Stratégie nationale de protection de la Suisse contre les cyberrisques 2018–2022

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Impressum

Éditeur
Unité de pilotage informatique de la Confédération UPIC
Schwarztorstrasse 59
CH-3003 Berne

info@isb.admin.ch
www.upic.admin.ch
intranet.upic.admin.ch

1 Introduction

La numérisation ne cesse de se développer en Suisse. La société, l'économie et l'État sont d'ores et déjà marqués par l'existence de multiples réseaux numériques et les progrès technologiques rapides sont appelés à stimuler encore davantage cette évolution. Ce processus offre de grandes chances, et la Suisse est décidée à en tirer profit pour garantir et accroître à long terme la prospérité dans notre pays.
Cependant, il convient de relever que le numérique présente non seulement des chances, mais aussi des risques. La dépendance croissante qu'il entraîne vis-à-vis des technologies de l'information et de la communication rend notre pays plus vulnérable aux pannes, aux perturbations et aux abus de ces technologies.
Il suffit d'observer l'évolution des menaces dans le cyberespace pour se rendre compte de cette vulnérabilité. La cybercriminalité, l'accumulation des cas d'espionnage à l'aide de cyberattaques, le cybersabotage d'infrastructures critiques telles que les hôpitaux ou les fournisseurs d'énergie, la diffusion d'informations volées ou manipulées à des fins de désinformation ou de propagande ainsi que l'augmentation des formes de conflits hybrides recourant à des cyberattaques pour déstabiliser des États et des sociétés montrent clairement la diversité de ces menaces et la rapidité avec laquelle elles se développent.
La dépendance accrue vis-à-vis du bon fonctionnement de l'informatique, conjuguée à l'intensification des menaces, oblige impérativement à tenir compte des risques qui en découlent (appelés cyberrisques) pour le développement de la société numérique. Sur le plan de la politique de sécurité, des mesures doivent être prises afin de préserver l'indépendance et la sécurité du pays face à l'apparition ou l'aggravation des menaces et des risques présentés par le cyberespace. Par ailleurs, sur le plan de la politique économique et sociale, la Suisse doit se protéger contre les cyberrisques pour pouvoir profiter de manière cohérente des chances de la révolution numérique et conserver les avantages compétitifs liés à sa sécurité. Il n'est toutefois pas possible d'assurer une protection exhaustive contre les cyberrisques par des mesures proportionnées. C'est pourquoi la Suisse doit accroître sa résilience en cas de cyberincidents.
La présente stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) indique comment atteindre ces objectifs d'ici à 2022. Elle s'appuie sur la première SNPC mise en œuvre de 2012 à 2017, la développe en fonction des vulnérabilités de la Suisse, de la modification et de l'intensification des menaces depuis 2012 et de leur extension prévisible au cours des prochaines années, et la complète par d'autres mesures. Elle constitue ainsi le cadre stratégique de l'amélioration de la prévention, du dépistage précoce, de la réaction et de la résilience dans tous les domaines pertinents pour les cyberrisques.
La protection contre les cyberrisques est du ressort conjoint des milieux économiques, de la société et de l'État. Cela signifie tout d'abord que tous les acteurs doivent répondre de leur propre protection. La SNPC soutient et coordonne ces efforts de protection individuels. Par ailleurs, elle formule des mesures supplémentaires là où les cyberrisques ont des répercussions essentielles sur le développement et le bien-être de notre société. L'application collective de la SNPC découle également de cette responsabilité conjointe. La Confédération, les cantons, les milieux économiques et la société sont appelés à appliquer les mesures de la SNPC en étroite coopération les uns avec les autres et dans les limites de leurs compétences respectives.
Les défis posés par la gestion des cyberrisques sont considérables et ne vont pas perdre en virulence. Il est donc d'autant plus important que tous les acteurs les relèvent ensemble et de manière coordonnée. Une collaboration aussi efficace que possible entre toutes les instances compétentes ainsi que la constitution systématique de réseaux internationaux sont des éléments décisifs pour créer un environnement sûr permettant d'introduire le numérique dans la société et dans l'économie. La SNPC 2018-2022, élaborée en commun par la Confédération, les cantons et les milieux économiques, vise à servir à cet égard d'instructions opérationnelles et d'aide à l'orientation. Le plan de mise en œuvre qui fait partie de la stratégie

définit les compétences et les responsabilités concernant la mise en œuvre des mesures retenues dans la stratégie.

2 État des lieux

Le premier pas vers une protection efficace de la Suisse contre les cyberrisques consiste à faire une estimation de la situation actuelle et future en matière de menaces. Il ne s'agit pas de calculer avec précision les risques pour la Suisse, mais d'apprécier l'importance stratégique des diverses menaces et de prévoir les tendances probables de leur évolution.
Outre la situation en matière de menaces, un autre facteur essentiel de l'état des lieux est le niveau actuel de la protection de la Suisse contre les cyberrisques. Les actions requises découleront de la confrontation entre la situation en matière de menaces et l'évolution future de celles-ci et le dispositif existant pour protéger la Suisse contre les cyberrisques.

2.1 Cybermenaces

C'est en décrivant les principales menaces pour la Suisse que l'on peut établir clairement d'où viennent les cyberrisques. Ce faisant, il convient de relever que les menaces évoluent de façon très dynamique. Les principaux moteurs en sont le numérique, qui rend notre société et notre économie de plus en plus vulnérables aux perturbations et aux pannes des systèmes informatiques, ainsi que le professionnalisme dont font preuve les auteurs des attaques et l'extension des luttes d'influence dans le cyberespace. Comme tout porte à croire que ces tendances vont se poursuivre, il faut s'attendre à ce que les menaces s'intensifient encore davantage.
Pour apprécier la situation, il est important de différencier les menaces dues à des actes illicites délibérés (cyberattaques) et les dangers dus à des événements provoqués de façon non intentionnelle (erreurs humaines et pannes techniques). Ces deux catégories seront donc décrites dans des sections distinctes.

2.1.1 Cyberattaques

On a observé ces dernières années une forte augmentation des menaces dues aux cyberattaques. En Suisse et à l'étranger, des attaques réussies, aux conséquences parfois graves, ont montré que non seulement la fréquence et la complexité des cyberattaques augmentaient, mais encore que celles-ci étaient de plus en plus dirigées contre des États ou des entreprises.
Pour apprécier la situation, il est important, vu la diversité des cyberattaques possibles, d'établir une distinction entre plusieurs phénomènes, en fonction du but poursuivi par les attaques, des acteurs impliqués et des cibles visées. Sur cette base, il est possible de distinguer cinq types de cyberattaques, étant entendu que celles-ci sont souvent combinées et présentent également des chevauchements.

Cybercriminalité: Au sens étroit, la cybercriminalité regroupe les infractions qui ne sont possibles que grâce à l'informatique, car elles sont commises à l'aide d'outils informatiques ou exploitent les vulnérabilités de ceux-ci. Au sens large, la cybercriminalité regroupe aussi les infractions qui auraient pu être commises sans recourir à des outils informatiques, mais pour lesquelles ces derniers ont été utilisés comme moyens d'action ou supports de stockage. L'enrichissement est le but premier de ces activités, ce qui n'est pas le cas pour les menaces décrites ci-après. Le cyberespace convient bien à ce genre d'activités, car celles-ci présentent un risque faible pour les auteurs, mais une possibilité de gains importants en raison du grand nombre de victimes faciles à atteindre. Il n'est donc pas étonnant que la cybercriminalité ait fortement progressé ces dernières années. Elle affecte de la même manière les entreprises, les autorités et la population, et constitue la menace dont la probabilité de réalisation

est la plus élevée. Comme le but véritable des auteurs de ces attaques n'est pas de compromettre le fonctionnement de la société, de l'économie ou de l'État, les effets immédiats se limitent souvent aux victimes concernées. Néanmoins, les cybercriminels acceptent d'importants dommages collatéraux, voire utilisent leur connaissance de ces répercussions pour faire chanter les victimes et leur soutirer de plus fortes sommes. C'est la raison pour laquelle les attaques lancées par des cybercriminels présentent un potentiel de nuisance élevé pour l'ensemble de la société et de l'économie.
Dans le sillage de la cybercriminalité, on voit apparaître de véritables secteurs d'activité qui permettent de gagner beaucoup d'argent. En raison de la grande concurrence, mais aussi de la remise à niveau constante des mesures de défense, les criminels sont soumis à une forte pression à l'innovation, si bien qu'ils ne cessent de développer de nouvelles méthodes. En conséquence, il faut s'attendre à ce que la fréquence et la spécialisation des activités criminelles dans le cyberespace continuent à augmenter.

Cyberespionnage: Le cyberespionnage est une activité visant à obtenir des informations de manière non autorisée à des fins politiques, militaires ou économiques. Elle est pratiquée par des acteurs étatiques aussi bien que non étatiques. Ses auteurs se concentrent à la fois sur des entreprises et sur des institutions étatiques, sociales ou internationales. L'économie suisse est l'une des plus innovantes au monde, et de nombreux groupes internationaux y possèdent leur siège ou de grands centres de données. En outre, la Suisse héberge de nombreuses organisations internationales et accueille souvent des négociations internationales. Cela fait de notre pays une cible attrayante pour le cyberespionnage, dont les conséquences peuvent être très variables selon la nature et l'étendue des données que les auteurs des attaques peuvent se procurer. En général, ces conséquences ne sont pas immédiatement visibles, car les préjudices politiques et économiques n'apparaissent qu'au moment où les auteurs des attaques mettent à profit les connaissances qu'ils ont acquises.
Le cyberespionnage va continuer à gagner en attractivité, car il constitue un moyen efficace de se procurer des informations. Ses auteurs ont élaboré des méthodes pour rester indétectables le plus longtemps possible après avoir pénétré dans des réseaux. Comme la Suisse est largement tributaire de fabricants étrangers sur le plan informatique, le risque demeure que ces fabricants, en collaboration avec les services de renseignements de leurs pays, laissent délibérément ouvertes des failles de sécurité à des fins d'espionnage.

