# La stratégie cyber du DDPS

Autor(en): **Eglin, Maurice**

Objekttyp: **Article**

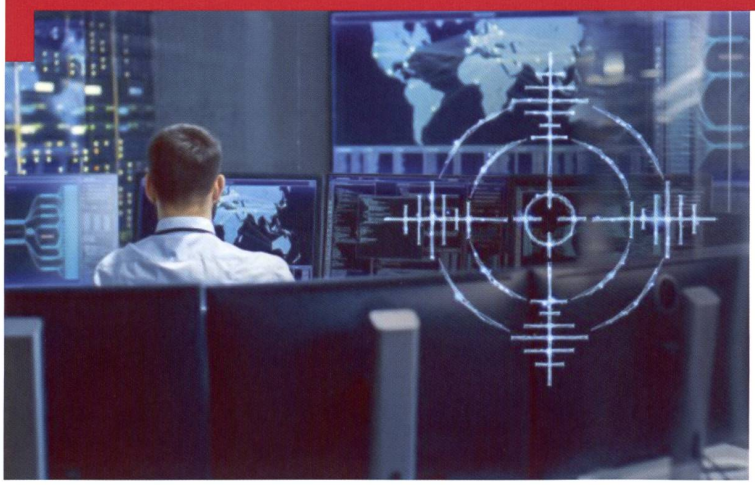
Zeitschrift: **Revue Militaire Suisse**

Band (Jahr): **- (2021)**

Heft 5

PDF erstellt am: **22.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-977715



*Cyber*

## La stratégie cyber du DDPS

**Col EMG Maurice Eglin**
Chef réseau et interopérabilité cyberdéfense DDPS, remplaçant du chef cyberdéfense DDPS

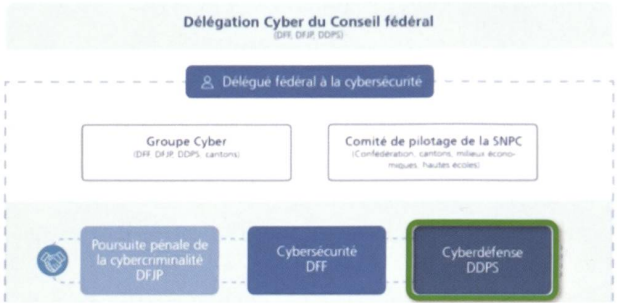
Le Conseil fédéral affronte activement les cyberrisques et prend les mesures nécessaires pour protéger le pays des menaces provenant du cyberespace.

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 délégué fédéral à la cybersécurité, du Centre national pour la cybersécurité (National Cyber Security Centre – NCSC), rattaché au Département fédéral des finances (DFF).

### Qui est protégé ?

Dans le cadre de la cybersécurité, il s'agit d'une part de protéger les citoyennes et les citoyens face à la criminalité dans le cyberespace. D'autre part, il s'agit de protéger les infrastructures 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 Etat, 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 des cybermenaces ses instruments de politique de sécurité, et au travers d'eux, la Suisse, sa population et ses conditions d'existence. En cas de perturbation non malveillante de grande ampleur, la cyberdéfense peut intervenir à titre de renfort de la cybersécurité selon le principe de la subsidiarité.

