Berne, le 20 septembre 2024

DDPS. Subsidiarité et cybersécurité

Rapport du Conseil fédéral en réponse au postulat 22.3368 du 9 mai 2022 de la Commission de la politique de sécurité du Conseil national

Table des matières

Condensé

Le principe de subsidiarité est un élément essentiel du droit public suisse. Selon ce principe, les tâches sont exécutées en priorité par le niveau étatique le plus bas. La Confédération prend donc en charge seulement les tâches que les cantons n'ont pas la force d'assumer. Le principe de subsidiarité inscrit dans la Constitution vaut aussi bien pour la répartition des tâches et des compétences entre la Confédération, les cantons et les communes que pour l'exercice des compétences. La sécurité intérieure relève de la compétence à la fois de la Confédération et des cantons ; la responsabilité en incombe toutefois en principe aux cantons. L'armée apporte son appui aux autorités civiles lorsque leurs moyens ne suffisent plus et lorsque les conditions de l'art. 67 de la loi du 3 février 1995 sur l'armée (LAAM)[1] sont remplies. La Confédération et les cantons sont tenus de s'entraider dans l'accomplissement de leurs tâches en vertu de l'art. 44 de la Constitution (Cst.)[2] consacré à la collaboration fédérale. Quant aux unités administratives de la Confédération, elles sont tenues de collaborer entre elles en vertu de l'art. 14 de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[3]. (Chapitre 2)

La protection contre les cybermenaces relève de la responsabilité commune des milieux économiques, de la société et de l'État. En principe, chaque acteur est responsable de sa propre sécurité. Au sein du DDPS, les offices assument diverses tâches dans le domaine de la cybersécurité. En matière de cybersécurité, seuls deux types de prestations sont fournis à titre subsidiaire, à savoir le service d'appui de l'armée et le soutien technique de l'Office fédéral de la cybersécurité aux exploitants privés d'infrastructures critiques. Les autres tâches cyber effectuées par le DDPS peuvent être réparties en deux catégories : (1) les prestations fournies à des tiers, pour lesquelles la question de la subsidiarité a déjà été analysée au cours du processus législatif, (2) les prestations fournies par les offices du DDPS à la Confédération elle-même, et qui ne nécessitent donc pas d'examen de la subsidiarité. (Chapitre 3)

Le DDPS dispose de compétences cyber étendues aussi bien dans le domaine civil que dans le domaine militaire. Le présent rapport montre cependant que la collaboration entre les éléments militaires du commandement Cyber et l'Office fédéral de la cybersécurité n'est possible que si les conditions d'un service d'appui de l'armée sont réunies. Or, la compétence de décider de la mise sur pied d'un service d'appui échoit au Conseil fédéral. Cette voie procédurale qui passe par le gouvernement rend difficile une collaboration à la fois efficace et juridiquement fondée entre le commandement Cyber et l'Office fédéral de la cybersécurité, car dans le domaine cyber, il faut engager le personnel spécialisé de manière rapide et ciblée. Le DDPS peut en revanche décider seul de la mise sur pied d'un service d'appui en cas de catastrophe en Suisse. Une base juridique permettant au commandement Cyber de fournir des prestations d'appui militaires à l'Office fédéral de la cybersécurité avec la même simplicité fait encore défaut. Afin de faire face à cette problématique, il y a lieu d'envisager la création d'une base juridique permettant d'intervenir rapidement et de manière efficace, raison pour laquelle le rapport propose la mesure suivante :

[1] RS **510.10**
[2] RS **101**
[3] RS **172.010.1**

L'Office fédéral de la cybersécurité (OFCS) étudie, en collaboration avec le commandement des Opérations, le commandement Cyber, le Secrétariat général du DDPS, le Secrétariat d'État à la politique de sécurité et le Réseau national de sécurité, la création d'une base juridique permettant au commandement Cyber de fournir des prestations d'appui à l'OFCS selon un processus simplifié. L'OFCS proposera, d'ici la fin 2026, plusieurs options au Conseil fédéral pour la suite de la procédure. (Chapitre 4)

Liste des abréviations

ACEM	service Actions dans le cyberespace et l'espace électromagnétique
al.	alinéa
AOSS	autorités et organisations chargées du sauvetage et de la sécurité
armasuisse	Office fédéral de l'armement
art.	article
ATF	Recueil officiel des arrêts du Tribunal fédéral suisse
CCD CoE	Centre d'excellence pour la cyberdéfense en coopération à Tallinn
CCDJP	Conférence des directrices et directeurs des départements cantonaux de justice et police
CCPCS	Conférence des commandantes et commandants des polices cantonales de Suisse
CERT	Computer Emergency Response Team
cf.	confer
ch.	chiffre
ch. marg.	chiffre(s) marginal(aux)
CMS	système mobile de communication sécurisée à large bande
consid.	considérant d'un ATF
CSN	cyberstratégie nationale
CSS	Center for Security Studies
Cst.	Constitution fédérale de la Confédération suisse du 18 avril 1999 (RS *101*)
CTC	Cyber Training Center
CYD Campus	Cyber-Defence Campus
DDPS	Département fédéral de la défense, de la protection de la population et des sports
DFAE	Département fédéral des affaires étrangères
éd.	éditeur, édition
en part.	en particulier
env.	environ
et al.	et alii
etc.	et cetera
fedpol	Office fédéral de la police
FF	Feuille fédérale
LAAM	Loi du 3 février 1995 sur l'armée (RS *510.10*)
let.	lettre
LMSI	Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (RS *120*)
LOGA	Loi du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (RS *172.010*)
LPPCi	Loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (RS *520.1*)
LRens	Loi fédérale du 25 septembre 2015 sur le renseignement (RS *121*)
LSI	Loi du 18 décembre 2020 sur la sécurité de l'information (RS *128*)