Cybersabotage et cyberterrorisme: Le cybersabotage désigne une activité destinée à perturber ou à détruire le fonctionnement de l'informatique, ce qui peut également avoir des conséquences physiques en fonction de la nature du sabotage et de la cible attaquée. La motivation de tels actes peut être très variable. Ainsi, il est possible que des collaborateurs frustrés décident de saboter les systèmes informatiques d'une organisation. On parle de cyberterrorisme lorsque l'acte de sabotage est commis à des fins terroristes. Le cybersabotage et le cyberterrorisme ont pour but non seulement de provoquer des dégâts aussi importants que possible, mais aussi de faire une démonstration de force avec l'intention de déstabiliser une organisation, voire l'ensemble de la société. Alors que, sur le plan international, divers actes de sabotage ont été commis, portant notamment sur l'approvisionnement des États en énergie, la Suisse n'a été confrontée à aucun cas de grande envergure à ce jour. Mais si la Suisse ou des organisations situées en Suisse ou opérant depuis notre pays se retrouvaient, pour des raisons politiques, dans le viseur d'acteurs étatiques ou non étatiques suffisamment compétents, la probabilité de tels actes augmenterait fortement. Les préjudices correspondants pourraient être considérables.
La pertinence de cette menace continuera à croître avec les progrès de la numérisation de la société et de l'économie. La croissance des réseaux numériques d'appareils physiques par le biais de l'Internet des objets permet également de nouvelles formes de manipulation, ayant à leur tour des incidences directes sur l'environnement physique.

Désinformation et propagande: La menace due à la diffusion ciblée d'informations erronées ou obtenues illégalement par des cyberattaques dans le but de discréditer des acteurs politiques, militaires ou civils a beaucoup gagné en importance. Dans divers pays, on a observé des activités de ce genre avant des élections importantes. En Suisse aussi, il faut s'attendre à ce que des acteurs étatiques ou non étatiques essaient de saper la confiance des citoyens dans l'État et dans les institutions.

Comme l'importance des réseaux sociaux en tant que source d'informations continue à progresser, il est là aussi possible de supposer que ces canaux seront utilisés à des fins de propagande, avec un mélange de fausses informations, d'arguments politiques et d'informations volées qu'il est très difficile de démêler.

Cyberconflits: Si le scénario d'une guerre menée exclusivement dans le cyberespace (cyberguerre) est actuellement considéré comme peu réaliste, il est avéré en revanche que des cyberattaques de toutes sortes sont utilisées comme des moyens de guerre dans divers conflits. En règle générale, il s'agit de conflits hybrides qui font appel à des moyens militaires, mais aussi politiques, économiques et criminels. Un objectif des conflits hybrides est de dissimuler les responsabilités dans le cadre d'un conflit. Les cyberattaques sont un instrument adéquat pour cela, car elles sont difficiles à attribuer clairement à un auteur, sont relativement peu coûteuses, ont un effet immédiat, sont utilisables sans limitations de distances et permettent d'avoir un impact politico-militaire tout en restant sous le seuil d'une guerre déclarée officiellement.

Les investissements considérables effectués par de nombreux États pour se protéger et se défendre activement contre les cybermenaces soulignent l'importance des cybermoyens dans le cadre de conflits. En conséquence, il y a lieu de s'attendre à ce que l'importance des cyberattaques ciblées à des fins stratégiques continue à s'accroître. La Suisse doit donc faire appel à la cyberdéfense et à la cyberdiplomatie pour se prémunir contre ces activités et se préparer aux conflits.

2.1.2 Erreurs humaines et défaillances techniques

Outre les cyberattaques ciblées et délibérées, il est également possible que des actes involontaires ou des événements liés aux conditions naturelles et techniques provoquent des dégâts touchant le cyberespace ou l'environnement physique. Ceux-ci sont dus à des erreurs humaines dans la préparation et l'utilisation de l'informatique (p. ex. utilisation inappropriée ou négligente des systèmes informatiques, mauvaises administration ou configuration, perte de supports de données, etc.) ou à des défaillances techniques dont les causes peuvent être multiples (par ex. vieillissement des infrastructures, phénomènes naturels, surcharge, défaut de conception ou entretien insuffisant). De tels événements d'ampleur variable surviennent fréquemment et font partie du quotidien des départements informatiques des entreprises et des pouvoirs publics. En conséquence, les répercussions de ces erreurs et de ces défaillances sont généralement faciles à maîtriser. Néanmoins, l'expérience montre que derrière bon nombre de ces cyberincidents se cachent non pas des attaques ciblées, mais un enchaînement de diverses circonstances, telles qu'erreurs humaines ou pannes techniques, liées à une préparation insuffisante. Il est donc essentiel de ne pas négliger les mesures de prévention contre de tels événements lors la planification et de la mise en œuvre des mesures de protection.

Les cyberrisques dus aux erreurs humaines ou aux défaillances techniques resteront très importants. En outre, la complexité croissante due à la mise en réseau des domaines les plus divers permet mal d'apprécier et de délimiter les conséquences de ces événements involontaires. Une bonne préparation et une planification soigneuse vis-à-vis de tels incidents restent donc des éléments centraux de la gestion des cyberrisques.

2.2 État de la protection de la Suisse contre les cyberrisques

Les travaux effectués jusqu'ici reposaient sur la première SNPC, décidée en 2012 et mise en œuvre jusqu'à la fin de 2017. Il convient cependant aussi de tenir compte du contexte stratégique de la SNPC. Diverses stratégies de la Confédération ont une incidence directe sur la manière dont la Suisse se protège contre les cyberrisques et ont ainsi fixé le cadre de la suite des travaux.

2.2.1 Stratégie nationale de protection de la Suisse contre les cyberrisques 2012-2017

La première SNPC comportait 16 mesures, qui ont été réalisées de manière décentralisée par les diverses unités administratives compétentes de l'administration fédérale, en collaboration avec des associations et des exploitants d'infrastructurescritiques . Dans le détail, les résultats de la SNPC sont décrits dans le rapport d'évaluation de l'efficacité des mesures mises en œuvre[1]. Pour apprécier le point de départ de la SNPC 2018-2022, il est important de rappeler les objectifs suivants atteints jusqu'à présent:

- **Acquisition de capacités, de compétences et de connaissances:** Un objectif central de la SNPC était l'acquisition de capacités, de compétences et de connaissances dans les organisations compétentes. Il a été constaté en 2012 que les ressources nécessaires et les connaissances professionnelles faisaient défaut dans de nombreux domaines. Cette situation s'est améliorée grâce à la mise en œuvre des mesures SPNC.
- **Mise en place de processus, de structures et de bases:** Du fait que les cyberrisques concernent de nombreux acteurs différents, il était essentiel d'organiser la collaboration entre les diverses instances, d'attribuer les compétences et d'élaborer les bases. Les processus, structures et bases prévus ont été mis en place et il convient désormais de les utiliser et de les perfectionner en permanence.
- **Accent mis sur la protection des infrastructures critiques:** Les mesures de la SNPC se rapportaient en premier lieu à la protection des infrastructures critiques. Pour les secteurs partiels critiques, des analyses des risques et des vulnérabilités ont été réalisées, des mesures ont été identifiées, le soutien en cas d'incidents a été consolidé et un tableau de la situation en matière de cybermenaces a été dressé. Ces travaux, qui ont constitué le cœur de la SNPC, peuvent désormais être approfondis et consolidés.
- **Renforcement de la collaboration avec des tiers:** Outre l'amélioration de la coordination à l'intérieur de l'administration, la collaboration avec d'autres partenaires est également importante. La SNPC a intensifié la collaboration avec les cantons, les milieux économiques et divers partenaires internationaux. L'établissement de ces coopérations a permis de renforcer la confiance mutuelle et d'encourager l'échange d'informations. Il existe ainsi une base solide pour approfondir et étendre davantage la collaboration à tous les niveaux.

2.2.2 Contexte stratégique

Diverses stratégies de la Confédération fixent des lignes directrices qui sont déterminantes pour la thématique des cyberrisques. Elles constituent le contexte stratégique pour la protection de la Suisse contre les cyberrisques. Ces stratégies fondamentales sont les suivantes:

- **Rapport du Conseil fédéral sur la politique de sécurité de la Suisse:** Dans son rapport de 2016 sur la politique de sécurité, le Conseil fédéral définit l'orientation stratégique fondamentale de la politique de sécurité de la Suisse. Ce rapport explique l'importance élevée et croissante des cybermenaces pour la politique de sécurité et définit des notions importantes en liaison avec ce sujet. Il renvoie à la SNPC en tant que base pour la protection de la Suisse contre les cyberrisques et souligne qu'une place encore plus grande doit être réservée à l'avenir à la protection des systèmes et infrastructures informatiques dans la politique de sécurité.
- **Stratégie du Conseil fédéral pour une Suisse numérique:** Cette stratégie indique comment la Suisse se propose de profiter des chances offertes par le numérique. Un des objectifs stratégiques majeurs consiste à créer la transparence et la sécurité pour que les

[1] https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie-2012/wirksamkeitsueberpruefung.html

habitants de la Suisse soient en mesure d'exercer leur droit à l'autodétermination en matière d'information. Cela présuppose que l'État assume sa mission de protection de la société et de l'économie également à l'ère du numérique. En outre, la stratégie et le plan d'action y afférent fixent les objectifs et les mesures permettant de positionner la Suisse dans le contexte international sur les questions de numérique et sur les processus de transformation qui s'y rapportent. Dans le domaine de la cybersécurité, ces résultats doivent notamment être atteints par la mise en œuvre de la SNPC.

