recherche et de la formation interdisciplinaires en cybersécurité 5. Encouragement du piratage éthique (*ethical hacking*)

Projets de mise en œuvre

1. Actualisation de l'analyse des besoins de formation et comblement des lacunes de l'offre	
Description du projet	L'analyse des besoins d'offres de formation adaptées aux groupes cibles est mise à jour. À partir de là, identification des différentes offres proposées dans les structures de formation existantes, et indication de mesures adaptées aux besoins pour combler les lacunes de l'offre.
Compétence	Centre de compétences pour la cybersécurité, en collaboration avec les associations de branche (p. ex. ICT Formation professionnelle Suisse), EPFL
Étapes	***T4/2019*** Analyse des besoins et définition des groupes cibles ***T4/2020*** Aperçu des offres de formation ***T4/2021*** Identification des lacunes de l'offre et passage en revue des possibilités de les combler ***T4/2021*** Réalisation de mesures de formation au niveau suisse

2. Création par l'EPFZ et l'EPFL d'un centre commun de recherche et d'assistance en cybersécurité	
Description du projet	Création d'un centre de recherche et d'assistance en cybersécurité commun à l'EPFZ et à l'EPFL. Ce centre collaborera étroitement avec les services compétents de la Confédération (notamment le Centre de compétences pour la cybersécurité) et des cantons, et servira de guichet unique du domaine des EPF pour l'administration. Il contribuera également à la mise en réseau de la recherche et au transfert de savoir vers l'économie.
Compétence	EPFL et EPFZ
Étapes	***T3/2019*** Projet de centre de recherche et d'assistance ***T4/2019*** Règlement des questions du financement et du site d'implantation ***T2/2020*** Mise en service du centre de recherche, et expansion par étapes en 2021 et 2022

3. Mise en œuvre des projets de recherche du Campus cyberdéfense	
Description du projet	Le Campus cyberdéfense met en place son propre programme, avec des projets de recherche liés à la cyberdéfense. À cet effet, il collabore directement avec l'EPFZ et l'EPFL et établit ses propres sites de recherche auprès de ces hautes écoles.
Compétence	armasuisse S+T
Étapes	***T1/2019*** Mise en service du site de Thoune ***T2/2019*** Mise en service du site de l'EPFL ***T3/2019*** Mise en service du site de l'EPFZ

4. Encouragement de la recherche et de la formation interdisciplinaires en cybersécurité	
Description du projet	Les échanges sont encouragés entre les divers axes de la recherche dans le domaine des cyberrisques. Un réseau informel de chercheurs favorise la compréhension mutuelle et la réalisation de projets de recherche communs.
Compétence	armasuisse S+T et Centre de compétences pour la cybersécurité, en collaboration avec la SATW (mise en réseau des chercheurs, sensibilisation)
Étapes	***T4/2019*** Identification des principaux instituts de recherche sur les cyberrisques des hautes écoles suisses ***T2/2020*** Évaluation des besoins des instituts identifiés ***T1/2021*** Définition de la forme et de la teneur de l'échange régulier entre les participants ***T1/2022*** Concrétisation de l'échange

5. Encouragement du piratage éthique (*ethical hacking*)	
Description du projet	Le soutien et l'encouragement de divers événements actuels liés au piratage éthique visent à renforcer l'acquisition et l'échange de connaissances dans ce domaine et à agrandir le réseau existant. L'organisation d'un Swiss Hacking Contest permettra aux participants de se mesurer dans une compétition et de présenter au grand public le thème du piratage éthique. En outre, il sera ainsi possible d'identifier et d'encourager les jeunes talents dans ce secteur.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2019*** Identification des événements existants dans le domaine du piratage éthique ***T3/2019*** Conception des instruments d'encouragement: demande si nécessaire de moyens financiers ***T1/2020*** Obtention des fonds nécessaires ***T3/2020*** Réalisation du Swiss Hacking Contest

7.1.3 Création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité (M3)

Aperçu de la mesure	
Objectif	La Suisse doit devenir un site d'implantation attrayant pour les entreprises spécialisées dans la cybersécurité. L'intensification des échanges entre l'économie et la recherche favorisera l'innovation et l'émergence de start-up.
Responsabilité	Centre de compétences pour la cybersécurité
Participation de services fédéraux	armasuisse S+T, Innosuisse
Participation de tiers	hautes écoles, associations économiques, ICTswitzerland
Comités / processus / projets	• Réseau de compétences du Campus cyberdéfense • Instruments d'encouragement d'Innosuisse • Centres d'innovation existants
Nécessité de légiférer	Il faut déterminer quelles tâches la Confédération peut assumer dans le cadre de la création d'un «écosystème de la cybersécurité» en s'appuyant sur les bases légales existantes, ou s'il est nécessaire de légiférer.
Projets de mise en œuvre	1. Création d'un écosystème de la cybersécurité 2. Mise à disposition de moyens d'encouragement 3. Création de centres d'innovation 4. Établissement d'un laboratoire d'idées pour la cybersécurité

Projets de mise en œuvre

1. Création d'un écosystème de la cybersécurité	
Description du projet	Le Centre de compétences pour la cybersécurité fait office d'intermédiaire entre les milieux économiques, les hautes écoles, les autorités et les centres d'innovation existants, afin de promouvoir un écosystème de la cybersécurité novateur en Suisse. Il collabore à cet effet avec le Campus cyberdéfense d'armasuisse S+T, qui représente le pôle de compétence pour la collaboration entre les hautes écoles et les milieux économiques dans le domaine de la cyberdéfense.
Compétence	Centre de compétences pour la cybersécurité, conjointement avec le Campus cyberdéfense d'armasuisse S+T et ICTswitzerland
Étapes	***T1/2020*** Planification commune, par le centre de compétences et le Campus cyberdéfense, des mesures d'échange avec les milieux économiques et les hautes écoles ***T2/2021*** Réalisation de premières mesures destinées à encourager les échanges ***T2/2022*** Bon établissement de l'écosystème de la cybersécurité

2. Mise à disposition de moyens d'encouragement	
Description du projet	Des moyens d'encouragement destinés aux projets d'innovation des hautes écoles, des associations et des entreprises dans le domaine de la cybersécurité sont identifiés et indiqués comme tels. Il s'agit de vérifier quels instruments d'encouragement (p. ex. réseaux thématiques nationaux, projets d'innovation R&D, programme d'encouragement ad hoc) sont les plus efficaces pour promouvoir l'innovation dans le domaine de la cybersécurité.
Compétence	Centre de compétences pour la cybersécurité, conjointement avec Innosuisse
Étapes	***T3/2020*** Fin de l'analyse des possibilités d'encouragement; les instruments utiles ont été définis ***T4/2021*** Conception des instruments d'encouragement ***T4/2022*** Mise à disposition des instruments d'encouragement

3. Création de centres d'innovation	
Description du projet	Analyse des possibilités de former autour du Centre de compétences pour la cybersécurité un pôle de cybersécurité (incluant le centre de recherche de l'EPFZ, avec la participation de l'écosystème de la cybersécurité et du Campus cyberdéfense, ainsi que du réseau de recherche). L'innovation en matière de cybersécurité sera spécialement encouragée dans ce réseau, dans les centres d'innovation régionaux existants ou spécialement créés.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2020*** Proposition sur la création et le financement d'un pôle de cybersécurité national ***T4/2020*** Décision sur la création d'un pôle de cybersécurité national ***T2/2021*** Plan pour la création de centres régionaux d'innovation en cybersécurité sur différents sites ***T4/2021*** Financement des centres régionaux d'innovation en cybersécurité

4. Établissement d'un laboratoire d'idées pour la cybersécurité	
Description du projet	Le centre de recherche et d'assistance commun aux deux EPF se dote de capacités d'analyse et d'anticipation dans le domaine de la cybersécurité. Grâce à ses compétences en technologie et en bonne gouvernance, il aide la Suisse à créer un cadre attrayant pour les entreprises technologiques.
Compétence	EPFL et EPFZ

Étapes	***T3/2019*** Conception du centre de recherche et d'assistance ***T4/2019*** Règlement du financement et choix du site ***T2/2020*** Inauguration du centre de recherche avec son laboratoire d'idées; consolidation par étapes en 2021 et en 2022

7.2 Situation de la menace

Une vue d'ensemble des cybermenaces actuelles est essentielle, dans l'optique de la protection contre les cyberrisques. Elle constitue la base en vue du choix et du classement par ordre de priorités des mesures préventives et réactives, et elle est indispensable pour pouvoir prendre les bonnes décisions en cas d'incident ou en situation de crise. Pour protéger la Suisse face aux cyberrisques, il faut continuer de dresser un tableau d'ensemble de la situation. Les capacités actuelles doivent être augmentées face à l'aggravation des menaces, et les échanges d'informations avec les milieux économiques et les cantons être encore renforcés. En outre, les découvertes faites sur la situation de la menace ne seront plus réservées aux autorités et aux exploitants d'infrastructures critiques, mais seront également mises à la disposition, sous une forme adéquate, d'autres entreprises suisses ainsi que de la population.

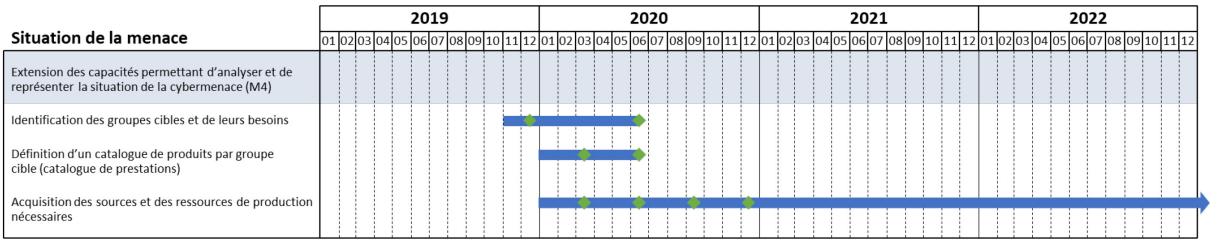


Figure 6: feuille de route «Situation de la menace»

7.2.1 Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace (M4)

Aperçu de la mesure	
Objectif	Pour se protéger face aux cyberrisques, la Suisse dispose d'un tableau d'ensemble de la situation. • La situation de la menace est prise en compte conformément aux besoins des destinataires, qui se situent tant au niveau technique et opérationnel qu'au niveau stratégique et politique. • Une extension des capacités disponibles garantit le traitement et l'inventaire systématiques et durables des cyberincidents. • Les renseignements en sources ouvertes dans le cyberespace (*open source intelligence*, OSINT) font l'objet d'une utilisation systématique et livrent les informations nécessaires. • Les évaluations de la situation faites par les autorités de poursuite pénale, par les experts en cybersécurité, par l'armée et le service des renseignements seront dûment prises en compte dans l'appréciation des menaces. L'échange d'informations avec les milieux économiques et les cantons sera encore renforcé. En outre, les découvertes faites sur la situation de la menace ne seront plus réservées aux autorités et aux exploitants d'infrastructures critiques, mais seront également mises à la disposition, sous une forme adéquate, des entreprises suisses ainsi que de la population.
Responsabilité	SRC (OIC MELANI)

Participation de services fédéraux	fedpol, MPC, Centre de compétences pour la cybersécurité (GovCert), BAC (MilCERT, CYD), SRC (Cyber SRC, CFS)
Autres participants	Cantons (surtout par l'intermédiaire du Cyberboard), partenaires issus des milieux économiques (cercle fermé de MELANI, SCE), des milieux scientifiques (hautes écoles) et des cantons
Comités / processus / projets	• Les processus servant à l'établissement de la situation de la menace, des processus organisationnels, du rythme de conduite ainsi que des responsabilités respectives de MELANI-UPIC/GovCERT, de l'OIC MELANI et de Cyber SRC ont été consignés dans le cadre de la SNPC 1, et le cas échéant complétés, testés et mis en œuvre. • Collaboration avec des partenaires nationaux et internationaux.
Projets de mise en œuvre	1. Identification des groupes cibles et de leurs besoins 2. Définition d'un catalogue de produits par groupe cible 3. Identification/acquisition des sources et production

Projets de mise en œuvre

1. Identification des groupes cibles et de leurs besoins	
Description du projet	Identification des besoins déjà figurés (tableaux de la situation disponibles) et définition de groupes cibles. Analyse de leurs besoins face aux cybermenaces, en termes de contenus et de mode de transmission (degré d'actualité, à court et à moyen terme, niveaux opérationnel ou stratégique).
Compétence	SRC (OIC MELANI) en collaboration avec des représentants des milieux économiques, de la société, des cantons et de la Confédération (autorités de poursuite pénale, armée, OFAE/OFPP)
Étapes	***T4/2019*** Identification des groupes cibles élargis et de leurs besoins ***T2/2020*** Identification des canaux de communication des divers groupes cibles (guichet unique national, Alertswiss, radar de la situation, rapports trimestriels, bulletin du groupe Cybersécurité, etc.)

2. Définition d'un catalogue de produits par groupe cible (catalogue de prestations)	
Description du projet	Le format des produits destinés aux divers groupes cibles, leur fréquence de parution et leurs contenus ont été définis. Il s'agit encore de délimiter dans ce contexte le rôle de la Confédération et celui des milieux économiques (fournisseurs de services commerciaux en rapport avec la menace), selon le principe de subsidiarité.

Compétence	SRC (OIC MELANI), en collaboration avec des représentants des milieux économiques, de la société, des cantons (autorités de poursuite pénale) et de la Confédération (autorités de poursuite pénale, armée, OFAE/OFPP)
Étapes	***T1/2020*** Délimitation des compétences respectives de la Confédération et des milieux économiques ***T2/2020*** Catalogue de prestations défini par groupe cible

3. Acquisition des sources et des ressources de production nécessaires	
Description du projet	Identification des sources supplémentaires requises pour fournir les prestations définies, et création des nouveaux réseaux nécessaires avec les milieux économiques et avec d'autres organismes internationaux. Création de ressources analytiques servant à vérifier, hiérarchiser et évaluer les informations disponibles; assistance technique pour structurer et évaluer l'afflux d'informations.
Compétence	SRC (OIC MELANI), en collaboration avec le Centre de compétences pour la cybersécurité
Étapes	***T1/2020*** Liste des sources supplémentaires nécessaires ***T2/2020*** Estimation et allocation des ressources requises pour intensifier les relations internationales ***T2/2020*** Plan visant à systématiser l'approvisionnement interne ***T3/2020*** Projet de mise en place du soutien technique ***T4/2020*** Estimation et allocation des ressources requises pour l'acquisition des sources et pour la systématisation de l'approvisionnement et de la production

7.3 Gestion de la résilience

Les mesures visant à réduire les vulnérabilités informatiques des infrastructures critiques revêtent une grande importance dans l'optique de la protection de la Suisse contre les cyberrisques. Elles ne se limitent pas à renforcer sa défense, mais incluent des mesures propres à atténuer les dommages et à réduire les interruptions en cas d'incident. Il incombe à chaque organisation ou entreprise de mettre en œuvre les mesures destinées à améliorer sa résilience informatique. La Confédération joue un rôle actif dans la définition de telles mesures pour les secteurs-clés de notre société, et en surveille la mise en œuvre. De leur côté, la Confédération et les cantons se doivent d'adopter les mesures nécessaires à la protection de leurs propres infrastructures informatiques critiques.
Les mesures identifiées pour améliorer la résilience informatique des sous-secteurs et des administrations seront mises en œuvre, harmonisées et ajustées, sur la base d'analyses périodiquement actualisées des risques et des vulnérabilités.

