La Stratégie cyber du DDPS

en bref

Mars 2021

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

**Département fédéral de la défense,
de la protection de la population et des sports DDPS**

Résumé de la Stratégie cyber du DDPS

La Suisse et la protection dans le cyberespace

Le Conseil fédéral affronte activement les cyberrisques et prend les mesures nécessaires pour protéger le pays des menaces provenant du cyberespace.

La Suisse dispose depuis 2012 d'une **Stratégie nationale de protection de la Suisse contre les cyberrisques** (SNPC), afin de pouvoir gérer les chances et les défis inhérents au cyberespace. En 2018, cette stratégie a été complétée par plusieurs mesures, et l'importance de la collaboration entre la Confédération, les cantons, les partenaires économiques et les hautes écoles y a été soulignée. Elle tient compte de la numérisation et de la mise en réseau croissantes de la société et de l'administration. Le responsable de ces questions au niveau de la Confédération est le ou la délégué·e fédéral·e à la cybersécurité du Centre national pour la cybersécurité (*National Cyber Security Centre* – NCSC), qui est rattaché au Département fédéral des finances (DFF).

*Par **cyberespace**, on entend un espace virtuel informatique créé par l'homme. Il sert à traiter et à mettre en réseau des données numériques et à saisir et piloter des systèmes et des processus.*

*Les mesures de protection contre les cyberrisques sont, conformément à l'art 6 de l'ordonnance sur les cyberrisques, subdivisées en trois domaines : cybersécurité, cyberdéfense et cybercriminalité. Dans le présent document, nous utiliserons d'une manière générale le terme **cyberdéfense** afin de garantir l'uniformité linguistique.*

Qui est protégé ?

Il s'agit d'une part de protéger les citoyennes et les citoyens face à la criminalité dans le cyberespace. D'autre part, les infrastructures doivent être protégées des pannes et des perturbations, qu'elles soient provoquées, voulues ou involontaires, pouvant impacter la population, l'économie et l'administration. En cas d'attaque de grande ampleur, par exemple en raison des intentions malveillantes d'un État, la **cyberdéfense** entre en jeu. Elle comprend plusieurs moyens du Département fédéral de la défense, de la protection de la population et des sports (DDPS) et protège la Suisse, sa population et ses conditions d'existence des cybermenaces. En cas de perturbation non malveillante de grande ampleur, la **cyberdéfense** peut intervenir à titre de renfort.

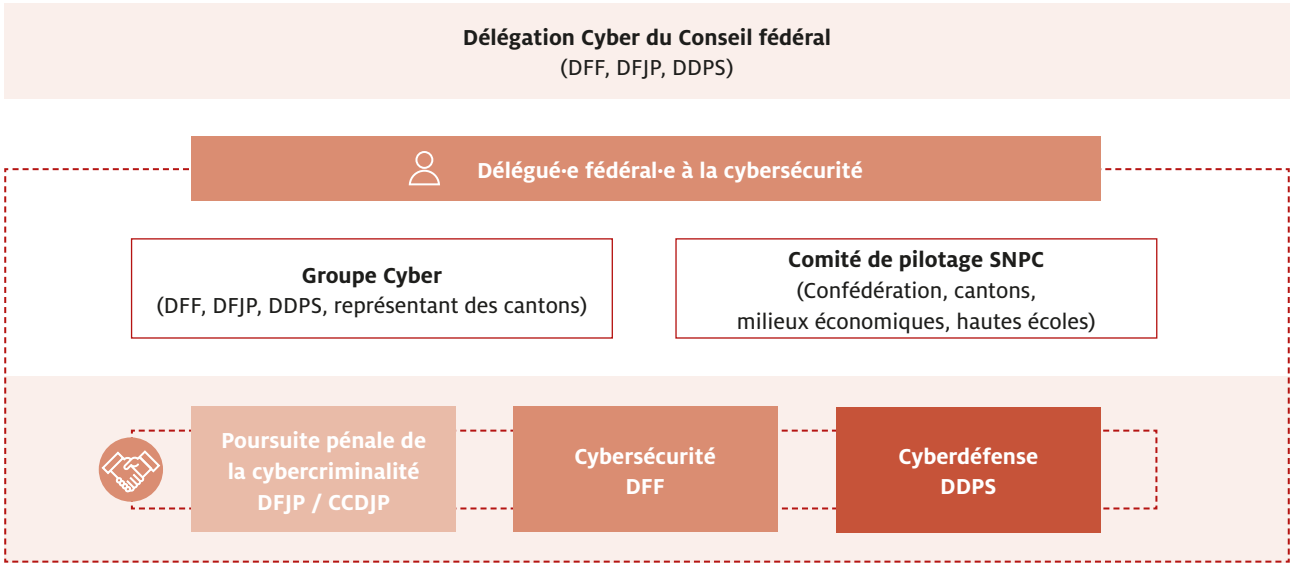


Illustration 1 – Responsabilités en matière de cybersécurité au sein de l'administration fédérale