- **Stratégie nationale de protection des infrastructures critiques:** Cette stratégie définit la notion d'infrastructures critiqueset détermine les secteurs et parties de secteurs considérés comme critiques en Suisse. Elle contient des mesures visant à améliorer la résilience de la Suisse sur le plan des infrastructures critiques. La SNPC couvre à cet égard tous les risques encourus par les infrastructures critiques dans le cyberespace.

2.3 Action requise: perfectionner la SNPC

Les objectifs atteints par la première SNPC et le contexte stratégique constituent la base de la suite des actions à entreprendre. La comparaison entre la situation actuelle en matière de menace et son évolution attendue et le dispositif actuel de protection de la Suisse contre les cyberrisques montre cependant clairement qu'il ne suffit pas de préserver le statu quo pour garantir un niveau de protection suffisant. Il est nécessaire d'agir à plusieurs niveaux. D'une part, il s'agit de continuer à étendre les capacités et les compétences existantes et d'utiliser les processus, les structures et les bases créés pour mettre en œuvre des mesures. Mais d'autre part, des adaptations stratégiques sont également nécessaires. La SNPC doit présenter une plus grande efficacité en tant que stratégie nationale au-delà de l'administration fédérale et des infrastructures critiques afin de tenir compte du fait que les cybermenaces affectent l'ensemble de l'économie, de la société et de la politique. Pour cela, les groupes cibles de la SNPC doivent être étendus en conséquence et la collaboration existante doit être développée de telle manière à créer un réseau de protection contre les cyberrisques. Enfin, la structure d'organisation décentralisée doit également être complétée par un pilotage stratégique plus ferme ainsi que par un point de contact unique pour le public, afin que vu la forte dynamique des cyberrisques, il soit possible de réagir à tout moment aux évolutions nouvelles et que la SNPC soit perçue plus clairement dans le public et dans les milieux politiques.

Le tableau 1 récapitule les actions requises.

Niveau	SNPC 2012-2017	Actions requises
Capacités, compétences et connaissances	Amélioration des capacités et meilleures connaissances par rapport à 2012	La poursuite de la consolidation des capacités et des connaissances est nécessaire pour répondre à l'intensification des menaces.
Objectifs des mesures de la SNPC	Élaboration des processus, des structures et des bases	Appliquer les processus, structures et bases pour réduire les cyberrisques. Les mesures et produits conçus doivent être mis en œuvre, développés et complétés si nécessaire.
Structure d'organisation	Mise en œuvre assurée de manière décentralisée par les instances compétentes	La pertinence politique, économique et sociale accrue et le développement rapide des cyberrisques nécessitent un pilotage stratégique plus ferme de la SNPC. La structure d'organisation décentralisée doit être complétée dans ce sens.
Groupe cible	Accent mis sur la protection des infrastructures critiques contre les cyberrisques	Les cybermenaces affectent toute la Suisse, de sorte que le groupe cible de la SNPC doit être élargi.
Collaboration	Établissement de la collaboration avec les cantons, les milieux économiques et les partenaires internationaux	L'existence croissante de réseaux renforce l'importance de la collaboration à tous les niveaux. Les coopérations et les partenariats public-privé existants doivent être renforcés et reliés de manière à créer un réseau de protection de la Suisse contre les cyberrisques.

La deuxième SNPC doit poursuivre les travaux de la première, les étendre si nécessaire et les compléter par de nouvelles mesures. De même, elle doit garantir la continuité des travaux de la première SNPC et veiller à ce que ses objectifs, ses principes, des champs d'action et ses mesures tiennent compte des évolutions intervenues depuis 2012 et anticipent autant que possible les tendances futures.

3 Orientation stratégique de la SNPC 2018-2022

L'orientation stratégique de la SNPC 2018-2022 découle des champs d'action identifiés. La vision et les objectifs stratégiques prescrivent ce qui doit être atteint durant cette période, les principes stratégiques décrivent comment procéder et la section «groupes cibles» définit à quels destinataires la stratégie s'adresse.

3.1 Vision et objectifs stratégiques

Du fait que les cyberrisques touchent simultanément divers domaines de l'économie, de la politique et de la société, des mesures doivent être prises dans différents domaines. Pour que la stratégie reste cohérente malgré sa diversité, il est décisif de poursuivre une vision commune et de formuler des objectifs stratégiques supérieurs.

Vision de la SNPC 2018-2022

«Tout en utilisant les chances offertes par le numérique, la Suisse est protégée de façon appropriée contre les cyberrisques et est résiliente en cas de cyberincidents. La capacité d'agir et l'intégrité de sa population, de l'économie et de l'État face aux cybermenaces sont garanties.»

Objectifs stratégiques:

Cette vision ne pourra être réalisée que lorsque les sept objectifs stratégiques de la SNPC 2018-2022 auront été atteints:

- La Suisse dispose des compétences, des connaissances et des capacités pour repérer à temps et évaluer les cyberrisques.
- La Suisse élabore des mesures efficaces pour réduire les cyberrisques et les met en œuvre dans le cadre de la prévention.
- La Suisse dispose dans toutes les situations des capacités et des structures d'organisation requises pour repérer rapidement les cyberincidents et les gérer, même si ceux-ci durent un certain temps et concernent plusieurs domaines en même temps.
- La résilience informatique de la Suisse est assurée. La capacité des infrastructures critiques de mettre à disposition des biens et des services importants demeure garantie même en cas de cyberincidents de grande ampleur.
- La protection de la Suisse contre les cyberrisques est perçue comme une tâche commune de la société, des milieux économiques et de l'État; les responsabilités et compétences respectives sont clairement définies et sont assumées par toutes les parties prenantes.
- La Suisse s'engage en faveur de la coopération internationale pour accroître la cybersécurité. Elle encourage le dialogue dans le cadre de la politique extérieure de cybersécurité, participe activement aux instances internationales spécialisées et entretient des échanges avec d'autres États et organisations internationales.
- La Suisse tire des leçons des cyberincidents survenus en Suisse et à l'étranger. Ceux-ci sont soigneusement analysés et des mesures correspondantes sont prises sur la base des constats dressés.

3.2 Principes

La vision et les objectifs stratégiques prescrivent *ce que* la SNPC 2018-2022 se propose d'atteindre. Les principes définissent *de quelle manière* il convient de procéder.

- La SNPC s'appuie sur une **approche exhaustive basée sur les risques**, qui a pour but d'améliorer la résilience de la Suisse en matière de cyberrisques. Cela implique l'hypothèse qu'aucune protection intégrale contre les cyberrisques n'est possible, mais que les risques peuvent être traités de manière à ce que le risque résiduel soit tolérable. Dans une approche exhaustive, toutes les vulnérabilités pertinentes et toutes les menaces sont prises en compte.
- La cybersécurité concerne quasiment tous les domaines de la vie, de l'économie et de l'administration. Tous doivent agir et assumer ensemble la responsabilité de la protection de la Suisse contre les cyberrisques. La SNPC renforce cette responsabilité commune en demandant des efforts aux acteurs ayant les compétences requises et en utilisant les structures existantes. Il en découle une **mise en œuvre décentralisée**, mais pilotée de façon centrale par la direction stratégique de la SNPC et présentant une répartition claire des tâches et des rôles.
- La SNPC s'appuie sur une approche accordant un **rôle subsidiaire à l'État**, ce qui signifie que l'État n'intervient que lorsque le bien-être de notre société est sensiblement touché et que les acteurs privés ne sont pas capables ou désireux de résoudre le problème eux-mêmes. Dans ce cas, l'État peut agir à titre de soutien, fixer des incitations ou intervenir sur un plan réglementaire.
- La SNPC poursuit une approche coopérative. Elle renforce et coordonne au niveau national le **partenariat public-privé** existant, encourage d'autres coopérations public-privé et consolide la coopération entre Confédération, cantons et communes.

- Au niveau international, la SNPC encourage la **collaboration avec des partenaires internationaux**.
- La SNPC est mise en œuvre de manière transparente dans la mesure où cela ne porte pas atteinte à l'efficacité des mesures. Ce résultat est obtenu par le biais d'une **communication active de la SNPC** vis-à-vis de la société ainsi que des milieux économiques et politiques.

3.3 Groupes cibles

La Confédération s'engage à appliquer les mesures définies dans la SNPC en collaboration avec les cantons, les entreprises et la société. L'effet recherché par la SNPC concerne ainsi toute la Suisse. La SNPC s'adresse aux groupes cibles suivants:

- **Infrastructures critiques:** Le groupe cible principal de la SNPC est celui des exploitants d'infrastructures critiques. Ceux-ci garantissent la disponibilité des biens et services essentiels. C'est pourquoi leur fonctionnement est indispensable pour la population et pour les milieux économiques suisses. Leur protection a la priorité maximale et est le point de mire de toutes les mesures de la SNPC.
- **Autorités:** Parmi les infrastructures critiquesfigurent également les services des administrations et des autorités. Leur protection relève de la responsabilité directe de la Confédération, des cantons et des communes.
- **Population:** La protection de la population est, en définitive, le but de toutes les mesures de la SNPC (par exemple la protection contre les défaillances d'infrastructures critiques). Mais elle est notamment au centre des efforts de lutte contre la cybercriminalité. Par ailleurs, la SNPC contribue, par une information transparente, à ce que la population bénéficie d'une gestion de l'informatique sûre, informée et fiable.
- **Économie:** Pour l'économie, un contexte sûr et fiable constitue une base importante et un facteur de compétitivité. Les cyberrisques posent de grands défis non seulement aux infrastructures critiques, mais aussi à toutes les autres entreprises et en particulier aux PME. La SNPC crée des conditions aussi sûres que possible pour les entreprises de Suisse et met à leur disposition un soutien ciblé pour la gestion des cyberrisques, subsidiairement aux offres du marché.