LSIrev	Modification du 29 septembre 2023 de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques) (FF 2023 2296)
MELANI	Centrale d'enregistrement et d'analyse pour la sûreté de l'information
MPC	Ministère public de la Confédération
N	note(s) marginale(s)
nbp.	note de bas de page
NCSC	Centre national pour la cybersécurité
NEOC	National Emergency Operations Center, anciennement Centrale nationale d'alarme (CENAL)
OAMC	Ordonnance du 21 novembre 2018 sur l'aide militaire en cas de catastrophe dans le pays (RS *513.75*)
OCMil	Ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (RS *510.921*)
OFCS	Office fédéral de la cybersécurité
OFDF	Office fédéral de la douane et de la sécurité des frontières
OFPP	Office fédéral de la protection de la population
OGE	Ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio (RS *510.292*)
OLOGA	Ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (RS *172.010.1*)
OProP	Ordonnance du 11 novembre 2020 sur la protection de la population (RS *520.12*)
ORens	Ordonnance du 16 août 2017 sur le renseignement (RS *121.1*)
Org-DDPS	Ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (RS *172.214.1*)
OSI	Ordonnance du 8 novembre 2023 sur la sécurité de l'information (RS *128.1*)
p. ex.	par exemple
p.(pp.)	page(s)
po.	postulat
RDS+	réseau de données sécurisé plus
ResMaB	Gestion fédérale des ressources
RNS	Réseau national de sécurité
RPT	Réforme de la péréquation financière et de la répartition des tâches entre la Confédération et les cantons
RS	recueil systématique du droit fédéral
s./ss	page(s) suivante(s)
SEPOS	Secrétariat d'État à la politique de sécurité
SG-DDPS	Secrétariat général du DDPS
SGK	*St. Galler Kommentar* (commentaire de la Constitution fédérale)
SRC	Service de renseignement de la Confédération
stratégie PIC	stratégie nationale de protection des infrastructures critiques
TIC	technologies de l'information et de la communication
WEP 2030	Maintien de la valeur de Polycom
y c.	y compris

1 Contexte

1.1 Mandat

Le présent rapport répond au postulat 22.3368 « DDPS. Subsidiarité et cybersécurité », déposé par la Commission de la politique de sécurité du Conseil national le 21 mars 2022 et adopté le 9 mai de la même année. Le texte déposé est le suivant :

> *Le Conseil fédéral est chargé de produire un rapport dans lequel il exposera la manière dont la notion de subsidiarité est réexaminée au sein du DDPS et dont elle sera applicable, en particulier dans le cadre de la collaboration en matière de prestations de sécurité dans le cyberespace.*
>
> *La situation en Ukraine montre que la notion de sécurité doit être envisagée de manière plus large, notamment dans le cyberespace. En cas d'aggravation de la situation, différents domaines peuvent rapidement être touchés : l'économie, la société, la défense, l'approvisionnement, etc. Afin de lutter efficacement contre les risques multiples, il convient, au niveau fédéral, de mettre à profit de manière ciblée les compétences disponibles et d'éviter les doublons. Le DDPS dispose de compétences aussi bien dans le domaine civil que dans le domaine militaire. Séparer ces compétences est une approche qui n'a plus d'avenir.*

Le mandat du postulat, comme le Conseil fédéral le comprend, ne remet pas en question l'application du principe de subsidiarité dans le domaine cyber. La subsidiarité est un principe politique dont la modification relève du constituant.

Le mandat peut être scindé en deux parties. Dans la première, il s'agit d'examiner la notion de subsidiarité en lien avec la cybersécurité (en se concentrant sur le DDPS). L'on y exposera ce que signifie le principe de subsidiarité. Dans la deuxième, il s'agit de présenter les compétences existantes dans le domaine cyber et de monter comment la collaboration entre les intervenants peut être renforcée.

1.2 Structure

Le présent rapport expliquera dans un premier temps le principe de subsidiarité (chapitre 2). Il examinera ensuite la notion de cybersécurité, en explicitant les responsabilités et les tâches des offices fédéraux du DDPS (chapitre 3). Enfin, il indiquera s'il y a lieu de prendre des mesures dans ce domaine (chapitre 4).

2 Principe de subsidiarité

Selon le principe de subsidiarité, les tâches ne sont confiées à un niveau étatique supérieur (comme la Confédération) que s'il est prouvé qu'elles pourront y être mieux accomplies qu'à un niveau inférieur (comme les cantons ou les communes)[4]. En Suisse, le principe de subsidiarité se fonde sur les art. 5*a* et 43*a*, al. 1, de la Constitution (Cst.)[5].

[4] Message du 14 novembre 2001 concernant la Réforme de la péréquation financière et de la répartition des tâches entre la Confédération et les cantons (RPT), FF **2002** 2155, 2168.
[5] RS **101**

Le principe de subsidiarité est un élément essentiel du droit public suisse. Le chapitre qui suit approfondit la définition introduite plus haut en éclairant trois aspects fondamentaux du principe de subsidiarité en Suisse : le rapport entre État et particuliers, entre Confédération, cantons et communes et enfin, entre armée et autorités civiles. Il présentera ensuite d'autres formes de soutien mutuel avant de récapituler les principales conclusions.