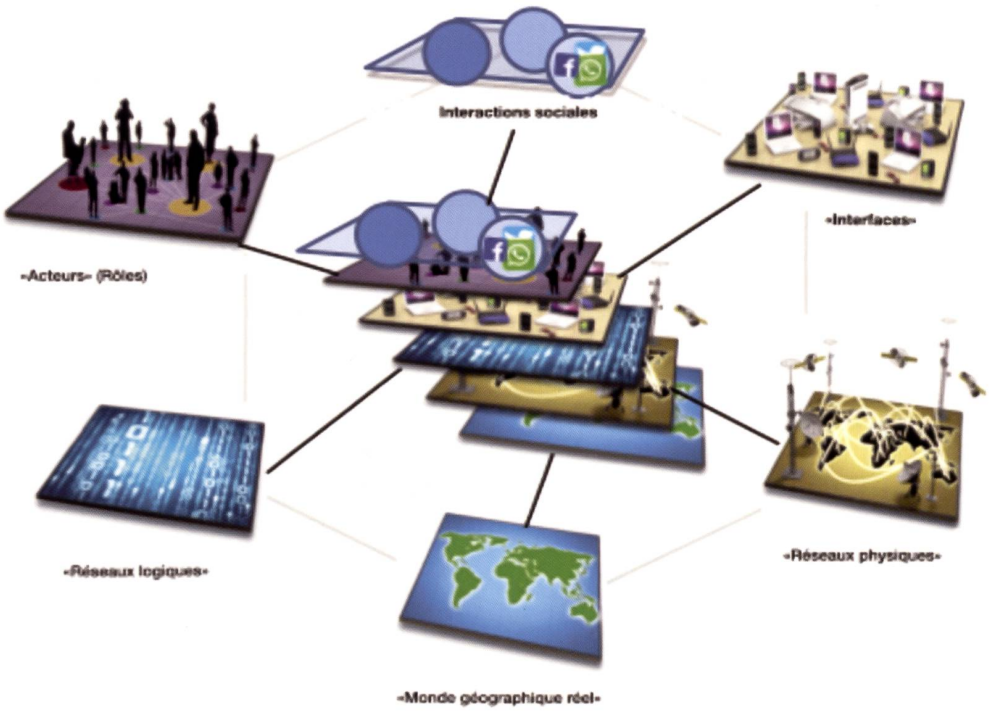
Le DDPS et la cyberdéfense dans l'écosystème de la Confédération.




### 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 milieux économiques et les hautes écoles par le biais du Cyber Campus, avec les cantons par le biais du RNS, et là où nécessaire ou opportun, avec des partenaires internationaux comme par exemple le Centre coopératif de cyberdéfense de l'OTAN à Tallinn en Estonie (Cooperative Cyber Defence Centre of Excellence). Le DDPS dispose ainsi 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.




Une représentation du cyberespace.

Dans la continuité du PACD, la Stratégie cyber du DDPSa été définie pour la période 2021-2024. Elle garantit que le DDPS et ses unités administratives développent leurs capacités et concentrent leur action sur les défis en constante évolution qui se présentent.

La Stratégie cyber du DDPS porte sur les menaces, les défis et les tendances globales du cyberespace. Elle décrit les évolutions technologiques, politiques, économiques attendues ces prochaines années de même que celles qui concerneront le personnel.

Elle aborde également les actions malintentionnées qui se produiront de manière toujours plus automatisée en se fondant sur l'intelligence artificielle. De telles actions exploitent 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.

**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.

**Une définition et description du cyberespace**

*« Espace, au sein duquel, les données sont acquises, stockées, transmises, modifiées, ordonnées, codées et représentées pour être transformées en actions physiques ou informationnelles »*


Les mesures de protection contre les cyberrisques sont, conformément à l'article 6 de l'ordonnance sur les cyberrisques, subdivisées en trois domaines : cybersécurité, cyberdéfense et lutte contre la cybercriminalité.