Le DDPS et le cyberespace : une protection stratégique, intégrale et continue

De 2017 à 2020

Le **Plan d'action Cyberdéfense DDPS (PACD)**, conçu en 2017 comme une partie de la SNPC, définissait spécifiquement les tâches, les compétences et les processus des unités administratives du DDPS au niveau de la cyberdéfense. Fin 2020, les mesures prévues dans le PACD étaient presque toutes mises en œuvre.

En coordonnant ses compétences et capacités, le DDPS a gagné en efficacité. La collaboration entre les départements a été améliorée. Le DDPS collabore avec **les cantons, les milieux économiques et les hautes écoles** et, si nécessaire, avec des partenaires internationaux. Il dispose aujourd'hui de capacités à même d'assurer une protection et des prestations défensives élevées dans le cyberespace et peut s'appuyer sur un réseau fiable en Suisse et à l'étranger.

De 2021 à 2024

La **Stratégie cyber du DDPS** se fonde sur le PACD. Elle garantit que le DDPS et ses unités administratives concentrent leur action sur les défis en constante évolution qui se présentent.

La **Stratégie cyber du DDPS** porte tout d'abord sur les menaces, les défis et les tendances dans le cyberespace à l'échelle mondiale.[1] Elle décrit les évolutions technologiques, politiques, économiques attendues ces prochaines années de même que celles qui concerneront le personnel.

Par exemple, les actions malintentionnées se produiront de manière toujours plus automatisée en se fondant sur l'intelligence artificielle. Elles exploiteront systématiquement les failles laissées par les configurations de sécurité insuffisantes des systèmes appartenant à des générations différentes (systèmes hérités). L'utilisation du cyberespace à des fins de manipulation devrait continuer d'augmenter parallèlement à l'importance croissante des médias sociaux et de la mise en réseau numérique.

1 Cf. le rapport annuel du Service de renseignement de la Confédération (SRC) : « La sécurité de la Suisse 2020 »

La **Stratégie cyber du DDPS**, qui succède au PACD, présente une **analyse de la situation actuelle** et montre comment les tâches et les mesures prévues précédemment ont été mises en œuvre. Il s'agit par exemple de la mise en place du stage de formation cyber à l'école de recrues et du campus cyberdéfense d'armasuisse. La Suisse participe également à des exercices cyber internationaux.

L'analyse des menaces, défis et tendances par rapport à la situation actuelle permet d'identifier les développements potentiels. Les constats qui en sont tirés servent à formuler les objectifs de la Stratégie cyber du DDPS. Celle-ci détermine qui au DDPS assume ou assumera quelles tâches. Cette stratégie se concentre sur la cyberdéfense. La **SNPC**, dont elle fait partie, et des documents de référence couvrent d'autres aspects de la cybersécurité.

*Par **menace**, on entend les actions malveillantes entreprises par des acteurs étatiques ou non-étatiques que ce soit dans le but de s'enrichir ou de défendre des intérêts politiques. La menace peut prendre la forme d'actes ciblés d'espionnage, de sabotage, de désinformation ou de déstabilisation.*

*Les **défis** sont des développements et dépendances technologiques ainsi que la politique de puissance. Entrent en ligne de compte les limites des ressources naturelles (en particulier les terres rares et l'alimentation électrique), les besoins en formation et la pénurie de spécialistes.*

*La **résilience** est la capacité d'un système, d'une organisation ou d'une société à faire face à des perturbations et à maintenir son bon fonctionnement ou à le rétablir rapidement.*

Stratégie cyber du DDPS

Nous contribuons à la protection du pays, le défendons dans le cyberespace et augmentons ainsi considérablement sa liberté d'action.