2.1 Subsidiarité entre État et particuliers

Les concepts d'autonomie et de responsabilité individuelle alimentent la réflexion sur la subsidiarité entre État et particuliers. Selon le principe de subsidiarité, les pouvoirs publics interviennent uniquement lorsque les particuliers ou la société ne sont pas en mesure d'accomplir par eux-mêmes les tâches nécessaires. L'État ne prend en charge que des tâches d'intérêt public qui revêtent une importance telle qu'elles doivent être accomplies même si elles ne sont pas (ou ne peuvent pas être) effectuées par des particuliers[6].

Le principe de subsidiarité entre État et particuliers trouve en partie son fondement dans la Constitution. Selon l'art. 6 Cst., toute personne est responsable d'elle-même et contribue selon ses forces à l'accomplissement des tâches de l'État et de la société. C'est en situation de détresse uniquement, lorsqu'elle n'est pas en mesure de subvenir à son entretien, qu'une personne a le droit d'obtenir de l'aide en vertu de l'art. 12 Cst[7]. L'art. 41, al. 1, Cst., précise d'ailleurs que l'État ne s'engage pour les buts sociaux qu'*en complément de la responsabilité individuelle et de l'initiative privée*.

La responsabilité individuelle est un principe qui s'applique dans tous les domaines de la vie, y compris la cybersécurité. La cyberstratégie nationale (CSN)[8] retient ainsi que la protection contre les cybermenaces est une tâche commune de la société, des milieux économiques et de l'État. Les responsabilités et compétences respectives sont clairement réglées et sont portées par toutes les parties prenantes. La CSN est donc mise en œuvre de manière décentralisée et sous responsabilité commune, selon les principes du fédéralisme. Les acteurs privés sont fondamentalement responsables de leur propre cybersécurité[9].

2.2 Subsidiarité entre Confédération, cantons et communes

Le principe de subsidiarité veut qu'une tâche soit exécutée, si possible, par la plus petite unité, l'unité supérieure n'intervenant que si la collectivité territoriale en question ne parvient pas, seule ou avec l'aide d'autres, à accomplir la tâche. Cette conception de la subsidiarité est ancrée dans la Constitution[10]. Le chapitre qui suit explique l'interaction entre les différents articles constitutionnels.

---

[6] JOHAN ROCHEL, commentaire de l'art. 6 Cst., in : Stefan Schlegel/Odile Ammann (éd.), Commentaire en ligne de la Constitution fédérale – version : 01.09.2023, N 39 ss, <https://onlinekommentar.ch/fr/kommentare/bv6> (dernière date de consultation de toutes les sources sur Internet : 15.05.2024).
[7] JOHAN ROCHEL, commentaire de l'art. 6 Cst. (nbp. 6), N 34.
[8] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » d'avril 2023 <https://www.newsd.admin.ch/newsd/message/attachments/76794.pdf>.
[9] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 12.
[10] Message RPT, FF **2002** 2155 (nbp. 4), 2168.

L'art 3 Cst. règle la répartition des compétences entre la Confédération et les cantons. Il dispose que les cantons exercent tous les droits qui ne sont pas délégués à la Confédération. En Suisse, selon la Constitution fédérale, les tâches étatiques relèvent donc en principe de la responsabilité des cantons (compétence générale). La Confédération est compétente uniquement là où la Constitution lui en octroie le pouvoir. En définitive, ses compétences et ses tâches sont ainsi réglées par la Constitution, ce qui est expressément formulé à l'art. 42, al. 1, Cst. : la Confédération accomplit les tâches que lui attribue la Constitution. Elle ne peut par conséquent exercer de responsabilité dans un domaine que si la Constitution la déclare compétente en la matière et lui donne la compétence d'agir (principe de l'habilitation ponctuelle)[11]. À l'inverse, cela signifie que toutes les compétences qui n'ont pas été attribuées à la Confédération relèvent des cantons (répartition intégrale des compétences)[12].

Pour examiner l'attribution et l'exercice des compétences, il s'agit de tenir compte du principe de subsidiarité fondé sur l'art. 5*a* Cst. Selon l'art. 5*a* Cst., la Confédération et les cantons doivent attribuer et accomplir les tâches étatiques en observant le principe de subsidiarité.

Ce principe est concrétisé à l'art. 43*a* Cst., en vertu duquel la Confédération ne règle que les domaines qui excèdent les possibilités des cantons ou qui nécessitent une réglementation uniforme[13]. La Confédération ne peut ainsi exercer aucune tâche que les cantons sont en mesure d'accomplir eux-mêmes à satisfaction[14]. Également imposés par l'art. 43*a*, al. 5, Cst., les principes de la rationalité et de l'adéquation, applicables dans l'accomplissement des tâches étatiques, ne remettent pas non plus en question la répartition constitutionnelle des tâches : même si la Confédération pouvait apporter une prestation de manière plus rentable que les cantons, cela ne suffirait pas pour lui attribuer la tâche en question[15].

Le principe de subsidiarité trouve également son expression dans l'art. 46, al. 1, Cst., selon lequel il appartient aux cantons de mettre en œuvre le droit fédéral. En vertu de l'art. 46, al. 3, Cst., la Confédération doit laisser aux cantons une marge de manœuvre aussi large que possible pour mettre en œuvre le droit fédéral et tenir compte de leurs particularités. Elle doit également leur laisser suffisamment de tâches propres, respecter leur autonomie d'organisation, leur laisser des sources de financement suffisantes et contribuer à ce qu'ils disposent des moyens financiers nécessaires pour accomplir leurs tâches (art. 47 Cst.).