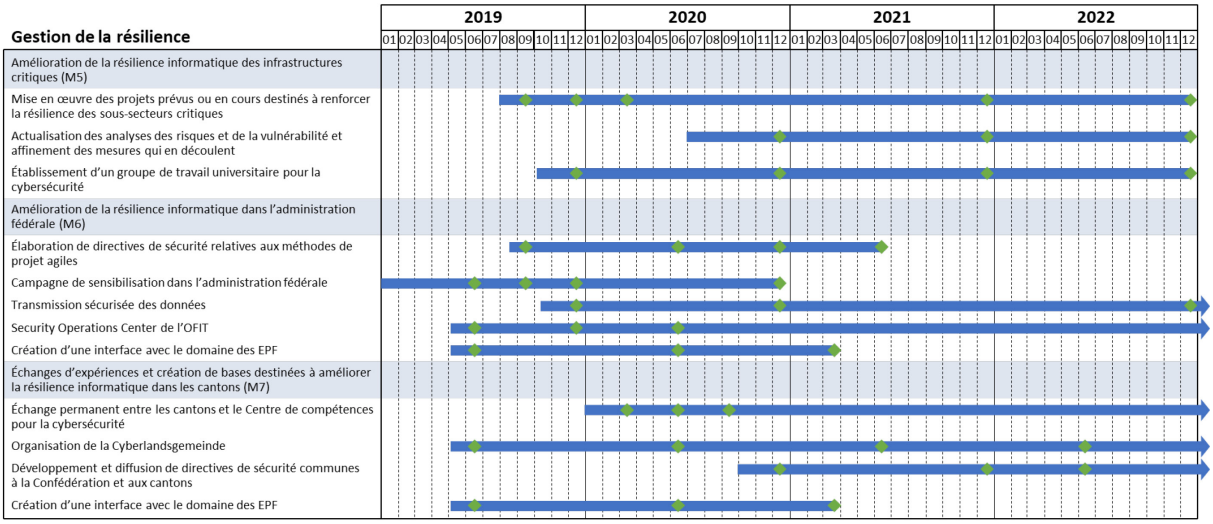


Figure 7: feuille de route «Gestion de la résilience»

7.3.1 Amélioration de la résilience informatique des infrastructures critiques (M5)

Aperçu de la mesure	
Objectif	Il s'agit surtout ici de mettre en œuvre des mesures destinées à améliorer la résilience informatique des sous-secteurs, avec la participation des autorités de régulation et des offices spécialisés. On se basera sur les analyses disponibles des risques et des vulnérabilités, et sur les mesures proposées à partir de là. En plus de mettre en œuvre les mesures identifiées, il faudra régulièrement actualiser les analyses et les mesures et, le cas échéant, les adapter aux découvertes ou développements récents.
Responsabilité	OFPP, en collaboration avec les offices spécialisés dans les secteurs réglementés
Participation de services fédéraux	Offices spécialisés (OFCOM, OFSP, OFT, OFAC, OFEN), OFAE, Centre de compétences pour la cybersécurité
Autres participants	Régulateurs, associations de branche, exploitants d'infrastructures critiques

Comités / processus / projets	• Analyses des risques et de la vulnérabilité des sous-secteurs critiques de la SNPC 2012 – 2017 • Mise en œuvre de la stratégie nationale de protection des infrastructures critiques 2018 – 2022 • (Actualisation de l')analyse des risques de catastrophes et de situations d'urgence en Suisse de 2015 • Collaboration entre les milieux économiques et les autorités, dans le cadre de l'approvisionnement économique • Prescriptions spécifiques aux secteurs
Projets de mise en œuvre	1. Mise en œuvre des projets prévus ou en cours destinés à renforcer la résilience des sous-secteurs critiques 2. Actualisation des analyses des risques et de la vulnérabilité 3. Établissement d'un groupe de travail universitaire pour la cybersécurité

Projets de mise en œuvre

1. Mise en œuvre des projets prévus ou en cours destinés à renforcer la résilience des sous-secteurs critiques	
Description du projet	Mises en œuvre dans les sous-secteurs critiques des mesures prévues dans le cadre de la SNPC 2012 – 2017 et décrites dans les rapports qui en résultent.
Compétence	Coordination, accompagnement et soutien des travaux par l'OFPP dans les secteurs réglementés, en étroite collaboration avec les offices spécialisés. La mise en œuvre des mesures incombe aux associations économiques, aux offices spécialisés et aux entreprises.
Étapes	***T3/2019*** État des lieux des projets déjà réalisés ou encore à réaliser selon les rapports sur les mesures ***T4/2019*** Clarification des responsabilités pour la mise en œuvre ***T1/2020*** Feuille de route/planification des mesures actuelles ou à venir ***T4/2021*** Coordination et information, avec les responsables de la mise en œuvre, sur l'état des travaux et sur les prochaines étapes prévues ***T4/2022*** Aperçu et rapport d'étape sur les mesures mises en œuvre

2. Actualisation des analyses des risques et de la vulnérabilité et affinement des mesures qui en découlent	
Description du projet	Actualisation périodique et affinement des travaux portant sur la cyberrésilience, analyses des risques et de la vulnérabilité avec propositions de mesures dans les sous-secteurs (branches) critiques

Compétence	OFPP, en collaboration avec l'OFAE et les offices spécialisés, les associations économiques et les entreprises / organisations des sous-secteurs critiques
Étapes	***T4/2020*** Contrôle et actualisation du premier tiers des analyses des risques et de la vulnérabilité, examen et ajustement le cas échéant des mesures correspondantes ***T4/2021*** Contrôle et actualisation du deuxième tiers des analyses des risques et de la vulnérabilité, examen et ajustement le cas échéant des mesures correspondantes ***T4/2022*** Contrôle et actualisation du troisième tiers des analyses des risques et de la vulnérabilité, examen et ajustement le cas échéant des mesures correspondantes

3. Établissement d'un groupe de travail universitaire pour la cybersécurité	
Description du projet	Établissement d'un groupe de travail universitaire pour la cybersécurité des infrastructures critiques, se concentrant sur l'analyse des risques à long terme inhérents aux nouvelles technologies.
Compétence	EPFL et EPFZ
Étapes	***T4/2019*** Bilan des projets et des groupes actifs ***T4/2020*** Institutionnalisation du groupe de travail ***T4/2021*** Coordination et analyse des risques ***T4/2022*** Rapport sur les mesures et mise en œuvre

7.3.2 Amélioration de la résilience informatique dans l'administration fédérale (M6)

Aperçu de la mesure	
Objectif	L'amélioration de la résilience informatique dans l'administration fédérale découle de la mise en œuvre et de l'actualisation des directives et plans, dans le cadre d'une gestion de la sécurité de l'information, de la sensibilisation du personnel de l'administration fédérale, ainsi que de mesures techniques destinées au transfert sécurisé des données.
Responsabilité	Centre de compétences pour la cybersécurité
Participation	Fournisseurs de prestations informatiques de la Confédération, délégués à la sécurité informatique des départements, Protection des informations et des objets (PIO), Gestion des risques au sein de la Confédération
Comités / processus / projets	Comité pour la sécurité informatique de la Confédération

Projets de mise en œuvre	1. Élaboration de directives de sécurité relatives aux méthodes de projet agiles 2. Campagne de sensibilisation dans l'administration fédérale 3. Transmission sécurisée des données grâce aux nouvelles technologies: phase de test avec SCION[2] 4. Security Operations Center de l'OFIT 5. Création d'une interface avec le domaine des EPF

Projets de mise en œuvre

1. Élaboration de directives de sécurité relatives aux méthodes de projet agiles	
Description du projet	Les méthodes de projet (p. ex. HERMES) doivent d'emblée prendre en compte l'aspect de la sécurité (*security by design*). Il convient donc de réexaminer les directives de sécurité, et de les adapter de façon à ce que les méthodes de projet agiles s'y conforment de bonne heure.
Compétence	Centre de compétences pour la cybersécurité en accord avec le groupe spécialisé HERMES d'eCH
Étapes	***T3/2019*** Analyse des tâches liées à la sécurité prescrites dans les méthodes de projet, avec leurs résultats ***T2/2020*** Identification et description de tâches supplémentaires avec leurs résultats, et des compléments ponctuels à apporter aux directives existantes ***T4/2020*** Consultation interne au groupe spécialisé sur les projets de modifications concernant la sécurité ***T2/2021*** Modification de la norme relative aux projets

2. Campagne de sensibilisation dans l'administration fédérale	
Description du projet	Conception et réalisation, pour le personnel de l'administration fédérale, d'une campagne de sensibilisation sur la cybersécurité adaptée à ses destinataires
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T4/2018*** Première ébauche de la campagne de sensibilisation interne à la Confédération portant sur la sécurité informatique ***T2/2019*** Début de la campagne ***T3/2019*** Coordination avec d'autres acteurs pour une transformation en campagne nationale (voir M29 «Sensibilisation du public aux cyberrisques») ***T4/2019*** Élaboration d'un nouveau plan de mesures pour les années 2021/2022 ***T4/2020*** Rapport sur le déroulement et l'efficacité de la campagne de sensibilisation

[2] Scalability, Control, and Isolation on Next-Generation Networks

3. Transmission sécurisée des données	
Description du projet	L'EPFZ a développé, avec l'architecture SCION[3], une technologie extrêmement sûre pour les réseaux de communication. Des projets pilotes seront conçus et réalisés sur cette base. Les résultats de la phase pilote seront documentés dans un rapport d'évaluation. Les enseignements tirés à cette occasion devront également servir à mettre à disposition une infrastructure résiliente pour les tâches critiques (M5 et M7).
Compétence	EPFZ et OFIT, en accord avec les autres FP (BAC surtout)
Étapes	***T4/2019*** Déclaration d'intention des services intéressés à devenir utilisateurs pilotes ***T4/2020*** Conception et mise en service des applications pilotes ***T4/2022*** Rapport d'évaluation sur l'exploitation pilote

4. Security Operations Center de l'OFIT	
Description du projet	La gestion des incidents de sécurité gagnera en efficacité après la création d'un Security Operations Center (SOC) à l'OFIT et son passage en phase opérationnelle. Les tâches répétitives seront déléguées à des profils de postes moins coûteux (première ligne de défense). Le monitorage des incidents affectant la sécurité des systèmes sera étendu, et le traitement des incidents définis comme normaux sera délégué au SOC. Celui-ci sera aussi chargé de traiter les propositions de changement comportant des risques (p. ex. ouvertures de ports dans le pare-feu). Ces mesures visent en outre à optimiser les processus de gestion des incidents et le monitorage du système. Les spécialistes du CSIRT OFIT pourront ainsi davantage se consacrer aux analyses utiles.
Compétence	OFIT
Étapes	***T2/2019*** Projet et plan de mise en œuvre ***T4/2019*** Fin des travaux ***T2/2020*** Maturité opérationnelle

[3] SCION: https://www.scion-architecture.net/

5. Création d'une interface avec le domaine des EPF	
Description du projet	Le centre de recherche et d'assistance commun aux deux EPF constitue une interface unique idéale pour coordonner les interactions des cantons avec les universités dans le domaine de la cybersécurité, pour surveiller l'attitude de la Confédération et des cantons en cas d'évolution disruptive et les aider à s'adapter à la nouvelle situation.
Compétence	EPFL et EPFZ
Étapes	***T2/2019*** Coordination avec le délégué du Conseil fédéral à la cybersécurité ***T2/2020*** Mise en œuvre des mesures concrètes ***T1/2021*** Coordination commune

7.3.3 Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons (M7)

Aperçu de la mesure	
Objectif	Un réseau ad hoc est créé (ou les réseaux existants sont utilisés) pour les échanges d'expériences et pour l'élaboration de bases communes destinées à renforcer la résilience informatique dans les cantons. Le but est ici que les autorités se soutiennent mutuellement et que les efforts soient coordonnés entre la Confédération et les cantons.
Responsabilité	Centre de compétences pour la cybersécurité, RNS
Participation	Conférence suisse sur l'informatique (CSI), Conférence suisse des Chanceliers d'État, CCPCS et autres conférences spécialisées des cantons
Comités / processus / projets	• Cyberlandsgemeinde du RNS (= conférence des cantons sur la cybersécurité) -> plateforme opérationnelle du RNS • Groupe spécialisé Cybersécurité du RNS • Matériel de formation de la CCPCS sur la cybersécurité
Projets de mise en œuvre	1. Échange permanent entre les cantons et le Centre de compétences pour la cybersécurité 2. Organisation annuelle de la Cyberlandsgemeinde 3. Développement et diffusion de directives de sécurité communes à la Confédération et aux cantons 4. Création d'une interface avec le domaine des EPF

Projets de mise en œuvre

1. Échange permanent entre les cantons et le Centre de compétences pour la cybersécurité	
Description du projet	Le personnel cantonal doit avoir la possibilité de travailler au Centre de compétences pour la cybersécurité, à des fins d'échange d'informations et d'expériences dans la lutte contre les cybermenaces (transfert de connaissances).

Compétence	Centre de compétences pour la cybersécurité
Étapes	***T1/2020*** Évaluation des besoins liés au poste de travail (catalogue des exigences) ***T2/2020*** Initialisation et demande pour l'infrastructure de bureau ***T3/2020*** Identification et définition, avec le RNS et la CCDJP, des formes et canaux de communication

2. Organisation de la Cyberlandsgemeinde	
Description du projet	Une conférence sur les cyberrisques est organisée chaque année pour les cantons. Elle sert à des échanges d'informations entre cantons, ainsi qu'entre les cantons et la Confédération.
Compétence	RNS
Étapes	***T2/2019*** Organisation d'une Landsgemeinde ***T2/2020*** Organisation d'une Landsgemeinde ***T2/2021*** Organisation d'une Landsgemeinde ***T2/2022*** Organisation d'une Landsgemeinde

3. Développement et diffusion de directives de sécurité communes à la Confédération et aux cantons	
Description du projet	Développement et diffusion parmi les autorités suisses d'une norme minimale dans le domaine de la cybersécurité
Compétence	Centre de compétences pour la cybersécurité, OFAE, représentants cantonaux (CSI, RNS)
Étapes	***T4/2020*** Évaluation des besoins (catalogue d'exigences) ***T4/2021*** Adoption d'une norme commune ***T2/2022*** Fixation par les cantons et la Confédération des modalités du suivi et d'un développement éventuel de cette norme

4. Création d'une interface avec le domaine des EPF	
Description du projet	Le centre de recherche et d'assistance commun aux deux EPF constitue une interface unique idéale pour coordonner les interactions des cantons avec les universités dans le domaine de la cybersécurité, pour surveiller l'attitude de la Confédération et des cantons en cas d'évolution disruptive et les aider à s'adapter à la nouvelle situation.
Compétence	EPFL et EPFZ
Étapes	***T2/2019*** Coordination avec le RNS ***T2/2020*** Mise en œuvre des mesures concrètes ***T1/2021*** Coordination commune

7.4 Normalisation et réglementation

Les normes ou réglementations informatiques représentent d'importants instruments de protection contre les cyberrisques. Les exigences minimales pour les mesures de protection à adopter renforcent la prévention et les prescriptions relatives à la gestion des incidents (p. ex. obligation de notifier) contribuent à améliorer la réaction. La normalisation et la réglementation sont également importantes dans le contexte international, car elles contribuent à améliorer la transparence de la société du numérique à l'ère de la mondialisation et instaurent un climat de confiance. Dans ce champ d'action, il s'agit de tenir compte des différences considérables entre les secteurs économiques ainsi qu'entre les entreprises de tailles différentes. Le contexte international doit être pris en considération dans tous les cas. Comme le cyberespace ignore les frontières, les normes et les réglementations doivent si possible être compatibles à l'échelle internationale. Des normes minimales vérifiables contribuent à la sécurité ainsi qu'à la confiance accordée à l'économie et à la société numériques; il importe de les évaluer avec le concours du secteur privé, et de les appliquer là où cela est judicieux. De même, il convient de vérifier s'il y a lieu d'introduire une obligation de notifier les cyberincidents, et quelles en seraient les modalités. Les mesures tiendront compte du contexte international, qui les influence de manière essentielle et dont l'évolution doit ainsi être suivie de près.