La Suisse a un intérêt de politique de sécurité à protéger la liberté d'action et l'intégrité de l'État, de l'économie et de la population dans le cyberespace et à les défendre en cas de conflit.

Le DDPS est, avec le concours de ses partenaires fédéraux et cantonaux, les milieux économiques, les hautes écoles et, si nécessaire, ses partenaires internationaux, responsable de la cyberdéfense de la Suisse. Il anticipe et analyse, dans le cadre de ses compétences, les défis et les menaces cyber et fournit des prestations de sécurité permettant de maîtriser les tensions, les conflits et les cyberincidents en temps de paix.

Le DDPS contribue (à titre subsidiaire) à protéger les infrastructures critiques des cyberattaques et à renforcer leur résilience.

Les six objectifs stratégiques

La *Stratégie cyber du DDPS* est mise en œuvre conformément aux décisions prises dans le cadre de la Conférence sur la cyberdéfense du DDPS, dirigée par le ou la secrétaire général·e du DDPS. Le DDPS entend réaliser les objectifs suivants :

1. **Le DDPS connaît les défis et les développements du cyberespace.** Il comprend les menaces, les chances et les risques qui en découlent et s'adapte en permanence afin de les maîtriser.
2. Le DDPS **est capable de prévenir les menaces et les attaques** provoquant des dégâts, ayant des répercussions nationales ou mettant en danger des intérêts nationaux[2]. Il peut déceler, perturber ou empêcher les menaces et les attaques à temps et dans toutes les situations.
3. Le DDPS **offre des formations et des cours de perfectionnement** pour son personnel civil et militaire et pour les militaires de milice afin de les préparer aux cyberdéfis.
4. Le DDPS est résistant et **minimise la vulnérabilité face aux cyberrisques.** En cas d'événement ou de crise, il rétablit aussi rapidement que possible les fonctions de base, peut accomplir ses tâches et est résilient.
5. Le DDPS fait en sorte que son matériel informatique, les logiciels et les réseaux correspondent à la technologie actuelle. Il veille à la fiabilité de l'exploitation et s'assure que le matériel nécessaire soit toujours disponible. Il est aussi indépendant que possible des prestataires et des fournisseurs et accroît ainsi son **autonomie.**
6. Le DDPS se positionne en tant que **précurseur et modèle** dans le domaine de la cyberdéfense, et aussi en tant qu'**employeur attrayant.**

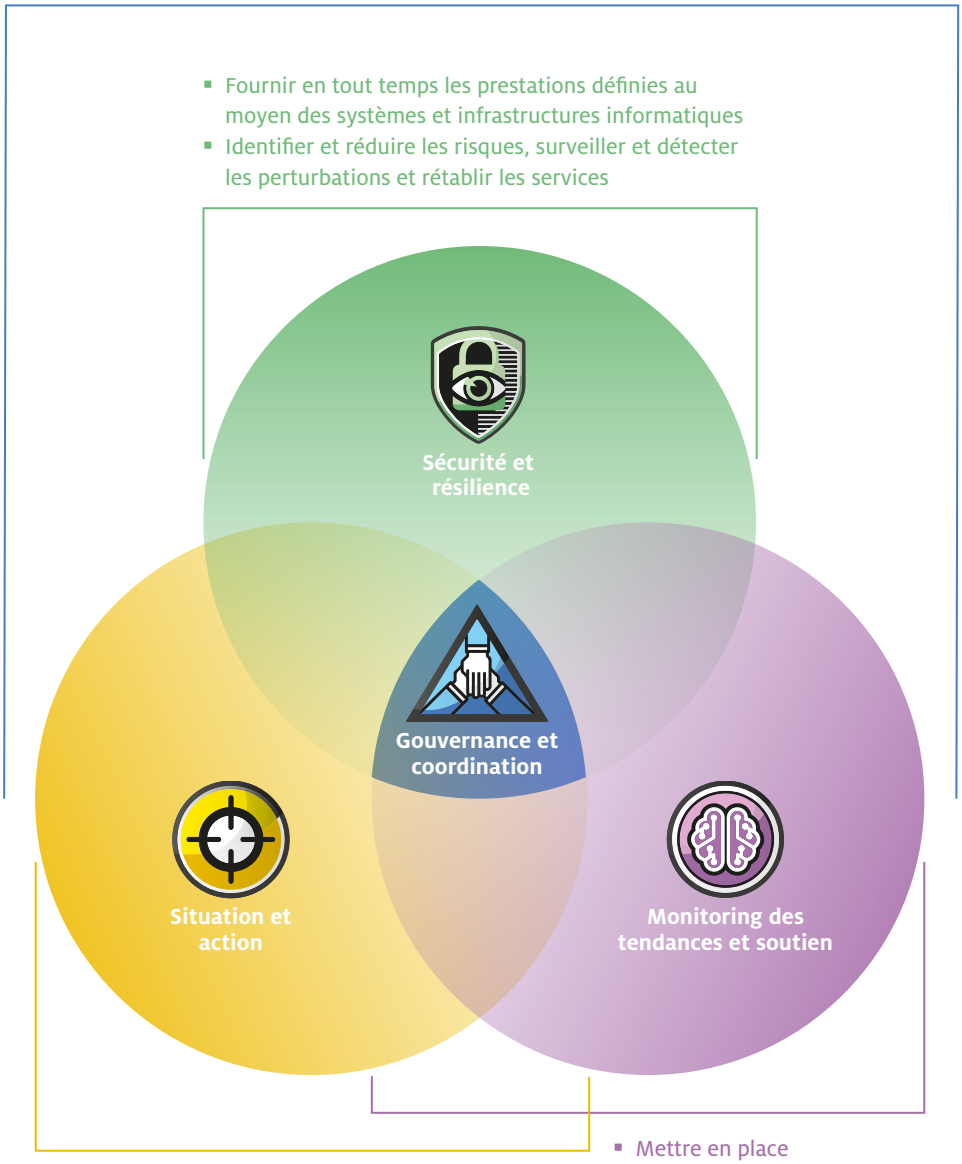
Résistance : *lorsque de nombreuses mesures de protection ont été prises, qu'il existe peu de failles et que la protection peut être garantie longtemps.*