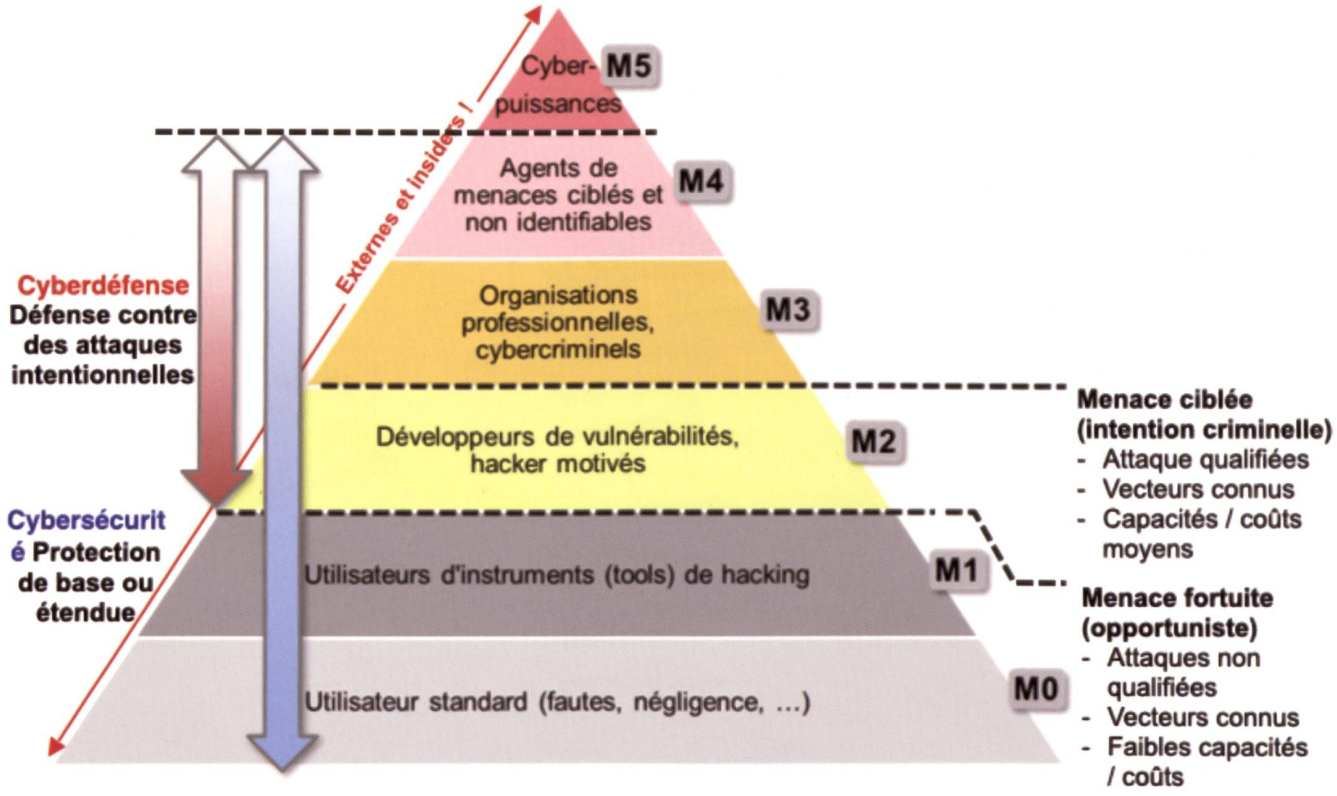
**Glossaire Cyber**

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.