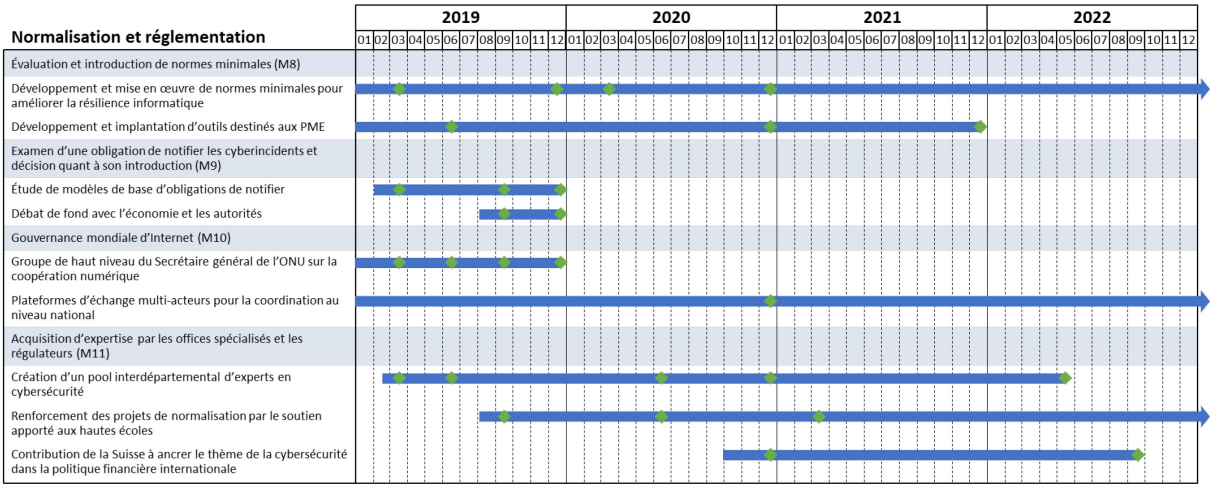


Figure 8: feuille de route «normalisation et réglementation»

7.4.1 Évaluation et introduction de normes minimales (M8)

Aperçu de la mesure	
Objectif	À partir des analyses des risques et des vulnérabilités effectuées, des normes minimales seront élaborées et introduites, dans le cadre d'une étroite collaboration entre les autorités spécialisées, le secteur privé et les associations de branche. Les nouvelles normes minimales se fonderont sur les normes existantes (p. ex. norme minimale pour les TIC mise au point par l'approvisionnement économique du pays [AEP]). Les autorités compétentes vérifieront pour quelles organisations ou activités les normes doivent être contraignantes.
Responsabilité	OFAE

Participation de services fédéraux	Centre de compétences pour la cybersécurité, OFPP, offices spécialisés (OFPP, OFSP, OFCOM, OFT, OFAC, OFEN)
Participation de tiers	Régulateurs, associations de branche et associations actives dans la cybersécurité (p. ex. ICTswitzerland), Association suisse pour le label de cyber-sécurité, ASA), SATW (expertise, sensibilisation) et hautes écoles
Comités / processus / projets	• Analyses des risques et des vulnérabilités remontant à la SNPC 2012 – 2017 • Rapport final du groupe d'experts Avenir du traitement et de la sécurité des données • Collaboration instaurée entre les milieux économiques et la Confédération, dans le cadre de l'AEP • Collaboration sectorielle en place
Nécessité de légiférer	Il faut déterminer dans les secteurs s'il est nécessaire de légiférer pour introduire des normes minimales de cybersécurité et, si oui, dans quelle mesure.
Projets de mise en œuvre	1. Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique 2. Développement et implantation d'outils destinés aux PME

Projets de mise en œuvre

1. Développement et mise en œuvre de normes minimales pour améliorer la résilience informatique	
Description du projet	Afin d'améliorer sa résilience informatique, la Suisse dispose déjà d'une norme minimale basée sur un standard international, le cadre du NIST, et d'outils pour sa mise en œuvre. Il s'agit de formuler et d'introduire, en collaboration avec les associations de branche, des normes sectorielles à partir de la norme minimale définie par l'AEP. Les secteurs qui disposent de leur propre réglementation en matière de sécurité informatique se conformeront à celle-ci.
Compétence	OFAE, en collaboration avec les autorités compétentes, les offices spécialisés (OFSP, OFCOM, OFT, OFAC, OFEN) et les associations de branche; participation des offices spécialisés et des régulateurs compétents pour les sous-secteurs, entreprises/organisations critiques, et des hautes écoles
Étapes	***T2/2018*** Publication de la norme minimale et d'un outil d'évaluation ***T2/2018*** Norme minimale Manuel Protection de base de l'Association des entreprises électriques suisses (AES) ***T1/2019*** Approvisionnement en eau potable ***T1/2019*** Approvisionnement en denrées alimentaires ***T4/2019*** Approvisionnement en gaz naturel ***T1/2020*** Transports ***T4/2020*** Télécommunications

2. Développement et implantation d'outils destinés aux PME	
Description du projet	La Confédération met au point avec les milieux économiques et les associations de branche, pour soutenir les PME, des outils permettant aux entreprises de voir facilement et rapidement si elles sont au point en matière de cybersécurité, d'évaluer les cyberrisques encourus et de savoir avec quelles mesures elles pourraient améliorer leur sécurité. Des analyses montreront encore s'il y a lieu de créer ou de soutenir des labels ou normes spécifiques, et qui s'en chargera le cas échéant.
Compétence	Centre de compétences pour la cybersécurité, OFAE, associations économiques
Étapes	***T3/2018*** Publication d'un test rapide Cybersécurité pour PME (SATW) ***T2/2019*** Analyse du besoin d'autres outils spécifiques aux PME (outils techniques, labels, guides et instructions) ***T4/2020*** Fin de l'examen en vue de l'introduction éventuelle de labels et de normes ***T4/2021*** Analyse des outils créés, et le cas échéant conception d'instruments supplémentaires

7.4.2 Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction (M9)

Aperçu de la mesure	
Objectif	Examiner l'introduction d'une obligation de notifier les cyberincidents, et statuer sur sa mise en place. Plusieurs questions seront examinées au préalable: à qui s'appliquerait une telle obligation, quels seraient les incidents concernés, à qui devrait-on les notifier, et une obligation de notifier permettrait-elle d'améliorer notablement l'état des lieux? On élaborera alors différentes solutions pour la mise en œuvre de l'obligation de notifier dans les différents secteurs, en montrant les bases légales à prévoir. Ces travaux seront accomplis avec la participation des autorités compétentes, des milieux économiques, des hautes écoles et des cantons. C'est sur eux que sera fondée la décision d'introduire une obligation de notifier.
Responsabilité	Centre de compétences pour la cybersécurité
Participation de services fédéraux	OFPP, offices spécialisés (OFSP, OFCOM, OFT, OFAC, OFEN), fedpol
Participation de tiers	Associations économiques (ASA, p. ex.), cantons, FINMA (obligation de notifier), hautes écoles, ICTswitzerland

Comités / processus / projets	Il existe des obligations de notifier sectorielles (dans les télécommunications, dans le nucléaire ou dans l'aviation, p. ex.). Dans les télécommunications, il faudra réfléchir au développement des obligations existantes.
Nécessité de légiférer	Les bases légales d'une telle introduction devront être remaniées ou élaborées si elles n'existent pas déjà (loi sur les télécommunications, p. ex.).
Projets de mise en œuvre	1. Étude de modèles de base d'obligations de notifier 2. Débat de fond avec l'économie et les autorités

Projets de mise en œuvre

1. Étude de modèles de base d'obligations de notifier	
Description du projet	Élaboration de bases par la saisie d'obligations de notifier existantes, et élaboration de modèles de base d'obligations de notifier les (cyber)incidents de sécurité
Compétence	Centre de compétences pour la cybersécurité, OFPP, participation des offices spécialisés, de la FINMA et ICTswitzerland
Étapes	***T1/2019*** Appel d'offres pour l'étude de base «Examen d'une obligation de notifier les (cyber)incidents de sécurité» ***T3/2019*** Réalisation de l'étude de base «Examen d'une obligation de notifier les (cyber)incidents de sécurité» ***T4/2019*** Compte rendu sur les modèles de base et recommandations les concernant

2. Débat de fond avec l'économie et les autorités	
Description du projet	Création de bases de décision par la tenue d'un débat de fond sur les variantes d'«obligations de notifier les (cyber)incidents de sécurité» avec l'économie et les autorités
Compétence	Centre de compétences pour la cybersécurité, OFPP, participation des offices spécialisés et de la FINMA
Étapes	***T3/2019*** Évaluation des modèles par les milieux économiques et politiques sur la base des résultats de l'étude de base ***T4/2019*** Compte rendu avec recommandation concernant l'obligation de notifier et informations complémentaires à l'intention du Parlement

7.4.3 Gouvernance mondiale d'Internet (M10)

Aperçu de la mesure	
Objectif	La Suisse doit s'engager activement et de façon coordonnée pour la fixation de règles internationales portant sur l'usage d'Internet et son développement, en accord avec la conception suisse de la liberté, de la démocratie et de la responsabilité (individuelle), du service public, de l'égalité des chances, de la sécurité, des droits de l'homme et de l'état de droit. Il convient d'associer à ces démarches les parties prenantes nationales, ainsi que de leur exposer les développements pertinents.
Responsabilité globale	OFCOM
Participation de services fédéraux	DFAE
Participation de tiers	EPFL, EPFZ
Comités / processus / projets	Aperçu des processus pertinents classées par ordre de priorité, forum suisse sur la gouvernance de l'internet (Swiss IGF), Plateforme Tripartite, Geneva Internet Platform (GIP)
Projets de mise en œuvre	1. Groupe de haut niveau du Secrétaire général de l'ONU sur la coopération numérique 2. Plateformes d'échange multi-acteurs pour la coordination au niveau national

Projets de mise en œuvre

1. Groupe de haut niveau du Secrétaire général de l'ONU sur la coopération numérique	
Description du projet	Le Secrétaire général de l'ONU a constitué le groupe de haut niveau sur la coopération numérique afin qu'il formule des propositions pour améliorer la coopération de tous les acteurs gouvernementaux et privés dans le domaine de la gouvernance numérique. Objectif: favoriser la confiance entre les acteurs et, partant, la sécurité dans le cyberespace. La Suisse entend influer sur le contenu et sur l'orientation stratégique de ce groupe et développer ainsi pour le numérique des structures de gouvernance axées sur l'avenir, afin d'intégrer des valeurs et des principes fondamentaux tels que l'état de droit, les droits de l'homme et la démocratie.
Compétence	OFCOM en collaboration avec le DFAE
Étapes	***T2/2018*** Mise en place du groupe ***T3/2018*** Première réunion à New York ***T1/2019*** Deuxième réunion à Genève ***T2/2019*** Troisième réunion à Helsinki ***T3/2019*** Rapport final ***T4/2019*** Évaluation des possibilités de mise en œuvre

2. Plateformes d'échange multi-acteurs pour la coordination au niveau national	
Description du projet	Doter le cyberespace d'une gouvernance aussi démocratique que possible et fondée sur les principes de l'état de droit est un gage de sécurité. La Suisse soutient les plateformes, notamment le Swiss IGF et la GIP, qui coordonnent les intérêts de toutes les parties prenantes en matière de gouvernance d'Internet et permettent à toutes de participer au débat. Les échanges impliquant toutes les parties prenantes, et les positions suisses étant largement étayées, celles-ci ont plus de poids dans les manifestations et les organes internationaux déterminants.
Compétence	OFCOM, DFAE, EPFL et EPFZ en collaboration avec d'autres acteurs intéressés de tous les groupes concernés
Étapes	***T4/2018*** Swiss IGF 2018 ***T4/2020*** Swiss IGF 2020 ***En continu*** Soutien de la GIP

7.4.4 Acquisition d'expertise par les offices spécialisés et les régulateurs (M11)

Aperçu de la mesure	
Objectif	Les offices spécialisés et les régulateurs ont pour mission d'élaborer des mesures ciblées visant à renforcer la cybersécurité, ce qui implique notamment d'édicter des réglementations. Or les autorités compétentes manquent souvent de savoir-faire en matière de numérique. Un pool d'experts va donc être créé au sein du Centre de compétences pour la cybersécurité, lequel sera mis à la disposition des services compétents en complément de l'expertise de l'OFAE en matière de normalisation et de l'OFPP en matière d'analyses des risques et de la vulnérabilité.
Responsabilité	Centre de compétences pour la cybersécurité
Participation	Offices spécialisés (OFSP, OFCOM, OFT, OFAC, OFEN), régulateurs (FINMA, ElCom, ComCom), OFPP, OFAE, armasuisse S+T, SFI (responsable de la contribution de la Suisse au développement des capacités dans le cadre de la politique financière internationale)
Comités / processus / projets	Collaboration établie entre MELANI, l'OFPP, l'OFAE, les offices spécialisés et les régulateurs
Nécessité de légiférer	Conventions à élaborer entre les unités administratives associées

Projets de mise en œuvre	1. Création d'un pool interdépartemental d'experts en cybersécurité à l'appui des offices spécialisés 2. Renforcement des projets de normalisation par le soutien apporté aux hautes écoles 3. Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale

Projets de mise en œuvre

1. Création d'un pool interdépartemental d'experts en cybersécurité	
Description du projet	Il faut définir les tâches et les ressources du pool d'experts et déterminer qui fournit des compétences et quels services y ont droit, à quelles conditions.
Compétence	Centre de compétences pour la cybersécurité, OFPP, OFAE, armasuisse S+T, OFIT, BAC, participation des offices spécialisés
Étapes	***T1/2019*** Évaluation des besoins avec les services concernés ***T2/2019*** Conception du pool d'experts et détermination des ressources ***T2/2020*** Signature des conventions entre les services concernés ***T4/2020*** Fin du recrutement, pool d'experts opérationnel ***T2/2022*** Évaluation du pool d'experts et propositions pour son développement

2. Renforcement des projets de normalisation par le soutien apporté aux hautes écoles	
Description du projet	Le centre de recherche et d'assistance commun aux deux EPF soutiendra la participation des deux hautes écoles aux activités de normalisation dans le domaine de la cybersécurité.
Compétence	EPFL et EPFZ
Étapes	***T3/2019*** Élaboration du projet de centre de recherche et d'assistance commun EPFL-EPFZ ***T2/2020*** Établissement d'une vue d'ensemble des activités de la Suisse dans ce domaine ***T1/2021*** Mise en œuvre des activités dans les groupes de travail identifiés comme stratégiques

3. Contribution de la Suisse à ancrer le thème de la cybersécurité dans la politique financière internationale	
Description du projet	La Suisse s'engage activement au sein des organes internationaux en faveur de la cybersécurité dans le secteur financier (p. ex. G20 et Conseil de stabilité financière) et contribue à renforcer les intérêts suisses en matière de cybersécurité internationale dans ce secteur.
Compétence	SFI
Étapes	***T4/2020*** Premier rapport intermédiaire sur les activités de renforcement des cybercapacités internationales dans le secteur financier ***T3/2022*** Deuxième rapport intermédiaire sur les activités de renforcement des cybercapacités internationales dans le secteur financier

7.5 Gestion des incidents

Sachant qu'il n'existe pas de protection absolue contre les cyberincidents et comme il faut s'attendre à une recrudescence d'attaques ciblées, une tâche prioritaire de la gestion des cyberrisques consiste à mettre en place et exploiter une organisation chargée de traiter les incidents (*incident management*). Afin de mener à bien ces tâches, il faut des compétences techniques, des instruments d'analyse, une organisation efficace et une collaboration étroite entre tous les services concernés. Les échanges d'informations entre partenaires dignes de confiance au sujet des incidents et des contre-mesures possibles sont déterminants, car les incidents se produisent souvent à plusieurs endroits à la fois, et donc pourront être gérés plus rapidement et plus efficacement si tous les acteurs concernés échangent des informations à ce sujet. Beaucoup d'organisations en Suisse ont créé ou mandaté des équipes spécialisées dans la gestion des cyberincidents. La Confédération exploite la centrale MELANI dans le Centre de compétences pour la cybersécurité pour soutenir les exploitants d'infrastructures critiques. L'élargissement du groupe cible de la SNPC implique d'étendre à de nouveaux bénéficiaires le soutien en cas d'incident. La collaboration déjà étroite avec d'autres centres de compétences sera encore renforcée de manière ciblée, de façon à utiliser les ressources limitées à disposition de manière aussi efficace et rationnelle que possible.

