Cyberstratégie nationale (CSN)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Le Conseil fédéral

Impressum

Éditeur
Centre national pour la cybersécurité (NCSC)
Schwarztorstrasse 59
CH-3003 Berne

info@ncsc.admin.ch
www.ncsc.admin.ch

Vue d'ensemble

1 Introduction

La cybersécurité a gagné en importance dans tous les domaines. Élément clé de la politique de sécurité, elle est non seulement un prérequis essentiel pour la transformation numérique, un facteur central de la protection des données et une chance pour la place économique et les milieux scientifiques suisses, mais joue aussi un rôle de plus en plus important dans la politique extérieure. Au-delà de ces enjeux institutionnels, la cybersécurité s'invite dans le quotidien des citoyens qui utilisent les technologies numériques. Par conséquent, une stratégie nationale de cybersécurité se doit de couvrir un large champ thématique et d'inclure des mesures très diverses. En même temps, elle doit s'efforcer de faire un tri dans ce vaste portefeuille de thèmes, de les pondérer et de les mettre en relation les uns avec les autres. Ce chapitre introductif passe d'abord en revue les menaces à appréhender. Un deuxième sous-chapitre rappelle les fondements de cette stratégie. La cybersécurité est loin d'être un thème nouveau, et il existe déjà en Suisse de solides bases dans ce domaine. C'est pourquoi il est important de s'appuyer sur ces travaux, mais aussi de les remettre en question et de les compléter s'il y a lieu. Troisièmement, il s'agit de préciser les compétences des différents acteurs. Cette délimitation s'est avérée à maintes reprises être un grand défi, principalement en raison du caractère transversal de la cybersécurité.

1.1 État de la cybermenace

Le terme cybermenace désigne dans la présente stratégie toute circonstance susceptible de causer un cyberincident. Par cyberincident, il faut entendre un événement survenant lors de l'utilisation des technologies de l’information et de la communication (TIC) qui peut compromettre la confidentialité, la disponibilité et l'intégrité des informations ou la traçabilité de leur traitement. Sur la base de ces définitions, il est possible de déterminer tout un éventail de cybermenaces potentielles, décrites ci-après. Afin d'identifier les contre-mesures qui s'imposent, il est en outre nécessaire d'avoir une vue d'ensemble systématique sur les facteurs qui affectent directement l’état de la cybermenace.

1.1.1 Menace liée aux cyberattaques

Par cyberattaque, il faut entendre un cyberincident provoqué intentionnellement. La protection face à de telles menaces est au cœur des mesures de cybersécurité. Elle revêt une importance d'autant plus grande que les cyberattaques représentent une menace sérieuse depuis des années, tandis que l'économie et la société sont toujours plus tributaires du bon fonctionnement de leur environnement TIC. Compte tenu de la diversité des cyberattaques possibles, il est important de distinguer plusieurs phénomènes pour apprécier correctement la situation et les mécanismes de gestion envisageables. Il convient ainsi de classer les cyberattaques en fonction l’objectif des 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 se recoupent.

Cybercriminalité: À la différence des menaces décrites ci-après, la cybercriminalité comprend surtout des infractions contre le patrimoine. Elle englobe la totalité des actes punissables commis ou omis dans le cyberespace. Une distinction s'impose ici entre «cybercrime» et «criminalité numérique». Un «cybercrime» désigne des infractions commises contre Internet, les systèmes informatiques ou leurs données, et requiert un travail d'investigation technique de la part des autorités de poursuite pénale. La «criminalité numérique» désigne des infractions qui jusqu'alors avaient principalement lieu dans le monde analogique. En raison de la progression de la transformation numérique, les délits classiques sont toujours plus souvent commis à l'aide des TIC.

De toutes les menaces décrites ici, la cybercriminalité est celle dont la probabilité de survenance 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 en règle générale aux victimes concernées. Néanmoins, les cybercriminels s'accommodent d'importants dommages collatéraux, voire misent sur la possibilité de telles répercussions pour faire chanter les victimes et leur soutirer de grosses sommes d'argent. 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 secteur de la cybercriminalité, de véritables domaines d'activité voient le jour, dans lesquels opèrent des groupes organisés se répartissant le travail. En raison de la grande concurrence, les cybercriminels sont soumis à une forte pression à l'innovation, si bien qu'ils ne cessent de développer ou d'acquérir de nouvelles méthodes et se professionnalisent toujours plus. En conséquence, il faut s'attendre à ce que la fréquence et la spécialisation des activités criminelles dans le cyberespace continuent à augmenter.

Cyberespionnage: les tentatives de cyberespionnage visent à s'emparer d'informations confidentielles à des fins politiques, militaires ou économiques, ou à observer les activités des victimes. Leurs auteurs essaient bien souvent de rester indétectables le plus longtemps possible après avoir pénétré dans des réseaux. Il s'agit typiquement d'attaques sophistiquées prolongées du type APT (Advanced Persistent Threat). Le cyberespionnage est fréquemment pratiqué par des acteurs étatiques, mais il l'est aussi par des acteurs non-étatiques ou privés. Ceux-ci ciblent à la fois des entreprises et des institutions étatiques, sociales ou internationales. L'économie suisse est l'une des plus innovantes du monde, et de nombreux groupes internationaux ont établi leur siège principal ou de grands centres de données sur le territoire helvétique. En outre, la Suisse héberge de nombreuses organisations internationales et accueille souvent des négociations et des conférences internationales. Ces activités font 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 parviennent à se procurer. De telles répercussions peuvent rapidement mettre en péril la survie des PME tributaires de leur capacité d'innovation. Mais en général, les 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. En outre, de telles opérations entraînent souvent des dommages collatéraux, car les cybercriminels exploitent à plusieurs reprises les vecteurs d'attaques. Alors que les tensions géopolitiques s'exacerbent, la pratique du cyberespionnage s'intensifie elle aussi. La menace est d'autant plus grande que les gouvernements ont un pouvoir d'influence sur les fabricants de produits informatiques, ce qui augmente la probabilité que ceux-ci laissent délibérément des failles de sécurité dans leurs produits. Étant donné que les chaînes d'approvisionnement des produits TIC sont d'une grande complexité et que la Suisse est largement tributaire des fabricants étrangers, répondre à cette menace de manière adéquate est un grand défi pour la Suisse.

Cybersabotage: le cybersabotage désigne une activité visant à manipuler, à perturber ou à détruire le bon fonctionnement des TIC au moyen de cyberattaques, ce qui peut également avoir des conséquences physiques en fonction de la nature du sabotage et de la cible attaquée. Les tentatives de cybersabotage peuvent avoir des motifs très divers. Elles peuvent émaner tant de «loups solitaires» mus par exemple par des convictions idéologiques ou en proie à des frustrations personnelles que d'acteurs étatiques poursuivant des objectifs politiques ou militaires. Dans tous les cas, l'objectif de ce genre d'attaques est lié à la démonstration de force et à l'intimidation, associée à l'intention de déstabiliser une organisation, voire la société. Alors que divers actes de sabotage de grande envergure ont été commis sur le plan international, notamment en lien avec l'approvisionnement des États en énergie, la Suisse a été épargnée à ce jour. La probabilité de survenance de tels actes ta toutefois augmenté en raison de la recrudescence des tensions géopolitiques. Ceci est aussi valable pour la Suisse, pour laquelle les dommages potentiels pourraient être considérables.

Cybersubversion: on parle de cybersubversion quand des acteurs étatiques, non-étatiques ou animés de mobiles politiques se livrent à des cyberattaques pour saper le système politique d'un autre État. De telles attaques visent par exemple les processus démocratiques, les institutions politiques ou les organisations d'intérêt public. Les auteurs de ce genre d'attaques tentent ainsi d'ébranler la confiance en l'État et combinent souvent leurs attaques

à des campagnes de désinformation.

Cyberopérations lors de conflits armés: l'utilisation de moyens réguliers et irréguliers dans les conflits armés est aujourd'hui une pratique courante. Les cyberopérations sont un instrument particulièrement adéquat, car elles sont difficiles à attribuer, sont relativement peu coûteuses, peuvent être peuvent être utilisées à n'importe quelle distance sans présence physique et permettent d'avoir un impact même sans lien direct avec les opérations militaires.

Les investissements considérables effectués par de nombreux États dans la protection et la défense active contre les cybermenaces soulignent l'importance des cybermoyens lors de conflits armés. En conséquence, il y a lieu de s'attendre à ce que l'importance des cyberopérations lancées à des fins politiques 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 en cas de conflit.

1.1.2 Erreurs humaines et défaillances techniques

Outre les cyberattaques ciblées et délibérées, des actes involontaires ou des événements liés aux conditions naturelles et à la technique sont parfois à l'origine de cyberincidents. Ceux-ci sont dus à des erreurs humaines dans la préparation et l'utilisation des TIC (p. ex. utilisation inappropriée ou négligente des systèmes TIC, mauvaises administration ou configuration ou perte de supports de données) ou à des défaillances techniques dont les causes peuvent être multiples (p. ex. vieillissement des infrastructures, phénomènes naturels, surcharge, défaut de conception ou entretien insuffisant, pénurie énergétique). De tels événements d'ampleur variable se produisent souvent et font partie du quotidien des départements informatiques des entreprises et des pouvoirs publics. En conséquence, les effets de ces erreurs et de ces défaillances sont généralement faciles à maîtriser. Néanmoins, il est important de souligner que bon nombre de ces cyberincidents ne cachent pas des attaques ciblées, mais reposent sur 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 la prévention lors la planification et de l'application des mesures de protection.

Les cyberrisques dus aux erreurs humaines ou aux défaillances techniques resteront fréquents. 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. La formation des collaborateurs et, plus généralement, une préparation et une planification rigoureuses de ces incidents restent donc au cœur de la protection contre les cybermenaces.

1.1.3 Facteurs influençant l’état de la cybermenace

Les développements technologiques, politiques et sociaux ont une influence marquée sur l’état de la menace. Tout peut en principe changer d'un instant à l'autre. Il est néanmoins possible d'identifier divers facteurs qui, selon toute probabilité, influenceront à l'avenir l'évolution des cybermenaces. Il est important d'en tenir compte dans le contexte stratégique. Par ailleurs, il faut toujours garder à l'esprit qu'aucune liste de facteurs d'influence ne peut prétendre à l'exhaustivité et que l'évolution permanente de la menace se doit de repérer de bonne heure d'autres influences possibles ainsi que de réévaluer en permanence les facteurs déjà identifiés.

L'évolution de la cybermenace dépend largement des changements géopolitiques et des innovations technologiques. En ce qui concerne la géopolitique, on peut dire pour simplifier qu'une hausse des tensions géopolitiques ravive la cybermenace. Sachant qu'Internet met en réseau les États, les entreprises et les individus du monde entier, les tensions internationales affectent directement leurs interactions. Une recrudescence de cyberattaques est donc à prévoir de part et d'autre sous toutes les formes décrites ci-dessus. Il faut par ailleurs s'attendre à des tensions croissantes entre les pays comptant parmi les principaux

fabricants de matériel informatique et de logiciels, y compris à des blocages mutuels. Cela complique l'achat de tels outils et rend d'autant plus important, pour les bénéficiaires de prestations, d'évaluer très précisément les risques lors de chaque acquisition.
Quant aux développements technologiques, il convient de rappeler que les innovations techniques peuvent aussi bien améliorer la situation que la détériorer, et qu'elles font parfois les deux à la fois. En effet, les nouvelles technologies ont beau renforcer la sécurité dans bien des cas, elles créent par ailleurs de nouvelles dépendances, ajoutent à la complexité voire aboutissent directement à de nouvelles menaces, les agresseurs tirant directement parti des avancées en question. Il est par conséquent essentiel, à des fins de protection, de réfléchir de bonne heure aux nouveaux développements technologiques et d'anticiper les menaces potentielles.