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

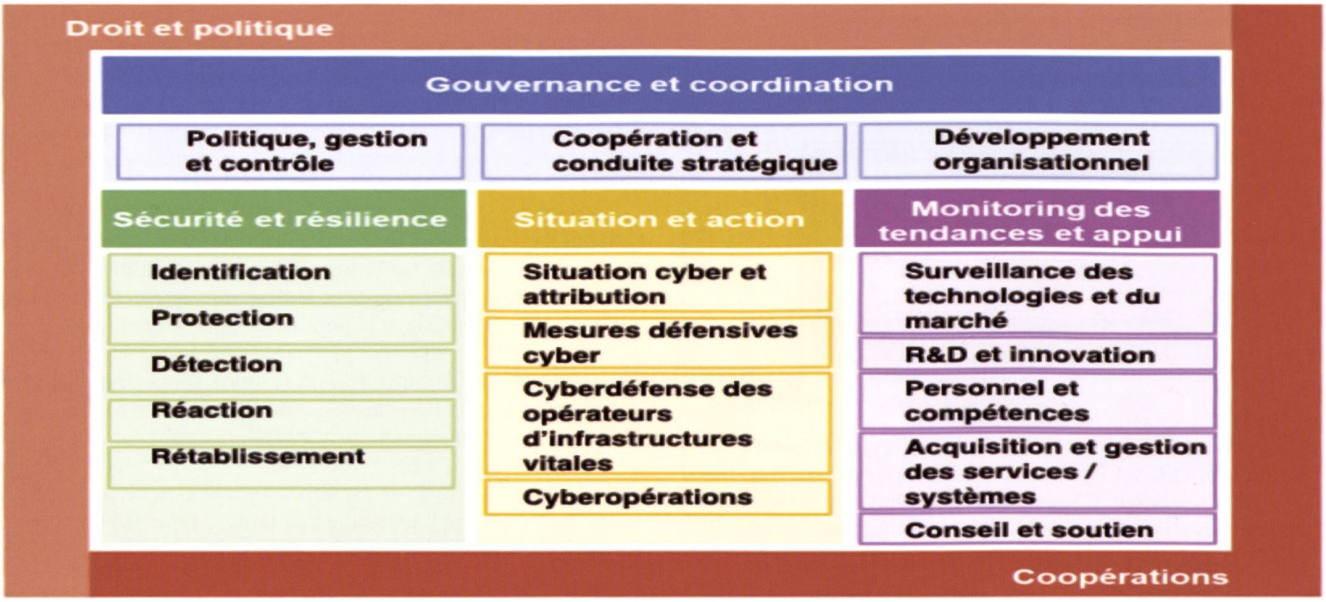



Motivations et capacité des acteurs.

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 et du développement 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 et risques potentiels. Les constats qui en sont tirés servent à formuler les objectifs et les domaines centraux de la Stratégie cyber du DDPS. Celle-ci détermine qui au DDPS assume ou développera quelles tâches. La stratégie se concentre sur la cyberdéfense mais elle s'aligne sur les mesures que le DDPS implémente également dans le cadre de la SNPC.

Stratégie Cyber du DDPS : Architecture détaillée.



## 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'Etat, 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 secrétaire général du DDPS. Le DDPS entend réaliser les objectifs suivants :

- 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.

### 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.

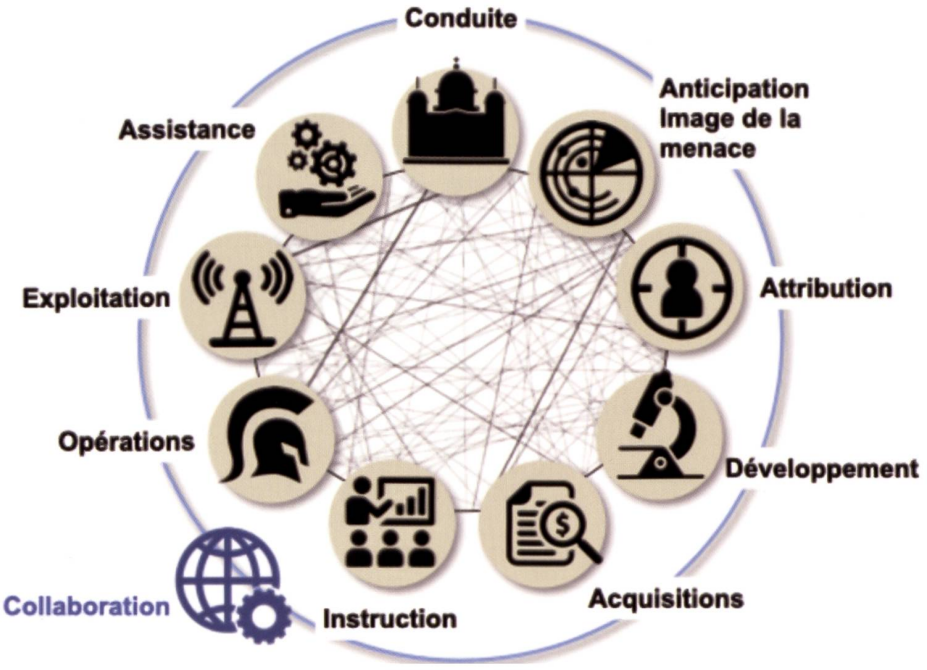
- Tous les services du DDPS chargés de tâches liées à la cyber- sécurité se coordonnent dans le cadre de la Stratégie cyber du DDPS.