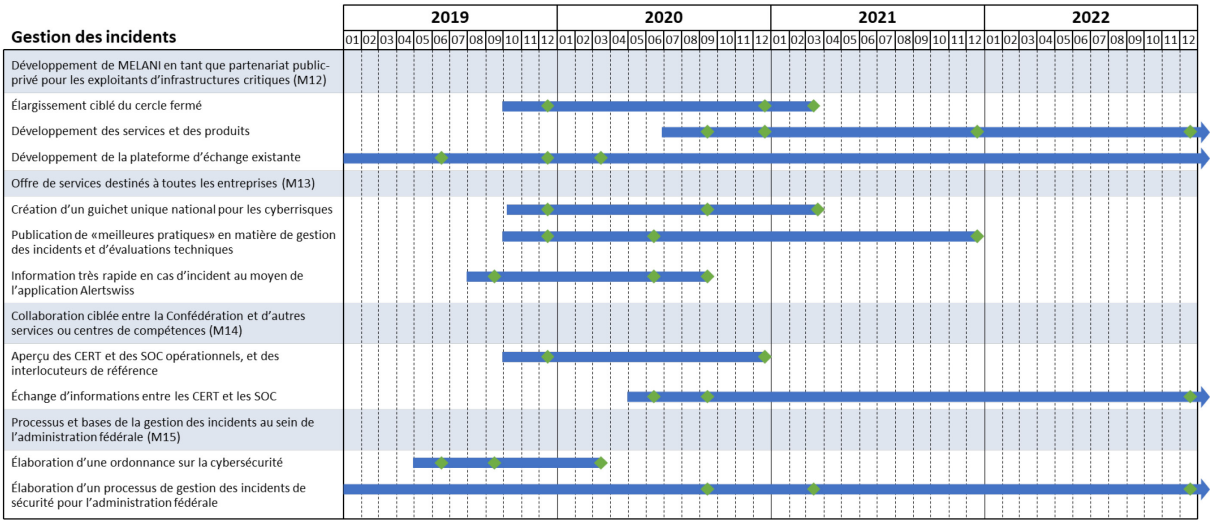


Figure 9: feuille de route «Gestion des incidents»

7.5.1 Développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques (M12)

Aperçu de la mesure	
Objectif	MELANI gère une plateforme qui permet aux exploitants d'infrastructures critiques d'échanger des informations. Ce soutien, qui prend la forme d'un partenariat public-privé pour la cybersécurité, est développé afin d'inclure tous les secteurs dans l'échange d'informations et de donner à celui-ci une dimension intersectorielle. On veillera à préserver la qualité de l'offre et à définir clairement qui a droit à quels services et à quelles informations.
Responsabilité	Centre de compétences pour la cybersécurité avec la participation du SRC
Participation de tiers	Exploitants d'infrastructures critiques

Comités / processus / projets	Cercle fermé de MELANI
Nécessité de légiférer	MELANI s'appuie sur la loi sur le renseignement (LRens) s'agissant de l'alerte précoce des infrastructures critiques (art. 6) et sur l'ordonnance sur l'informatique dans l'administration fédérale (OIAF). Il faut créer, pour le développement de MELANI, une base légale qui aille au-delà du service d'alerte précoce.
Projets de mise en œuvre	1. Élargissement ciblé du cercle fermé 2. Développement des services et des produits 3. Développement de la plateforme d'échange existante

Projets de mise en œuvre

1. Élargissement ciblé du cercle fermé	
Description du projet	Définition d'un accès aux produits et aux informations de MELANI pour tous les secteurs critiques et les offices spécialisés compétents, en fonction de leurs besoins
Compétence	Centre de compétences pour la cybersécurité avec la participation du SRC
Étapes	***T4/2019*** État des lieux de l'utilisation de MELANI par les différents secteurs critiques ***T4/2020*** Plan d'organisation du cercle fermé de MELANI ***T1/2021*** Développement ciblé du cercle fermé

2. Développement des services et des produits	
Description du projet	Développement des produits et des services de MELANI à l'appui des membres du cercle fermé en matière de gestion des incidents, de détection, d'analyse et de suivi
Compétence	Centre de compétences pour la cybersécurité avec la participation du SRC
Étapes	***T3/2020*** Analyse des produits et services MELANI existants et des besoins ***T4/2020*** Établissement du portefeuille des produits et services MELANI avec feuille de route ***T4/2021*** Premier rapport succinct sur le développement du portefeuille selon la feuille de route ***T4/2022*** Deuxième rapport succinct sur le développement du portefeuille selon la feuille de route

3. Développement de la plateforme d'échange existante	
Description du projet	Développement conforme aux besoins de la plateforme de collaboration «MELANI-NET» comme plaque tournante d'information pour les membres du cercle fermé de MELANI
Compétence	Centre de compétences pour la cybersécurité avec la participation du SRC
Étapes	***T3/2018*** Réalisation de l'étude avec recommandation d'une solution pour MELANI-NET 2.0 ***T2/2019*** Réalisation de la preuve du concept (*proof of concept*) pour la solution recommandée ***T4/2019*** Plan pour MELANI-NET 2.0 au point ***T1/2020*** MELANI-NET 2.0 productif

7.5.2 Offre de services destinés à toutes les entreprises (M13)

Aperçu de la mesure	
Objectif	L'économie suisse, et notamment les petites et moyennes entreprises, doivent être soutenues par MELANI. C'est pourquoi MELANI élargit le groupe cible et développe à son intention une offre de services complémentaires dans le domaine de la prévention et de la gestion des incidents. Ce soutien sera toutefois subsidiaire aux offres en matière de protection et de gestion des incidents disponibles sur le marché.
Responsabilité	Centre de compétences pour la cybersécurité
Participation de tiers	Associations économiques (ICTSwitzerland, p. ex.)
Comités / processus / projets	Services existants de MELANI pour le public (alertes, meilleures pratiques, instructions)
Nécessité de légiférer	Les bases légales des services décrits restent à élaborer.
Projets de mise en œuvre	1. Création d'un guichet unique national pour les cyberrisques 2. Publication de «meilleures pratiques» en matière de gestion des incidents et d'évaluations techniques 3. Information très rapide en cas d'incident -> application Alertswiss

Projets de mise en œuvre

1. Création d'un guichet unique national pour les cyberrisques	
Description du projet	Création d'un guichet unique national (en priorité un portail en ligne) pour les cyberrisques, qui permet de notifier les cyberincidents et propose des instruments d'aide à l'auto-assistance, des informations et des instructions supplémentaires
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T4/2019*** Traçage des grandes lignes du projet de portail en ligne pour la notification de cyberincidents ***T3/2020*** Mise à la disposition du public du portail en ligne pour la notification de cyberincidents ***T1/2021*** Intégration dans la plateforme d'information sur les cyberrisques (voir M29)

2. Publication de «meilleures pratiques» en matière de gestion des incidents et d'évaluations techniques	
Description du projet	Mise à disposition de l'économie suisse de produits ou de «meilleures pratiques» de gestion des cyberincidents et d'évaluations techniques
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T4/2019*** Analyse de la situation et des besoins concernant les éventuelles «meilleures pratiques» (instruments de travail / outils, etc.) pour la gestion des cyberincidents et analyses techniques pour le public ***T2/2020*** Projet sur les «meilleures pratiques» (instruments de travail / outils, etc.) pour la gestion des cyberincidents, analyses techniques pour le public, moyens et canaux de communication de celles-ci ***T4/2021*** Développement adapté aux besoins des informations et des services de MELANI relatifs aux «meilleures pratiques», et mise à disposition de celles-ci pour l'économie suisse

3. Information très rapide en cas d'incident au moyen de l'application Alertswiss	
Description du projet	L'application «Alertswiss» de l'OFPP est utilisée en cas d'incident pour informer rapidement un large public sur des cybermenaces aiguës.
Compétence	OFPP, Centre de compétences pour la cybersécurité
Étapes	***T3/2019*** 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 ***T1/2020*** Établissement du plan d'intégration des cyberinformations dans l'application Alertswiss ***T3/2020*** Possibilité d'informer le public d'un cyberincident au moyen de l'application Alertswiss ***T3/2020*** Publication d'un communiqué de presse sur la nouvelle fonction de l'application Alertswiss (cyberincident)

7.5.3 Collaboration ciblée entre la Confédération et d'autres services ou centres de compétences (M14)

Aperçu de la mesure	
Objectif	Renforcement ciblé de la concertation déjà étroite de MELANI avec d'autres services compétents au niveau tant fédéral que cantonal et promotion des échanges entre ces services
Responsabilité	Centre de compétences pour la cybersécurité
Participation de services fédéraux	CSIRT OFIT, milCERT
Participation de tiers	Switch, SOC cantonaux
Comités / processus / projets	CH-CERT: plateforme d'échange pour les CERT de Suisse
Nécessité de légiférer	Les bases légales de la collaboration entre MELANI et les autres services restent à élaborer.
Projets de mise en œuvre	1. Aperçu des SOC opérationnels et des interlocuteurs de référence 2. Échange d'informations avec les CERT et les SOC

Projets de mise en œuvre

1. Aperçu des CERT et des SOC opérationnels, et des interlocuteurs de référence	
Description du projet	Élaboration d'un aperçu actualisé des CERT et des SOC opérationnels, et des interlocuteurs de référence
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T4/2019*** Exécution et documentation du recensement des CERT et des SOC opérationnels, et des interlocuteurs de référence ***T4/2020*** Clarification du processus et des responsabilités concernant la mise à jour continue de l'aperçu

2. Échange d'informations entre les CERT et les SOC	
Description du projet	Il s'agit de vérifier quelles sont les informations que les CERT et les SOC peuvent échanger, et comment peut s'organiser cet échange.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2020*** Analyse des besoins et des possibilités concernant un échange d'informations systématique ***T3/2020*** Définition et attribution des projets d'établissement d'un échange d'informations ***T4/2022*** Mise en œuvre des projets définis

7.5.4 Processus et bases de la gestion des incidents au sein de l'administration fédérale (M15)

Aperçu de la mesure	
Objectif	Élaboration d'un processus qui définit les voies de notification et les responsabilités, dans l'optique d'une standardisation de la gestion des incidents au sein de l'administration fédérale
Responsabilité	Centre de compétences pour la cybersécurité
Participation	Tous les départements fédéraux
Comités / processus / projets	Comité de la sécurité informatique de la Confédération (C-SI)
Nécessité légiférer	La base existante est l'ordonnance sur l'informatique dans l'administration fédérale (OIAF). Une adaptation au centre de compétences est nécessaire.
Projets de mise en œuvre	1. Élaboration d'une ordonnance sur la cybersécurité 2. Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale

Projets de mise en œuvre

1. Élaboration d'une ordonnance sur la cybersécurité	
Description du projet	Élaboration d'une ordonnance pour donner une base juridique au Centre de compétences pour la cybersécurité, qui précise que celui-ci peut prendre la haute main dans la gestion des incidents de sécurité informatique au sein de l'administration fédérale.
Compétence	Secrétariat général du DFF
Étapes	***T2/2019*** Élaboration de l'ordonnance ***T3/2019*** Approbation de l'ordonnance par le Conseil fédéral ***T1/2020*** Entrée en vigueur de l'ordonnance

2. Élaboration d'un processus de gestion des incidents de sécurité pour l'administration fédérale	
Description du projet	Élaboration d'un processus de gestion des incidents de sécurité dans l'administration fédérale afin de matérialiser l'attribution des responsabilités et des compétences définie dans l'ordonnance sur la cybersécurité
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T3/2018*** Premier projet de processus, discussion avec les fournisseurs de prestations et les services concernés ***T3/2020*** Adaptation du processus à l'ordonnance sur la cybersécurité ***T1/2021*** Mise en place du processus ***T4/2022*** Vérification du processus et propositions d'amendements

7.6 Gestion des crises

Les cyberincidents peuvent être lourds de conséquences, et s'aggraver au point d'exiger une gestion de crise au niveau national. Il est essentiel pour maîtriser les crises de brosser un tableau actuel, uniforme et complet de la situation, de définir des processus de prise de décision efficaces et d'adopter une stratégie de communication. La gestion de crise ne dépend pas d'un scénario en particulier. Autrement dit, la gestion générale de la crise (procédures et processus de conduite) des cantons et de la Confédération vaut également pour les crises comportant des aspects relevant du cyberespace. Mais il est important, le cas échéant, que les états-majors de crise bénéficient d'un savoir spécifique et que tous les services compétents de la Confédération, des cantons et du secteur privé collaborent étroitement. Comme le temps presse pour rétablir la cybersécurité, il convient au préalable de s'exercer à appliquer les processus et d'élaborer des plans tant pour les activités de conduite que pour la communication.
Une implication directe du Centre de compétences fédéral pour la cybersécurité en tant qu'organe spécialisé et plateforme d'information est nécessaire dans la gestion des crises à l'échelon de la Confédération, laquelle incombe aux états-majors existants ou constitués ad hoc.

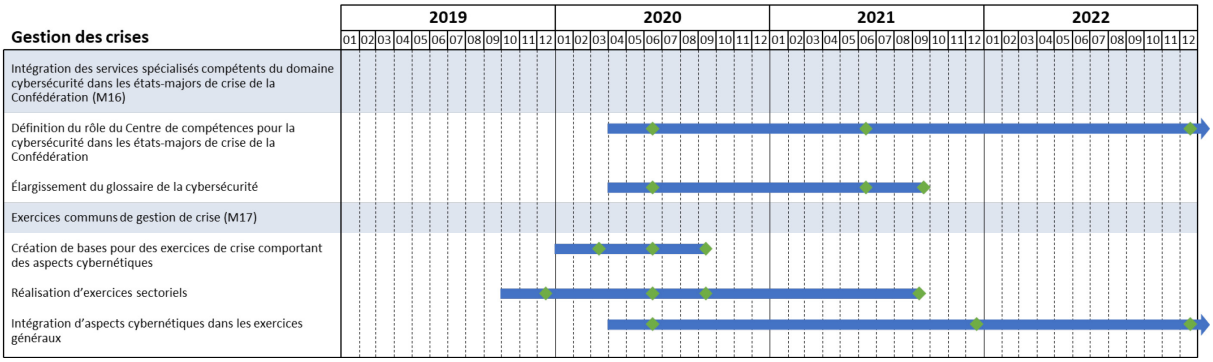


Figure 10: feuille de route «Gestion des crises»

7.6.1 Intégration des services spécialisés compétents du domaine cybersécurité dans les états-majors de crise de la Confédération (M16)

Aperçu de la mesure	
Objectif	Face à une cybercrise, les états-majors de crise existants peuvent être sollicités (notamment l'État-major fédéral Protection de la population, état-major de crise de l'AEP), ou des états-majors de crise ad hoc constitués. Pour gérer des crises en collaboration avec les milieux économiques, des organisations de crise spécifiques aux branches doivent en outre être créées et utilisées. Les services spécialisés compétents du domaine de la cybersécurité doivent être mis en contact avec les états-majors et avoir les compétences, en cas de crise à caractère cybernétique, pour assurer la coordination technique.
Responsabilité	Centre de compétences pour la cybersécurité
Participation	OFPP, ChF, OFAE, SG-DDPS, SRC

Comités / processus / projets	Concept pour les procédures et processus de conduite en cas de crises comportant des aspects cybernétiques
Projets de mise en œuvre	1. Définition du rôle du Centre de compétences pour la cybersécurité dans les états-majors de crise de la Confédération 2. Élargissement du glossaire de la cybersécurité

Projets de mise en œuvre

1. Définition du rôle du Centre de compétences pour la cybersécurité dans les états-majors de crise de la Confédération	
Description du projet	Clarification de la représentation, des canaux de communication et des compétences du Centre de compétences pour la cybersécurité dans les états-majors de crise existants.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2020*** Le Centre de compétences a défini son rôle au sein des états-majors de crise en accord avec eux ***T2/2021*** Examen de l'adaptation éventuelle des principes normatifs des états-majors ***T4/2022*** La participation du Centre de compétences aux états-majors est établie

2. Élargissement du glossaire de la cybersécurité	
Description du projet	Clarification des principaux termes de la cybersécurité pour une compréhension commune
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2020*** Inventaire des définitions existantes ***T2/2021*** Révision/élaboration du glossaire de la cybersécurité ***T3/2021*** Communication d'informations sur le glossaire de la cybersécurité

7.6.2 Exercices communs de gestion de crise (M17)

Aperçu de la mesure	
Objectif	Des exercices communs à la Confédération, aux cantons et à des représentants des infrastructures critiques serviront à tester la gestion des crises. Il s'agira à la fois d'introduire des aspects cybernétiques dans des exercices généraux, et d'organiser des exercices spécifiques consistant à résoudre une cybercrise. Les exercices seront évalués, et les résultats serviront à optimiser les procédures et processus de conduite.
Responsabilité	Centre de compétences pour la cybersécurité, SG-DDPS
Participation de services fédéraux	Offices spécialisés (OFSP, OFT, OFCOM, OFEN, OFAC, fedpol), OFAE, OFPP, EMFP, SG-DDPS, RNS
Participation de tiers	Associations de branche, représentants des banques (exercices sectoriels et transsectoriels), FINMA (exercices sectoriels) et hautes écoles
Comités / processus / projets	Exercice de conduite stratégique (ECS) Exercice du Réseau national de sécurité (ERNS) Exercice stratégique global Cyber Pakt du DDPS Participation à des exercices organisés au niveau international
Projets de mise en œuvre	1. Création de bases pour des exercices de crise comportant des aspects cybernétiques 2. Réalisation d'exercices sectoriels 3. Intégration d'aspects cybernétiques dans les exercices généraux