Durant les années à venir, il faudra notamment suivre de près les développements de trois technologies utilisées pour la transformation numérique:

- **Informatique en nuage (*cloud computing*)**: l'informatique en nuage permet le déploiement de nouvelles applications ou d'innovations technologiques et peut très bien renforcer la cybersécurité, en veillant par exemple à la disponibilité élevée de l'information. Elle présente toutefois de nouveaux risques. Il arrive en effet que des données revêtant une grande importance pour la Suisse soient traitées à l'étranger, si bien que la législation suisse n'est plus seule à régir la protection juridique applicable à l'accès par des tiers et à l'utilisation des données. En outre, l'informatique en nuage pourrait aboutir à une dépendance élevée d'un petit nombre de prestataires. En l'absence de contre-mesures appropriées, ces effets de l'informatique en nuage risquent d'être préjudiciables à la cybersécurité.
- **Internet des objets (IdO)**: la mise en réseau des objets physiques progresse à une vitesse vertigineuse. L'IdO sert à la gestion, à la surveillance et à l'interconnexion des systèmes de contrôle industriels, mais aussi des biens de consommation. Cet essor de l'IdO crée tout d'abord un contexte favorable aux cybermenaces. Avec leurs milliers d'objets connectés, les environnements système gagnent en complexité, et leur exposition potentielle aux attaques augmente. Ensuite, la mise en réseau accroît d'autant le risque de cybersabotage. Il devient toujours plus simple de causer des dommages matériels à l'aide de cyberattaques. On notera enfin que bien souvent, par souci d'économie, la sécurité des appareils de l'IdO tend à être négligée lors de la fabrication et durant tout leur cycle de vie. Les dispositions de droit national ou européen portant sur la sécurité des appareils de l'IdO (p. ex. ordonnance de l'OFCOM sur les installations de télécommunication) remédient toutefois à cette situation.
- **Intelligence artificielle (IA)**: la puissance de calcul élevée et les données disponibles ont contribué à l'essor de l'IA. Douées de capacités d'apprentissage automatique plus ou moins autonome, les applications de l'IA viennent à bout d'analyses très complexes en très peu de temps. Ces possibilités peuvent servir à mieux protéger les systèmes ou, a contrario, à lancer des cyberattaques plus efficaces et rentables. Et comme beaucoup d'organisations se fient toujours plus aux analyses de leurs applications d'IA quand elles ont des décisions à prendre, des attaques ciblant ces applications constituent un scénario de menace à ne pas négliger. En outre, les applications de l'IA peuvent présenter un danger même sans intervention extérieure, si une application défectueuse devait provoquer un dysfonctionnement ou une fuite de données.

En plus de l'évolution de technologies soutenant la transformation numérique, il convient de suivre de près les développements technologiques dont l'usage à grande échelle n’est pas encore en vigueur, mais dont l’utilisation pourrait avoir une influence directe sur la cybersécurité. C'est le cas par exemple des technologies quantiques, qui permettent de résoudre certains problèmes mathématiques bien plus efficacement qu'avec les ordinateurs actuels. Comme elles sont susceptibles de déjouer les procédures de cryptage asymptotiques très répandues aujourd'hui, il faudra développer et utiliser des algorithmes post-quantiques. Il s'agira de ne pas perdre de vue ces avancées technologiques lors de l'application des mesures découlant de la présente stratégie.

1.2 État de la protection de la Suisse contre les cyberrisques

La présente stratégie se base sur les travaux liés à l'élaboration des deux premières stratégies nationales de protection contre les cyberrisques, qui ont déployé leurs effets de 2012 à 2017 et de 2018 à 2022. Elle tient également compte des orientations stratégiques définies par la Suisse pour sa transformation numérique et sa politique de sécurité. D'un point de vue institutionnel, l'organisation adoptée à la Confédération ainsi que les organes créés aux fins de l'encouragement de la collaboration entre la Confédération, les cantons, les milieux économiques et les hautes écoles permettent de juger de l'état de protection de la Suisse face aux cybermenaces.

1.2.1 Les deux premières cyberstratégies nationales

Les deux premières stratégies se sont concentrées sur la mise en place, puis sur l'extension des capacités, des structures et des processus. Leur mise en œuvre a jeté les bases nécessaires à une politique cohérente en matière de cybersécurité sur le plan suisse. Dans le cadre de ces stratégies, des décisions de principe ont été prises à propos des structures organisationnelles de la politique de cybersécurité. Un centre de compétence a vu le jour à l'échelon fédéral, soit le Centre national pour la cybersécurité (NCSC), et les organes nécessaires à la collaboration entre les services fédéraux comme avec les cantons, les milieux économiques et les hautes écoles ont été institués. Les travaux accomplis ont ainsi jeté les bases nécessaires et la présente stratégie peut désormais fixer des priorités matérielles dans les travaux en cours ou à venir.

1.2.2 Contexte stratégique de la présente cyberstratégie

Plusieurs stratégies de la Confédération fixent les lignes directrices déterminantes pour la protection de la Suisse contre les cybermenaces. Elles servent de base à la présente stratégie:

- **Stratégie Suisse numérique**: cette stratégie indique comment la Suisse compte tirer le meilleur parti possible des chances que la transformation numérique offre à la société et à l'économie. La confiance et la sécurité constituent l'un des cinq domaines d'application de la stratégie.
- **Stratégie nationale de protection des infrastructures critiques (stratégie nationale PIC):** cette stratégie définit la notion d'infrastructures critiques et détermine les secteurs et parties de secteurs réputés sensibles en Suisse. Elle contient des mesures visant à améliorer la résilience de la Suisse sur le plan des infrastructures critiques.
- **Rapport du Conseil fédéral sur la politique de sécurité de la Suisse:** dans son rapport sur la politique de sécurité, le Conseil fédéral fixe l'orientation stratégique fondamentale de la politique de sécurité de la Suisse. Ce rapport et le rapport complémentaire de 2022 décrivent l'importance des cybermenaces pour la politique de sécurité et définissent les notions utiles dans ce contexte.
- **Conception générale cyber de l'armée suisse:** la Conception générale cyber met en évidence les défis du cyberespace et de l'espace électromagnétique (CYBEEM) ainsi que ceux des technologies de l'information et de la communication, puis décrit les capacités que l'armée suisse devra développer d'ici 2035 environ pour être à même de faire face aux défis à venir.
- **Stratégie de politique extérieure numérique:** cette stratégie définit les champs d'action de la politique extérieure numérique du Conseil fédéral pour les années à venir. Dans le domaine de la cybersécurité, la Suisse milite pour l'adoption de normes de droit international relatives au cyberespace, pour l'intégration des acteurs privés dans la politique de cybersécurité et pour l'instauration de mesures propices à la création d'un climat de confiance. Elle propose également ses bons offices sur les questions liées à la cybersécurité.

1.3 Organisation de la protection contre les cybermenaces en Suisse

La cybersécurité est un thème transversal, qui ne peut relever de la compétence d'une seule et même autorité. À plus forte raison en Suisse, où la répartition des tâches est régie par le fédéralisme. Bien que les interactions numériques soient dépourvues d'ancrage territorial, le principe constitutionnel des compétences étatiques s'applique également dans le cyberespace.
Sur cette base, la Confédération et les cantons ont mis en place leurs cyberorganisations respectives. Les structures de la Confédération et des cantons sont certes définies dans les grandes lignes, mais il reste important de les examiner en permanence et de les développer si nécessaire.
De même que la répartition des tâches entre les divers échelons étatiques, l'aspect de la collaboration entre les acteurs publics et privés revêt une importance décisive dans le domaine de la cybersécurité. Il se fait par le biais d'organisations composées d'acteurs publics et privés, par l'implication directe d'associations et d'entreprises dans la mise en œuvre des mesures de la CSN ou encore dans la coopération quotidienne et l'échange d'expériences entre les équipes de sécurité privées et publiques. Plutôt que de passer en revue toutes les organisations ou les formes de coopération pertinentes pour la cybersécurité, ce sous-chapitre expose les grandes lignes de l'organisation de la Confédération et des cantons et décrit les mécanismes de pilotage de la mise en œuvre de la stratégie.

1.3.1 Organisation et compétences de la Confédération

La Confédération déploie des activités dans trois grands domaines:

- **la cybersécurité:** ensemble des mesures visant à prévenir et à gérer les incidents et à améliorer la résilience face aux cyberrisques ainsi qu'à développer la coopération internationale à cet effet;
- **la cyberdéfense:** ensemble des mesures prises par les services de renseignement et l'armée dans le but de protéger les systèmes critiques dont dépend la défense nationale, de se défendre contre les cyberattaques, de garantir la disponibilité opérationnelle de l'armée dans toutes les situations ayant trait au cyberespace et de développer ses capacités et compétences afin qu'elle puisse apporter un appui subsidiaire aux autorités civiles; ce domaine inclut également des mesures actives visant à identifier les menaces et les attaquants ainsi qu'à contrer et à bloquer les attaques;
- **la poursuite pénale de la cybercriminalité:** ensemble des mesures prises par la police et les ministères publics de la Confédération et des cantons pour lutter contre la cybercriminalité.

Les tâches principales dans le domaine de la cybersécurité ainsi que la coordination avec les autres services compétents sont du ressort du NCSC. Le Conseil fédéral a décidé le 2 décembre 2022 de le transformer en un office fédéral. Les tâches du nouvel office portent exclusivement sur la cybersécurité civile et sont ainsi clairement délimitées par rapport aux tâches assumées par le Service de renseignement de la Confédération et par l'armée dans le domaine de la cyberdéfense. L'office n'a pas non plus hérité des tâches sectorielles de surveillance ou de réglementation des autorités spécialisées. Ces dernières demeurent chargées d'accorder les autorisations requises au secteur de l'industrie et aux entreprises concessionnaires, veillant en permanence au niveau opérationnel au respect des directives sectorielles en matière de cybersécurité. Dans ce contexte, le NCSC collabore directement avec les offices spécialisés et met à leur disposition son savoir lié à la cybersécurité

Le domaine de la poursuite pénale de la cybercriminalité est avant tout du ressort des cantons. Les autorités compétentes à l'échelon de la Confédération sont l'Office fédéral de la police (fedpol) et le Ministère public de la Confédération (MPC).

Les bases légales de ces deux organisations précisent encore les compétences des services impliqués. Les unités administratives veilleront par ailleurs entre elles, dans le cadre fixé par la loi, à pratiquer un échange continu d'informations et d'expériences, à des fins de coordination optimale et d'exploitation des synergies.

1.3.2 Organisation et compétences des cantons

Les cantons définissent de manière autonome leur organisation de la cybersécurité, en fonction de leurs besoins. Ils peuvent se référer à cet effet aux «Recommandations de mise en œuvre des organisations cantonales pour la cybersécurité», élaborées par le Réseau national de sécurité (RNS) et adoptées en 2020 par la Conférence des directrices et directeurs des départements cantonaux de justice et police (CCDJP). La structure organisationnelle recommandée prévoit la désignation d'une personne chargée de la coordination des tâches liées à la cybersécurité (coordinateur cyber) et la création d'un comité politique à l'échelon du Conseil d'État. De telles structures garantissent la prise en compte du caractère transversal de la cybersécurité.
Même si la coordination intercantonale sur les thèmes de cybersécurité est du ressort de la CCDJP, d'autres conférences des directeurs peuvent s'occuper d'aspects spécifiques, selon leur domaine de compétence. L'ANS coordonne et encourage ici la collaboration avec la Confédération.