Le principe de subsidiarité exprime l'autonomie de chaque niveau administratif dans l'organisation de ses tâches et dans le choix des moyens engagés. Cette autonomie est explicitée à l'art. 43 Cst. : les cantons définissent les tâches qu'ils accomplissent

---

[11] Réponse du Conseil fédéral du 2 mars 2012 donnant suite au postulat Malama 10.3045 du 3 mars 2010. Sécurité intérieure. Clarification des compétences, FF **2012** 4161, 4180 s.
[12] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4181.
[13] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4181 ; message RPT, FF **2002** 2155 (nbp. 4), 2321 s.
[14] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4181 ; message RPT, FF **2002** 2155 (nbp. 4), 2321 s.
[15] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4181 ; message RPT, FF **2002** 2155 (nbp. 4), 2191 et 2321 s.

dans le cadre de leurs compétences[16]. Le principe de subsidiarité répond ainsi aux exigences d'un fédéralisme moderne[17].

Le niveau supérieur de l'État ne peut prendre le relais qu'à partir du moment où le niveau inférieur n'est pas (ou plus) en mesure d'accomplir une tâche. Les compétences de la Confédération doivent donc, dans leur étendue et leur expression, toujours être limitées à ce qui est nécessaire. L'élargissement d'un champ de compétences existant ou l'introduction de nouvelles compétences doit toujours être justifié et reposer sur une base légale pertinente (cf. art. 3 Cst.).

Le principe de subsidiarité vaut non seulement pour l'attribution des tâches, mais également pour la réalisation de celles-ci. La répartition judicieuse des tâches, à un niveau approprié, permet une certaine marge d'appréciation politique.

2.3 Subsidiarité entre armée et autorités civiles

Le terme de *subsidiarité* n'est pas seulement utilisé dans le contexte des dispositions constitutionnelles sur la répartition des tâches étatiques. D'autres bases juridiques également qualifient d'appui *subsidiaire* des prestations fournies dans certaines conditions par l'État à des tiers. L'Office fédéral de la cybersécurité (OFCS) soutient, par exemple, les exploitants d'infrastructures critiques quand des cyberincidents mettent en danger leur fonctionnement. Un tel soutien est fourni aux privés subsidiairement aux prestations informatiques disponibles sur le marché (cf. chapitre 3.4.7).

L'armée fournit ce qu'on appelle des engagements subsidiaires lorsqu'elle vient en aide aux autorités civiles qui font face à une grave menace contre la sécurité intérieure ou à d'autres situations d'exception. Le chapitre qui suit examine de manière plus approfondie les engagements subsidiaires de l'armée.

Conformément à l'art. 57 Cst. la Confédération et les cantons pourvoient à la sécurité du pays et à la protection de la population dans les limites de leurs compétences respectives. Ils coordonnent leurs efforts en matière de sécurité intérieure. Cela signifie que la sécurité relève aussi bien de la compétence des cantons que de celle de la Confédération[18]. Les cantons assument en principe la responsabilité primaire pour la sécurité intérieure sur leur territoire (souveraineté en matière de police)[19]. Là aussi, la Confédération ne remplit que les tâches qui lui sont expressément attribuées (p. ex. par les art. 58 ss Cst. et l'art. 61 Cst.).

La mise sur pied de l'armée relève de la compétence exclusive de la Confédération (art. 58 Cst.). La mission de l'armée est fixée à l'art. 58, al. 2, Cst. (1) L'armée contribue à prévenir la guerre et à maintenir la paix ; (2) elle assure la défense du pays et de sa population, et (3) elle apporte son soutien aux autorités civiles lorsqu'elles doivent faire face à une grave menace pesant sur la sécurité intérieure ou à d'autres situations

[16] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4182.
[17] Message RPT, FF **2002** 2155 (nbp. 4), 2169.
[18] Message relatif à une nouvelle constitution fédérale du 20 novembre 1996, FF **1997** I 1, 239 ; SGK BV-MÜLLER/MOHLER, art. 57 N 1.
[19] Message Cst., FF **1997** I 1 (nbp. 18), 239 ; cf. aussi art. 4 de la loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI ; RS **120**).

d'exception. La suite du chapitre se concentre sur le troisième volet de cette mission, à savoir le soutien aux autorités civiles lorsqu'elles doivent faire face à une grave menace pesant sur la sécurité intérieure ou à d'autres situations d'exception.

L'art. 65 de la loi du 3 février 1995 sur l'armée (LAAM)[20] distingue trois types d'engagements de l'armée : le service de promotion de la paix, le service d'appui et le service actif[21]. Ce sont particulièrement le service actif et le service d'appui qui sont intéressants dans le cas examiné.

Le service actif est accompli pour défendre la Suisse et sa population (service de défense nationale), soutenir les autorités civiles en cas de menaces graves contre la sécurité intérieure (service d'ordre) et améliorer le niveau de l'instruction de l'armée en cas d'accroissement de la menace (art. 76 LAAM)[22].

En vertu de l'art. 173, al. 1, let. d, Cst., il appartient à l'Assemblée fédérale d'ordonner le service actif. Cette compétence est déléguée au Conseil fédéral uniquement dans les cas d'urgence. L'Assemblée fédérale doit alors être convoquée sans délai si plus de 4000 militaires sont mis sur pied ou si l'engagement dure plus de trois semaines (art. 185, al. 4, Cst.)[23].