Projets de mise en œuvre

1. Création de bases pour des exercices de crise comportant des aspects cybernétiques	
Description du projet	Élaboration d'une vue d'ensemble des exercices de crise nationaux et internationaux comportant des aspects cybernétiques dans des sous-secteurs choisis, puis analyse destinée à savoir quels exercices supplémentaires sont nécessaires. Une expertise systématique des scénarios pour les exercices comportant des aspects cybernétiques est également réalisée.
Compétence	Centre de compétences pour la cybersécurité, SG-DDPS, en collaboration avec les hautes écoles

Étapes	***T1/2020*** Inventaire des exercices de crise nationaux et internationaux comportant des aspects cybernétiques existants et planifiés ***T2/2020*** Réalisation d'une expertise sur les scénarios et les exercices comportant des aspects cybernétiques ***T3/2020*** Analyse des priorités et du besoin de nouveaux exercices

2. Réalisation d'exercices sectoriels	
Description du projet	Organisation d'exercices de crise spécifiques comportant des aspects cybernétiques dans les sous-secteurs où les risques sont importants
Compétence	Offices spécialisés dans les secteurs concernés et FINMA pour le secteur financier, avec le soutien technique du SG-DDPS et sous la coordination du Centre de compétences pour la cybersécurité en collaboration avec l'OFPP / OFAE
Étapes	***T4/2019*** Analyse des besoins concernant les exercices de crise sectoriels ***T2/2020*** Clarification de la feuille de route et des responsabilités avec les partenaires concernés ***T3/2020*** Élaboration d'un ou plusieurs programmes pour les exercices de crise (nature, objectifs, participants, infrastructure, pilotage, scénario, etc.) avec les secteurs identifiés ou leurs représentants ***T3/2021*** Réalisation et documentation d'exercices sectoriels

3. Intégration d'aspects cybernétiques dans les exercices généraux	
Description du projet	Intégration d'aspects cybernétiques dans les exercices de crise et de sécurité de grande ampleur
Compétence	Centre de compétences pour la cybersécurité, SG-DDPS, EMFP
Étapes	***T2/2020*** Concertation avec les partenaires responsables afin d'intégrer les critères cybernétiques pertinents dans l'exercice ***T4/2021*** Prise en compte des aspects cybernétiques dans l'ECS/ERNS/EGU et d'autres exercices ***T4/2022*** Réflexion sur les conclusions spécifiques liées au cyberespace et discussion avec les représentants des états-majors de crise existants

7.7 Poursuite pénale

Le cyberespace fournit aux criminels potentiels de nouvelles opportunités, susceptibles d'entraîner de sérieux dommages pour la société et l'économie. Les actes ne sont plus véritablement limités dans le temps et l'espace. Dans ce contexte, il faut agir dans toute la Suisse et en collaboration avec des partenaires internationaux afin d'améliorer l'interopérabilité et la capacité de réaction et de coordonner efficacement les compétences professionnelles, techniques et humaines, sans devoir pour autant céder des prérogatives d'une autorité ou d'un niveau étatique à l'autre.
Créé en 2018 pour la coordination nécessaire à cet effet, le Cyberboard permet aux services compétents d'échanger, de développer des stratégies et de se coordonner entre eux au niveau opérationnel.

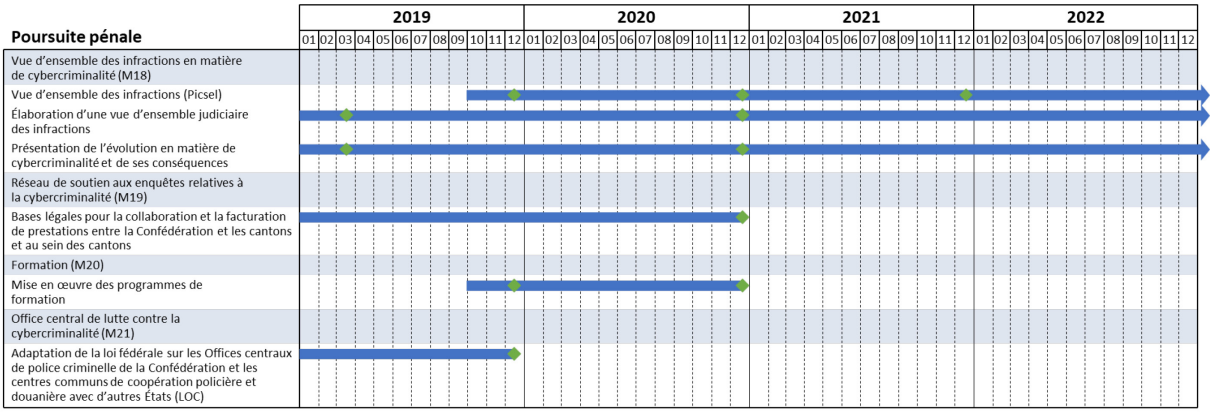


Figure 11: feuille de route «Poursuite pénale»

7.7.1 Vue d'ensemble des infractions en matière de cybercriminalité (M18)

Aperçu de la mesure	
Objectif	La Confédération (fedpol) et les cantons (CCPCS) étudient et conçoivent le cadre technique nécessaire à l'élaboration d'une vue d'ensemble des infractions en matière de cybercriminalité en Suisse (données policières).
Responsabilité	fedpol dans le cadre des activités du Cyberboard
Participation	Cyberboard, Office de l'auditeur en chef / justice militaire / police militaire
Comités / processus / projets	HiP, (Picar-Picsel), NEDIK, Cyber-CASE
Projets de mise en œuvre	1. Vue d'ensemble des infractions (Picsel) 2. Élaboration d'une vue d'ensemble judiciaire des infractions 3. Présentation de l'évolution en matière de cybercriminalité et de ses conséquences

Projets de mise en œuvre

1. Vue d'ensemble des infractions (Picsel)	
Description du projet	Regrouper les données policières au niveau national grâce à Picsel. Processus en trois phases: • Création du cadre technique • Cadre juridique • Utilisation de la vue d'ensemble des infractions
Compétence	fedpol, HiP
Étapes	***T4/2019*** Démarrage de la phase test de Picsel ***T4/2020*** Diffusion nationale par l'intermédiaire des cantons; participation d'au moins 3 concordats ***T4/2021*** Précision du cadre technique ***T4/2023*** LOC en vigueur (au niveau légal) ***T4/2023*** Mise en service de Picsel (données cantonales)

2. Élaboration d'une vue d'ensemble judiciaire des infractions	
Description du projet	Élaboration d'un instrument de saisie, au niveau national, de toutes les affaires de cybercriminalité en suspens dans les cantons (vue d'ensemble intercantonale des infractions)
Compétence	Cyberboard (Cyber-CASE, cantons, MPC et fedpol)
Étapes	***T1/2019*** Outil Cyber-CASE; liste des infractions pour tous les procureurs qui font office d'interlocuteurs uniques dans le domaine de la cybercriminalité (opérationnelle) ***T4/2020*** Outil en ligne pour la vue d'ensemble des procédures en cours ***T1/2021 Combinaison de l'état de la situation selon la police (Picsel) et de la vue d'ensemble judiciaire des infractions***

3. Présentation de l'évolution en matière de cybercriminalité et de ses conséquences	
Description du projet	Développement continu de produits pour la police et la justice (tendances, meilleures pratiques, rapport d'analyse, etc.)
Compétence	Cyberboard (NEDIK), cantons (polices cantonales, ministères publics cantonaux), MPC, fedpol et Office de l'auditeur en chef / justice militaire / police militaire
Étapes	***T1/2019*** Bulletin mensuel (de la police) ***T4/2020*** Vue d'ensemble des procédures en cours (police et justice)

7.7.2 Réseau de soutien aux enquêtes relatives à la cybercriminalité (M19)

Aperçu de la mesure	
Objectif	La Confédération (fedpol) et les cantons (CCPCS) élaborent le cadre de la collaboration et de la coordination entre les centres de cybercompétences national et cantonaux dans le cadre du NEDIK.
Responsabilité	CCPCS
Participation de services fédéraux	fedpol avec le Cyberboard
Participation de tiers	Police cantonale, CCPCS
Comités / processus / projets	Groupe de travail NEDIK
Projets de mise en œuvre	1. Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons

Projets de mise en œuvre

1. Bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons	
Description du projet	Élaboration des bases légales pour la collaboration et la facturation de prestations entre la Confédération et les cantons et au sein des cantons
Compétence	CCPCS et fedpol
Étapes	***T4/2020*** Signature et adoption d'une ou plusieurs conventions

7.7.3 Formation (M20)

Aperçu de la mesure	
Objectif	Des programmes de formation sont spécifiquement définis avec la collaboration de la CCPCS et la Conférence des procureurs de Suisse (CPS), en vue de l'acquisition durable des connaissances nécessaires dans le domaine de la poursuite pénale.
Responsabilité	CCPCS (y c. fedpol), CPS (y c. MPC)
Participation	Cyberboard

Comités / processus / projets	• Groupe de travail sur les formations dans le domaine de la cybercriminalité • Formations existantes (HEG-ARC ERMP) • Académie des avocats (HSLU) • Cyber-CASE
Projets de mise en œuvre	1. Mise en œuvre des programmes de formation

Projets de mise en œuvre

1. Formations	
Description du projet	Mise en œuvre du modèle à 5 échelons -> formations
Compétence	Institut Suisse de Police (ISP), formations du groupe de travail cybercrime
Étapes	***T4/2019*** Aperçu des possibilités de formations académiques (policières) ***T4/2020*** Offres de formation des hautes écoles utilisables par la police

7.7.4 Office central de lutte contre la cybercriminalité (M21)

Aperçu de la mesure	
Objectif	fedpol prépare une modification de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC) en vue de la création d'un office central de lutte contre la cybercriminalité et des bases légales nécessaires, afin de permettre la collaboration avec les cantons dans le cadre de la lutte contre la cybercriminalité.
Responsabilité	fedpol
Participation	Cyberboard, Office fédéral de la justice
Comités / processus / projets	LOC
Projets de mise en œuvre	1. Adaptation de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)

Projets de mise en œuvre

1. Adaptation de la loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États (LOC)	
Description du projet	Création d'une base légale pour un office central de lutte contre la cybercriminalité Entre autres, réglementation de l'échange de données de la police
Compétence	fedpol et Office fédéral de la justice (OFJ)
Étapes	***T4/2022*** LOC révisée et adoptée

7.8 Cyberdéfense

Des cyberattaques à grande échelle ou ciblant des infrastructures critiques peuvent mettre en danger la sécurité de la population et de l'économie du pays. La Suisse doit donc disposer, en toutes circonstances, des capacités et des ressources permettant de parer aux attaques en cours et d'identifier les acteurs responsables. En cas d'attaques mettant en danger le fonctionnement d'infrastructures critiques, il faut pouvoir, en concertation avec les autorités spécialisées compétentes, mettre en œuvre si nécessaire des contre-mesures actives, afin d'assurer le fonctionnement des infrastructures touchées. Les bases légales pour ce faire ont été créées par la loi sur le renseignement et la révision de la loi sur l'armée. La cyberdéfense comprend ainsi toute mesure servant à la défense des systèmes critiques et à la défense contre des attaques dans le cyberespace dans toutes les circonstances, c'est-à-dire jusqu'à des cas de conflit et de guerre. Dans le cadre de son «Plan d'action pour la cyberdéfense» (PACD), le DDPS a identifié la nécessité d'agir et les besoins en ressources supplémentaires dans le domaine de la cyberdéfense. Il a également défini les missions des différentes unités (dont l'armée) et a décrit quelles mesures sont nécessaires en vue de remplir les missions attribuées.

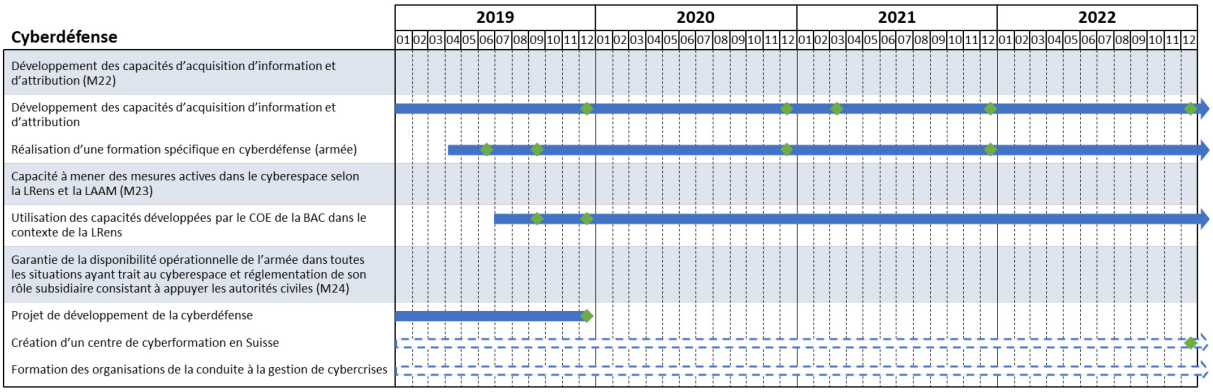


Figure 12: feuille de route «Cyberdéfense»

7.8.1 Développement des capacités d'acquisition d'information et d'attribution (M22)

Aperçu de la mesure

Objectif	Le SRC est en mesure d'identifier de nouveaux modes opératoires aussi vite que possible, à l'aide d'une acquisition et appréciation systématique d'information. Il peut établir l'origine des attaques (attribution) aussi précisément que possible, afin de préserver la marge de manœuvre des autorités politiques et des autorités de poursuite pénale. Lors d'attaques visant des exploitants d'infrastructures critiques, le SRC est en mesure, avec le soutien des unités partenaires et des autorités spécialisées, de remplir sa mission dans le cadre de la LRens. • *Les connaissances spécifiques et les compétences du SRC nécessaires à l'acquisition d'information en vue de la détection précoce des cyberattaques et de l'identification des auteurs sont développées.* • *Le SRC mène des analyses approfondies des acteurs et des environnements.* • *Le SRC utilise et développe des moyens techniques, la surveillance des télécommunications et des méthodes dans le domaine du renseignement humain (Human Intelligence, HUMINT).* • *Les cyberattaques sont systématiquement traitées et suivies.*
Responsabilité	SRC
Participation	BAC (Computer Network Operations, CNO) et Renseignement militaire (RM)
Comités / processus / projets	• Cyber SRC pour le traitement des informations pertinentes dans le domaine de compétences du SRC • Accord de niveau de service avec la BAC -> liaison des capacités techniques de la BAC pour le soutien du SRC
Projets de mise en œuvre	1. Développement des capacités d'acquisition d'information et d'attribution 2. Réalisation d'une formation spécifique en cyberdéfense (armée)

Projets de mise en œuvre

1. Développement des capacités d'acquisition d'information et d'attribution	
Description du projet	Augmentation des capacités d'analyse générales (linguistiques et géopolitiques) et techniques ainsi que des facultés d'acquisition d'information, avec des capacités/ressources appropriées
Compétence	SRC

Étapes	***T4/2019*** La première étape du développement est réalisée ***T4/2020*** La deuxième étape du développement est réalisée ***T1/2021*** Le rapport intermédiaire sur le développement des capacités est disponible ***T4/2021*** La troisième étape du développement est réalisée ***T4/2022*** Rapport final sur le développement des capacités

2. Réalisation d'une formation spécifique en cyberdéfense (armée)	
Description du projet	Détermination des besoins de l'armée en matière de formation et réalisation d'une formation spécifique avec l'aide de l'expertise de l'EPFL / EPFZ (connaissances techniques mais aussi pédagogiques). Les opérations bilatérales EPFL-DDPS seront complétées par des opérations communes EPFL-EPFZ-DDPS (*Joint Master in Cybersecurity – Defence part*).
Compétence	Composante bilatérale: EPFL + DDPS Composante triangulaire: EPFL + EPFZ + DDPS
Étapes	***T2/2019*** Premier entraînement avec la BAC des Forces terrestres ***T3/2019*** Lancement du master commun EPFL-EPFZ-DDPS ***T3/2019*** Premières formations EPFL-DDPS ***T4/2020*** Lancement du «Cyber Defense Curriculum» ***T4/2021*** Autres mesures de sensibilisation, développement de la première étape