1.3.3 Pilotage commun de la CSN par la Confédération, les cantons, les milieux économiques et les hautes écoles

Le Conseil fédéral désigne un comité chargé de piloter la mise en œuvre de la CSN en coordonnant les travaux de mise en œuvre de tous les acteurs impliqués, de même qu'en recensant et en évaluant les progrès réalisés. Formé d'experts des divers domaines de la cybersécurité, ce comité de pilotage a pour mission d'intégrer les besoins respectifs des cantons, des milieux économiques, de la société, des hautes écoles et de la Confédération.
Le comité de pilotage élabore un plan pour sa coordination des travaux, d'entente avec les acteurs centraux. Ce plan vise à faire coïncider les priorités des acteurs concernés afin que les travaux de mise en œuvre se déroulent de manière cohérente et ciblée.
Pour pouvoir juger des progrès réalisés dans la mise en œuvre des mesures, le comité de pilotage définit des indicateurs de performance pour chacun d'entre elles. Ces indicateurs doivent lui permettre de savoir si les activités de mise en œuvre de la mesure en question ont permis d'atteindre les objectifs de la stratégie avec les exigences de qualité voulues.
Le comité de pilotage informe régulièrement le Conseil fédéral et les cantons de l'avancement des activités de mise en œuvre de la stratégie et leur livre son appréciation qualitative des travaux effectués. Il incombe au NCSC, qui assure son secrétariat, de transmettre ces informations au Conseil fédéral et aux cantons, en passant par le DDPS. Le comité de pilotage peut encore proposer au Conseil fédéral et aux cantons, par le même canal, de compléter, modifier ou supprimer des mesures ou encore de compléter la stratégie par d'autres objectifs ou mesures.

2 Orientation stratégique de la CSN

2.1 Vision et objectifs stratégiques

2.1.1 Vision

«La Suisse saisit les chances offertes par la transformation numérique et engage des mesures de protection pour réduire les cybermenaces et leurs conséquences. Elle compte parmi les leaders mondiaux en matière de connaissances, de formation et d'innovation dans le domaine de la cybersécurité. Dans le contexte des cybermenaces, la capacité d'action et l'intégrité de sa population, de son économie, de ses autorités et des organisations internationales basées sur son territoire sont garanties.»

2.1.2 Objectifs stratégiques

- **Responsabilisation:** la Suisse renforce sa position de leader mondial en matière de connaissances, de formation et d'innovation, y compris dans le domaine de la cybersécurité. Elle utilise ces compétences pour évaluer de manière autonome les cyberrisques qui pèsent sur les chaînes d'approvisionnement, pour anticiper les développements technologiques et y réagir avec agilité. La population est informée des cyberrisques et gagne ainsi en confiance dans l'utilisation des services numériques.
- **Fiabilité des infrastructures et des services numériques:** la Suisse met en œuvre des mesures de renforcement de la cyberrésilience sur l'ensemble de son territoire. La Confédération et les cantons créent les conditions-cadres nécessaires afin qu'un niveau de protection élevé soit garanti, que des infrastructures, produits et services numériques sûrs soient utilisés et que des risques puissent être pris en connaissance de cause.
- **Détection, prévention, gestion et défense efficaces contre les cyberincidents**: la Suisse dispose dans toutes les situations des capacités et des structures d'organisation requises pour repérer rapidement les cybermenaces ou cyberincidents et en limiter l'impact. Elle les maîtrise même si ceux-ci s'inscrivent dans la durée et concernent plusieurs domaines en même temps.
- **Lutte et poursuites pénales efficaces contre la cybercriminalité:** la Suisse renforce ses capacités à identifier les auteurs de cyberattaques, de les poursuivre pénalement en coopération avec d'autres États et de les condamner, dans le cadre des possibilités légales.
- **Rôle de premier plan dans la coopération internationale:** la Suisse s'engage, aux niveaux opérationnel et stratégique, pour un cyberespace ouvert, libre et sûr et pour la pleine reconnaissance, le respect et l'application du droit international dans le cyberespace. La Genève internationale est la plateforme principale des débats sur la cybersécurité. La Suisse peut jouer un rôle de médiateur en cas de divergences sur la réponse à donner à des cyberopérations.

2.2 Principes

La vision et les objectifs stratégiques représentent *ce que* la CSN se propose d'atteindre. Les principes définissent *comment* y parvenir.

- La CSN s'appuie sur une **approche exhaustive basée sur les risques**, qui a pour objectif d'améliorer la résilience de la Suisse face aux cybermenaces. Si elle admet qu'il est impossible de se protéger contre toutes les cybermenaces en employant l'expression «basée sur les risques», cette stratégie énonce néanmoins que ces menaces peuvent être abordées de manière à ce que le risque résiduel soit acceptable. L'approche est dite «exhaustive», car elle prend en compte toutes les vulnérabilités pertinentes et tous les risques.

- La protection de la Suisse contre les cybermenaces est une **tâche commune de la société, des milieux économiques et de l'État**. Les responsabilités et compétences respectives sont clairement définies et sont portées par toutes les parties prenantes. La stratégie est donc mise en œuvre de manière décentralisée et sous responsabilité commune, selon les principes du fédéralisme.
- La CSN repose sur une conception du **rôle subsidiaire et partenarial de l'Etat**. Ce dernier intervient seulement lorsque le bien-être de la société est gravement menacé et que les acteurs privés ne peuvent ou ne veulent pas résoudre le problème eux-mêmes. Le cas échéant, l'État peut apporter son soutien et mettre en place des incitations ou une réglementation, tout en définissant les mesures qui s'imposent en accord avec les acteurs concernés et en s'efforçant de coopérer étroitement avec eux.
- Pour autant que cela ne compromette pas l'efficacité des mesures décidées, la mise en œuvre de la CSN obéit au principe de la transparence. Celui-ci est satisfait au moyen d'une **communication active** envers la société, les milieux économiques, scientifiques et politiques, et l'implication directe des partenaires clés issus de l'administration, de la société et du secteur privé.

2.3 Groupes cibles

La Confédération et les cantons déterminent dans la CSN les objectifs qu'ils entendent atteindre en étroite collaboration avec les milieux économiques, scientifiques et la société. L'effet recherché par la CSN concerne ainsi toute la Suisse. La stratégie s'adresse aux groupes cibles suivants:

- **Population:** la protection de la population est le but commun de toutes les mesures de la CSN. De tous les cyberincidents, ce sont les attaques lancées par des cybercriminels qui touchent la population le plus directement, ou du moins ses données personnelles. La CSN contribue ici à sensibiliser la population, à la mettre en garde contre de telles menaces et à lui permettre d'utiliser les technologies numériques en toute sécurité. Elle renforce la protection des données, en veillant à ce que les services responsables et les individus concernés gardent le contrôle des données personnelles et en empêchant tout accès abusif par des tiers.
- **Milieux économiques:** les milieux économiques ont besoin de sécurité pour être compétitifs. Les cybermenaces constituent de grands défis pour toutes les entreprises, en particulier les petites et moyennes entreprises (PME). La mise en œuvre de la CSN sert à renforcer la sécurité au profit des entreprises suisses. Le NCSC y définit l'aide leur étant fournie pour la gestion des cybermenaces en complément des offres disponibles sur le marché. Les entreprises restent toutefois responsables d'assurer leur propre protection.
- **Infrastructures critiques:** les infrastructures critiques garantissent la disponibilité de biens et de services essentiels. Leur fonctionnement est indispensable pour la population et pour les milieux économiques suisses. Hautement prioritaire, leur protection constitue le point de mire de toutes les mesures de la CSN, qui tiendront compte de la diversité des situations quant à l'exposition aux risques.
- **Autorités:** il incombe à la Confédération, aux cantons et aux communes de protéger leurs services. Les collectivités publiques doivent garantir un haut niveau de disponibilité pour accomplir leur mission. Quel que soit leur échelon, elles traitent des informations sensibles et proposent de plus en plus de prestations en ligne. La mise en œuvre de la CSN permet d'améliorer la résilience des autorités.
- **Organisations internationales et organisations non gouvernementales (ONG):** la Suisse aide les organisations internationales à se protéger contre les cybermenaces et garantit une cybersécurité élevée pour les activités des organisations internationales et des ONG.

3 Mesures découlant de la CSN

Les mesures décrites dans le présent chapitre doivent permettre d'atteindre les cinq objectifs stratégiques définis. Elles se fondent sur les activités existantes et indiquent comment les étendre, les développer et les compléter pour parvenir auxdits objectifs. On voit aussi dans ce chapitre où se situent les priorités dans la mise en œuvre des mesures et quels sont les acteurs impliqués. La liste des priorités reflète la situation au moment de l'élaboration de la stratégie. Le comité de pilotage de la CSN la contrôle en permanence et la complétera en cas de besoin.
La liste des acteurs n'est pas exhaustive, mais entend plutôt montrer au comité de pilotage à qui il convient de s'adresser pour l'évaluation et le développement de la mesure en question. À propos des acteurs principaux de l'administration fédérale, la liste indique toujours en tête, en italique, l'unité chef de file, puis les autres acteurs pertinents par ordre alphabétique. Les organisations des cantons, des hautes écoles, de l'économie et de la société sont à chaque fois indiquées séparément. Seul l'acronyme est utilisé. La table des abréviations indique toutefois le nom complet des organisations.
Avant toute mise en œuvre des mesures, il faut d'abord vérifier si les bases légales nécessaires sont en place ou s'il faut commencer par adapter le droit à l'échelon étatique concerné. Il en va notamment ainsi pour les échanges de données, dont les modalités devront être réglées dans toutes les lois et ordonnances applicables, a fortiori pour les données personnelles.

3.1 Mesures concernant l'objectif «Responsabilisation»

Pour renforcer la responsabilisation de la Suisse dans la protection face aux cybermenaces, des mesures seront prises dans les domaines de la formation, de la recherche et de l'innovation, de la sensibilisation et de l'évaluation de la cybermenace, ainsi que de l'extension des capacités d'analyse des liens de dépendance et des risques.

M1 Formation, recherche et innovation en matière de cybersécurité

Aperçu de la mesure	
Description	Pour se protéger contre les cybermenaces, la Suisse a besoin de personnel spécialisé en suffisance. Il faut également s'assurer que la population possède les compétences de base pour faire bon usage des technologies et services numériques. Les établissements de formation et de recherche doivent privilégier la transversalité dans l'acquisition des compétences correspondantes, dans leur transmission et dans leur enrichissement. La formation, la recherche et l'innovation ne sont pas seulement nécessaires pour renforcer la protection contre les cybermenaces. Elles doivent aussi et surtout contribuer directement au succès de la place économique suisse. État neutre possédant un niveau de formation élevé et un système d'innovation robuste, la Suisse entend tirer parti de ses atouts pour faire partie des leaders mondiaux des services et produits dédiés à la cybersécurité.