2 Des mesures préventives doivent être prises entre autres dans les domaines de la technologie, des processus et du personnel.

Cyberdéfense DDPS : quatre axes principaux

La Stratégie cyber du DDPS classe les mesures dans quatre domaines : situation et action ; sécurité et résilience ; monitoring des tendances et soutien ; gouvernance et coordination. Chaque domaine départemental répartit également ses tâches en fonction de ces domaines.

- Créer les conditions favorisant le développement et l'utilisation de toutes les ressources nécessaires
- Surveiller l'avancement de la mise en œuvre et coordonner la collaboration avec les participants



- Fournir en tout temps les prestations définies au moyen des systèmes et infrastructures informatiques
- Identifier et réduire les risques, surveiller et détecter les perturbations et rétablir les services

- Anticiper, détecter à un stade précoce, empêcher et attribuer les cyberattaques touchant la politique de sécurité
- Représenter la situation et évaluer la menace
- Collecter des informations relevant du renseignement et mener des cyberopérations

- Mettre en place les compétences-clés servant au développement des moyens techniques, spécialisés et personnels
- Procéder à l'acquisition et au transfert des connaissances en collaboration avec les hautes écoles et l'industrie

Domaines de compétence et tâches du DDPS

Gouvernance et coordination
Au niveau stratégique de toute unité administrative du DDPS, les conditions sont créées pour développer et utiliser les ressources nécessaires. L'avancement de la mise en œuvre est surveillé et la collaboration avec toutes les personnes impliquées coordonnée.
Exemple : *développement de l'organisation : les domaines départementaux établissent une analyse des défis du cyberespace et une vue d'ensemble pour les différents échelons ; si nécessaire, ces analyses donnent lieu à des décisions rapides et à des développements.*

Sécurité et résilience
Ce domaine structure les tâches afin que tous les systèmes et toutes les infrastructures informatiques soient organisés et gérés de manière à pouvoir fournir les prestations définies. Les unités administratives du DDPS peuvent ainsi accomplir leurs tâches en tout temps et en toute situation. Ces tâches vont de l'identification et de la réduction des risques au rétablissement des services en passant par la surveillance et la détection des perturbations.
Exemple : *développer des mesures permettant de rétablir les systèmes après un incident.*

Situation et action
Ce domaine comprend toutes les tâches nécessaires pour anticiper, détecter à un stade précoce, empêcher et attribuer les cyberattaques touchant la politique de sécurité. Il évalue et représente la situation. À cela s'ajoutent l'acquisition d'informations dans le domaine du renseignement et les cyberopérations (contre-mesures de cyberdéfense et actions dans le cyberespace en cas de conflit).
Exemple : *pouvoir mener des contre-mesures défensives en cas d'attaque.*