7.8.2 Capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM (M23)

Aperçu de la mesure	
Objectif	Le DDPS (SRC et armée) dispose des compétences adéquates en nombre et en qualité et des capacités pour le cas échéant perturber, empêcher ou ralentir des attaques visant les infrastructures critiques. De telles mesures sont mises en œuvre en concertation avec les offices spécialisés compétents conformément aux dispositions de la LRens et de la LAAM.
Responsabilité	SRC, COE de la BAC
Participation	
Comités / processus / projets	Le SLA (*Service Level Agreement*) avec le COE de la BAC a été adapté. L'acquisition de connaissances spécifiques par le COE est terminée.
Projets de mise en œuvre	1. Utilisation des capacités développées par le COE de la BAC dans le contexte de la LRens

Projets de mise en œuvre

1. Utilisation des capacités développées par le COE de la BAC dans le contexte de la LRens	
Description du projet	Perturber, empêcher ou ralentir des attaques visant les infrastructures critiques
Compétence	SRC, COE de la BAC
Étapes	***T3/2019*** Les effets collatéraux des activités prévues ont été envisagés avec les offices spécialisés ***T4/2019*** Les capacités sont présentes

7.8.3 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 (M24)

Aperçu de la mesure	
Objectif	Le DDPS en général et l'armée en particulier doivent être en mesure d'atteindre les objectifs ci-après en étroite collaboration avec leurs partenaires, avec l'économie et avec les hautes écoles: 1) maîtriser le nombre, l'intensité et la complexité de cybermenaces de plus en plus variées, au quotidien comme en cas de crise ou de conflit; 2) mettre en œuvre les aspects de la loi sur le renseignement et de la loi sur l'armée relevant du cyberespace; 3) être capable d'apporter, en cas de besoin, un soutien (subsidiaire) efficace et durable aux exploitants d'infrastructures critiques victimes de cyberattaques.
Responsabilité globale	SG-DDPS et BAC en étroite collaboration
Participation	Commandement des Opérations, commandement de l'Instruction, BLA, SRC, armasuisse S+T, OFPP
Comités / processus / projets	Le plan d'action Cyberdefence du DDPS contient / décrit notamment: • les processus (mise en œuvre au profit de l'armée et soutien des infrastructures critiques); • les règles de subsidiarité; • les instruments de coordination.
Projets de mise en œuvre	1. Projet de développement de la cyberdéfense 2. Création d'un centre de cyberformation en Suisse 3. Formation des organisations de la conduite à la gestion de cybercrises

Projets de mise en œuvre

1. Projet de développement de la cyberdéfense	
Description du projet	Ce projet (en gestation depuis 2015) vise à rendre progressivement l'armée capable d'effectuer ses tâches dans le cyberespace. Ces tâches comprennent la conduite, l'anticipation, la prévention, la protection, l'action, la réaction et le soutien.
Compétence	BAC avec le soutien des Ressources de l'armée, d'armasuisse et du SG-DDPS
Étapes	Selon projet => Clôture du projet: ***T4/2019***

2. Création d'un centre de cyberformation en Suisse	
Description du projet	Création par l'armée suisse d'un centre de cyberformation (Cyber Training Center, CTC) afin de former des spécialistes et des cadres à la gestion des cyberattaques. Le CTC formera du personnel de l'armée et de l'administration. Il coopérera étroitement avec les autorités, les exploitants d'infrastructures critiques et les hautes écoles. Objectif principal: faire augmenter rapidement la proportion de personnel opérationnel.
Compétence	BAC (avec le commandement de l'Instruction de l'armée)
Étapes	Échéancier en cours d'élaboration. À préciser. Mise en service prévue pour la **fin de 2022**.

3. Formation des organisations de la conduite à la gestion de cybercrises	
Description du projet	L'armée suisse donne aux tiers intéressés (autorités, organes de gestion de crise des communes ou des cantons, exploitants d'infrastructures critiques) la possibilité de s'entraîner à la gestion de crise en cas de cyberincident (logiquement, dans le cadre du réseau de sécurité). Objectif: interopérabilité du RNS.
Compétence	BAC (avec le commandement de l'Instruction de l'armée)
Étapes	Échéancier en cours d'élaboration. À préciser. Mise en service prévue pour la **fin de 2022**.

7.9 Positionnement actif de la Suisse dans la politique internationale de cybersécurité

La défense des intérêts de politique extérieure et de politique de sécurité de la Suisse doit aussi être assurée dans le cyberespace. La Suisse s'engage donc, au niveau diplomatique comme sur le plan technique et opérationnel, en vue du renforcement de la coopération internationale pour réduire les cyberrisques. Elle s'engage pour la reconnaissance, le respect et l'application du droit international sur le terrain de la cybersécurité, s'investit activement pour l'instauration d'un climat de confiance entre les États et soutient ou conçoit des initiatives visant à développer les capacités d'États tiers. Dans toutes ces activités, une attention particulière sera accordée à la promotion de la Suisse et de la Genève internationale, comme plateforme de discussion de nouvelles mesures de politique de cybersécurité.

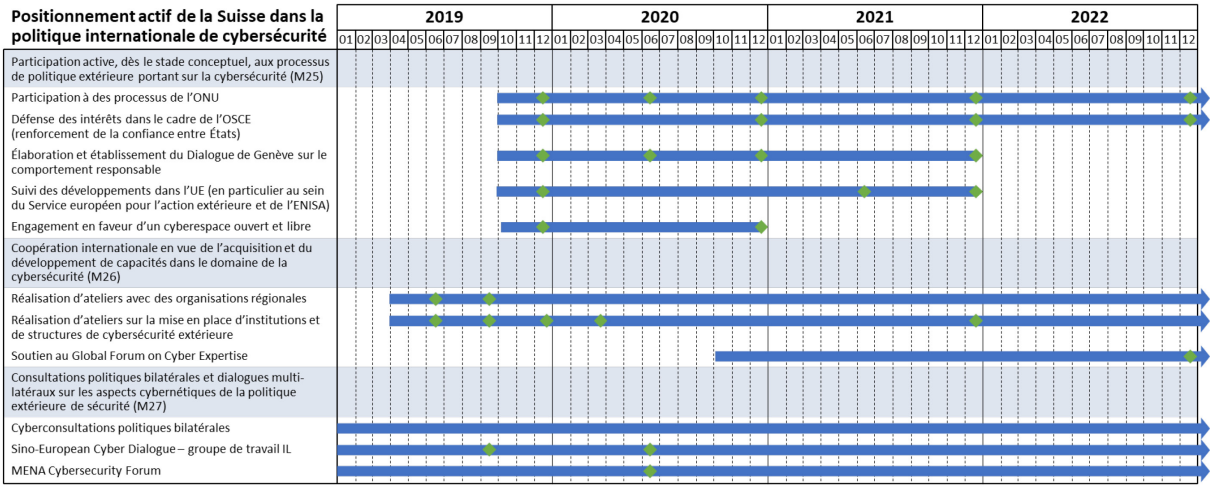


Figure 13: feuille de route «Positionnement actif de la Suisse dans la politique internationale de cybersécurité»

7.9.1 Participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité (M25)

Aperçu de la mesure	
Objectif	La Suisse contribue au développement et à la mise en œuvre de normes de comportement étatiques et non étatiques dans le cyberespace. Elle œuvre pour la reconnaissance du droit international et la protection des droits de l'homme, et contribue à clarifier diverses questions d'application. Elle s'engage pour l'instauration de la confiance entre les États dans le cyberespace, en soutenant les mesures prises par des organisations régionales telles que l'OSCE. La Suisse travaille activement en vue de l'application de régimes de contrôle des exportations de technologies de surveillance.
Responsabilité	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, SECO
Participation	DFAE: DDIP, DOI, DSH; DDPS: SG-DDPS (domaine POLSEC)

Comités / processus / projets	ONU, OSCE, UE, OTAN, contrôle des armements, Processus de Londres
Projets de mise en œuvre	1. Participation à des processus de l'ONU 2. Défense des intérêts dans le cadre de l'OSCE (renforcement de la confiance entre États) 3. Établissement du Dialogue de Genève sur le comportement responsable 4. Suivi des développements dans l'UE (en particulier au sein du Service européen pour l'action extérieure et de l'ENISA) 5. Engagement en faveur d'un cyberespace ouvert et libre

Projets de mise en œuvre

1. Participation à des processus de l'ONU	
Description du projet	Dans le cadre de l'ONU, la Suisse œuvre pour la cybersécurité internationale, notamment au sein du groupe d'experts gouvernementaux sur la cybersécurité (*UN Governmental Group of Experts on Cyber Security*, UN GGE) et du groupe de travail à composition non limitée (Open Ended Working Group, OEWG). Ces deux processus ont été mis en place par l'Assemblée générale de l'ONU. L'UN GGE élabore des recommandations sur les thèmes des normes de comportement étatiques, de l'instauration de la confiance, du renforcement des capacités et de l'application du droit international. Deux des quatre débats se déroulent à Genève. L'OEWG a pour objectif de développer treize règles de conduite et de les adapter et modifier au besoin. Il prévoit également l'intégration d'acteurs non étatiques.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace Pour la mise en œuvre du droit international: Direction du droit international public (DDIP)
Étapes	***T4/2019-2022*** Rapports annuels ***T4/2021*** Développement de recommandations conformes aux intérêts de la Suisse dans le rapport de l'UN GGE ***T2/2020*** Participation au document final de l'OEWG conforme aux intérêts de la Suisse

2. Défense des intérêts dans le cadre de l'OSCE (renforcement de la confiance entre États)	
Description du projet	La Suisse œuvre pour le développement et la mise en œuvre de mesures visant à renforcer la confiance dans le cyberespace. Elle soutient à cette fin le processus de l'OSCE. L'OSCE a adopté en 2013 et en 2016 un catalogue de mesures visant à renforcer la confiance dans le domaine de la cybersécurité. Cet accord international, le premier du genre, comprend 16 mesures visant à réduire les risques liés aux nouvelles technologies d'information et de communication et à améliorer la transparence entre les États membres de l'OSCE.
Responsabilité	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace
Étapes	***T4/2019-2022*** Participation aux négociations et contribution active au processus ***T4/2019-2022*** Rapports annuels ***T4/2021*** Soutien d'échanges interrégionaux

3. Élaboration et établissement du Dialogue de Genève sur le comportement responsable	
Description du projet	Le *Geneva Dialogue on Responsible Behaviour in Cyberspace* réunit diverses parties prenantes afin de faciliter les discussions sur les rôles et responsabilités de tous les acteurs dans l'utilisation du cyberespace et sert de plateforme de consultation pour les débats ou processus multilatéraux de normalisation. Il comprend un processus d'experts visant à examiner l'application des principes fondamentaux du droit international dans le cyberspace. La Suisse y renforce son rôle de défenseur du droit international et de la sécurité dans le cyberespace.
Responsabilité	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace Pour le droit international: DDIP Services de soutien: DDIP, MiGe, DOI

Étapes	***T4/2019*** Plan pour l'établissement du Dialogue de Genève comme plateforme multi-acteurs pour les processus internationaux dans le domaine de la politique étrangère et de cybersécurité ***T4/2019*** Deux voire trois dialogues du processus d'experts sur l'application du droit international dans le cyberespace ont eu lieu ***T4/2021*** Établissement du Dialogue de Genève comme plateforme multi-acteurs ***T2/2020*** Intégration des enseignements du processus d'experts dans l'UNGGE et l'OEWG ***T4/2020*** 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

4. Suivi des développements dans l'UE (en particulier au sein du Service européen pour l'action extérieure et de l'ENISA)	
Description du projet	L'Union européenne a pris de nombreuses mesures visant à lutter contre la menace croissante que représentent les cyberattaques. N'appartenant pas à l'UE, la Suisse n'a pas été associée à ces travaux mais est directement ou indirectement concernée par ces mesures. Il est donc important d'analyser les actions prévues ou mises en place par l'UE et de vérifier leurs conséquences pour la Suisse.
Compétence	Co-compétence: Centre de compétences pour la cybersécurité et DFAE (Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace). Services de soutien: DDIP, DAE
Étapes	***T4/2019*** La vue d'ensemble des principaux acteurs, processus et mesures de l'UE est établie, et les services de la Suisse qui s'engagent dans les différents processus sont identifiés ***T2/2021*** Les conséquences possibles des différentes mesures de l'UE pour la Suisse sont analysées ***T4/2021*** Les processus et compétences pour l'observation des processus de l'UE et les éventuelles participations sont établis

5. Engagement en faveur d'un cyberespace ouvert et libre	
Description du projet	La Suisse œuvre, sur le plan international, pour un cyberespace sûr, libre et ouvert, où soient garantis la sécurité, la protection des droits universels de l'homme, la protection de la vie privée ou encore la liberté d'opinion. Elle estime que les droits de l'homme doivent être respectés de la même façon en ligne que hors ligne. Plusieurs organisations et processus internationaux sont concernés. Il faut y défendre les intérêts de la Suisse de manière ciblée. Pour ce faire, il faut dresser un état des lieux des organisations et des processus concernés.

Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DSH et DDIP
Étapes	***T4/2019*** État des lieux des processus concernant les droits de l'homme et des forums internationaux concernés ***T4/2020*** Évaluation relative à la participation suisse à des processus et forums choisis

7.9.2 Coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité (M26)

Aperçu de la mesure	
Objectif	La Suisse recherche de manière ciblée l'échange avec des services étatiques et non étatiques internationaux pour l'acquisition et le développement de capacités nationales dans le domaine de la cybersécurité. Dans le même temps, elle contribue activement à la création et au renforcement de telles capacités dans des États tiers, et aide ainsi à améliorer la cybersécurité au niveau mondial.
Responsabilité	DFAE/DPS, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace
Participation	DOI, DSH, DDIP
Comités / processus / projets	CCDCoE, Global Forum on Cyber Expertise, G20 et Conseil de stabilité financière (CSF) dans le domaine de la politique financière internationale
Projets de mise en œuvre	1. Réalisation d'ateliers avec des organisations régionales 2. Réalisation d'ateliers sur la mise en place d'institutions et de structures de cybersécurité extérieure 3. Soutien au Global Forum on Cyber Expertise

Projets de mise en œuvre

1. Réalisation d'ateliers avec des organisations régionales	
Description du projet	La Suisse soutient les membres d'organisations régionales (p. ex. Union africaine) pour l'acquisition de capacités liées au cyberespace. Pour cela, elle organise une série d'ateliers à Genève et dans diverses régions du monde (p. ex. Afrique, Addis-Abeba).
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DOI, DDIP
Étapes	***T2/2019*** Élaboration du plan et planification de la manifestation ***T3/2019*** Tenue du premier atelier à Genève

2. Réalisation d'ateliers sur la mise en place d'institutions et de structures de cybersécurité extérieure	
Description du projet	La Suisse soutient d'autres États dans la mise en place et le développement de structures de cybersécurité extérieure par son expertise et par les plateformes d'échange d'expérience. Elle organise des ateliers et des séminaires afin d'accroître le savoir et l'expertise relatifs aux instruments et aux processus internationaux. À cet égard, elle propose des plateformes internationales d'entraînement et des exercices, en collaboration avec les hautes écoles.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DOI, DDIP; en collaboration avec l'EPFL et l'EPFZ (soutien académique: expertise, ressources, acquisition de talents, etc.)
Étapes	***T2/2019*** Analyse des besoins et possibilités de soutien ***T3/2019*** Entraînement et développement d'un scénario ***T4/2019*** Élaboration du projet et planification de la manifestation ***T1/2020*** Tenue du premier atelier à Genève ***T4/2021*** Mise à disposition d'une plateforme commune

3. Soutien au Global Forum on Cyber Expertise	
Description du projet	La Suisse soutient le forum mondial sur la cyberexpertise et participe aux efforts internationaux pour développer le savoir et l'expertise relatifs à la réduction des cyberrisques. Pour ce faire, elle développe des projets existants et examine l'opportunité de participer à d'autres initiatives.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DOI, DDIP; DDPS: MELANI
Étapes	***T4/2022*** Poursuite du projet «critical information infrastructure protection» ***T4/2022*** Poursuite du projet «e-diplomacy» ***T4/2022*** Participation active à la constitution du groupe de travail «Diplomacy, international norms and CBMs»

7.9.3 Consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité (M27)

Aperçu de la mesure	
Objectif	La Suisse mène avec des pays choisis, dans le cadre de sa politique extérieure, des consultations sur la sécurité du cyberespace, notamment sur la situation de la menace et sur les tendances émergentes. Elle s'implique activement dans les dialogues multilatéraux (p. ex. Sino-European Cyber Dialogue).