Contexte et actions requises	La Suisse dispose d'un réseau performant d'établissements de formation et de recherche. Elle a mis en place ces dernières années diverses possibilités de formation dans la lutte contre les cyberrisques. Ce n'est toutefois pas suffisant pour couvrir les besoins élevés de spécialistes de la cybersécurité au sein de l'économie, et la transmission des compétences dans le domaine de la cybersécurité n'est pas encore assurée à tous les niveaux de formation (école obligatoire, secondaire II et tertiaire, formation continue). Ces dernières années, de nombreuses start-ups ont été créées en Suisse dans le domaine de la cybersécurité, et divers acteurs importants ont ouvert des succursales en Suisse. Une comparaison avec les régions leaders au niveau international ou avec la capacité d'innovation de la Suisse dans d'autres secteurs montre toutefois clairement qu'il faut continuer à améliorer les conditions cadres nécessaires à l'innovation en matière de cybersécurité.
Priorités	- Éducation: encourager à tous les niveaux la formation et le perfectionnement en matière de cybersécurité. Alors que la scolarité obligatoire doit avant tout permettre d'acquérir des compétences de base, la formation professionnelle (formation de base et formation professionnelle supérieure), l'enseignement supérieur et la formation continue nécessitent des offres ciblées, adaptées aux besoins du marché du travail. Afin d'encourager la formation en cybersécurité, il convient de tirer parti des instruments prévus dans la politique de formation de la Suisse qui ont démontré leur efficacité. Le personnel enseignant bénéficiera de matériel pédagogique adéquat et du soutien d'experts en vue de la transmission de compétences en cybersécurité et la coordination entre établissements de formation sera encouragée. Il s'agit de mettre en place en Suisse une offre plus large de cours et de filières de formation spécifiques (p. ex. pour le personnel des infrastructures critiques). - Recherche: la recherche sur la cybersécurité est promue au travers des moyens actuels de la politique suisse en matière de recherche. Il est essentiel que les travaux de qualité menés en Suisse aient davantage d'effet sur les politiques, les milieux économiques et la société. À cet effet, il est nécessaire renforcer la coordination entre les différentes disciplines de recherche en matière de cybersécurité, dans le but de formuler et de communiquer des recommandations communes. - Innovation: mettre en réseau des acteurs afin de promouvoir l'innovation. Les échanges entre les hautes écoles, les entreprises et les autorités doivent encore être intensifiés. Les services fédéraux compétents encourageront, dans le cadre des possibilités légales, l'implication d'experts dans leurs diverses activités de cybersécurité, en tirant parti du programme Innovation Fellowship et des programmes similaires en place.
Acteurs principaux	- Administration fédérale: *CYD Campus*, *NCSC*, *SEFRI* - Cantons: CCDJP, ISP, CDIP, CSHE - Hautes écoles: toutes les hautes écoles suisses, SSCC, swissuniversities, Conseil des EPF - Économie / société: Formation professionnelle suisse, associations du secteur des TIC, Innosuisse, ASST

M2 Sensibilisation

Aperçu de la mesure	
Description	Des mesures de sensibilisation s'imposent, afin que la population suisse fasse usage des produits et services électroniques en ayant connaissance des risques qu'ils comportent. Le but est de parvenir à une réelle prise de conscience à grande échelle en matière de cybersécurité et de fournir des instruments qui encouragent une utilisation responsable des technologies et services numériques. Cela comprend également l'objectif en matière de protection des données, à savoir que les individus conservent le contrôle de leurs données personnelles, et les organisations garantissent la transparence quant à leurs méthodes de traitement de ces données. Globalement, la sensibilisation vise à rendre la société plus résiliente face aux cyberrisques.
Contexte et actions requises	Beaucoup d'institutions, d'entreprises ou d'organisations sont déjà actives dans la sensibilisation à la cybersécurité, afin d'aider les entreprises et les particuliers à se prémunir contre les cyberrisques. Il faut toutefois une coordination accrue et une concentration des efforts actuels ou prévus, car il s'agit de sensibiliser les gens par groupe cible et par degré d'implication. À cet effet, il faut définir les groupes cibles et déterminer les mesures à prendre au plus près de chacun d'eux. Les expéditeurs coordonneront leurs messages, afin d'aider les destinataires à comprendre une matière parfois complexe par une communication équilibrée. De nombreuses compétences existent déjà pour atteindre certains groupes cibles. Il s'agira par conséquent de continuer à tirer parti des comités et organisations en place et de leurs canaux de diffusion (p. ex. manifestations et revues spécialisées d'associations professionnelles, de groupes d'intérêt ou d'organisations faîtières).
Priorités	- Evaluation des besoins: il convient de vérifier en permanence les besoins de sensibilisation et de prévention dans les différents domaines. Les incidents actuels et l'évolution de l'état de la menace serviront ici de point de départ, tout comme les estimations des autorités, des entreprises et des associations économiques sur le besoin de sensibilisation dans leurs secteurs respectifs. - Vue d'ensemble et coordination: les acteurs s'occupant de sensibilisation sont connus, et leurs échanges font l'objet d'encouragements ciblés. - Mesure des résultats: il convient de passer en revue les efforts consentis et les effets obtenus afin de déterminer le succès des mesures de sensibilisation adoptées et de les optimiser.
Acteurs principaux	- Administration fédérale: *NCSC*, OFPP, OFCOM, OFT, OFDF, OFEN, OFAS, OFAE, PFPDT, SRC - Cantons: communes et villes, centres de compétence cantonaux en cybersécurité, corps de police cantonaux, CCDJP, PSC - Économie / société: toutes les associations économiques ou professionnelles, les sociétés, les ONG et les entreprises qui le désirent pourront participer aux campagnes de sensibilisation, si c'est judicieux.

M3 État de la menace

Aperçu des mesures	
Description	Pour juger de l'état de la menace, il est nécessaire de déterminer quels acteurs exploitent ou pourraient exploiter quels vecteurs d'attaque et quelles vulnérabilités. On procédera à une pondération des menaces par la même occasion. L'évaluation de l'état de la menace qui s'ensuit doit fournir aux milieux économiques, à la société et à l'administration une base solide pour identifier et mettre en œuvre leurs mesures de réduction des risques de manière ciblée et à moindre coût. L'évaluation de la menace doit dès lors mettre en lumière non seulement les menaces globales et déployant des effets à large échelle, mais aussi les menaces spécifiques à certains processus ou domaines d'activité.
Contexte et actions requises	La Suisse a déjà défini les cybermenaces d'un point de vue tactique, opérationnel et stratégique et met à jour périodiquement les évaluations en question. Ces dernières se fondent sur l'observation des acteurs malveillants et des moyens effectifs et potentiels dont ils disposent, ainsi que sur les informations connues concernant les dégâts ou défaillances causés par les cyberincidents. La progression de la transformation numérique des processus dans divers secteurs économiques augmente le besoin de procéder à des évaluations spécifiques de la menace qui pèse sur ces secteurs. En réponse à ce besoin, il convient d'assurer un traitement adapté des informations pertinentes sur les menaces. Ces informations relatives aux menaces sont ensuite transmises aux entreprises et aux autres organisations, en fonction de leurs besoins.
Priorités	- Développement du suivi de la situation, en se concentrant sur les acteurs représentant une menace tactique, opérationnelle ou stratégique pour la Suisse. - Développement de l'évaluation et de la préparation des informations pertinentes concernant la situation. Mise à disposition à tous les niveaux pour les milieux économiques, pour la société et l'administration. - Soutenir la création de centres de partage et d'analyse de l'information (ISAC) propres aux secteurs, et instaurer une collaboration étroite pour évaluer les menaces spécifiques.
Acteurs principaux	- Confédération: *SRC*, NCSC - Cantons: corps de police cantonaux, centres de compétence cantonaux en cybersécurité, offices informatiques, NEDIK - Économie / société: CERT/SOC de l'économie, ISAC, prestataires de services de sécurité, SWITCH

M4 Analyse des tendances, des risques et des dépendances

Aperçu de la mesure	
Description	Il est essentiel pour la Suisse de comprendre l'ampleur de sa dépendance aux technologies numériques, son évolution et les risques qui en découlent. L'évolution dynamique des technologies numériques exige d'identifier de bonne heure les nouveaux développements et d'en comprendre les effets sur la sécurité. Une telle approche doit aussi aider la Suisse à se renforcer en tant que place économique développant et utilisant des technologies et des services numériques sûrs. Une autre raison de procéder à des analyses vient de ce qu'aujourd'hui, les technologies numériques clés sont surtout produites à l'étranger. Or, il est important pour la Suisse de comprendre les dépendances qui existent par rapport à ces producteurs et les risques qui s'ensuivent. La Suisse doit pouvoir prendre des décisions souveraines, basées sur des analyses et des évaluations autonomes et indépendantes quant à l'usage qu'elle compte faire des technologies et services numériques.
Contexte et actions requises	Le Cyber-Defence Campus (CYD Campus) d'armasuisse a collaboré étroitement avec les hautes écoles et les milieux économiques afin de mettre en place un monitorage des technologies axé sur la cybersécurité. Les Académies suisses des sciences ont par ailleurs pour mandat d'évaluer les chances et risques des nouvelles technologies. La Suisse est par contre à la traîne dans l'analyse systématique des liens de dépendance et des risques inhérents aux produits informatiques. Bientôt opérationnel, l'Institut national de test pour la cybersécurité (NTC) disposera des capacités d'examiner en détail l'exposition aux attaques des produits informatiques. Le NTC complétera et renforcera les capacités actuelles du CYD Campus et celles dont se dotent toujours plus souvent les entreprises de sécurité privées. De telles capacités sont nécessaires à toute évaluation indépendante de la sécurité des produits auxquels recourent par exemple les infrastructures critiques. L'évaluation systématique des incidents recèle elle aussi un potentiel. Elle peut aider à mieux comprendre qui est visé par quelles attaques et à prévenir les attaques en question. Cela suppose l'instauration d'échanges d'informations entre les autorités, les prestataires de services de sécurité et les hautes écoles, ainsi que la volonté des entreprises concernées d'informer de manière transparente sur les incidents survenus et leurs conséquences.

Priorités	- Mettre en place un monitorage des nouvelles technologies: le CYD Campus anticipe avec les hautes écoles les développements des cybertechnologies et partage les conclusions de cette veille avec les acteurs concernés. - Développer les compétences d'enquête sur les cyberincidents: examiner de plus près les causes et le déroulement des cyberincidents et exploiter systématiquement les résultats de ces investigations pour les caractériser. Encourager à cet effet, dans le cadre des possibilités légales, l'échange de données entre les autorités, les assureurs et les fournisseurs de services de sécurité. Les enquêtes seront facultatives pour les acteurs concernés et aideront à tirer les leçons des cyberincidents. - Faire examiner les produits TIC et les réseaux numériques par des centres de test basés en Suisse, comme le NTC, ou par des fournisseurs d'analyses de vulnérabilité et de tests d'intrusion. Le développement du NTC permettra de renforcer, conjointement avec les hautes écoles et le secteur privé ainsi qu'avec des partenaires internationaux, les compétences et les capacités de test présentes en Suisse pour l'analyse indépendante des risques inhérents aux produits TIC. Le CYD Campus renforcera également ses capacités à effectuer de telles analyses lors des préparatifs en vue d'un achat et de l'acquisition de produits TIC critiques pour la sécurité de la Confédération. - Accélérer la mise en place du NTC qui fournira, avec le concours des hautes écoles et du secteur privé, des capacités d'analyse indépendantes des risques inhérents aux produits TIC. - Analyser le degré de dépendance de la Suisse par rapport à des produits ou à des fournisseurs spécifiques. Les entreprises, les hautes écoles et les autorités définiront ensemble la manière d'effectuer ces analyses et de les mettre à jour en continu. - Surveiller les applications de l'IA utilisées dans les infrastructures critiques: procéder à un monitorage régulier dans ce domaine, sur mandat de la Confédération et des cantons, afin de mieux comprendre les capacités de ces applications et leur impact sur la société. - Renforcer encore et mieux coordonner les échanges en place entre les centres de recherche dans le cadre du CYD Campus, des hautes écoles et de l'ASST.
Acteurs principaux	- Administration fédérale: *CYD Campus, NCSC*, TNI, SRC - Hautes écoles: SSCC - Économie / société: NTC, ASST, prestataires de services de sécurité

3.2 Mesures concernant l'objectif «Fiabilité et disponibilité de l'infrastructure et des services numériques»

Des mesures s'imposent à différents niveaux pour garantir la sécurité des services et des infrastructures numériques. Il est important d'identifier et de corriger de manière précoce les vulnérabilités présentes au sein des services et des infrastructures, ainsi que de concevoir de nouveaux services et infrastructures qui en comportent d'emblée un minimum. En plus de détecter et prévenir les vulnérabilités, il est essentiel de gérer la résilience des systèmes. Sur la base des analyses des risques et des vulnérabilités, il faut définir les mesures techniques et organisationnelles à réaliser afin d'accroître la résilience des prestations et des infrastructures. À ce titre, il convient aussi de vérifier dans quels domaines il faut légiférer sur les normes ou les réglementations à respecter. En fin de compte, il s'agit pour les autorités de protéger leurs propres services face aux cybermenaces.