4 Champs d'action et mesures de la SNPC 2018-2022

Pour que les objectifs stratégiques soient atteints, des mesures doivent être appliquées dans des domaines très différents. La SNPC distingue dix champs d'action qui abordent divers aspects partiels des cyberrisques. Un total de 29 mesures est formulé dans ces champs d'action.

Le tableau 2 dresse la liste des champs d'action et des mesures de la SNPC 2018-2022:

Champ d'action	Mesures
Acquisition de compétences et de connaissances	1. Détection précoce des tendances ou technologies et acquisition des connaissances utiles 2. Extension et encouragement des compétences en matière de recherche et de formation 3. Création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité
Situation de la menace	4. Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace
Gestion de la résilience	5. Amélioration de la résilience informatique des infrastructures d'importance vitale 6. Amélioration de la résilience informatique dans l'administration fédérale 7. Échange d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons
Normalisation et réglementation	8. Définition et introduction de normes minimales 9. Examen d'une obligation de notifier les cyberincidents et décision quant à son introduction 10. Gouvernance mondiale d'Internet 11. Acquisition d'expertise sur les questions de normalisation dans le domaine de la cybersécurité
Gestion des incidents	12. Développement de MELANI en tant que partenariat public-privé pour les exploitants d'infrastructures critiques 13. Offre de services destinés à toutes les entreprises 14. Collaboration ciblée entre la Confédération et d'autres services ou centres de compétences 15. Processus et bases de la gestion des incidents au sein de l'administration fédérale
Gestion des crises	16. Intégration du service spécialisé compétent du domaine cybersécurité dans les états-majors de crise de la Confédération 17. Exercices communs de gestion de crise
Poursuite pénale	18. Tableau de la situation en matière de cybercriminalité 19. Réseau de soutien aux enquêtes relatives à la cybercriminalité 20. Formation à la lutte contre la cybercriminalité 21. Office central de lutte contre la cybercriminalité
Cyberdéfense	22. Développement des capacités d'acquisition d'information et d'attribution 23. Capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM 24. Garantie de la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et réglementation de son rôle subsidiaire consistant à appuyer les autorités civiles
Positionnement actif de la Suisse dans la politique internationale de cybersécurité	25. Participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité 26. Coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité 27. Consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité
Visibilité et sensibilisation	28. Élaboration et mise en œuvre d'un concept de communication pour la SNPC 29. Sensibilisation du public aux cyberrisques (*awareness*)

Ces champs d'action et ces mesures sont décrits plus en détail ci-après. Les compétences

et les bases juridiques nécessaires à la mise en œuvre, déjà existantes ou à élaborer, sont définies dans un plan de mise en œuvre séparé.

4.1 Acquisition de compétences et de connaissances

Aperçu du champ d'action	
Description	La détection aussi précoce que possible des cyberrisques ainsi que leur évaluation correcte sont deux conditions nécessaires pour limiter la menace. À cet effet, les acteurs de l'économie, de la société civile et du secteur étatique ont tous besoin non seulement de compétences de base, mais aussi d'un savoir technique spécifique. 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 multiplicité des cyberrisques ainsi que leur évolution incessante constituent deux défis majeurs dans ce contexte.
Contexte	La Suisse dispose à tous les niveaux d'un réseau performant d'institutions de formation et de recherche. Comme les cyberrisques évoluent très vite, le besoin de compétences et de connaissances en la matière a fortement augmenté. Or on manque aujourd'hui de connaissances spécifiques et de spécialistes dans les divers domaines s'occupant des cyberrisques. Cela complique la protection face aux cyberrisques et limite les possibilités des acteurs économiques de se profiler sur le marché en plein essor de la cybersécurité. De façon générale, il reste très difficile d'identifier suffisamment tôt les tendances et les technologies importantes. À ce jour, elles ne sont pas recensées de façon systématique et coordonnée, en tenant compte des aspects internationaux.
Objectifs et actions requises	Les milieux de la formation et de la recherche en Suisse accorderont au thème des cyberrisques l'importance qu'il mérite, et fourniront à la société, à l'économie et aux autorités les compétences et les connaissances scientifiques nécessaires. Il faut identifier les tendances ou technologies émergentes dans le domaine de la cybersécurité, afin de se préparer à affronter les risques potentiels et de pouvoir prendre au plus vite des mesures adéquates. Les acteurs économiques doivent disposer d'un savoir-faire suffisant et de la main-d'œuvre qualifiée requise, afin de pouvoir gérer avec compétence les cyberrisques et exploiter les chances du marché en plein essor de la cybersécurité. Il convient d'examiner si les solutions de cybersécurité pourraient toujours plus souvent être conçues en Suisse en renforçant la collaboration entre les acteurs économiques, la recherche et l'État, rendant ainsi les conditions-cadres plus favorables à l'émergence, la production et la commercialisation de solutions innovantes dans le domaine de la cybersécurité. Les travaux de recherche menés dans le domaine de la cybersécurité créent les bases utiles pour atteindre ces objectifs. Ces bases sont non seulement essentielles au développement des connaissances et à la détection précoce des tendances ou technologies, mais elles permettent également de créer un environnement attrayant pour la main-d'œuvre hautement spécialisée et les entreprises innovantes, grâce à l'échange de connaissances entre les secteurs scientifiques et économiques. Il s'agit donc de coordonner le mieux possible la recherche dans ce domaine interdisciplinaire.

Mesures
1) Détection précoce des tendances ou technologies et acquisition des connaissances utiles Les nouvelles tendances ou technologies dans le domaine de l'informatique ainsi que les opportunités et les risques qui en résultent doivent être identifiés à intervalles réguliers et de bonne heure. Les résultats de ce monitoring seront communiqués aux acteurs scientifiques, économiques, politiques et sociaux. La recherche fondamentale et appliquée sera encouragée dans le cadre des structures et processus en place (par ex. des programmes nationaux de recherche), en fonction des besoins et des possibilités
2) Extension et encouragement de l'offre de formation 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.
3) Création de conditions-cadres propices à l'innovation en Suisse, sur le marché de la cybersécurité 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 doit contribuer à favoriser l'émergence de start-up innovantes dans ce domaine. À cet effet, on pourra également faire appel aux structures mentionnées à la mesure 1. Le cas échéant, d'autres mesures visant à améliorer les conditions-cadres de la recherche en matière de cybersécurité seront étudiées et réalisées, avec le concours des associations et des hautes écoles.

4.2 Situation de la menace

Aperçu du champ d'action	
Description	Comme signalé au chapitre sur l'état des lieux, la cybermenace se caractérise par une multitude de menaces possibles. La finalité des attaques, leurs auteurs et le cercle des victimes diffèrent à chaque fois. Il est souvent difficile de tracer des limites claires entre les diverses menaces, car les agresseurs poursuivent plusieurs buts à la fois, ainsi que de combiner différents vecteurs d'attaque ou plusieurs cibles. Et comme en plus de leur complexité et de leur caractère diffus les cyberrisques évoluent très vite, il est très difficile d'avoir une vue d'ensemble des cybermenaces. Or une telle vue d'ensemble 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. C'est pourquoi il faut évaluer les menaces existantes et leur évolution future (description et analyse de la situation).
Contexte	Les capacités de description et d'analyse de la situation, de détection précoce et d'attribution ont été renforcées dans le cadre de la mise en œuvre de la SNPC 2013-2017. Les processus nécessaires à l'établissement d'un tableau d'ensemble de la situation sont établis, et les informations sur la situation globale de la menace sont résumées et présentées à l'aide d'un radar dynamique et interactif de la situation et mises à la disposition des autorités et des exploitants d'infrastructures critiques.

Objectifs et actions requises	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. Ni l'évaluation systématique ni le recensement des cyberincidents ne sont garantis, aujourd'hui où les ressources à disposition sont accaparées par les affaires courantes. Il est donc important de parvenir à une évaluation plus approfondie et nuancée des menaces pesant sur la Suisse. 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.

Mesures

4) Extension des capacités permettant d'analyser et de représenter la situation de la cybermenace

Les capacités de recherche, d'appréciation et de vérification des informations sur la situation de la menace doivent être encore renforcées au SRC. Pour ce faire, il faudra exploiter systématiquement le renseignement en source ouverte (*open source intelligence, OSINT)* et son expertise*,* tirer parti des moyens techniques, ainsi qu'entretenir et étendre le réseau de partenaires au niveau tant national qu'international. Les connaissances acquises sur la situation de la menace seront analysées systématiquement, régulièrement actualisées et présentées dans le radar de la situation de manière adaptée aux groupes cibles. Il s'agira aussi à cet effet de créer une version grand public du radar de la situation.