Selon l'art. 1, al. 2, LAAM, l'armée apporte son appui aux autorités civiles lorsque leurs moyens ne suffisent plus (service d'appui). Il s'agit maintenant de traiter plus en détail ce service d'appui (art. 67 LAAM).

L'art. 67, al. 1, let. a à e, LAAM décrit les situations dans lesquelles l'armée peut soutenir les autorités civiles en Suisse. Elle le fait pour :

- faire face à des situations extraordinaires dans lesquelles la sécurité intérieure n'est pas gravement menacée et qui ne nécessitent pas un recours au service d'ordre ;

- assurer la protection de personnes et la protection de biens particulièrement dignes de protection, en particulier les infrastructures indispensables au fonctionnement de la société, de l'économie ou de l'État (infrastructures critiques) ;

- accomplir des tâches relevant du Réseau national de sécurité ou des services coordonnés ;

- faire face à des catastrophes, à des situations de surcharge extrême ou accomplir des tâches que les autorités civiles ne peuvent accomplir seules faute de moyens ou de personnel appropriés ;

- accomplir d'autres tâches d'importance nationale ou internationale.

[20] RS **510.10**
[21] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4212.
[22] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4215.
[23] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4215.

Les conditions suivantes doivent être remplies pour permettre un engagement subsidiaire de l'armée dans le domaine de la sécurité intérieure (art. 1, al. 2, et art. 67, al. 2, LAAM)[24].

- Tous les moyens civils appropriés sont engagés à tous les niveaux et ne suffisent pas, par manque de matériel, de personnel ou de temps, pour maîtriser la situation.

- L'appui est apporté à la demande des autorités fédérales ou cantonales concernées.

- La tâche est d'intérêt public.

Cela signifie que l'armée n'intervient que ponctuellement, pour faire face à une surcharge extraordinaire, et non pas pour combler des lacunes permanentes[25]. L'essentiel des contraintes est ainsi supporté par les cantons[26]. Enfin, il faut encore retenir que les autorités fédérales peuvent aussi être des autorités civiles au sens de l'art. 58, al. 2, Cst. Cet article limite cependant la possibilité de soutien de l'armée aux autorités civiles qui font face à une grave menace pesant sur la sécurité intérieure ou à d'autres situations d'exception[27].

Il convient en outre de distinguer l'armée du Groupement Défense (administration militaire). Cette différenciation est importante, dans la mesure où les deux organisations sont soumises à des bases légales différentes. Leurs possibilités en matière d'appui ne sont par conséquent pas identiques, raison pour laquelle le prochain paragraphe abordera la structure de l'armée et celle du Groupement Défense de manière plus approfondie et se penchera également sur leurs missions d'appui respectives.

Structure

- L'armée ne fait pas partie de l'administration fédérale, mais constitue une organisation étatique *sui generis*.

- Le Groupement Défense fait, quant à lui, partie intégrante de l'administration fédérale.

- Nonobstant cette différenciation, les structures organisationnelles du Groupement Défense sont en partie identiques à celles de l'armée[28]. Cela a pour effet que les structures de l'armée se confondent avec celles du Groupement Défense, ce qui peut aussi conduire le personnel militaire à exercer des fonctions de l'administration.

[24] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4212 s.
[25] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4212.
[26] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4213.
[27] Rapport po. Malama, FF **2012** 4161 (nbp. 11), 4213.
[28] DDPS, Conception générale cyber de mars 2022, p. 55 <Cybercapacités de l'armée : autoprotection et flexibilité de l'engagement accrues (admin.ch)>.

Missions d'appui

- La mission d'appui en faveur des autorités civiles mentionnée dans la loi sur l'armée est une tâche attribuée à l'armée et non pas au Groupement Défense.

- Le Groupement Défense appuie les prestations de l'armée mais ne fournit aucune prestation directe en faveur de tiers. À titre d'appui, l'art. 67, al. 3, LAAM, mentionne expressément l'envoi de troupes et la mise à disposition de matériel et de biens d'approvisionnement de l'armée ; il n'est possible de faire appel à du personnel de l'administration fédérale qu'en cas de nécessité.

- Tout comme les autres unités administratives de la Confédération, le Groupement Défense dépend de la loi fédérale du 21 mars 1997 sur l'organisation du gouvernement et de l'administration (LOGA)[29] et de l'ordonnance du 25 novembre 1998 sur l'organisation du gouvernement et de l'administration (OLOGA)[30]. Les possibilités d'entraide prévues par la LOGA et l'OLOGA sont abordées au chapitre suivant. Le Groupement Défense ne dispose d'aucune base juridique lui permettant de fournir directement des prestations subsidiaires à des tiers. L'art. 67, al. 2, LAAM, en revanche, permet à l'armée d'effectuer un service d'appui.

Le chapitre 4 (Mesure) abordera la question des difficultés résultant des structures décrites ci-avant et du fait que chacune des deux organisations est soumise à des bases légales différentes.

En principe, la compétence de mettre sur pied un service d'appui échoit au Conseil fédéral (art. 70, al. 1, let. a, LAAM). La loi sur l'armée prévoit toutefois deux exceptions. En cas de catastrophe en Suisse, le DDPS a la compétence de décider seul de la mise sur pied et de l'attribution d'un service d'appui aux autorités civiles (art. 70, al. 1, let. b, LAAM). Il peut également prendre seul une telle décision sur demande du Département fédéral des affaires étrangères (DFAE) en cas de catastrophe à l'étranger exigeant un engagement immédiat (art. 70, al. 1, let. c, LAAM).