M5 Identifier les vulnérabilités et y remédier

Aperçu de la mesure	
Description	L'utilisation des technologies numériques conduit à l'automatisation des processus et à l'interconnexion. Il en résulte des systèmes complexes qui présentent potentiellement une grande surface d'attaque. Cette complexité, de même que la fréquente pression sur les coûts et les délais lors du développement et de l'utilisation de telles technologies accroissent le risque de failles de sécurité dans les systèmes. Or, il est essentiel pour la cybersécurité de prévenir autant que possible l'apparition de ce genre de vulnérabilités, de les repérer à temps et d'y remédier rapidement. Il importe aussi de ne publier les vulnérabilités qu'après avoir identifié et dûment mis en œuvre les contre-mesures à prendre (*coordinated vulnerability disclosure*), car en annonçant les failles trop tôt, on renforce la position des agresseurs.
Contexte et actions requises	La Suisse possède d'importantes compétences spécialisées pour identifier les vulnérabilités et en analyser les causes. Le potentiel disponible est cependant trop peu exploité. Les chercheurs en sécurité ne sont guère incités à rechercher activement et à signaler les vulnérabilités, dont l'analyse n'est pas coordonnée sur le plan suisse. Il importe aussi de collaborer étroitement avec les services spécialisés d'autres pays et les organisations internationales compétentes. Une gestion plus efficace des vulnérabilités nécessite la création de bases juridiques obligeant à les examiner, à les signaler et à les publier. Enfin, il importe d'agir pour garantir que les vulnérabilités soient rapidement annoncées et comblées. De trop nombreuses entreprises et organisations continuent de s'exposer à des risques parce qu'elles ne corrigent pas les vulnérabilités, alors que des correctifs (patches) existent depuis longtemps.

Priorités	- Institutionnaliser le piratage éthique: réaliser des programmes de primes aux bogues. Encourager le piratage éthique en améliorant la sécurité juridique au profit des pirates éthiques. - Divulgation coordonnée des vulnérabilités: promouvoir une approche coordonnée en cas de découverte de vulnérabilités afin d'accroître la sécurité et la confiance en misant sur la transparence. Définir et diffuser des directives standardisées et créer des incitations pour que les vulnérabilités soient annoncées. - Centraliser la communication relative aux vulnérabilités: positionner le NCSC comme la principale plateforme chargée de coordonner la publication des annonces de vulnérabilités et de diffuser des informations et des mises en garde sur les nouvelles failles ainsi que sur les solutions techniques et organisationnelles permettant d'y remédier. - Détection automatisée des vulnérabilités : mettre au point et utiliser des solutions en vue de l'identification et de la résolution automatisées des vulnérabilités. - Écosystème de logiciels: soutenir le développement de logiciels sûrs (en particulier dans le domaine des logiciels open source) en collaboration avec les organisations et les initiatives pertinentes. Le but étant de créer des incitations à prendre très tôt en compte la sécurité dans le développement de logiciels. Il s'agit de définir, pour le développement des composantes informatiques, des caractéristiques de sécurité formellement vérifiables. - Cybersécurité des appareils sans fil connectés à Internet: faire respecter, au moyen d'une surveillance efficace du marché, les exigences de l'ordonnance révisée de l'OFCOM sur les installations de télécommunication.
Acteurs principaux	- Confédération: *OFCOM, CYD Campus, NCSC* - Cantons: offices informatiques, centres de compétence en matière de cybersécurité - Hautes écoles: instituts de recherche en sécurité informatique - Économie / société: Alliance Sécurité Digitale Suisse, NTC, entreprises de services de sécurité

M6 Résilience, normalisation et régulation

Aperçu de la mesure	
Description	De nombreuses mesures techniques et organisationnelles permettent déjà de se protéger contre les cybermenaces. L'application rigoureuse de mesures fondamentales (protection de base) serait à même d'éviter la majeure partie des cyberincidents. Les décisions relatives aux mesures adéquates reposent sur des analyses approfondies de l'exposition aux risques des cybermenaces. À condition de comprendre comment ces risques se manifestent dans les divers secteurs, il devient possible de définir des mesures permettant d'améliorer la résilience. Les mesures s'appuient sur des normes internationales. Ces dernières constituent dès lors un instrument essentiel pour la mise en œuvre des mesures de protection. Diverses approches permettent d'encourager le respect des normes. Au-delà de la possibilité d'imposer des normes pour les mesures réglementaires, il convient surtout de prévoir des incitations à leur mise en œuvre. La transparence peut être ici une forte incitation, notamment grâce aux labels signalant qui respecte quelles normes: grâce à une telle transparence, les investissements consacrés à la cybersécurité renforcent la confiance des clients.

Contexte et actions requises	Les analyses des risques et des vulnérabilités des secteurs critiques faisaient déjà partie intégrante des deux premières stratégies en matière de cybersécurité. Il faut toutefois vérifier et adapter régulièrement les évaluations disponibles et les mesures de résilience identifiées. Des normes de cybersécurité bien établies existent par ailleurs déjà au niveau international et sont appliquées en Suisse aussi. L'OFAE a élaboré avec les milieux économiques et les offices compétents une norme minimale pour les secteurs critiques, d'où ont été tirées des normes minimales par secteur. Le respect de ces normes n'est généralement pas obligatoire. La nouvelle loi sur la protection des données, qui entrera en vigueur en septembre 2023, comporte toutefois des exigences minimales pour la sécurité des données en cas de traitement de données personnelles. Par ailleurs, certains secteurs ont entrepris des travaux pour déterminer quelles normes devraient avoir une valeur contraignante et pour quelles organisations. Outre les normes propres à certains secteurs, celles qui sont spécifiques à certaines technologies revêtent également de l'importance. Les normes de sécurité régissant le recours à l'informatique en nuage (cloud computing) ou l'IdO jouent un rôle crucial pour garantir la sécurité des nouvelles applications technologiques. La Suisse a déjà édicté dans l'ordonnance de l'OFCOM sur les installations de télécommunication des prescriptions sur la sécurité des appareils sans fil connectés à Internet. Elle examine désormais quelles exigences s'imposent dans l'informatique en nuage. Le travail à mener au niveau législatif ne se limite toutefois pas à la question de savoir s'il faut adopter des normes contraignantes. Le projet déjà mis au point sur l'obligation d'annoncer les cyberattaques en est un exemple. Il convient d'examiner en tout temps où il serait nécessaire de mettre en place des bases légales.
Priorités	- Mettre à jour selon les besoins les analyses des risques et des vulnérabilités dans les sous-secteurs critiques (OFPP et offices compétents). Prendre en compte les risques identifiés dans la gestion de la résilience en définissant des champs d'action adaptés et des mesures visant à améliorer la résilience. Vérifier régulièrement la mise en œuvre des mesures et encourager les échanges entre la Confédération et les cantons à propos des risques, des vulnérabilités et des mesures de résilience. - Promouvoir la diffusion et le respect des normes. Il convient en particulier d'encourager l'utilisation de normes dans les PME et les communes, en mettant à la disposition des instruments simples et pratiques à cet effet. Lors des marchés publics, il faudra en outre exiger et vérifier le respect des normes de sécurité informatique. - Encourager la diffusion des labels existants: des labels de cybersécurité ont été introduits avec succès en Suisse. Il est important d'en assurer la coordination au niveau tant national qu'international. Il convient dès lors d'encourager la diffusion des labels existants, en soutenant les échanges d'expériences dans ce contexte. - Vérifier dans quelle mesure et comment des prescriptions légales pourraient rendre les entreprises davantage responsables de leur propre protection contre les cyberincidents. Dans ce contexte, il convient de préférer les réglementations efficaces à des prescriptions opérationnelles détaillées. Les règlementations devront en outre être harmonisées entre les différents secteurs, pour limiter autant que possible les disparités entre les éventuelles exigences en vigueur. - Déterminer s'il est nécessaire d'adopter des réglementations par secteur; élaborer au besoin les modèles correspondants. - L'obligation d'annoncer les cyberattaques subies par les infrastructures critiques est déjà à l'étude. En cas d'adoption, les modalités de sa mise en œuvre seront fixées en étroite collaboration avec les acteurs concernés.

Acteurs principaux	- Confédération: *OFPP, OFCOM, OFT, OFDF, OFEN, NCSC*, OFAE, PFPDT - Cantons: centres de compétence cantonaux en cybersécurité - Hautes écoles: SSCC - Économie / société: cyber-safe.ch, ITSec4KMU, organisations de normalisation, NTC, prestataires de services de sécurité, associations des secteurs économiques concernés, assurances

M7 Accroître la collaboration entre les autorités

Aperçu de la mesure	
Description	La cybersécurité est devenue un enjeu central pour les autorités à tous les niveaux de l'État. Les prestations administratives en ligne doivent satisfaire un haut degré de disponibilité et être sécurisées. Si les tentatives de cyberespionnage comptent depuis des années parmi les principales cybermenaces, les attaques criminelles dirigées contre les autorités se sont également multipliées ces derniers temps. Leurs auteurs menacent par exemple les autorités de chiffrer ou de publier les données traitées. Il importe de relever ces défis à tous les niveaux de l'État.
Contexte et actions requises	Chaque autorité est responsable de sa propre cybersécurité. La loi sur la sécurité de l'information (LSI) définit le cadre et les procédures de sécurité au sein de la Confédération. Elle s'applique également aux cantons lorsque ceux-ci accèdent aux moyens informatiques de la Confédération ou qu'ils traitent des informations classifiées de la Confédération. Garantir la cybersécurité dans toutes les structures fédérales représente un défi de taille. Comme le personnel spécialisé et, souvent aussi, les ressources financières font défaut, il importe de miser sur la collaboration entre les autorités de tous les échelons de l'État. Les structures nécessaires à la collaboration existent déjà, mais il reste beaucoup de potentiel à exploiter pour renforcer la collaboration opérationnelle. Il convient par ailleurs de déterminer dans quelle mesure et dans quelles situations la Confédération peut apporter un soutien aux cantons et aux communes.
Priorités	- Mise en œuvre de la LSI au sein de l'administration fédérale. - Encourager l'échange d'informations sur la cybersécurité au sein de l'administration fédérale, en particulier entre le NCSC et les offices spécialisés. - Renforcer la collaboration entre la Confédération et les cantons. - Déterminer le soutien que la Confédération peut apporter aux cantons, aux villes et aux communes. - Encourager les échanges avec les autorités internationales.
Acteurs principaux	- Confédération et cantons: RNS, TNI, ANS, centres cantonaux de compétence en matière de cybersécurité, organisations de communes (Association des communes suisses, Union des villes suisses, p. ex.), NCSC

3.3 Mesures destinées à réaliser l'objectif «Détection, prévention, gestion et défense efficaces contre les cyberattaques»

La prévention, la détection, la gestion et la défense efficaces contre les cyberattaques sont des facteurs clés de la cybersécurité. Il est essentiel de connaître clairement la nature de la menace pour définir les mesures de protection adéquates. Si un incident devait malgré tout se produire, il faut disposer d'outils, de données et de processus appropriés pour la gestion de l'incident. Il importe ensuite d'identifier aussi précisément que possible l'auteur de l'attaque (attribution), cette identification contribuant à mieux cerner l'état de la menace et à prévenir de futures attaques. Si les cyberincidents ont un impact sur le bon fonctionnement d'infrastructures critiques ou causent un grave préjudice à la sécurité du pays, une gestion de crise s'impose. Celle-ci doit faire l'objet d'exercices réguliers afin d'assurer son bon fonctionnement.
Enfin, les possibilités de déjouer les cyberattaques ne se limitent pas aux mesures destinées à assurer la protection des systèmes attaqués. Il importe de collecter des données techniques sur les agresseurs ainsi que sur leurs modes opératoires et de les mettre à la disposition d'éventuels acteurs concernés. Des mesures actives visant à détecter la menace, à identifier les agresseurs ainsi qu'à perturber et bloquer leurs attaques sont également envisageables.