Responsabilité	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace
Participation	Services fédéraux intéressés de différents départements
Comités / processus / projets	Consultations politiques, Sino-European Cyber Dialogue CDC OTAN 29+1
Projets de mise en œuvre	1. Cyberconsultations politiques bilatérales 2. Sino-European Cyber Dialogue – groupe de travail IL 3. Dialogue MENA

Projets de mise en œuvre

1. Cyberconsultations politiques bilatérales	
Description du projet	La Suisse mène avec des pays choisis, dans le cadre de sa politique extérieure et avec la participation d'autres départements, des consultations sur la sécurité du cyberespace, notamment sur la situation de la menace et sur les tendances émergentes. Le choix de ces pays est effectué en collaboration avec les départements concernés.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, autres départements intéressés
Étapes	Mise en place des consultations correspondantes

2. Sino-European Cyber Dialogue – groupe de travail IL	
Description du projet	Le cyberdialogue sino-européen (*Sino-European Cyber Dialogue*, SECD) est un dialogue dans lequel des représentants chinois et européens gouvernementaux et non gouvernementaux échangent sur des thèmes relevant de la cybersécurité et de la gouvernance d'Internet. Ce dialogue est en soi une mesure d'instauration de la confiance: l'échange d'informations est encouragé et la transparence améliorée. La Suisse s'engage pour la concrétisation du SECD et propose la mise en place d'un groupe de travail sur le thème du droit international.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DDIP
Étapes	***T3/2019*** Maintien du SECD ***T2/2020*** Établissement du groupe de travail International Law

3. MENA Cybersecurity Forum	
Description du projet	Le MENA Cybersecurity Forum offre un cadre de débat pour les États de la région MENA (Moyen-Orient et Afrique du Nord). Il permet de discuter d'un vaste choix de thèmes relevant de la cybersécurité. Le forum a été mis en place par le GCSP, avec la participation du DFAE. Le GCSP et le DFAE ont pour objectif le maintien et l'établissement du forum.
Compétence	DFAE, Bureau de l'Envoyé spécial pour la politique étrangère et de sécurité relative au cyberspace, DMOAN, GCSP
Étapes	***T2/2020*** Maintien du MENA Cybersecurity Forum

7.10 Visibilité et sensibilisation

Les cyberrisques préoccupent la population et les milieux économiques, par leur rapide évolution et leur gravité croissante. La communication active à propos des mesures adoptées et des progrès réalisés fait dès lors partie des tâches de mise en œuvre de la stratégie. En plus de sa communication active à propos de la SNPC, la Confédération s'engage sur le terrain de la sensibilisation. Son travail d'information de la population à propos des cyberrisques et des mesures de protection envisageables contribue à la prévention et à l'amélioration de la résilience, et aide à réduire le sentiment d'insécurité. Les récents incidents ont confirmé qu'il reste nécessaire de sensibiliser le grand public aux cyberrisques et d'attirer son attention sur les possibilités de protection de base à disposition. À l'avenir, le grand public sera informé de manière plus active sur la mise en œuvre de la SNPC, afin que les mesures que la Confédération met en œuvre pour protéger la Suisse face aux cyberrisques soient connues au-delà du cercle des spécialistes. Dans un esprit de prévention, la Confédération et les cantons contribueront en outre davantage à sensibiliser la population, les milieux économiques et le monde politique aux cyberrisques et aux mesures de protection possibles.

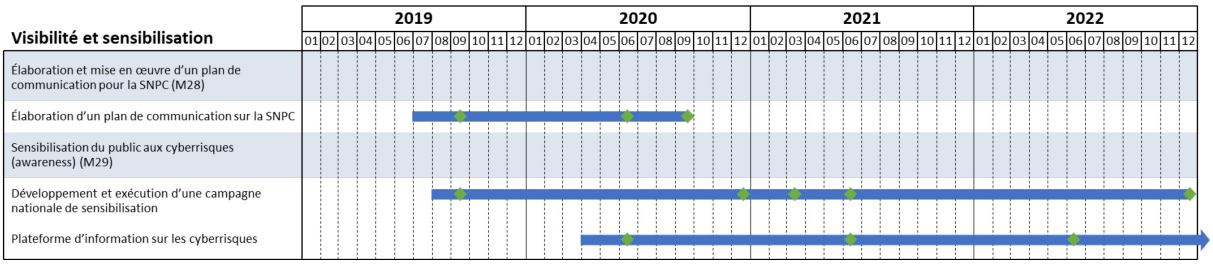


Figure 14: feuille de route «Visibilité et sensibilisation»

7.10.1 Élaboration et mise en œuvre d'un plan de communication pour la SNPC (M28)

Aperçu de la mesure	
Objectif	Un plan précisera les lignes directrices, les compétences et les processus en matière de communication. Il s'agit ici de trouver un juste équilibre entre confidentialité et besoin d'information. La mise en œuvre du plan prendra en compte les divers publics et sera activement poursuivie dans le cadre du travail de relations publiques et de communication.
Responsabilité	Centre de compétences pour la cybersécurité
Participation	En concertation avec les acteurs principaux de la SNPC
Comités / processus / projets	Campagnes de sensibilisation permanentes
Projets de mise en œuvre	1. Élaboration d'un plan de communication sur la SNPC

Projets de mise en œuvre

1. Élaboration d'un plan de communication sur la SNPC	
Description du projet	Élaboration d'un plan de communication sur la SNPC
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T3/2019*** Analyse de la situation établie ***T2/2020*** Plan de communication sur la SNPC élaboré (objectifs, groupes cibles, messages, poursuite des objectifs [stratégie], instruments/mesures, mesure des résultats et budget) ***T2/2020*** Responsabilités et délais de communication (plan) définis, et coordination à cette fin avec d'autres acteurs de la SNPC réalisée ***T3/2020*** Début de la mise en œuvre du plan de communication

7.10.2 Sensibilisation du public aux cyberrisques (*awareness*) (M29)

Aperçu de la mesure	
Objectif	La Confédération veut contribuer à sensibiliser le grand public aux cyberrisques. Elle renforce ses activités de communication sur les cyberrisques, en tirant parti des capacités existantes des associations, fédérations ou autorités déjà actives dans ce domaine.
Responsabilité	Centre de compétences pour la cybersécurité
Participation de services fédéraux	SG-DDPS, offices spécialisés
Participation de tiers	Cantons, représentants des banques, SATW, ICTswitzerland
Comités / processus / projets	Campagnes et instruments d'aide des organisations suivantes: SATW (unités de cours pour enseignants, défi en ligne 2019 pour les jeunes), Swiss Internet Security Alliance (StopThinkConnect), Prévention suisse de la criminalité, e-banking en toute sécurité, Association suisse pour le label de cybersécurité (jeunesse et médias), ICON NRO (KINDER4CYBER, formation en kit), collaboration entre l'ASA et l'AFA (programme de formation pour commerciaux, pour la sensibilisation des PME), etc.
Nécessité de légiférer	Les bases légales des tâches de sensibilisation restent à élaborer.

Projets de mise en œuvre	1. Développement et exécution d'une campagne nationale de sensibilisation 2. Plateforme d'information sur les cyberrisques gérée par les interlocuteurs nationaux

Projets de mise en œuvre

1. Développement et exécution d'une campagne nationale de sensibilisation	
Description du projet	Exécution d'une campagne nationale de sensibilisation du public aux cyberrisques (*awareness*); sur tous les domaines de la cybersécurité, de la cybercriminalité et de la cyberdéfense Utilisation de synergies avec les campagnes en cours et les capacités existantes de sensibilisation des acteurs déjà actifs dans ce domaine (associations, fédérations, autorités, etc.)
Compétence	Centre de compétences pour la cybersécurité, en coordination transversale avec les acteurs actifs (fedpol, SG-DDPS, POLSEC, SISA, PSC, etc.), ICTswitzerland
Étapes	***T3/2019*** Coordination réalisée avec les acteurs actifs sur la conception d'une campagne nationale ***T4/2020*** Programme de campagne nationale établi ***T1/2021*** Plan de mise en œuvre présent ***T2/2021*** Début/production de la campagne nationale ***T4/2022*** Rapport sur l'exécution et l'efficacité de la campagne nationale

2. Plateforme d'information sur les cyberrisques	
Description du projet	Création d'une plateforme nationale d'information sur les cyberrisques pour la prévention et la sensibilisation. La plateforme est gérée par le Centre de compétences pour la cybersécurité, en étroite collaboration avec les associations économiques, les cantons, les hautes écoles et d'autres organes intéressés.
Compétence	Centre de compétences pour la cybersécurité
Étapes	***T2/2020*** Le projet de conception de la plateforme est élaboré (contenus) ***T2/2021*** Lancement de la plateforme dans le cadre de la campagne de sensibilisation ***T2/2022*** Évaluation de l'utilisation de la plateforme et adaptation des contenus

Liste des figures

Liste des abréviations

AES ..... Association des entreprises électriques suisses
AFA ..... Association pour la formation professionnelle en assurance de l'industrie suisse de l'assurance
ASA ..... Association Suisse d'Assurances
BAC ..... Base d'aide au commandement
BLA..... Base logistique de l'armée
Canvas ..... Constructing an Alliance for Value-driven Cybersecurity
CBMs..... Confidence building measures
CCDCoE..... Centre d'excellence de cyberdéfense coopérative
CCDJP ... Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS ..... Conférence des Commandants des polices cantonales de Suisse
CDC..... Cyber Defence Committee
CERT..... Computer Emergency Response Team
CFS ..... Centre fédéral de situation
CG MPS .... Conférence gouvernementale des affaires militaires, de la protection civile et des sapeurs-pompiers
CNO ..... Computer Network Operations
COE..... Centre des opérations électroniques
ComCom ..... Commission fédérale de la communication
CSI ..... Conférence suisse sur l'informatique
CSIRT..... Computer Security Incident Response Team
CTC ..... Cyber Training Center
CYD-Campus..... Campus cyberdéfense
DAE ..... Direction des affaires européennes
DDIP..... Direction du droit international public
DDPS ..... Département fédéral de la défense, de la protection de la population et des sports
DFAE..... Département fédéral des affaires étrangères
DFF ..... Département fédéral des finances
DFJP ..... Département fédéral de justice et police
DOI..... Division Nations Unies et organisations internationales
DSH..... Division Sécurité humaine
ECS ..... Exercice de conduite stratégique
EGU..... Exercice général d'urgence
ElCom..... Commission fédérale de l'électricité
EMFP ..... État-major fédéral Protection de la population
ENISA..... Agence européenne chargée de la sécurité des réseaux et de l'information
EPFL ..... École polytechnique fédérale de Lausanne
EPFZ ..... École polytechnique fédérale de Zurich
ERNS ..... Exercice du Réseau national de sécurité
fedpol..... Office fédéral de la police
FINMA ..... Autorité fédérale de surveillance des marchés financiers
FRI..... Formation, recherche et innovation
G20..... Groupe des 20 principaux pays industrialisés et émergents
GCSP ..... Geneva Centre for Security Policy
GIP ..... Geneva Internet Platform
GovCert ..... Centre de compétences pour la cybersécurité
HiP..... Harmonisation de l'informatique policière suisse
HSLU..... Haute école de Lucerne
ICT..... Technologies de l'information et de la communication
ISP..... Institut Suisse de Police

LAAM ..... Loi sur l'armée
LOC ..... Loi fédérale sur les Offices centraux de police criminelle de la Confédération et les centres communs de coopération policière et douanière avec d'autres États
LRens ..... Loi sur le renseignement
MELANI ..... Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MiGe ..... Mission permanente de la Suisse auprès de l'Office des Nations Unies et des autres organisations internationales à Genève
MilCERT ..... Military Computer Emergency Readiness Team
MPC ..... Ministère public de la Confédération
NEDIK ..... Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique
OEWG ..... Open Ended Working Group
OFAC ..... Office fédéral de l'aviation civile
OFAE ..... Office fédéral pour l'approvisionnement économique du pays
OFCOM ..... Office fédéral de la communication
OFEN ..... Office fédéral de l'énergie
OFIT ..... Office fédéral de l'informatique et de la télécommunication
OFJ ..... Office fédéral de la justice
OFPP ..... Office fédéral de la protection de la population
OFSP ..... Office fédéral de la santé publique
OFT ..... Office fédéral des transports
OIAF ..... Ordonnance sur l'informatique dans l'administration fédérale
OIC ..... Operation Information Center
ONU ..... Organisation des Nations unies
OSCE ..... Organisation pour la sécurité et la coopération en Europe
OSINT ..... Open source intelligence
OTAN ..... Organisation du traité de l'Atlantique nord
PACD ..... Plan d'action pour la cyberdéfense
PIO ..... Protection des informations et des objets
POLSEC ..... Politique de sécurité
PSC ..... Prévention suisse de la cybercriminalité
RM ..... Renseignement militaire
RNS ..... Réseau national de sécurité
S+T ..... Sciences et technologies
SATW ..... Académie suisse des sciences techniques
SCE ..... Swiss Cyber Experts
SCION ..... Scalability, Control, and Isolation on Next-Generation Networks
SECD ..... Sino-European Cyber Dialogue
SEFRI ..... Secrétariat d'État à la formation, à la recherche et à l'innovation
SFI ..... Secrétariat d'État aux questions financières internationales
SG ..... Secrétariat général
SISA ..... Swiss Internet Security Alliance
SOC ..... Security Operations Center
SRC ..... Service de renseignement de la Confédération
Swiss IGF ..... Swiss Internet Governance Forum
UE ..... Union européenne
UN GGE ..... UN Governmental Group of Experts on Cyber Security
UPIC ..... Unité de pilotage informatique de la Confédération

Annexe Plan de mise en œuvre des cantons

Le plan de mise en œuvre par les cantons de la Stratégie nationale de protection de la Suisse contre les cyberrisques 2018-2022 (SNPC) a été élaboré par un groupe de travail du Réseau national de sécurité (RNS). Il est à la fois distinct et complémentaire du plan de mise en œuvre national. Il consiste en treize projets concernant sept des dix champs d'action de la SNPC. Les cantons manifestent par là la volonté d'améliorer encore, sous leur propre responsabilité et de leur propre initiative, la protection de leur population contre les cyberrisques.

1. Acquisition de compétences et de connaissances

(1) Développement d'un concept de formation continue et d'un module pour les administrations cantonales M2 Extension et encouragement des compétences	
Objectifs définis	Il est essentiel de développer de manière proactive les compétences en matière cyber de tous. Les administrations cantonales et les institutions qui y sont attachées constituent l'un des piliers du fonctionnement de notre société, à ce titre elles doivent impérativement être formées en la matière. Les services informatiques cantonaux ont pris la mesure de l'environnement dans lequel nous évoluons et veillent à engager les moyens techniques et organisationnels nécessaires au maintien d'espaces de travail sécurisés. Certaines initiatives ont déjà été prises afin de développer les compétences du personnel, mais ceci n'a à ce jour pas été réalisé de manière systématique, or il est indéniable que le facteur humain est un maillon essentiel de la sécurité de l'information.
Mise en œuvre (responsabilité)	Haute école de gestion Arc – Institut de lutte contre la criminalité économique (ILCE) en collaboration avec le Service informatique de l'Entité neuchâteloise, le Secrétariat d'État à la formation, à la recherche et à l'innovation SEFRI, la cellule de coordination SNPC, la Conférence suisse sur l'informatique (CSI)
Participation	Hautes écoles, Associations faîtières économiques, Associations professionnelles spécialisées (ASECE, Association suisse de la sécurité de l'information CLUSIS, etc.)
Instances et processus existants	Les mesures qui ont déjà été prises en la matière seront prises en compte et intégrées à la démarche s'il s'avère qu'il est pertinent de le faire.
Instruments	• Proposer un programme de formation destiné au personnel des administrations cantonales, définissant clairement et de manière pragmatique les buts à atteindre et les compétences visées ; • Assurer la pérennité du système de formation du personnel des administrations en matière cyber ; • Favoriser la propagation de cette formation à l'ensemble des administrations concernées en Suisse • La validation des contenus du programme de formation devrait idéalement être validée par la réalisation d'un pilote de formation présentiel qui pourrait être réalisé à Neuchâtel et ce, dès que le concept de formation est finalisé.