4.3 Gestion de la résilience

Aperçu du champ d'action	
Description	Les infrastructures critiques sont tributaires du bon fonctionnement et de la sûreté des systèmes et des infrastructures informatiques. Les mesures visant à réduire leurs vulnérabilités informatiques revêtent donc 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. Le but est d'améliorer la résilience (capacité de résistance et de réactivation) des infrastructures critiques en Suisse. En Suisse, une grande partie des infrastructures critiques sont exploitées par des entreprises privées. Il leur incombe de mettre en œuvre les mesures destinées à améliorer la résilience informatique. Dans le cadre de son mandat constitutionnel consistant à garantir la sécurité du pays, l'État est toutefois responsable de protéger les infrastructures critiques et par là de garantir à la population et à l'économie la disponibilité des biens et services de première nécessité. Il doit s'en charger subsidiairement, en étroite collaboration avec l'économie. Pour cette raison, la Confédération joue un rôle actif dans la définition de mesures destinées à améliorer la cyberrésilience des secteurs partiels, et en surveille la mise en œuvre. Selon la mesure, les travaux peuvent s'effectuer à différents niveaux (dans les entreprises ou au niveau de la branche). Les infrastructures informatiques des autorités constituent ici un cas à part: la Confédération et les cantons se chargent eux-mêmes de la mise en œuvre des mesures nécessaires.
Contexte	Entre 2013 et 2017, l'OFPP et l'OFAE ont identifié, conjointement avec les autorités compétentes, les associations de branche et des représentants d'exploitants d'infrastructures critiques , les risques et les vulnérabilités des 28 secteurs partiels définis en Suisse et élaboré ensemble (et en partie déjà réalisé) des propositions de mesures pour améliorer la résilience informatique. Afin de protéger sa propre infrastructure informatique, la Confédération a élaboré un concept garantissant que les systèmes de l'administration fédérale seront soumis à des analyses régulières de leurs vulnérabilités. Les cantons aussi ont procédé, dans le cadre de deux projets du RNS, à des analyses des risques au sein de leurs administrations.
Objectifs et actions requises	Les mesures identifiées pour améliorer la résilience informatique des secteurs partiels et des administrations seront mises en œuvre et ajustées, sur la base d'analyses périodiquement actualisées des risques et des vulnérabilités. La coordination sera assurée avec les mesures du champ d'action Normalisation et réglementation, en bonne synergie avec les travaux entrepris par la Confédération au titre de la protection des infrastructures critiques, de la gestion des crises, de la protection de la population (réseau de données sécurisé RDS+), de l'approvisionnement économique du pays, de la gestion des risques au sein de la Confédération et de la sécurité informatique, ainsi qu'avec les autres services concernés.

Mesures
5) Amélioration de la résilience informatique des infrastructures critiques Il s'agit surtout ici de mettre en œuvre des mesures destinées à améliorer la résilience informatique des secteurs partiels, 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.
6) Amélioration de la résilience informatique dans l'administration fédérale L'amélioration de la résilience informatique dans l'administration fédérale découle du concept d'analyse et consiste à remédier aux vulnérabilités existantes. Le concept prévoit d'opérer directement une sélection de mesures de sécurité informatique pertinentes, sur la base des vulnérabilités identifiées. Afin d'améliorer la résilience informatique, les personnes responsables de la protection des infrastructures informatiques et du traitement opérationnel des incidents dans les départements sont sensibilisées et formées de manière ciblée. Les accords de confidentialité des contrats conclus par l'administration fédérale avec des prestataires externes sont conçus de manière à ce que les informations concernant les failles et incidents de sécurité puissent être transmises aux services compétents en matière de gestion des incidents et aux délégués à la sécurité informatique des départements concernés.
7) Échanges d'expériences et création de bases destinées à améliorer la résilience informatique dans les cantons 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.

4.4 Normalisation et réglementation

Aperçu du champ d'action	
Description	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 (par 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. Les branches ne sont pas toutes autant exposées aux cyberrisques, tandis que les possibilités financières et les ressources en personnel varient fortement d'une entreprise à l'autre. Les normes ou réglementations doivent donc être conçues et introduites en étroite collaboration entre le secteur privé et l'État. 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. Les travaux des organismes de normalisation internationaux ainsi que l'évolution de la réglementation autour de la Suisse sont par conséquent déterminants. L'axe thématique de la normalisation et de la réglementation inclut également les divers processus liés à la gouvernance d'Internet instituée par le Sommet mondial de l'ONU sur la société de l'information (SMSI). Ces processus ont trait à l'élaboration de principes, normes, règles et mécanismes de décision régissant le développement et l'utilisation d'Internet au niveau international. L'Union internationale des télécommunications (UIT) joue un rôle de facilitateur dans divers projets ou travaux de mise en œuvre de la ligne d'action C5 du SMSI (sécurité et confiance). D'autres acteurs internationaux, à l'instar de l'OCDE ou du Forum économique mondial, ont encore lancé des processus et activités visant à améliorer la sécurité dans le domaine numérique. L'objectif fondamental du SMSI d'engagement actif de tous les groupes d'intérêt (approche des multipartenariats) tient compte de l'évolution actuelle. Dans le monde numérique, les normes et règles tendent toujours plus à être fixées par des acteurs mondiaux issus du secteur privé, et donc la coopération entre acteurs étatiques et privés revêt une importance majeure.
Contexte	La cybersécurité fait l'objet de diverses normes sectorielles et aussi de quelques normes générales. Un premier inventaire des besoins de normalisation et de réglementation dans les divers secteurs a été dressé, en collaboration avec les milieux économiques. Les développements en cours, dans les organismes de normalisation internationaux ou dans d'autres pays actifs sur le terrain de la réglementation, sont par ailleurs connus. Au niveau européen, la directive sur la sécurité des réseaux et de l'information (directive SRI) a été adoptée, et les États membres sont tenus de la transposer en droit national. Elle prévoit des exigences minimales communes, ainsi que l'obligation de notifier les incidents. Dans le domaine de la gouvernance d'Internet, les comités, processus ou manifestations prioritaires pour la Suisse ont été identifiés, les compétences à chaque fois précisées au sein de l'administration fédérale et la coordination assurée avec tous les acteurs concernés, grâce aux processus établis dans le cadre de la SNPC.

Objectifs et actions requises	Il faut tenir compte du rôle accru de la normalisation et de la réglementation informatiques. Des normes minimales contraignantes et 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 introduire là où c'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. La Suisse fera par conséquent valoir ses intérêts et ses valeurs dans les processus majeurs.

Mesures

8) Définition et introduction de normes minimales

À partir des analyses des risques et des vulnérabilités effectuées, des normes minimales seront évaluées et introduites, dans le cadre d'une étroite collaboration entre les autorités spécialisées, le secteur privé et les associations de branche. Les normes existantes seront reprises, et adaptées le cas échéant. Les autorités compétentes vérifieront pour quelles organisations ou activités les normes doivent être contraignantes. À cet effet, elles se baseront sur les résultats des analyses des vulnérabilités.

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

Afin d'améliorer le tableau de la situation, il convient d'étudier l'introduction d'une obligation de notifier les cyberincidents, et de 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 annoncer, et une obligation de notifier permettrait-elle d'améliorer notablement l'état des lieux? Différentes solutions possibles seront élaborées pour la mise en œuvre de l'obligation de notifier dans les différents secteurs, en montrant les bases légales à prévoir. Ce travail sera accompli avec la participation à chaque fois des autorités compétentes, du secteur privé et des associations de branche, en coordination avec la stratégie nationale pour la protection des infrastructures critiques et en tenant compte des développements internationaux. La décision d'introduire une obligation de notifier les cyberincidents se prendra sur la base de ces vérifications et, le cas échéant, les démarches nécessaires seront entreprises.

10) Gouvernance mondiale d'Internet

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.

11) Acquisition d'expertise sur les questions de normalisation dans le domaine de la cybersécurité

La Confédération crée un pool d'experts des questions de normalisation dans le domaine de la cybersécurité. Le pool d'experts conseille les régulateurs pour l'élaboration et la mise en œuvre de normes, règlements ou lignes directrices. Il soutient en cas de besoin les cantons, observe l'évolution de la normalisation et de la réglementation au niveau international, et échange des informations à ce sujet avec les milieux économiques. Ce faisant, il contribue à une approche coordonnée et en phase avec les développements internationaux.

4.5 Gestion des incidents

Aperçu du champ d'action	
Description	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 maîtriser les incidents, il importe de les repérer dès que possible, d'identifier et de mettre en œuvre des contre-mesures, ainsi que d'analyser les incidents survenus et d'en tirer les conclusions utiles pour améliorer la prévention. 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. Les responsabilités et les processus doivent être claires, efficaces et exercés. L'échange d'informations et leur analyse doivent être coordonnés de façon centrale, de manière à identifier rapidement l'importance d'un incident pour la politique de sécurité et la stratégie et à pouvoir informer les organes compétents. Dans le cas de la Confédération, il s'agit notamment et en fonction du type et de l'ampleur de l'événement du Groupe Sécurité et de la Délégation du Conseil fédéral pour la sécurité.
Contexte	Beaucoup d'organisations en Suisse ont créé ou mandaté des équipes spécialisées dans la gestion des cyberincidents. Elles portent différents noms (par ex. Security Operations Centers, Computer Emergency Response Teams, Computer Security Incident Response Teams), et leurs compétences varient selon leur mission. Beaucoup de cantons ainsi que la Confédération disposent aussi de telles équipes. La gestion des cyberincidents se fait principalement à ce niveau. La Confédération exploite la centrale MELANI pour soutenir les exploitants d'infrastructures critiques. Véritable guichet unique au niveau étatique, MELANI apporte son aide en cas d'incident pour l'analyse technique comme pour l'analyse des renseignements, pour laquelle une plateforme d'échange d'informations est en place. MELANI assume également un rôle de coordination au sein de l'administration fédérale dans la gestion des incidents. En règle générale, les services fédéraux concernés informent MELANI, qui analyse les cas et les transmet aux services compétents. Les processus ne sont toutefois pas standardisés. Il n'est de plus pas défini à partir de quel point MELANI doit informer le Groupe Sécurité et/ou la Délégation du Conseil fédéral pour la sécurité. La SNPC 2012-2017 a permis d'accroître la dotation en personnel de MELANI et de développer de nouvelles collaborations avec des équipes spécialisées en activité, à l'intérieur comme à l'extérieur de l'administration fédérale. Cela a rendu possible l'élargissement du cercle d'entreprises ayant accès à sa plateforme d'échange d'informations ainsi qu'à son soutien technique. Or même après cette expansion, les services de MELANI destinés aux acteurs économiques s'adressent en priorité aux exploitants d'infrastructures critiques.