Quelle que soit l'autorité habilitée à décider, un service d'appui requiert toujours l'approbation de l'Assemblée fédérale si la mise sur pied dure plus de trois semaines ou comprend plus de 2000 militaires[31].

Le chapitre 4 (Mesure) se réfère à une intervention en cas de catastrophe en Suisse, raison pour laquelle ce sujet est traité de manière plus détaillée ici. L'ordonnance du 21 novembre 2018 sur l'aide militaire en cas de catastrophe dans le pays (OAMC)[32] règle les détails d'un tel engagement. Ainsi, l'art. 3, let. c, OAMC, précise que l'aide militaire en cas de catastrophe peut consister à engager des troupes de l'armée de même que du personnel militaire ou civil du Groupement Défense. Cette base juridique permet donc d'engager aussi bien l'armée que le Groupement Défense pour fournir les prestations d'appui.

[29] RS **172.010**
[30] RS **172.010.1**
[31] Rapport Po. Malama, FF **2012** 4161 (Fn. 11), 4214.
[32] RS **513.75**

L'art. 6 OAMC règle la procédure et la prise de décision en la matière. L'autorité civile adresse sa demande directement au commandement des Opérations. Celui-ci prépare la décision à l'attention du DDPS (art. 6, al. 1, OAMC). En cas d'urgence, lorsqu'une intervention rapide est nécessaire, le commandement des Opérations peut ordonner la mise en œuvre d'une aide militaire en cas de catastrophe. De tels ordres doivent être soumis dès que possible au DDPS pour décision (art. 6, al. 2, OAMC). Des dispositions particulières, sur lesquelles l'on ne s'attardera pas ici, s'appliquent lorsque le service de défense nationale a été ordonné.

En cas d'intervention de ce type, l'autorité civile détermine l'engagement des moyens ainsi que la mission en accord avec le commandement des Opérations (art. 8, al. 1, OAMC). L'art. 8, al. 3, OAMC, précise à ce propos que l'autorité civile assume la responsabilité globale de l'engagement.

Il est plus simple d'engager un service d'appui en cas de catastrophe en Suisse que dans d'autres situations, car la décision relève uniquement de la compétence du DDPS, et non pas de celle de l'ensemble du Conseil fédéral. Il n'existe pas de procédure simplifiée équivalente pour les prestations d'appui en cas de cyberincident. Le chapitre 4 (Mesure) reviendra sur cette lacune.

Dans son rapport intitulé *La subsidiarité et les principes de coordination des moyens de milice de l'armée, de la protection civile et du service civil en cas de crise*, le Réseau national de sécurité (RNS) a fixé neuf conditions nécessaires à l'admission d'une demande de service d'appui[33]. Le rapport ne décrit toutefois pas la situation en cas de cyberincident. Ce point sera également abordé au chapitre 4 (Mesures).

2.4 Autres formes de soutien

Le principe de subsidiarité est complété par ce qu'on appelle le fédéralisme coopératif[34]. On entend par là des formes de collaboration entre cantons et entre les cantons et la Confédération[35]. Ces collaborations permettent aux autorités de partager des ressources, des savoirs et des informations afin d'accomplir leurs tâches de manière efficace et effective.

Concernant l'accomplissement des tâches, l'art. 44 Cst. rend obligatoire aussi bien l'entraide entre la Confédération et les cantons (relation verticale) que la collaboration entre les cantons (relation horizontale)[36]. Cela signifie que les cantons sont tenus de s'apporter une aide mutuelle[37], qui peut être réglée par des concordats[38].

Au niveau de la Confédération, l'obligation des unités administratives à collaborer découle de l'art. 14 OLOGA. Elles s'entraident et s'informent mutuellement. Elles

[33] Réseau national de sécurité, La subsidiarité et les principes de coordination des moyens de milice de l'armée, de la protection civile et du service civil en cas de crise, établi en réponse à la recommandation n°4 du Contrôle fédéral des finances (20542), novembre 2023, p. 13 ss, <https://www.svs.admin.ch/fr/themen-/krisenmanagement.html>.
[34] SGK BV- SCHWEIZER, art. 44 N 6.
[35] ULRICH HÄFELIN et al., Schweizerisches Bundesstaatsrecht, 10e éd., Zurich 2020, ch. marg. 1242.
[36] ULRICH HÄFELIN et al. (nbp. 35), ch. marg. 1245 et 1254.
[37] Message Cst., FF **1997** I 1 (nbp. 18), 210 s.
[38] PIERRE TSCHANNEN, Staatsrecht der Schweizerischen Eidgenossenschaft, 5e éd., Berne 2021, ch. marg. 556.

coordonnent en outre leurs activités et échangent des renseignements dans la mesure où c'est nécessaire à l'accomplissement de leurs tâches légales. Les prestations du Groupement Défense sont aussi concernées.