Objectifs mesurables (prestations)	• Rapport initial ; état des lieux • Concept de formation avec définition des objectifs en fonction des publics cibles • Programme complet de formation adapté à l'attention du personnel des autorités cantonales, visant les buts suivants : o Développer les compétences de base en matière cyber de l'ensemble du personnel ; o Donner à chacune et chacun les outils aptes à gérer de manières adéquate les flux d'information, en particulier ceux allant ou venant de l'extérieur des organisations ; o Permettre à toutes et à tous de mieux appréhender l'importance de l'information et par conséquent l'utilité des mesures visant à assurer les règles de base en matière de stockage, traitement et transfert d'informations ; o Octroyer à chaque employée, chaque employé les connaissances susceptibles d'en faire un prescripteur de bonnes pratiques en matière cyber dans son entourage privé et associatif. • Conception d'un outil didactique, par exemple dans un format e-Learning

2. Situation de la menace

(2) #MISP[4] – Malware Information Sharing Platform de MELANI pour et avec les cantons M4 Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace	
Objectifs définis	Pour améliorer leurs capacités de description et d'analyse des cyberrisques, les cantons établissent un radar des menaces exploitant les informations fournies par MELANI et y intègrent, si nécessaire, des indicateurs de menaces cantonales. Les cantons, en collaboration avec la Confédération, adoptent un vocabulaire (taxonomie) unique pour structurer et mieux représenter les cybermenaces en Suisse. De manière complémentaire, ils développent un cadre de collaboration opérationnelle pour mieux combattre les intrusions et les codes malveillants (virus) et incluant des services d'intelligence et de veille continue proactive des cybermenaces au niveau cantonal.
Mise en œuvre (responsabilité)	MELANI et les cantons
Participation	Hautes écoles, associations faîtières économiques, associations professionnelles spécialisées, acteurs privés spécialistes de cybersécurité.
Instances et processus existants	• Radar des cyber-menaces de MELANI ; • Plate-forme MISP (Malware Information Sharing Platform) de MELANI.

[4] MISP = Malware Information Sharing Platform est un logiciel permettant le partage d'informations sur les menaces cyber.

Instruments	En collaboration avec MELANI : 1. Adoption d'une taxonomie permettant de structurer et représenter les cyber-menaces de manières cohérente et homogène au sein de la Suisse (niveaux Confédération, cantons et communes) ; 2. Développement d'un modèle de radar cantonal des cyber-menaces ; 3. Mise en place d'un réseau suisse d'échange d'information sur les codes malveillants basé sur une solution MISP (Malware Information Sharing Platform); 4. Établissement d'un standard minimum pour détecter des vulnérabilités sur la périphérie des réseaux cantonaux exposée sur le web grâce à des scans périodiques de vulnérabilités[5] ; 5. Déploiement d'un processus de veille et d'analyse (OSINT - Open-source intelligence) simple, efficace et échangeable entre la Confédération et les cantons. Condition cadre : • Implication d'experts cantonaux en cybersécurité pour la mise en œuvre des mesures opérationnelles au sein des cantons.
Objectifs mesurables (prestations)	1. Une taxonomie unique décrivant les cyber-menaces est adoptée par la Confédération et les cantons ; 2. Les cantons disposent d'un radar actif de leurs cyber-menaces ; 3. Les cantons échangent activement des informations opérationnelles relatives aux codes malveillants ; 4. Les cantons évaluent périodiquement la sécurité de leurs points d'accès réseau périphériques exposés sur internet ; 5. Les cantons diffusent périodiquement des rapports de veille sur les cyber-menaces.

3. Gestion de la résilience

(3) Outil d'évaluation pour améliorer la résilience informatique dans les cantons M5 Amélioration de la résilience informatique des infrastructures critiques	
Objectifs définis	Pour améliorer leur résilience (capacité de résistance et de régénération), les cantons analysent les exigences minimales à satisfaire en matière de processus, de compétences et de tâches. Pour ce faire, ils utilisent notamment un outil d'évaluation conçu par l'Office fédéral pour l'approvisionnement économique du pays[6] et adapté à leurs besoins. Cet outil, qui propose des mesures pour améliorer la résilience informatique dans certains secteurs critiques, débouche sur une analyse permettant aux cantons d'élaborer des mesures complémentaires.
Mise en œuvre (responsabilité)	Chef suppléant de la sécurité de l'information (Deputy CISO) du canton de Bâle-Ville en collaboration avec le RNS
Participation	Chaque organisation et exploitant d'IC est responsable de sa propre sécurité de l'information. La direction, qui assume cette responsabilité,

[5] Vulnerability Scans sont possibles à travers des programmes informatiques conçu pour évaluer les vulnérabilités connues des ordinateurs, des réseaux ou des applications.

[6] Office fédéral pour l'approvisionnement économique du pays, Norme minimale pour les TIC, Berne, 2018, https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

	s'appuie sur divers interlocuteurs dans ce domaine : responsables de processus d'affaires, gestionnaires de risques, préposés à la sécurité de l'information, chefs de l'informatique, voire responsables de la gestion de crise.
Instances et processus existants	L'organisation met au point un plan de continuité d'activité (PCA) ou *business continuity management* (BCM) qui fait l'objet d'un contrôle externe. Les principales ressources considérées dans le PCA sont les suivantes : • personnel • sites, bâtiments et locaux • technologies de l'information et de la télécommunication (TIC) • fournisseurs et informations externes
Instruments	**Emploi de l'outil d'évaluation** À travers l'évaluation de sa propre résilience informatique, l'entreprise renforce son organisation de sécurité. Elle dispose ainsi d'une base claire pour répartir les responsabilités, les compétences et les tâches. Un indicateur permet de savoir rapidement si les mesures de sécurité préconisées sont réalisées, et dans quelle proportion. Si une faille est constatée, des mesures pour atténuer les risques peuvent être définies. **Tableau anonyme des organisations participantes** Les résultats de l'évaluation sont divisés en cinq fonctions définies (identifier, protéger, détecter, réagir et récupérer). Les organisations les communiquent au Réseau national de sécurité (RNS) pour qu'il les traite et les anonymise avant de les présenter sous forme anonymisée aux instances concernées. **PCA** Pour établir un PCA, il est nécessaire de documenter tous les processus d'affaires : gestion des risques, gestion de crise ou des situations d'urgence, gestion des situations d'urgence informatiques. La durée maximale d'une panne et les éventuels scénarios alternatifs font partie des informations importantes. Ces directives sont définies par les responsables des processus d'affaires et par la direction.
Objectifs mesurables (prestations)	Grâce à l'outil d'évaluation mis à leur disposition, les exploitants d'IC en Suisse ont identifié leurs failles et pris des mesures pour améliorer leur résilience informatique. Sont connus : • le degré de réalisation en % • le niveau de risque (faible, moyen ou important) • le risque maximal prévisible (indépendamment de toute donnée temporelle). L'évaluation a conduit les exploitants d'IC à appliquer des mesures ciblées pour améliorer leur résilience informatique. L'efficacité des mesures mises en œuvre fait l'objet de vérifications. Sont connues : • les mesures susceptibles d'être prises • les mesures en cours • les mesures appliquées. Les résultats ont été présentés dans certaines instances prédéfinies (Conférence suisse des chanceliers d'État, Conférence suisse sur l'informatique [CSI], etc.) sous forme anonymisée. Sont disponibles : • la liste des organisations concernées

	• la liste des présentations.

(4) Développement des échanges d'expériences à travers la Conférence suisse sur l'informatique (CSI) pour la création de bases communes M7 Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons	
Objectifs définis	En institutionnalisant les échanges d'expériences et le dialogue, les cantons favorisent leur collaboration en vue d'améliorer la résilience informatique. Pour ce faire, ils utilisent les réseaux existants et les optimisent si nécessaire. Ils participent activement au groupe de travail Sécurité informatique de la CSI. Ils renforcent leur confiance réciproque, se soutiennent mutuellement, coordonnent leurs procédures, en particulier en cas d'événement. Ils se dotent de bases de travail utiles (stratégies, listes de contrôle, etc.).
Mise en œuvre (responsabilité)	Groupe de travail Sécurité informatique de la CSI en collaboration avec les services gouvernementaux responsables dans les cantons et leurs préposés à la sécurité de l'information
Participation	RNS
Instances et processus existants	• Préposés cantonaux à la sécurité de l'information • Groupe de travail Sécurité informatique de la CSI
Instruments	• Stratégie informatique cantonale • Système cantonal de gestion des risques • Gestion cantonale des risques informatiques • Concept cantonal de formation • Système cantonal de gestion de la sécurité des informations
Objectifs mesurables (prestations)	• Les cantons s'assurent que leurs préposés à la sécurité de l'information participent au Groupe de travail Sécurité informatique de la CSI. ⇨ Les préposés cantonaux à la sécurité de l'information travaillent ensemble en toute confiance et veillent à la mise en œuvre, dans leur canton respectif, des recommandations du groupe de travail. • Les cantons s'assurent que, dans toutes les questions de sécurité de l'information et de cyberrisques, leurs collaborateurs et partenaires externes suivent des formations et des instructions régulières et adaptées aux besoins. ⇨ La liste de toutes les campagnes et formations effectuées est disponible. • **Les cantons ont mis en œuvre une gestion des risques informatiques** (en tant que partie intégrante de la gestion cantonale des risques) qui couvre les risques liés aux infrastructures critiques. ⇨ La gestion des risques informatiques est disponible et comprend une liste des mesures prises pour diminuer les risques.

	• Les cantons ont introduit un **système de gestion de la sécurité des informations** (SGSI) adapté à leur organisation. ⇨ Le SGSI est approuvé par la direction et dûment utilisé.

(5) Sensibilisation des jeunes et des aînés aux cyberrisques	
Objectifs définis	Cette mesure vise à renforcer la sensibilisation des jeunes et des aînés afin d'améliorer la résilience de la Suisse en matière de cyberrisques. Une conscience accrue des menaces dans le cyberespace conduit ces tranches d'âge à modifier leur comportement. Elles apprennent à profiter pleinement des possibilités du numérique tout en écartant les risques évitables. Grâce à un programme adapté à leur groupe-cible, les jeunes et les seniors enrichissent leurs connaissances dans le domaine numérique, en profitant des opportunités que celui-ci offre et en réduisant les risques qu'il comporte.
Mise en œuvre (responsabilité)	Conférence suisse des directeurs cantonaux de l'instruction publique en collaboration avec la Conférence des directrices et directeurs cantonaux des affaires sociales et la Prévention suisse de la criminalité (PSC)
Participation	pro senectute, pro juventute, privatim, RNS
Instances et processus existants	
Instruments	La sensibilisation aux cyberrisques dans le cyberespace peut passer par les enseignants pour les jeunes et par le personnel soignant pour les plus âgés.
Objectifs mesurables (prestations)	• Mise en place et consolidation d'un partenariat pour la sensibilisation des jeunes et des personnes d'un certain âge • Conception de contenus didactiques sur mesure

4. Normalisation et régulation

(6) Mise en œuvre de la politique de sécurité du réseau de la CSI M8 Définition et introduction de normes minimales	
Objectifs définis	Les cantons gèrent leurs réseaux et systèmes en toute sécurité. Ils placent des barrières de sécurité aussi solides que possible aux frontières extérieures des réseaux et assurent également une surveillance continue des activités au sein de leur propre réseau. Les cantons accroissent la sécurité au sein de leurs réseaux et applications partenaires sur cette base commune. • Encouragement de la collaboration dans le respect des normes prédéfinies • Consolidation de la confiance réciproque grâce aux normes définies • Mise à disposition de documentation utile (stratégies, listes de contrôle, etc.) • Classement sûr et adapté des documents
Mise en œuvre (responsabilité)	Conférence des gouvernements cantonaux
Participation	Conférence suisse sur l'informatique (CSI)
Instances et processus existants	• Groupe de travail Sécurité informatique de la CSI • Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération (MELANI)
Instruments	• Politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017) • Autres normes de même type • Processus appropriés (gestion des changements, des problèmes, des incidents, des risques et des crises) • Autres normes ou recommandations (ISO 2700x, BSI, SANS CSC, CIS 20, etc.)
Objectifs mesurables (prestations)	• Mise en œuvre par les cantons de leur propre politique de sécurité des réseaux (sur la base de celle établie par la CSI en 2017)7 • Normes définies et appliquées • Formation du personnel • Définition des processus (gestion des changements, des problèmes, des incidents, des risques et des crises et rapports sur ces sujets)

[7] La politique de sécurité des réseaux établie par la Conférence suisse sur l'informatique (CSI) est disponible sur Intranet pour tous les membres de la CSI.

5. Gestion des crises

(7) Cyberexercice avec des infrastructures critiques (IC) dans le secteur de la santé M17 Exercices communs de gestion de crise	
Objectifs définis	En cas de crise, la coordination opérationnelle entre la Confédération, les cantons et des exploitants d'IC fonctionne et les services concernés disposent d'une image de la situation actualisée. La stratégie de conduite a pu être testée dans le cas d'une crise comportant des aspects cyber.
Mise en œuvre (responsabilité)	RNS
Participation	Chancellerie fédérale, Conférence suisse des directrices et des directeurs cantonaux de la santé
Instances et processus existants	Gestion générale de la crise (procédures et processus de conduite) des cantons et de la Confédération indépendamment du scénario de l'ERNS19
Instruments	Concept M15 SNPC I élargi aux cantons et aux IC
Objectifs mesurables (prestations)	• Nombre d'exercices effectués en collaboration avec toutes les organisations concernées (un table top exercise d'ici 2020, un exercice-cadre d'état-major d'ici 2021) • Image précise et actuelle de la situation disponible à tout moment pendant tout l'exercice, considérée comme adéquate par tous les protagonistes (lors de l'évaluation) • Soutien des états-majors aux protagonistes sous forme de connaissances spécifiques (évaluation des expériences des protagonistes lors de l'exercice ; enquête) • Responsabilités et interlocuteurs connus des participants • Processus connus des participants • Évaluation des exercices et optimisation des déroulements et des processus de conduite en fonction des leçons tirées ; mise en place d'un plan de suivi (monitoring) ; compte rendu des résultats

(8) Création d'organisations cantonales pour la cybersécurité	
Objectifs définis	Cette mesure a pour but de créer dans chaque canton une organisation chargée de la cybersécurité sur le modèle de la nouvelle structure d'organisation mise en place dans le domaine cyber à l'échelle de la Confédération. Ce service cantonal, qui détient la souveraineté budgétaire et a la compétence d'édicter des directives, suit la situation au plus près, représente le canton pour toutes les questions du domaine cyber, siège à l'état-major de conduite cantonal et assure la coordination au sein du canton, entre les cantons et avec la Confédération.
Mise en œuvre (responsabilité)	Département cantonal compétent
Participation	Préposés cantonaux à la sécurité de l'information, états-majors de conduite cantonaux, polices cantonales, ministères publics, exploitants d'IC, RNS, délégué de la Confédération à la cybersécurité

Instances et processus existants	Avec son groupe de travail (GT) chargé de concrétiser la SNPC II, le RNS élabore un projet avec les cantons destiné à leur servir de ligne directrice et de base pour créer leur propre organisation cantonale pour la cybersécurité.
Instruments	
Objectifs mesurables (prestations)	• Ligne directrice et base de travail mise au point avec le GT du RNS • Comparaison effectuée dans chaque canton entre la situation réelle et la situation visée • Élaboration de stratégies cantonales dans le domaine cyber définissant tâches, compétences et responsabilités • Décision des exécutifs cantonaux quant à la création d'une organisation cantonale pour la cybersécurité

6. Visibilité et sensibilisation

(9) Communication active sur les activités des cantons dans le cadre de la SNPC II M28 Élaboration et mise en œuvre d'un concept de communication pour la SNPC	
Objectifs définis	La population intéressée en général et les partenaires du RNS en particulier peuvent s'informer à travers différents canaux sur les travaux des cantons en faveur de la SNPC II. La communication avec la population et les médias est conçue de manière active et dynamique par groupe cible. Les acteurs concernés attachent particulièrement d'importance à la collaboration entre cantons au niveau gouvernemental mais en appellent aussi à la responsabilité individuelle. Un concept de communication a été élaboré et appliqué.
Mise en œuvre (responsabilité)	RNS
Participation	CSI, CCDJP
Instances et processus existants	
Instruments	• Cyberlandsgemeinde • Site Internet du RNS • Rapports annuels sur la mise en œuvre de projets du plan • Communiqués de presse
Objectifs mesurables (prestations)	• Un concept de communication (directives, compétences, processus) existe et est appliqué. • Divers produits de communication ont été mis, en temps voulu, à disposition de la population intéressée et des partenaires du RNS à travers différents canaux (nombre de produits de communication publiés, écho, portée) • Enquête sur la notoriété