Objectifs et actions requises	L'élargissement du groupe cible de la SNPC implique d'étendre à de nouveaux bénéficiaires le soutien en cas d'incident. Il faudra toutefois préserver la qualité du soutien offert pour la détection, la gestion et l'analyse des incidents, et garantir à l'avenir aussi la confidentialité des échanges d'informations avec les exploitants d'infrastructures critiques. 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. Aux objectifs de développement et d'intensification de la collaboration avec des tiers vient s'ajouter un objectif d'amélioration des processus de l'administration fédérale en matière de détection des incidents. Si chaque département doit globalement être capable de régler correctement un incident, la centrale MELANI doit également être prête à apporter le soutien nécessaire sous la conduite de l'Unité de pilotage informatique de la Confédération (UPIC). Les incidents affectant plusieurs départements ou qui représentent une menace pour la sécurité intérieure ou extérieure selon les estimations de MELANI sont gérés de manière uniforme et centralisée sous la direction de l'UPIC et en collaboration avec les départements concernés. L'UPIC évalue les conséquences de l'incident pour la politique de sécurité et la stratégie, toujours en collaboration avec les départements concernés.

Mesures

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

Le soutien aux exploitants d'infrastructures critiques doit être encore développé. Le but est d'inclure tous les secteurs critiques dans l'échange d'informations, et d'intensifier ce dernier au niveau intersectoriel. Au cours du développement du partenariat public-privé, on veillera à préserver la qualité de l'offre. Il faut à cet effet clairement définir quels membres du cercle fermé ont droit à quels services.

13) Offre de services destinés à toutes les entreprises

MELANI élargit le groupe cible et propose des services dans le domaine de la prévention et de la gestion des incidents pour un large groupe cible, ne se limitant pas aux exploitants d'infrastructures critiques. L'économie suisse, et notamment les petites et moyennes entreprises, doivent être soutenues par MELANI. Ce soutien sera toutefois subsidiaire aux offres en matière de protection et de gestion des incidents disponibles sur le marché.

14) Collaboration ciblée entre la Confédération et d'autres services ou centres de compétences

La concertation déjà étroite de MELANI avec d'autres services compétents au niveau tant fédéral que cantonal doit encore être renforcée. Les spécialistes étant rares en Suisse, il s'agira à la fois d'intensifier de manière ciblée et de mieux coordonner la collaboration avec des centres de compétences dûment choisis, afin d'utiliser les ressources limitées à disposition de manière aussi efficace et rationnelle que possible.

15) Processus et bases de la gestion des incidents au sein de l'administration fédérale

Un processus qui définit les voies de transmission de l'information et les responsabilités est élaboré, dans l'optique d'une standardisation de la gestion des incidents au sein de l'administration fédérale. Il permet également d'assurer la collaboration avec les autorités de poursuite pénale et, en cas d'incidents graves sur le plan de la politique de sécurité ou de la stratégie, avec le Groupe Sécurité et la Délégation du Conseil fédéral pour la sécurité. Les départements désignent un interlocuteur chargé de la coordination dans le cadre de la gestion des incidents. L'UPIC dispose du pouvoir décisionnel nécessaire à la gestion des incidents. La coordination de la communication concernant les cyberincidents touchant plusieurs départements est assurée par la Chancellerie fédérale.

4.6 Gestion des crises

Aperçu du champ d'action	
Description	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 cybernétiques. 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. C'est l'unique façon d'obtenir à temps, et sous une forme compréhensible, toutes les informations utiles pour résoudre la crise. Comme le temps presse pour rétablir la cybersécurité, il convient au préalable de s'exercer à appliquer les processus et d'élaborer des concepts tant pour les activités de conduite que pour la communication.
Contexte	Pour bien gérer les cyberrisques en cas de crise, la Confédération s'est dotée, sur la base des résultats de l'exercice de conduite stratégique 2013, d'un concept en la matière, étendu par la suite conjointement avec les cantons et des représentants de l'économie pour aboutir à un concept de gestion nationale des crises à caractère cybernétique. Le concept a été testé et les exercices évalués. Il en ressort que la priorité absolue, et aussi le défi majeur pour résoudre une cybercrise, est d'établir un tableau à la fois précis et actuel de la situation.
Objectifs et actions requises	Les exercices ont révélé la nécessité de renforcer les capacités, sur le plan tant de la coordination opérationnelle que de la description de la situation. Une implication directe du service spécialisé compétent du domaine cybersécurité est nécessaire dans la gestion des crises à l'échelon de la Confédération, laquelle incombe aux états-majors existants ou constitués ad hoc. Il faudra en outre continuer d'exercer la collaboration tant avec les cantons qu'avec les milieux économiques, afin que les personnes concernées connaissent les compétences respectives et les points de contact.

Mesures
16) Intégration du service spécialisé compétent du domaine cybersécurité dans les états-majors de crise de la Confédération Face à une cybercrise, les états-majors de crise existants peuvent être sollicités (état-major fédéral, protection de la population, état-major de crise de l'AEP), ou des états-majors de crise ad hoc. Le service spécialisé compétent du domaine cybersécurité sera intégré dans les états-majors et doit avoir les compétences, en cas de crise à caractère cybernétique, d'assurer la coordination technique et d'adresser des recommandations à l'état-major de crise. Il s'agira encore d'examiner l'étendue du pouvoir décisionnel à conférer à MELANI, en cas de crise.
17) Exercices communs de gestion de crise Des exercices communs à la Confédération, aux cantons et à des représentants des infrastructures critiquesserviront 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.

4.7 Poursuite pénale

Aperçu du champ d'action	
Description	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. La cybercriminalité se joue des frontières territoriales, dans un processus hautement dynamique aux cycles d'innovation très courts. Plus l'interconnexion augmente, et plus il est à craindre que les cyberincidents débutent dans le monde virtuel pour déployer des effets préjudiciables dans le monde réel. Face à cette évolution, il est urgent de rechercher de nouvelles solutions en matière de poursuite pénale. Il convient d'agir dans toute la Suisse et en collaboration avec des partenaires internationaux, afin d'améliorer l'interopérabilité et la capacité de réaction ainsi que pour 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.
Contexte	Une étape importante dans la lutte contre la cybercriminalité consiste à établir une vue d'ensemble des infractions en matière de cybercriminalité en Suisse. Un concept consolidé a été établi à cet effet en collaboration avec les cantons. En outre, des mesures ont été définies en vue de l'enregistrement uniforme, de la coordination et de la diffusion des informations utiles; des mesures de police destinées à déterminer la compétence à raison du lieu et de la matière ont été définies; l'enregistrement et l'analyse des divers phénomènes de la cybercriminalité ont commencé. La vue d'ensemble des infractions en matière de cybercriminalité en Suisse et la coordination intercantonale des cas ne sont cependant que deux aspects parmi d'autres visant à relever le défi de la cybercriminalité. Divers aspects importants restent à régler, comme les enquêtes proprement dites, les structures nationales ou la formation dispensée aux divers échelons. C'est pourquoi la Conférence des commandants des polices cantonales de Suisse (CCPCS) met sur pied un dispositif national relatif à la cybercriminalité et à la forensique informatique. Les besoins en matière d'organisation et d'infrastructure y sont traités dans leur globalité, et la question de l'allocation des ressources nécessaires y est également réglée.
Objectifs et actions requises	Le dispositif national de lutte contre la cybercriminalité de la CCPCS et le plan de mise en œuvre correspondant couvriront tous les aspects de la lutte contre la cybercriminalité (vue d'ensemble des infractions en matière de cybercriminalité en Suisse, coordination des cas de cybercriminalité, formation, enquêtes); ils définiront également les étapes à entreprendre pour mettre ne œuvre les mesures et les concepts.

Mesures
18) Tableau de la situation en matière de cybercriminalité La Confédération (fedpol) et les cantons (CCPCS) étudient et concrétisent techniquement les conditions-cadres nécessaires à l'élaboration d'un tableau national figurant en temps réel la situation policière en matière de cybercriminalité. Ces travaux sont entrepris en synergie avec le programme d'harmonisation de l'informatique policière (HIP).

19) Réseau de soutien aux enquêtes relatives à la cybercriminalité La Confédération (fedpol) et les cantons (Conférence des directrices et directeurs des départements cantonaux de justice et police, CCDJP) élaborent une convention administrative sur la collaboration et la coordination entre le centre de cybercompétence national (National Cyber Competence Center actif NC3) et les centres de cybercompétence régionaux (Cyber Competence Centers RC3) dans le cadre du réseau de soutien aux enquêtes relatives à la cybercriminalité.
20) Formation à la lutte contre la cybercriminalité Des concepts 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.
21) Office central de lutte contre la cybercriminalité 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.