2.5 Principales conclusions

Le principe de subsidiarité est un élément essentiel du droit public suisse. Selon ce principe, les tâches sont exécutées en priorité par le niveau étatique le plus bas. La Confédération prend donc en charge seulement les tâches que les cantons n'ont pas la force d'assumer. Le principe de subsidiarité est inscrit dans la Constitution et il influence la répartition et l'exécution des tâches et des compétences entre la Confédération, les cantons et les communes. La sécurité intérieure relève de la compétence à la fois de la Confédération et des cantons ; la responsabilité en incombe toutefois en principe aux cantons. L'armée apporte son appui aux autorités civiles lorsque leurs moyens ne suffisent plus et que les conditions de l'art. 67 LAAM sont remplies. Le devoir de collaboration entre la Confédération et les cantons (entraide dans l'accomplissement de leurs tâches) est inscrit à l'art. 44 Cst. Quant à l'art. 14 OLOGA, il règle la collaboration entre les unités administratives de la Confédération.

Le chapitre suivant est consacré à l'examen approfondi de la notion de cybersécurité. Il présente les capacités et les compétences disponibles en matière cyber dans les différents offices du DDPS.

3 Cybersécurité

3.1 Notion de cybersécurité

Par cybersécurité, on entend une 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, fonctionne comme prévu[39].

3.2 Responsabilités en matière de cybersécurité

La cybersécurité est un thème transversal, qui ne peut relever de la compétence d'une seule autorité. Cette constatation est particulièrement vraie pour la Suisse et ses structures fédéralistes. Bien que les interactions numériques dépassent le cadre des frontières, le principe constitutionnel des compétences étatiques s'applique également dans le cyberespace. La Confédération et les cantons ont mis en place leurs organisations cyber respectives en se fondant sur ce principe. Parallèlement à la distribution des tâches entre les différents niveaux de l'État, la collaboration entre acteurs privés et publics joue aussi un rôle déterminant pour la cybersécurité. Organisée de manière diversifiée, cette collaboration est assurée par des organisations privées et publiques. Elle comprend aussi la participation directe d'associations et d'entreprises à la mise en œuvre des mesures de la cyberstratégie nationale (CSN) ainsi que la coopération quotidienne et l'échange d'expérience entre des équipes de sécurité privées et publiques[40].

[39] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 37.
[40] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 9.

La Confédération prend les mesures nécessaires pour augmenter sa propre cybersécurité et contribue à l'amélioration de la cybersécurité de l'économie et de la société en tenant compte du principe de subsidiarité. Dans le contexte de cette pesée d'intérêts, elle mesure l'importance capitale des infrastructures critiques. L'encouragement à la coopération internationale en matière de cybersécurité fait aussi partie des mesures considérées.

Les tâches principales en matière de cybersécurité et la coordination avec les autres services compétents sont du ressort de l'OFCS[41]. L'office se concentre sur la cybersécurité civile ; ses tâches sont ainsi clairement délimitées par rapport aux compétences de l'armée dans le domaine de la cyberdéfense[42]. L'OFCS n'assume pas de tâches sectorielles de surveillance ou de régulation des autorités spécialisées. Celles-ci conservent la compétence d'accorder des autorisations aux industries et aux entreprises concessionnaires et d'assurer la surveillance opérationnelle du respect des directives spécifiques au secteur de la cybersécurité[43].

L'OFCS collabore étroitement avec les offices spécialisés et met à leur disposition ses connaissances en cybersécurité. La poursuite pénale de la cybercriminalité est avant tout du ressort des cantons. Au niveau de la Confédération, les autorités compétentes sont l'Office fédéral de la police (fedpol) et le Ministère public de la Confédération (MPC). Les bases légales de ces deux organisations précisent les compétences des services impliqués. Les unités administratives veillent par ailleurs à pratiquer, dans le cadre fixé par la loi, un échange continu d'informations et d'expériences, à des fins de coordination et d'exploitation des synergies[44].

Les cantons organisent leur cybersécurité de manière autonome et 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)[45].

Même si la coordination intercantonale sur les thèmes de cybersécurité est assurée par la CCDJP, d'autres conférences intergouvernementales peuvent s'occuper d'aspects spécifiques, selon leur domaine de compétence. Le RNS coordonne et encourage la collaboration avec la Confédération[46].

3.3 Cyberstratégie nationale

La cyberstratégie nationale (CSN) joue un rôle capital dans le traitement des cybermenaces. Elle sert de ligne directrice à la Confédération, aux cantons, aux milieux économiques et à la société.

La cybersécurité concerne aussi bien la vie quotidienne, les activités économiques que l'administration. Tous ces domaines sont amenés à agir et tous doivent prendre leur

[41] Cf. tâches de l'OFCS au chapitre 3.4.7.
[42] Pour un aperçu de la lutte contre la cybercriminalité en Suisse, cf. le rapport du Conseil fédéral intitulé « Poursuites pénales en matière de cybercriminalité. Efficacité des cantons », donnant suite au postulat 22.3145, Andri Silberschmidt, 16 mars 2022, et 22.3017, Commission de la politique de sécurité du Conseil national, 15 février 2022.
[43] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 9.
[44] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 9 s.
[45] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 10.
[46] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 10.

part de responsabilité pour assurer la protection de la Suisse contre les cybermenaces. La CSN renforce cette responsabilité commune en mettant les acteurs dotés des compétences nécessaires face à leurs obligations et en utilisant les structures existantes. Il en découle une mise en œuvre décentralisée mais pilotée de manière centralisée par la direction stratégique de la CSN et une répartition claire des tâches et des rôles.

La responsabilité commune comprend aussi la mise en œuvre collective de la CSN. La Confédération, les cantons, les milieux économiques et la société doivent appliquer les mesures en étroite collaboration et en engageant leurs compétences respectives. Le plan de mise en œuvre qui accompagne la stratégie fixe les compétences et les responsabilités dans l'exécution des mesures spécifiques prévues.