M8 Gestion des incidents

Aperçu de la mesure	
Description	Sachant qu'il n'existe pas de protection absolue contre les cyberincidents, l'une des priorités en matière de cybersécurité est d'instituer et d'exploiter une organisation chargée de traiter les incidents *(incident management)*. À cette fin, il importe de détecter les cyberincidents le plus tôt possible, de les identifier et de prendre les contre-mesures de lutte appropriées. Il s'agit également d'analyser les incidents survenus et d'en tirer les conclusions nécessaires pour améliorer la prévention. Afin de mener à bien ces tâches, faut des compétences spécialisées, des outils d'analyse, une organisation efficace dotée de compétences décisionnelles clairement définies et une collaboration étroite de tous les services concernés. Il est essentiel que des partenaires dignes de confiance échangent entre eux les informations dont ils disposent sur les incidents et les mesures de lutte possibles, car les incidents se produisent souvent à plusieurs endroits à la fois. Le partage des informations pertinentes permet une gestion plus rapide et efficace des incidents.

Contexte et actions requises	Beaucoup d'organisations en Suisse, mais de loin pas toutes les infrastructures critiques, ont créé ou mandaté des équipes spécialisées dans la gestion des cyberincidents. Celles-ci se nomment par exemple Security Operations Centers (SOC), Computer Emergency Response Teams (CERT) ou Computer Security Incident Response Teams (CSIRT), et leurs compétences spécifiques varient selon leur domaine d'activité. De nombreux cantons ainsi que la Confédération disposent également de telles équipes. La gestion des cyberincidents est assurée en premier lieu par ces unités. La Confédération apporte à titre subsidiaire un appui aux équipes des cantons, des villes et des communes ainsi qu'aux exploitants d'infrastructures critiques et à leurs prestataires en matière de sécurité par l'intermédiaire du NCSC, afin de procéder à l'analyse technique des incidents et soutient l'échange d'informations entre ces divers acteurs. Le grand public peut également signaler des cyberincidents ou des cybermenaces au NCSC, qui lui fournira au besoin de premières évaluations et recommandations techniques quant aux actions à entreprendre. De telles annonces sont essentielles à l'évaluation des cybermenaces. Fournies par la Confédération, ces prestations ne reposent pour l'heure sur aucune base légale. Il en va de même des échanges d'informations. Les projets de modification de la législation existante ont déjà été élaborés, mais n'ont pas encore fait l'objet de décisions. La mise à l'échelle des capacités constitue un défi pour la gestion des incidents. Si plusieurs incidents majeurs se produisent simultanément, les ressources actuelles seront rapidement épuisées. Le cas échéant, il importe de déterminer comment faire intervenir des spécialistes supplémentaires dans les meilleurs délais.
Priorités	- Renforcer les capacités des infrastructures critiques à détecter et à gérer des cyberincidents en développant à cet effet, la création et l'utilisation commune de centres opérationnels de sécurité (SOC). - Développer le système de signalement des cyberincidents: il est nécessaire qu'un maximum de cyberincidents soient signalés afin d'obtenir une bonne image de la situation actuelle en matière de menaces. - Promouvoir l'échange d'informations: la plateforme existante du NCSC servant à l'échange d'informations entre les exploitants d'infrastructures critiques sera remaniée et développée, afin de faciliter les échanges et d'ouvrir progressivement l'accès à la plateforme à des milieux plus larges. - Renforcement des capacités par la collaboration: il est prévu d'intensifier encore la collaboration opérationnelle et d'améliorer l'harmonisation entre GovCERT, SWITCH-CERT et d'autres équipes de sécurité. On déterminera également quand et comment faire appel à des équipes de spécialistes volontaires afin de contribuer à la gestion d'incidents. Cet examen tiendra compte des organisations existantes. - Renforcer la collaboration avec les services spécialisés: le NCSC fournira aux services spécialisés des informations sur des incidents survenant dans leur secteur, afin de leur permettre d'évaluer la menace qui pèse sur celui-ci. Les informations qui permettent d'identifier les personnes concernées sont exclues, à moins que ces dernières ne soient d'accord d'informer les services spécialisés.
Acteurs principaux	- Confédération: *NCSC,* OFCOM, OFT, OFAC, OFEN, OFIT, MilCERT - Cantons: équipes cantonales CERT, CSIRT et SOC (ou organisations similaires), services d'alerte des polices cantonales - Milieux économiques et société: équipes CERT, CSIRT et SOC (ou organisations similaires) d'entreprises ou d'organisations, SWITCH

M9 Attribution

Aperçu de la mesure	
Description	L'attribution consiste à identifier les auteurs des attaques avec autant de précision que possible. Elle joue un rôle clé dans le choix des moyens à mettre en œuvre pour la suite des évènements. Les autorités suisses doivent être en mesure d'attribuer des cyberattaques dirigées contre notre pays ou importantes pour la politique de sécurité de la Suisse. Celles-ci comprennent aussi bien les cyberattaques visant des cibles suisses que l'utilisation des infrastructures suisses pour des attaques à l'étranger. L'attribution sert de base pour formuler les options d'action politique et juridique.
Contexte et actions requises	Pour pouvoir placer les auteurs d'une cyberattaque face à leurs responsabilités, il faut commencer par les identifier. C'est là un défi de taille dans le cyberespace, car les auteurs ne sont pas physiquement présents sur le lieu de l'attaque. Une telle identification n'a de chances d'aboutir que si les attaques ont été reconnues à temps et à condition d'être en mesure d'analyser leur contexte technique, opérationnel et stratégique. L'attribution des cyberattaques est l'une des tâches du Service de renseignement de la Confédération (SRC). Pour pouvoir remplir sa mission, ce dernier a besoin de connaissances issues de ses propres recherches, mais il dépend aussi de la collaboration avec d'autres services de la Confédération et de l'échange d'informations avec des services partenaires. Il convient dès lors de réglementer cette collaboration et ces échanges. L'attribution des cyberattaques est importante pour permettre aux décideurs politiques d'évaluer l'état de la menace. Elle sert notamment à déterminer si une action peut être attribuée en vertu du droit international et les possibilités de réaction que ce dernier autorise. C'est en outre la condition préalable aux décisions concernant les mesures techniques, politiques ou pénales.
Priorités	- Examiner et compléter les bases légales régissant l'analyse de cyberattaques visant la Suisse. - Assurer la coopération entre le SRC et d'autres services. - Développer les capacités du SRC à analyser les cyberattaques pertinentes pour la politique de sécurité. - Définition des priorités stratégiques : il faut déterminer quelles attaques seront analysées de manière approfondie.
Acteurs principaux	- Confédération: *SRC,* DFAE, fedpol, NCSC, SG-DDPS - Cantons: corps de police cantonaux, NEDIK

M10 Gestion de crise

Aperçu de la mesure	
Description	Les cyberincidents peuvent entraîner de graves conséquences, au point d'exiger la mise en place d'une gestion de crise au niveau national. Il est essentiel, pour la gestion de crises, de disposer d'une image actuelle, cohérente et complète de la situation, de définir des processus efficaces de prise de décision et d'établir une stratégie de communication. Il convient encore d'éprouver, de contrôler et de modifier régulièrement les capacités et les structures prévues.
Contexte et actions requises	Une bonne collaboration intersectorielle est déterminante en cas de crise. Dans une telle situation, le NCSC doit être en mesure de mettre en place rapidement la collaboration avec tous les partenaires. Il a établi à cet effet des contacts avec les organisations pertinentes au sein de l'administration fédérale et en dehors de celle-ci. Le NCSC a de plus été intégré aux états-majors de crise de la Confédération. Lors d'une éventuelle évolution ou refonte de la gestion de crise au niveau de la Confédération, il faudra également veiller à intégrer directement la cybersécurité dans les structures de gestion de crise. Quand le temps presse pour surmonter une crise, la collaboration entre les acteurs centraux de la Confédération, des cantons et de l'économie est compliquée. Des exercices réguliers s'imposent pour en assurer le bon fonctionnement. La Suisse participe aujourd'hui à des exercices internationaux et divers exercices de crise sectoriels ont été réalisés au niveau national. Il manque toutefois un concept général de planification et de mise en place d'exercices de crise dans le domaine de la cybersécurité. Il importe de l'élaborer et de l'intégrer dans la planification globale des exercices de gestion de crise.
Priorités	- Concevoir et mettre en œuvre des cyberexercices tant sectoriels (p. ex. approvisionnement énergétique, approvisionnement en eau, soins de santé) qu'intersectoriels. Il convient de coordonner leur planification et leur conception avec la planification générale des exercices de gestion de crise. - Inclure des aspects relevant de la cybersécurité dans tous les exercices prévus de gestion de crise. - Déterminer les règles de base en tenant compte des travaux prioritaires, visant à organiser la gestion de crise: quels sont les critères de définition d'une crise de cybersécurité et les structures habilitées à en livrer une évaluation ainsi qu'à introduire des mesures de gestion de crise? - Assurer la représentation de la cybersécurité dans le dispositif de gestion de crise (à l'échelon de la Confédération et des cantons). - Clarification du soutien (subsidiaire) à apporter à la gestion conjointe d'une crise, avec les moyens de communication à utiliser dans ce contexte.
Acteurs principaux	- Confédération: *ChF, OFPP, NCSC*, armée, OFCOM, OFT, OFAC, OFEN, OFAE, DFAE, SG-DDPS, RNS - Cantons: états-majors de conduite, centres cantonaux de compétence en matière de cybersécurité - Milieux économiques et société: exploitants d'infrastructures critiques - Développeurs/vendeurs de logiciels critiques, organisations sectorielles (comme Swiss FS-CSC ou SWITCH-CERT)

M11 Cyberdéfense

Aperçu de la mesure	
Description	Il importe de protéger la liberté d'action et l'intégrité de l'État, des milieux économiques et de la population dans le cyberespace et de les défendre en cas de conflit. La cyberdéfense inclut la totalité des mesures prises par les services de renseignement et les militaires qui servent à atteindre les objectifs suivants: protéger les systèmes critiques pour la défense nationale, assurer la défense contre les cyberattaques, préserver la disponibilité opérationnelle de l'armée suisse en toute circonstance et mettre en place des capacités et des aptitudes pour le soutien subsidiaire des autorités civiles. Cela comprend notamment des mesures actives de détection des menaces, d'identification des agresseurs et de perturbation et d'arrêt des cyberattaques.
Contexte et actions requises	Le Service de renseignement de la Confédération (SRC) et l'armée suisse ont développé leurs capacités pour assumer leurs tâches en matière de cyberdéfense. « La Conception générale cyber » décrit les capacités dont l'armée devra se doter d'ici au milieu des années 2030 pour être à même de faire face aux menaces dans le cyberespace et l'espace électromagnétique. La loi sur le renseignement (LRens) et la loi sur l'armée (LAAM), désormais révisée, créent les bases légales nécessaires sur lesquelles la Confédération peut s'appuyer pour engager des contre-mesures actives dans le cadre de la cyberdéfense. Or l'évolution des cyberattaques au cours des dernières années et leur complexité croissante mobilisent toujours plus de ressources, sur des périodes prolongées. Il reste par conséquent nécessaire de développer les capacités et la coordination avec les services compétents afin d'assurer le respect du droit international.
Priorités	- Développer les compétences centrales au niveau de l'armée. Ces capacités comprennent l'autoprotection dans le cyberespace et l'espace électromagnétique, l'anticipation, l'autonomie et l'acquisition de compétences de base en science des données. - Développer des capacités à un niveau décentralisé. Celles-ci comprennent par exemple le traitement fiable et sûr de données au sein des bataillons et des compagnies. Une autre priorité consiste à améliorer la résilience de l'infrastructure essentielle en cas d'intervention dans le domaine de l'autoprotection dans le cyberespace et l'espace électromagnétique. Il convient aussi d'adapter l'organisation des associations. - Affiner la gestion politique des cas pour mener des cybercampagnes jouant un rôle pour la politique de sécurité. - Intégrer davantage encore les capacités de la Suisse afin d'obtenir un effet protecteur direct pour les acteurs suisses. - Élargir les compétences de base du SRC et de l'armée pour qu'ils soient à même d'agir dans le cyberespace.
Acteurs principaux	- Confédération: *armée,* CYD Campus, SG-DDPS, SRC - Cantons: organisations cantonales de conduite

3.4 Mesures concernant l'objectif «Lutte et poursuites pénales efficaces contre la cybercriminalité»

L'infrastructure numérique disponible sur Internet offre aux délinquants potentiels de nouvelles possibilités d'entraîner de sérieux dommages pour la société et l'économie. La cybercriminalité se joue des frontières territoriales, dans un processus hautement dynamique aux cycles d'innovation très courts. Plus l'interconnexion augmente, plus il est à craindre que des cyberincidents trouvent certes leur origine dans le monde virtuel, mais déploient des effets préjudiciables dans le monde réel.
Face à cette évolution, il est important d'agir dans toute la Suisse et en collaboration avec des partenaires internationaux afin d'améliorer encore l'interopérabilité et la capacité de réaction, ainsi que de coordonner efficacement les compétences professionnelles, techniques et humaines, sans devoir pour autant transférer des compétences d'une autorité ou d'un niveau étatique à l'autre.