4.8 Cyberdéfense

Aperçu du champ d'action	
Description	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. Outre une vaste palette de mesures renforçant la protection contre les cyberrisques, il est ainsi nécessaire de disposer de capacités et 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 mettre en œuvre si nécessaire des contremesures actives, afin d'assurer le fonctionnement des infrastructures touchées. La cyberdéfense comprend ainsi toute mesure servant à la défense de systèmes d'importance vitale 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.
Contexte	Avec la loi fédérale sur le renseignement (LRens) et la révision de la loi fédérale sur l'armée (LAAM), la Confédération dispose des bases légales nécessaires pour le développement et la mise en œuvre de mesures actives et contremesures dans le cadre de la cyberdéfense. Le développement et l'augmentation de la complexité des cyberattaques ces dernières années demande cependant de plus en plus de disposer de ressources pouvant être engagées sur une longue période. Le risque est que des attaques se déroulant simultanément ne soient pas détectées à temps, lorsque les quelques spécialistes à disposition sont absorbés par leur engagement sur d'autres cas. Ce problème de ressources rend par ailleurs difficile le travail nécessaire et continu de suivi des cas. 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.

Objectifs et actions requises	Le Service de renseignement doit être en mesure d'identifier de nouveaux modes opératoires aussi vite que possible, à l'aide d'une acquisition et appréciation systématique d'information. Par ailleurs, il doit pouvoir établir l'origine des attaques (attribution) aussi précisément que possible, afin de préserver la marge de manœuvre des autorités politiques et de poursuite pénale. Lors d'attaques visant des opérateurs d'infrastructures critiques, le Service de renseignement doit être en mesure, avec le soutien des unités partenaires, de remplir sa mission dans le cadre de la LRens. L'armée joue un rôle décisif, en tant que réserve stratégique pour l'assistance subsidiaire aux unités civiles et en cas de mobilisation. Elle doit ainsi pouvoir assurer une disponibilité dans le domaine de la cyberdéfense, et ce dans toutes les situations.

Mesures

22) Développement des capacités d'acquisition d'information et d'attribution

Les connaissances spécifiques et les compétences nécessaires à l'acquisition d'information en vue de la détection précoce des cyberattaques et de l'identification des auteurs seront développées. La collaboration entre la Confédération et les cantons dans ce sens sera renforcée et l'échange d'information avec les acteurs privés développé. Le Service de renseignement de la Confédération mène des analyses approfondies des acteurs et des environnements, utilise et développe des moyens techniques, de surveillance des télécommunications et des méthodes de *Human Intelligence.* De cette manière, les cyberattaques réussies seront systématiquement traitées et suivies.

23) Capacité à mener des mesures actives dans le cyberespace selon la LRens et la LAAM

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 conformément aux dispositions de la LRens et de la LAAM.

24) Garantie de la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et réglementation de son rôle subsidiaire consistant à appuyer les autorités civiles

Dans le cadre de la mise en œuvre du projet de développement de l'armée (DEVA), l'armée s'assure de disposer de suffisamment de moyens, ressources et capacités pour remplir sa mission selon LAAM en situation exceptionnelle dans le cyberespace. L'armée doit en outre être suffisamment disponible pour soutenir les autorités civiles subsidiairement, en tant que réserve stratégique. Dans ce but elle forme ses cadres et collaborateurs en conséquence et définit avec les autorités civiles de la Confédération et des cantons les conditions-cadres de son soutien subsidiaire en cas de cyberincidents, les tâches dont elle peut assumer la responsabilité et le déroulement concret d'une telle intervention.

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

Aperçu du champ d'action	
Description	Le cyberespace est un nouvel aspect de la politique de sécurité extérieure. Les acteurs étatiques utilisent toujours plus le cyberespace pour démontrer leur puissance et pour atteindre des objectifs politiques, dans le cadre de projets de renseignement ou encore à des fins militaires. Non seulement des moyens cybernétiques sont engagés dans les conflits armés conventionnels, mais les affrontements se déroulent toujours plus souvent dans le cyberespace. La collaboration internationale est par conséquent indispensable, au niveau diplomatique comme sur le plan technique et opérationnel, afin de réduire les cyberrisques. 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.
Contexte	La SNPC de 2012 avait déjà souligné l'importance de la coopération internationale. Les processus et structures nécessaires à une politique extérieure coordonnée et cohérente dans le domaine de la cybersécurité ont été mis en place. La stratégie «Suisse numérique» adoptée en 2016 par le Conseil fédéral comprend également des réflexions sur la politique de sécurité. Dans les conférences internationales, la Suisse est perçue comme un partenaire actif, sûr et digne de confiance, et son avis compte. Elle s'est beaucoup engagée pour le développement et la mise en œuvre dans le cyberespace de premières mesures de confiance entre les États. Elle participe activement au développement de processus multilatéraux utiles à la cybersécurité, et intensifie sa coopération avec des pays ou organisations spécifiques.
Objectifs et actions requises	Une politique de cybersécurité cohérente s'impose afin de réduire les cyberrisques. Elle a pour objectif principal un cyberespace libre, ouvert et sûr. La Suisse se sert de différents instruments pour défendre ses intérêts face aux autres États et aux organisations internationales, ainsi que pour promouvoir la paix, la stabilité et la sécurité internationale. *Premièrement*, elle s'engage pour la reconnaissance, le respect et l'application du droit international sur le terrain de la cybersécurité, et contribue à ce que les modalités d'application du droit public dans le cyberespace soient précisées. *Deuxièmement*, la Suisse s'engage activement pour l'instauration d'un climat de confiance entre les États. Et *troisièmement*, elle soutient ou conçoit des initiatives visant à développer les aptitudes nationales et à renforcer les capacités d'États tiers. Dans le second cas, il convient de s'assurer que dans la mesure du possible, tous les acteurs intéressés pourront participer aux discussions internationales destinées à améliorer la cybersécurité. 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.

Mesures
25) Participation active, dès le stade conceptuel, aux processus de politique extérieure portant sur la cybersécurité La Suisse s'engage, dans sa politique extérieure de cybersécurité, pour l'élaboration de règles sur une utilisation responsable des technologies de l'information et de la communication. Elle s'y emploie dans le cadre de l'ONU, de l'OSCE et d'autres enceintes internationales. Elle prône une meilleure reconnaissance du droit international, et contribue à clarifier diverses questions d'application (groupe d'experts de l'ONU et processus de suivi, processus de Tallinn, etc.). La Suisse part du principe que les droits de l'homme s'appliquant dans le monde réel valent aussi dans le monde virtuel. Elle appelle donc à garantir le respect des droits de l'homme lors d'activité déployées dans le cyberespace au nom de la politique de sécurité. La Suisse s'engage encore, au sein de l'OSCE et dans d'autres enceintes, pour la mise en œuvre et le développement de mesures de confiance. Enfin, elle participe activement aux discussions portant sur l'interface entre cybersécurité et contrôle des armements, et appelle à consolider les connaissances et les capacités dans ce secteur.
26) Coopération internationale en vue de l'acquisition et du développement de capacités dans le domaine de la cybersécurité La Suisse tirera parti du savoir-faire étranger, acquis lors de collaborations et d'échanges avec d'autres États, organisations internationales ou centres de recherche spécialisés (par ex. Cooperative Cyber Defence Centre of Excellence), afin de développer les aptitudes nationales à réduire les risques. La Suisse soutient des projets et initiatives visant à renforcer les capacités de cybersécurité d'autres pays (par ex. échanges d'experts en vue de la création d'institutions ou de structures contribuant à la cybersécurité, organisation d'ateliers sur les processus internationaux, soutien de projets du Global Forum on Cyber Expertise).
27) Consultations politiques bilatérales et dialogues multilatéraux sur les aspects cybernétiques de la politique extérieure de sécurité 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 (par ex. Sino-European Cyber Dialogue).

4.10 Visibilité et sensibilisation

Aperçu du champ d'action	
Description	Les cyberrisques préoccupent la population et les milieux économiques, par leur rapide évolution et leur gravité croissante. Les particuliers et les entreprises ont de la peine à savoir à quels cyberrisques ils sont exposés, et quelles seraient les mesures de protection indiquées. Outre la difficulté d'apprécier les cyberrisques qu'ils courent eux-mêmes, ils ignorent souvent quelle aide de l'État ils peuvent attendre. Le large portefeuille d'activités de la SNPC et sa mise en œuvre décentralisée font que bien souvent, les mesures prises par l'État pour protéger la Suisse contre les cyberrisques sont méconnues. 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.
Contexte	Les résultats de la SNPC ont été consignés à ce jour dans les rapports annuels, présentés lors de conférences (conférence sur les cyberrisques, «cyber-landsgemeinde») et publiés sur le site Internet de l'UPIC. Or les réactions de la population, des milieux économiques et du monde politique ont montré que les instruments en place ne satisfont pas entièrement au besoin d'information dans ce domaine. 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.
Objectifs et actions requises	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 contribuera en outre davantage à sensibiliser la population, les milieux économiques et le monde politique aux cyberrisques et aux mesures de protection possibles.

Mesures
28) Élaboration et mise en œuvre d'un concept de communication pour la SNPC Un concept 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 concept prendra en compte les divers publics et sera activement poursuivie dans le cadre du travail de relations publiques et de communication.
29) Sensibilisation du public aux cyberrisques (*awareness*) 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.