- 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 Centre national pour la cybersécurité (NCSC).

Le DDPS « entrepreneur général pour la cyberdéfense ».



- Le DDPS est capable de prévenir les menaces et les attaques provoquant des dégâts, ayant des répercussions nationales ou mettant en danger des in- térêts nationaux2. Il peut déceler, perturber ou empêcher les menaces et les attaques à temps et dans toutes les situations.
- 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.

- 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.

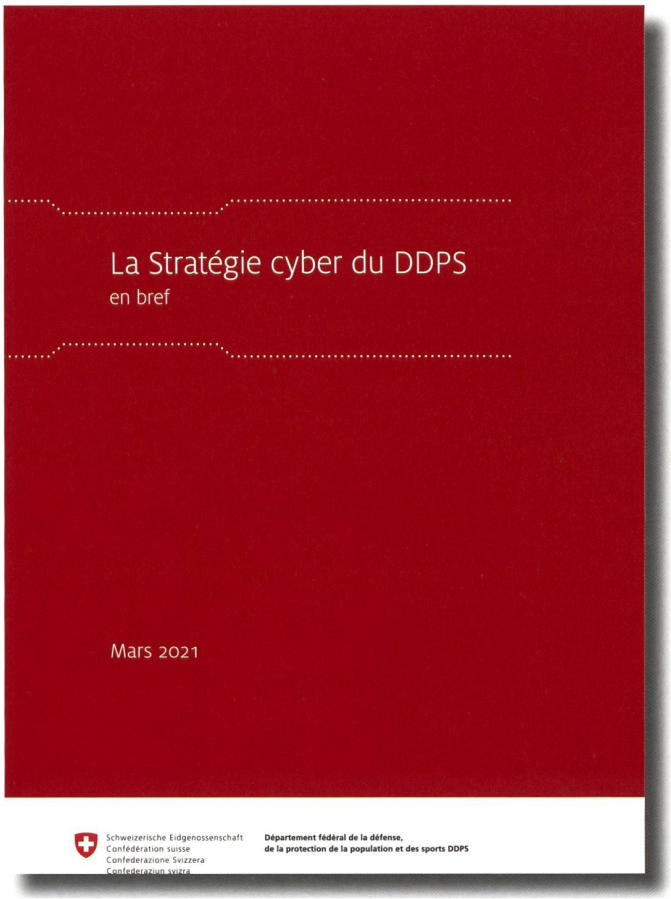
- Le DDPS fait en sorte que son matériel informatique, les logiciels et les réseaux correspondent à la technologie actuelle. Il veille à la fiabilité de l'exploitation et s'assure que le matériel nécessaire soit toujours disponible. Il est aussi in- dépendant que possible des prestataires et des fournisseurs et accroît ainsi son autonomie.

- Le DDPS se positionne en tant que précurseur et modèle dans le domaine de la cyberdéfense, et aussi en tant qu'employeur attrayant.

## Cyberdéfense DDPS : Quatre axes principaux

La Stratégie cyber du DDPS classe les mesures dans quatre domaines centraux: 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




## 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 collabora- tion avec ses partenaires de la politique de sécurité en Suisse. La collaboration se fait avec les cantons, les communes, les milieux économiques et scienti- fiques, 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.

M. E