M12 Collaboration accrue des autorités de poursuite pénale

Aperçu de la mesure	
Description	La collaboration entre la Confédération et les cantons, de même qu'entre cantons, doit encore être étendue en matière de poursuite pénale de cybercriminels. Elle est en effet déterminante pour mener les poursuites pénales de manière efficace et efficiente. Cette collaboration intervient déjà dans la mesure où la législation le permet, en particulier grâce au réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK). Il importe néanmoins de la renforcer et de la développer. À cet effet, il convient notamment d'examiner quelles modifications il serait nécessaire d'apporter aux bases légales. Diverses mesures complémentaires permettent de renforcer la collaboration. Définir des approches communes et standardiser les processus constitue une première base qui facilite la coopération. Des échanges directs entre spécialistes, voire un regroupement régional des compétences, peuvent s'avérer très utiles dans le cas des compétences professionnelles difficiles à acquérir (p. ex. dans le domaine de la forensique numérique), mais aussi pour coordonner des cours de formation et de perfectionnement. Il importe également de renforcer encore la collaboration internationale qui joue un rôle décisif dans les poursuites pénales. L'accent doit surtout être mis sur la coopération avec Europol.
Contexte et actions requises	Le Cyberboard est une plateforme de coordination et de coopération créée pour lutter contre la cybercriminalité, où tous les acteurs importants sont représentés. Il coordonne la gestion des cas, permet aux autorités de poursuite pénale d'échanger des informations sur les modes opératoires connus en Suisse, les cas typiques et les divers cas de figure, repère les interdépendances et examine puis lance au besoin des mesures visant à améliorer les processus existants. Dans le cadre du Cyberboard, le Cyber-CASE devrait faciliter les échanges d'informations et de connaissances entre les spécialistes des ministères publics et des organes d'enquête à l'occasion de trois à quatre réunions annuelles. Le Cyberboard mérite d'être encore renforcé. Le NEDIK et le Cyber Comptence Center (RC3) régional contribuent à renforcer la collaboration entre les polices cantonales. Le NEDIK assure une coordination régulière des thèmes stratégiques ou opérationnels. Grâce à ces organes, une bonne collaboration est déjà en place, qu'il s'agit néanmoins de renforcer. Il reste à l'encourager de manière ciblée dans les domaines où elle sera le plus utile. Les règles locales régissant les compétences en matière de poursuites pénales entravent l'action de la justice pénale contre la cybercriminalité. Il importe dès lors de déterminer en priorité les bases légales à créer pour assurer l'échange de données au niveau national.
Priorités	- Renforcer la collaboration déjà en place: normaliser les processus ainsi que les interfaces et encourager les échanges d'expériences. - Regrouper les compétences professionnelles (p. ex. en forensique informatique) et les achats se rapportant à la sécurité. - Coordonner la collaboration avec les acteurs nationaux et internationaux, principalement dans les domaines de la conservation des preuves ainsi que de l'entraide judiciaire. - Vérifier les bases légales de la collaboration: au besoin, en créer de nouvelles.
Acteurs principaux	- Confédération: *MPC, fedpol*, OFJ - Cantons: corps de police cantonaux, CCDJP, CCPCS, ministères publics, CPS - Organes communs: Cyberboard, NEDIK, CPS

M13 Vue d’ensemble des cas

Aperçu de la mesure	
Description	Pour bien évaluer l’état de la menace, il est important de disposer d'une vue d’ensemble des incidents. Celle-ci revêt également une grande importance pour les poursuites pénales. Elle permet d'améliorer l'efficacité, la qualité et le taux d'élucidation des affaires complexes d'envergure intercantonale ou internationale. Dans la vue d’ensemble des cas, il convient de distinguer trois niveaux: les événements (les incidents signalés, p. ex.), les plaintes reçues et la vue globale des procédures judiciaires en cours. Une vue d'ensemble ne sera complète que si les données des divers échelons peuvent être corrélées et évaluées en temps réel.
Contexte et actions requises	La création, au NCSC, du guichet unique qui consigne les cybermenaces et des services d'annonce auprès des polices cantonales (p. ex. cybercrimepolice.ch) a permis de collecter nettement plus d'informations sur les cyberincidents auprès de la population et des milieux économiques. De plus, l'Office fédéral de la statistique publie chaque année les chiffres clés concernant l'évolution de la criminalité numérique. Les autorités judiciaires et de poursuite pénale échangent d'ores et déjà les données disponibles dans les limites du cadre légal. En enregistrant les cas de manière systématique et structurée, la plateforme d'information de la criminalité sérielle en ligne (PICSEL) est un instrument qui permet de constater l'existence de séries et d'identifier les nouveaux phénomènes ou modes opératoires. La plateforme est d'ores et déjà opérationnelle et le centre suisse de compétences Technique et informatique policières assure son développement. Tous les cantons n'y participent toutefois pas encore. Cette situation s'explique par l'absence d'une base légale commune et uniforme qui permettrait à la PICSEL d'œuvrer à l'échelle de toute la Suisse. Il convient de déterminer comment créer la base légale requise pour mettre en place une plateforme garantissant l'échange d'informations. Le NEDIK établit un aperçu mensuel des événements actuels liés à la cybersécurité et le guichet unique du NCSC publie chaque semaine le nombre d'incidents signalés, ventilés par type. Chaque année, la statistique policière de la criminalité ventile par ailleurs les cas enregistrés par phénomène. Les échanges et le traitement des statistiques de cas ne sont pas encore systématiques ni ne font l'objet d'un pilotage stratégique. Une vue d'ensemble exhaustive des cas n'est donc pas disponible pour le moment.
Priorités	- Établir un aperçu des cyberincidents par événements: le guichet unique national consigne les cyberincidents lui ayant été signalés. Il échange des informations avec ses homologues des polices cantonales. - Préciser le cadre juridique applicable aux échanges de renseignements entre le guichet unique et les autorités de poursuite pénale. - Dresser une vue d'ensemble des plaintes reçues et des procédures judiciaires et policières en cours: les conditions juridiques et techniques seront créées pour permettre l'enregistrement centralisé des plaintes pénales déposées suite à des cyberincidents ainsi que des procédures en cours.
Acteurs principaux	- Confédération: *MPC, fedpol*, NCSC - Cantons: corps de police et ministères publics des cantons, CCDJP, NEDIK, CPS, TIP

M14 Formation des autorités de poursuite pénale

Aperçu de la mesure	
Description	La cybercriminalité comprend des délits très divers, commis avec des méthodes qui évoluent en permanence et qu'il est souvent difficile de délimiter et de cerner. La gestion des cyberdélits est donc complexe pour les autorités de poursuite pénale. Il faut s'assurer de la présence, à tous les échelons de la poursuite pénale, des connaissances en cybercriminalité nécessaires à l'exécution des tâches prévues.
Contexte et actions requises	La formation de base en cybercriminalité a lieu dans les écoles de police et à l'Institut suisse de police (ISP). En Suisse romande, deux autres institutions proposent des cours dans ce domaine: l'École romande de la magistrature pénale (ERMP) et l'Institut de lutte contre la criminalité économique (ILCE). Outre ces formations spécifiques, de nombreuses offres de formation des universités et des hautes écoles spécialisées sont pertinentes pour le personnel des autorités de poursuite pénale. Il existe ainsi déjà des cours pour les procureures et les procureurs, les juges, les greffières et les greffiers. À la demande de la Conférence des commandants des polices cantonales de Suisse (CCPCS), la nouvelle plateforme cyberpie.ch offre un panorama des formations continues pertinentes. Chaque année, le NEDIK met de plus sur pied plusieurs formations pour spécialistes en fonction des besoins et met à disposition une plateforme nationale de connaissances (CyberWiki). La PSC fournit aux polices cantonales des brochures sur les cas spécifiques qui contiennent des informations sur les différents phénomènes et renforce ainsi la formation du personnel de la police. Il convient d'exploiter les possibilités existantes pour favoriser la formation des autorités judiciaires et de poursuite pénale. Il est par ailleurs nécessaire d'intensifier encore les échanges d'expériences entre les autorités de poursuite pénale, ainsi qu'entre ces autorités et le secteur privé, car beaucoup de connaissances peuvent être transmises par ce moyen. L'Institut suisse de police devrait jouer un rôle central en assumant la coordination en la matière.
Priorités	- Développer les offres de formation, en vérifiant constamment si les formations existantes répondent aux besoins. En cas de besoin supplémentaire, examiner les possibilités de créer de nouvelles offres. - Encourager les échanges d'expériences: des stages, des équipes de spécialistes ou des plateformes en ligne faciliteront les échanges de connaissances entre les autorités de poursuite pénale.
Acteurs principaux	- Confédération: *MPC, fedpol*, NCSC - Cantons: corps de police cantonaux, CCPCS, NEDIK, ministères publics, CPS, ISP, SVR-ASM - Milieux économiques, société: ISP, hautes écoles

3.5 Mesures concernant l'objectif «Rôle de premier plan dans la coopération internationale»

La cybersécurité est un thème important en politique extérieure. Les acteurs étatiques recourent toujours plus à des cyberattaques pour démontrer leur puissance, pour atteindre des objectifs politiques ou propres aux opérations de leur service 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 et mettent aux prises des acteurs étatiques et non étatiques. Pour réduire les cyberrisques, la collaboration internationale est par conséquent indispensable, tant au niveau diplomatique que sur le plan technique et opérationnel de même que sous forme de coordination de la formation et du perfectionnement.
La défense des intérêts de politique extérieure et de politique de sécurité de la Suisse doit aussi être assurée dans le cyberespace. La Suisse œuvre donc au niveau diplomatique, sur le plan technique et opérationnel ainsi que dans le domaine de la formation et du perfectionnement afin de renforcer la coopération internationale et atténuer ainsi les cyberrisques.

M15 Renforcement de la Genève internationale dans le domaine numérique

Aperçu de la mesure	
Description	Le Conseil fédéral s'est fixé pour objectif de positionner la Suisse, et notamment la Genève internationale, comme lieu d'accueil privilégié des débats sur la transformation numérique et les nouvelles technologies. À cet effet, la Suisse doit être à même d'offrir le meilleur cadre possible aux organisations internationales et aux organisations non gouvernementales (ONG) internationales implantées sur son territoire. Comme beaucoup de ces organisations sont politiquement exposées, elles subissent souvent des cyberattaques. La Suisse doit par conséquent examiner comment elle peut améliorer le cadre général afin de permettre à ces organisations de se protéger contre les cybermenaces.
Contexte et actions requises	Les organisations de la Genève internationale sont de plus en plus confrontées à des menaces dans l'espace numérique. Pour que la Suisse reste un lieu d'implantation attrayant pour les organisations internationales et les organisations non gouvernementales (ONG), il faut vérifier comment offrir à ces dernières des conditions optimales également dans le cyberespace. Il importe par ailleurs d'apporter un appui aux organisations internationales et aux ONG implantées en Suisse dans leurs efforts de prévention ainsi que lors de cyberattaques. La Confédération contribue à ce soutien en mettant en place un centre de partage et d'analyse de l'information (Information Sharing and Analysis Centre, ISAC) à l'intention de ces organisations. Elle contribue et participe ainsi à l'échange réciproque d'expériences.
Priorités	- Mettre en place un ISAC pour la Genève internationale: la création d'un centre de partage et d'analyse favorisera l'échange d'informations et d'expériences entre les organisations internationales. - Vérifier et établir un cadre attrayant pour les services numériques destinés aux organisations internationales et aux ONG. - Assurer l'implantation de nouveaux acteurs contribuant à la sécurité numérique de la Genève internationale.