5 Mise en œuvre de la stratégie

Les mesures décrites dans les dix champs d'action seront mises en œuvre d'ici 2022. Pour ce faire, il est nécessaire de définir clairement qui est responsable de quelles mesures, sur quelles bases légales s'appuie la mise en œuvre des mesures et jusqu'à quand les objectifs doivent être atteints. Premièrement, cela implique que la Confédération doit déterminer, d'une part, quelles seront les compétences des unités administratives concernées ainsi que, d'autre part, qui portera la responsabilité globale de la mise en œuvre de la SNPC. Deuxièmement, il convient de clarifier les bases légales. Troisièmement, il est important de définir comment la Confédération collabore avec les cantons, les entreprises et la société et quel rôle ces acteurs jouent dans la mise en œuvre de chacune de ces mesures. Quatrièmement, les progrès réalisés dans la mise en œuvre de la SNPC doivent être transparents. Pour chaque mesure, il s'agit donc de définir des objectifs de prestations mesurables et jusqu'à quand ceux-ci doivent être remplis. Cinquièmement, il convient de définir qui mettra la SNPC à jour et comment, dans l'éventualité où des ajouts ou des modifications s'avèrent nécessaires avant fin 2022.
Étant donné que ces points concernent la mise en œuvre et non directement l'orientation stratégique, ils seront décrits dans un plan de mise en œuvre distinct. Ce dernier doit être perçu comme un élément à part entière de la SNPC, car il complète les objectifs stratégiques avec des objectifs opérationnels et décrit les responsabilités ainsi que les compétences. Ci-après sont décrits sous une forme condensée les éléments les plus importants des questions abordées ci-dessus afin d'illustrer la manière dont la SNPC sera mise en œuvre.

5.1 Responsabilités et compétences au sein de l'administration fédérale

En adoptant la SNPC, la Confédération s'engage avant tout elle-même à mettre en œuvre les mesures contenues dans cette stratégie. Étant donné que la SNPC contient un large éventail de mesures, plusieurs offices fédéraux prennent directement part à la mise en œuvre de la SNPC. Les tâches de la Confédération se répartissent globalement dans trois domaines:

- **Domaine de la cybersécurité**: il correspond à l'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 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:** mesures de la police et du ministère public dans la lutte contre la cybercriminalité.

5.2 Collaboration avec des tiers

Un des objectifs stratégiques de la SNPC est de garantir une coopération commune pour protéger la Suisse contre les cyberrisques. Il est par conséquent important de faire participer les cantons, les entreprises et la société directement aux travaux de mise en œuvre. Si la Confédération fixe les compétences et les obligations des offices fédéraux dans le plan de mise en œuvre, les tâches assumées par les cantons et les organisations des milieux économiques et de la société civile doivent aussi y être clairement définies. Ces derniers participent donc à l'élaboration du plan de mise en œuvre.

5.2.1 Participation des cantons à la mise en œuvre

Pour garantir que les cantons participent à la mise en œuvre des mesures concernées de la SNPC pour les années 2018 à 2022, la CCDJP élabore avec le RNS un plan de mise en œuvre cantonal. Sur cette base, les mesures nécessitant une participation directe des cantons et les objectifs qu'elles visent à atteindre seront inscrits dans le plan de mise en œuvre de la SNPC.

5.2.2 Participation des entreprises et de la société

Le plan de mise en œuvre de la SNPC recense les organisations des milieux économiques ou de la société civile qui s'engagent, sur une base volontaire, à mettre en œuvre des mesures ainsi que les mesures en question. La liste de ces organisations n'est pas exhaustive; une participation d'autres organisations est possible à tout moment.

5.2.3 Coordination de la mise en œuvre

Tous les participants coordonnent leurs activités sous la direction de projet, s'accordent régulièrement sur les travaux de mise en œuvre et vérifient si des mesures supplémentaires sont nécessaires pour atteindre les objectifs de la SNPC. Un organe de coordination, composé de représentants de la Confédération, des cantons et des entreprises, est constitué à cet effet.

5.3 Objectifs visés pour la mise en œuvre des mesures

Pour évaluer l'avancement des travaux, des objectifs mesurables doivent être établis pour chacune des mesures. L'état actuel des domaines concernés par les mesures détermine quels objectifs doivent être atteints et jusqu'à quand. Ces derniers prévoient par exemple un délai pour la création de produits concrets, des projets ou des étapes de projets à achever ou des processus à élaborer ou développer.

5.4 Mise à jour de la SNPC

La présente stratégie sera actualisée fin 2022. S'il est prévu de vérifier régulièrement la mise en œuvre et d'apporter le cas échéant des modifications, une mise à jour anticipée de la SNPC n'aura lieu que si les menaces évoluent de façon inattendue ou si d'autres facteurs remettant en question les hypothèses énoncées dans le chapitre «État des lieux» font leur apparition. Si une mise à jour anticipée est nécessaire, la nouvelle version de la SNPC sera soumise au Conseil fédéral, aux offices fédéraux, aux cantons et aux représentants des entreprises.

6 Liste des abréviations

CCDJP		Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS		Conférence des commandants des polices cantonales
CERT		*Computer emergency response team*
DDPS		Département fédéral de la défense, de la protection de la population et des sports
DEVA		Développement de l'armée
DFF		Département fédéral des finances
Fedpol		Office fédéral de la police
HUMINT		*Human intelligence*, renseignements d'origine humaine
IT		Technologies de l'information
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 Etats
LRens		Loi fédérale sur le renseignement
MELANI		Centrale d'enregistrement et d'analyse pour la sûreté de l'information
NEDK		Réseau de soutien aux enquêtes relatives à la cybercriminalité
OCDE		Organisation de coopération et de développement économiques
OFAE		Office fédéral pour l'approvisionnement économique du pays
OFPP		Office fédéral de la protection de la population
ONU		Organisation des nations unies
OSCE		Organisation pour la sécurité et la coopération en Europe
OSINT		*Open source intelligence*, renseignement en source ouverte
PACD		Plan d'action Cyberdéfense DDPS
par ex.		Par exemple
PIC		Protection des infrastructures critiques
PNR		Programmes nationaux de recherche
PPP		*Public-private partnership*, partenariat public-privé
RC3		Cyber Competence Centers régionaux
RDS+		Réseau de données sécurisé
RNS		Réseau national de sécurité
RTN		Réseaux thématiques nationaux
SMSI		Sommet mondial sur la société de l'information
SNPC		Stratégie nationale de protection de la Suisse contre les cyberrisques
SOC		*Security operations centers*
SRI		Directive UE sur la sécurité des réseaux et de l'information
TIC		Technologies de l'information et de la communication
UE		Union européenne
UIT		Union internationale des télécommunications
UPIC		Unité de pilotage informatique de la Confédération
WEF		Forum économique mondial
WSIS		World Summit on the Information Society

7 Glossaire

Cyberattaque	Acte illicite commis intentionnellement par une personne ou un groupe de personnes dans le cyberespace dans le but de nuire à l'intégrité, la confidentialité ou la disponibilité d'informations ou de données; selon la nature de l'attaque, celle-ci peut avoir des conséquences sur le plan physique.
Cyberrisques	Produit de la probabilité de survenance d'un cyberincident et de l'ampleur des dommages qui en résultent
Cybercriminalité	Au sens strict, la cybercriminalité renvoie aux infractions qui sont commises à l'aide de technologies de l'information et de la communication ou qui exploitent les vulnérabilités de ces technologies. Ces activités criminelles sont nouvelles et ne sont possibles que depuis l'avènement de ces technologies. La cybercriminalité au sens large utilise Internet comme moyen de communication en se servant à mauvais escient des possibilités offertes par cette technologie, par exemple les courriers électroniques ou l'échange et la mise à disposition de données à des fins malveillantes. Ces activités criminelles ne sont pas nouvelles, mais les médias utilisés pour les commettre ou pour stocker des données le sont (messagerie électronique, WhatsApp, Snapchat, Instagram, Telegram ou supports électroniques à la place du papier, services en nuage, etc.).
Cyberespace	Ensemble des infrastructures d'information et de communication (matériel et logiciel) qui échangent, créent, enregistrent et traitent des données ou transforment celles-ci en actions (physiques) ainsi que toutes les interactions permises par ces infrastructures entre des personnes, des organisations et des États.
Cybersabotage	Activité visant à perturber ou à détruire le bon fonctionnement des structures d'information et de communication dans le cyberespace; selon la nature du sabotage, celui-ci peut avoir des conséquences sur le plan physique.
Cyberespionnage	Activité visant à accéder de manière non autorisée à des informations à des fins politiques, militaires ou économiques dans le cyberespace.
Cyberdéfense	Ensemble des mesures prises par les services de renseignements et l'armée pour perturber, ralentir les cyberattaques ou mettre fin à celles-ci, en identifier les auteurs, garantir la disponibilité opérationnelle de l'armée dans toutes les situations et développer les capacités et les compétences pour apporter subsidiairement un soutien aux autorités civiles.
Cyberincident	Événement voulu ou non qui conduit à un processus nuisant à l'intégrité, la confidentialité ou la disponibilité de données et d'informations et pouvant occasionner des défauts de fonctionnement.
Infrastructures critiques	Processus, systèmes et installations nécessaires au fonctionnement de l'économie et au bien-être de la population.
Résilience	L'aptitude d'un système, d'une organisation ou d'une société à résister à des perturbations et à conserver sa capacité de fonctionnement ou à la retrouver aussi rapidement que possible.

Cybersécurité	Situation visée au sein du cyberespace dans laquelle la communication et l'échange de données entre les infrastructures d'information et de communication fonctionnent comme prévu. Cette situation est atteinte grâce aux mesures en matière de sécurité de l'information et à la cyberdéfense.
Sécurité de l'information / sécurité informatique	La sécurité de l'information (ou sécurité informatique) vise à garantir l'authenticité, la confidentialité, l'intégrité et la disponibilité des données traitées par un système d'information et de communication ou enregistrées dans celui-ci.
Cybermenace	Processus pouvant conduire à un cyberincident.