Monitoring des tendances et soutien
Les compétences-clés requises pour le développement des moyens techniques, spécifiques et personnels des unités administratives du DDPS sont mises en place et à disposition. L'acquisition et le transfert des connaissances s'effectue en collaboration avec les hautes écoles et l'industrie.
Exemple : *recherche, développement et innovation toujours à jour sur les plans technique, spécialisé et personnel.*

Principes d'action

Renforcer la cybersécurité en Suisse est une priorité pour le DDPS. Les principes suivants ont donc été formulés pour la mise en œuvre de la stratégie :

Subsidiarité : les cybercompétences dont dispose le DDPS peuvent, si la loi l'autorise, soutenir les acteurs civils en cas d'événement. La collaboration doit pour cela être régulièrement exercée et renforcée, par exemple par le transfert de connaissances.

Collaboration institutionnelle : le DDPS engage ses moyens dans la collaboration avec ses partenaires de la politique de sécurité en Suisse. La collaboration se fait avec les cantons, les communes, les milieux économiques et scientifiques, la société et les partenaires internationaux. Cette coopération est réglée dans l'ordonnance sur les cyberrisques (OPCy)[3]. Le ou la délégué·e fédéral·e à la cybersécurité coordonne les trois domaines suivants : cybersécurité, poursuite pénale de la cybercriminalité et cyberdéfense (selon la SNPC).

Coopération internationale : cette coopération, qui s'effectue avec les autres services fédéraux (DFAE, DFF, DFJP), peut être bilatérale ou multilatérale. Elle sert essentiellement à anticiper et à détecter les menaces et les défis du cyberespace à un stade précoce.

Ouverture : de par ses compétences, le DDPS apporte son aide à d'autres partenaires.

Commandement Cyber de l'armée : selon le mandat du Conseil fédéral, l'actuelle Base d'aide au commandement de l'armée (BAC) sera transformée en un commandement Cyber début 2024 ; la capacité d'engagement de l'armée dans le cyberespace devra être continuellement améliorée.

La Stratégie cyber du DDPS sert à protéger autant que possible la Suisse dans le cyberespace. Cette protection est assurée avec des partenaires et entend réduire la vulnérabilité de la Suisse dans le cyberespace.

Pour une plus grande efficacité, la maîtrise des événements et des crises repose sur une collaboration continuelle à l'interne du DDPS et avec ses partenaires externes. Les différents processus et le réseau sont rôdés et les tâches connues. Ainsi, en planifiant des mesures concrètes, la stratégie du DDPS garantit non seulement qu'elles soient mises en œuvre avec professionnalisme mais renforce également la préparation commune en vue de maîtriser une situation réelle.

3 RS 120.73 – Ordonnance du 27 mai 2020 sur les cyberrisques (OPCy) (admin.ch)

Département fédéral de la défense, de la protection de la population et des sports DDPS
Secrétariat général SG-DDPS
Digitalisation et cybersécurité DDPS (DCS VBS)
Maulbeerstrasse 9, 3003 Berne

Premedia
Centre des médias électroniques CME
80.256.01 f 03.2021

L’essentiel de la Stratégie cyber du DDPS

- Le DDPS est capable de maîtriser en permanence les menaces, événements et crises survenant dans le cyberespace et d’apporter son soutien dans ce domaine.
- Tous les services du DDPS chargés de tâches liées à la cybersécurité se coordonnent dans le cadre de la Stratégie cyber du DDPS.
- Les partenaires responsables du DDPS collaborent afin d’identifier les risques et les chances à saisir maintenant et à l’avenir et afin d’être prêts à les maîtriser ensemble.
- Le DDPS axe son développement, pour ce qui est des compétences spécifiques, du matériel, des processus et du personnel, sur les défis de la cybersécurité. L’accent est mis sur la formation et le perfectionnement de tout le personnel du DDPS et des militaires tant professionnels que de milice.
- Les responsables cyber du DDPS collaborent avec des partenaires. Il s’agit des cantons et des communes, des milieux scientifiques, de l’économie privée et de partenaires internationaux. Le DDPS collabore étroitement avec le NCSC.