Acteurs principaux	- Confédération: *DFAE,* OFCOM, SG-DDPS, NCSC, SRC - Milieux économiques et société: organisations internationales, ONG

M16 Règles internationales dans le cyberespace

Aperçu de la mesure	
Description	La Suisse s'engage activement pour un Internet ouvert, libre et sûr. Elle plaide pour la reconnaissance, le respect et l'application sans réserve et sans exception du droit international public dans le cyberespace et tire au clair l'application pratique des règles existantes en échangeant avec d'autres États. Elle contribue par ailleurs à créer un cadre général qui facilite la lutte contre la cybercriminalité. La Suisse poursuit ces objectifs tant au sein d'organismes internationaux, comme l'ONU, l'OSCE ou l'OCDE, qu'au niveau bilatéral.
Contexte et actions requises	Depuis 2004, la communauté internationale mène des négociations au sein de groupes de travail de l'ONU sur l'application du droit international dans le cyberespace. La Suisse a d'emblée participé aux discussions et s'engage avec des États partageant ses vues en faveur d'un Internet ouvert, libre et sûr ainsi que pour la reconnaissance pleine et entière, le respect ainsi que l'application du droit international public. Elle défend ici une approche inclusive multipartite. À un niveau plus concret, les défis de la lutte contre la cybercriminalité sont toujours plus grands. Il est nécessaire d'agir sur ce plan afin d'améliorer la collaboration internationale des autorités de poursuite pénale. Un défi particulier s'annonce avec l'informatique en nuage, où la gestion des données est toujours plus souvent assurée à l'étranger par des entreprises de pays tiers. La Suisse cherche ici à renforcer la sécurité juridique au moyen d'accords bilatéraux.
Priorités	- Participer activement aux processus de l'ONU, notamment au groupe de travail ouvert (OEWG) et aux négociations relatives à une nouvelle Convention de l'ONU sur la cybercriminalité. - Assurer une participation active de la Suisse au développement et à la mise en œuvre de la Convention sur la cybercriminalité (Convention de Budapest) du Conseil de l'Europe. - Participer activement à l'application des mesures de confiance de l'OSCE. - Mener des entretiens bilatéraux sur les questions et les préoccupations interétatiques, de sorte que la Suisse puisse conclure des accords avec des partenaires d'importance stratégique.
Acteurs principaux	- Confédération: *DFAE,* armée, OFT, OFCOM, OFAC, OFEN, OFJ, SG-DDPS, NCSC

M17 Coopération bilatérale avec des partenaires stratégiques et des centres de compétence internationaux

Aperçu de la mesure	
Description	La Suisse prend des mesures visant à renforcer, à coordonner et à développer de manière ciblée la coopération opérationnelle avec ses partenaires internationaux. Compte tenu de la dimension internationale de la cybersécurité, une coopération ciblée avec des partenaires internationaux, des centres de compétence internationaux et des organisations spécialisées de pointe revêt une importance décisive dans l'application efficace de toutes les mesures de protection face aux cybermenaces.
Contexte et actions requises	À l'ère de l'Internet mondialisé, la Suisse se doit de collaborer avec d'autres pays. L'expérience montre que de telles activités ne sont durables que lorsqu'elles sont largement soutenues et servent des intérêts communs. La Suisse entretient des relations bilatérales avec des partenaires stratégiques dans le cadre de différentes activités. La coopération internationale en matière de poursuite pénale joue un rôle particulier. En l'absence d'aide réciproque entre États, il s'avère impossible de poursuivre avec efficacité des auteurs d'infractions qui agissent à l'échelle mondiale. Dans ces domaines, la Suisse échange dès lors des informations au niveau opérationnel et stratégique avec les organismes spécialisés correspondants, mais aussi directement avec d'autres États. Outre la coopération interétatique, la collaboration avec des initiatives internationales privées et des centres de compétence techniques de cybersécurité revêt aussi une grande importance. Menée à un niveau élevé, une telle collaboration peut contribuer largement à comprendre l'état de la menace pertinente et son évolution, puis à assurer une protection efficace de la société, de l'économie et de l'administration. Une collaboration de ce type doit pouvoir se fonder sur de longues années de coopération, sur une confiance sans faille ainsi que sur un élargissement et un renforcement ciblé du réseau de relations des principaux acteurs en Suisse.
Priorités	- Poursuivre les cyberdialogues existants avec divers pays partenaires et en entamer de nouveaux avec d'autres États. - Examiner, dans le cadre d'échanges entre la Suisse et les pays partenaires, comment la conclusion d'accords bilatéraux peut améliorer les conditions dans lesquelles s'inscrit la poursuite pénale de la cybercriminalité. - S'engager avec des partenaires étrangers dans des programmes opérationnels, telle l'initiative de lutte contre les rançongiciels (Counter Ransomware Initiative). - S'efforcer de conclure des accords bilatéraux instituant une aide réciproque dans la lutte contre la cybercriminalité. - Établir, dans la mesure du possible, une collaboration avec le Centre européen de compétences en cybersécurité (ECCC). - Collaborer activement au sein d'organismes qui offrent un cadre à la coopération technique et opérationnelle et qui la favorisent, notamment FIRST, TF-CSIRT, NatCSIRT (CERT nationales). - Développer la collaboration au sein de groupes de travail consacrés à des aspects techniques (sécurité OT, hameçonnage, etc.).
Acteurs principaux	- Confederation: *DFAE,* OFT, OFCOM, OFAC, OFEN, fedpol, SG-DDPS, NCSC, SRC - Milieux économiques et société: associations professionnelles, CERT, entreprises de sécurité

4 Mise en œuvre de la stratégie

L'application de la stratégie est coordonnée par le comité de pilotage de la CSN, qui élabore à cet effet un plan de mise en œuvre d'entente avec les acteurs centraux des différentes mesures. Ceux-ci sont les interlocuteurs du comité pour l'application des mesures en question et lui signalent quelle contribution ils peuvent apporter et dans quel délai. Ils l'informent également de l'état d'avancement de leurs activités. S'ils ne parviennent pas à mettre en œuvre les mesures leur ayant été confiées, ils doivent le signaler. Dans ce cas, le comité de pilotage évalue les conséquences qui en découlent pour les objectifs de la stratégie et porte le cas échéant, par l'intermédiaire de son secrétariat (assuré par le NCSC), ces conséquences à la connaissance du Conseil fédéral et des cantons.
Les acteurs centraux financent en principe eux-mêmes les travaux de mise en œuvre. Au sein de la Confédération, ils emploient les ressources leur ayant été allouées pour la mise en œuvre des deux premières stratégies de cybersécurité. Les cantons et les organisations des milieux économiques et de la société indiquent au comité de pilotage à quelle hauteur ils peuvent financer eux-mêmes leur contribution. Le NCSC soutient les acteurs centraux dans la mise en œuvre. Il met à cet effet une équipe de spécialistes à disposition. Pour appliquer la CSN, les acteurs centraux de l'administration fédérale peuvent requérir un appui de l'équipe de spécialistes auprès du NCSC. Si le besoin de ressources pour une mesure dépasse les moyens à disposition des acteurs et s'il s'avère impossible de le couvrir autrement, il convient également d'en aviser le comité de pilotage.
Le comité de pilotage est responsable du contrôle de la mise en œuvre. Le NCSC, qui assume la gestion opérationnelle de celui-ci, enregistre et consigne régulièrement l'avancement de l'application de toutes les mesures.
Après cinq ans, la stratégie elle-même et sa mise en œuvre seront soumises à un examen. En fonction des résultats de cet examen, le comité de pilotage décidera s'il souhaite proposer aux cantons et à la Confédération de remanier la stratégie en profondeur ou y apporter des compléments et des modifications ponctuels en vue de sa reconduction.

5 Abréviations

ANS	Administration numérique suisse
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandants des polices cantonales de Suisse
CDIP	Conférence suisse des directeurs cantonaux de l'instruction publique
cdmt Cyber	Commandement Cyber
CERT	Computer Emergency Response Team
CSHE	Conférence suisse des hautes écoles
CSIRT	Computer Security Incident Response Team
CSN	Cyberstratégie nationale
CYD Campus	Cyber-Defence Campus d'armasuisse (Sciences et technologies)
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
DFF	Département fédéral des finances
Europol	Office européen de police
fedpol	Office fédéral de la police
GK Cyber	Conception générale cyber
IdO	Internet des objets
LAAM	Loi sur l'armée
LRens	Loi fédérale sur le renseignement
LSI	Loi sur la sécurité de l'information
MPC	Ministère public de la Confédération
NCSC	Centre national pour la cybersécurité
NEDIK	Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique
NTC	Institut national de test pour la cybersécurité
OCDE	Organisation de coopération et de développement économiques
OEWG	Groupe de travail ouvert
OFAE	Office fédéral pour l'approvisionnement économique du pays
OFCOM	Office fédéral de la communication
OFJ	Office fédéral de la justice
OFPP	Office fédéral de la protection de la population
ONU	Organisation des Nations Unies
OSCE	Organisation pour la sécurité et la coopération en Europe
PME	Petites et moyennes entreprises
PSC	Prévention suisse de la criminalité
RNS	Réseau national de sécurité
SATW	Académie suisse des sciences techniques
SEFRI	Secrétariat d'État à la formation, à la recherche et à l'innovation
SOC	Centre opérationnel de sécurité
SRC	Service de renseignement de la Confédération
SSCC	Swiss Support Center for Cybersecurity
TI	Technologies de l'information
TIC	Technologies de l'information et de la communication
TIP	Technique et informatique policières
TNI	Secteur Transformation numérique et gouvernance de l'informatique de la Chancellerie fédérale
UE	Union européenne

6 Glossaire

Cyberattaque	Cyberincident provoqué intentionnellement.
Cyber-criminalité	La cybercriminalité englobe l'ensemble des infractions et omissions commises dans le cyberespace. Une distinction est faite entre «cybercriminalité» et «criminalité numérique». Relèvent de la «cybercriminalité» les infractions qui sont dirigées contre l'Internet, des systèmes informatiques ou leurs données et qui exigent un travail d'investigation technique de la part des autorités de poursuite pénale. La «criminalité numérique» désigne les infractions qui étaient jusqu'ici principalement commises dans le monde analogique. En raison des progrès de la transformation numérique, ces délits classiques sont de plus en plus souvent commis à l'aide de moyens informatiques.
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.
Cyber-espionnage	Activité visant à accéder de manière non autorisée à des informations à des fins politiques, militaires ou économiques dans le cyberespace.
Cyberincident	Tout événement nuisant à la confidentialité, à l'intégrité, à la disponibilité ou à la traçabilité des données ou pouvant occasionner des dysfonctionnements, qu'il soit accidentel ou provoqué intentionnellement par un tiers non autorisé.
Cybermenace	Toute circonstance ou tout événement susceptible d'engendrer un cyberincident.
Cybersabotage	Activité visant à perturber ou à détruire le bon fonctionnement des structures d'information et de communication dans le cyberespace; selon sa nature, le sabotage peut avoir des conséquences sur le plan physique.
Cybersécurité	La situation dans laquelle le traitement des données, notamment l'échange de données entre les personnes et les organisations par l'intermédiaire d'infrastructures d'information et de communication, fonctionnent comme prévu.
Infrastructures critiques	Processus, systèmes et installations indispensables 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 faire face à des perturbations internes ou externes et à maintenir son bon fonctionnement ou à le rétablir aussi rapidement et complètement que possible.
Sécurité de l'information	La sécurité de l'information 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.