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. Elle admet qu'il n'existe pas de protection complète contre toutes les cybermenaces mais soutient qu'il est possible de les traiter de sorte que le risque résiduel soit acceptable. L'approche est dite « exhaustive », car elle prend en compte toutes les vulnérabilités pertinentes et toutes les menaces.

En résumé : la CSN repose sur une conception du rôle subsidiaire et partenarial de l'État. Celui-ci 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 fixant les mesures qui s'imposent en accord avec les acteurs concernés et en s'efforçant de coopérer étroitement avec eux[47].

3.4 Organisation et compétences du DDPS

Au niveau de la Confédération, l'organisation et les compétences en matière cyber s'articulent en trois grands domaines[48].

La *cybersécurité* se concentre sur les mesures préventives, la gestion des cyberincidents et la résilience face aux cyberrisques. Elle vise, parallèlement, à renforcer la collaboration internationale dans ce domaine.

La *cyberdéfense* regroupe des mesures relevant du renseignement et des mesures militaires qui servent à protéger les systèmes critiques dont dépend la défense nationale, à assurer la défense contre les cyberattaques, à garantir la disponibilité opérationnelle de l'armée en toute circonstance et à mettre en place des capacités et des compétences lui permettant d'apporter un appui subsidiaire aux autorités civiles. Elle inclut également des mesures visant à identifier les menaces et les attaquants ainsi qu'à entraver et à bloquer les attaques.

La *poursuite pénale de la cybercriminalité* comprend toutes les mesures prises par la police et les ministères publics fédéraux et cantonaux pour lutter contre la cybercriminalité. Il s'agit d'une approche coordonnée à différents niveaux pour lutter efficacement contre la cybercriminalité. Au niveau de la Confédération, les autorités

[47] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 12.
[48] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 9.

compétentes sont notamment l'Office fédéral de la police (fedpol) et le Ministère public de la Confédération (MPC). Le DDPS n'exerce aucune compétence dans ce domaine.

Il convient d'examiner ci-après les compétences cyber des différents offices du DDPS et de l'armée. Les unités organisationnelles considérées sont les suivantes : le Secrétariat général du DDPS (SG-DDPS), le Secrétariat d'État à la politique de sécurité (SEPOS), le Service de renseignement de la Confédération (SRC), le commandement Cyber, le Cyber-Defence Campus de l'Office fédéral de l'armement armasuisse (CYD Campus), l'Office fédéral de la protection de la population (OFPP) et l'Office fédéral de la cybersécurité (OFCS).

3.4.1 Secrétariat général du DDPS

Le DDPS compte sept offices ou groupes actifs dans le domaine cyber (SG-DDPS compris). Afin de garder un aperçu global et assurer un processus uniforme, le SG-DDPS joue un rôle de coordinateur et de conseiller politique en matière cyber au niveau du département. Dans ce rôle, il soutient la cheffe ou le chef du département ainsi que le secrétaire général ou la secrétaire générale du DDPS. Concrètement, il assume les tâches suivantes.

1. *Conseil et soutien politique* : le SG-DDPS soutient la cheffe ou le chef du département ainsi que le secrétaire général ou la secrétaire générale dans la planification politique, le pilotage et la coordination des activités du département en matière cyber. Il assure ainsi une vue globale des activités et des défis à relever par le département dans le domaine cyber. Le SG-DDPS veille en outre à ce que les actions entreprises aux niveaux politique et stratégique coïncident avec les priorités stratégiques de la cheffe ou du chef du DDPS et avec les développements stratégiques du département. Le SG-DDPS veille à ce que la planification et les activités du département soient coordonnées avec celles des autres départements et du Conseil fédéral. Lorsque des questions cyber se posent au niveau interdépartemental, il élabore une position consolidée du DDPS et apporte son soutien en vue d'unifier la communication. Il représente le département au sein de l'administration fédérale et des comités nationaux (comme le comité de pilotage de la CSN) pour les questions relatives au domaine cyber.

2. *Affaires politiques* : le SG-DDPS assure le suivi des affaires politiques (du département, du Conseil fédéral, du Parlement) qui relèvent du domaine cyber au niveau du département. Il donne à ce sujet des conseils politiques et assure la coordination opérationnelle des travaux.

3. *Fonction de rapporteur* : le SG-DDPS assume une fonction de rapporteur pour les groupes et les offices, également dans le domaine cyber. Dans ce rôle, il soutient la cheffe ou le chef du département ainsi que le secrétaire général ou la secrétaire générale du DDPS et les conseille dans la direction des offices qui disposent de capacités cyber.

4. *Fonction de surveillance* : le SG-DDPS assure le controlling pour les stratégies départementales, et notamment pour la stratégie cyber du DDPS. Il exerce aussi une fonction de surveillance dans le domaine de la cyberdéfense militaire et en assure le secrétariat.

5. *Gestion de la sécurité* : le SG-DDPS conseille le secrétaire général ou la secrétaire générale ainsi que les unités administratives du DDPS en matière de sécurité ; il réalise, sur mandat, des audits et des contrôles, coordonne la gestion des incidents de sécurité du département et dirige l'organe de sécurité opérationnel du DDPS.

3.4.2 Secrétariat d'État à la politique de sécurité

Le SEPOS veille, en collaboration avec d'autres unités administratives de la Confédération, à ce que celle-ci dispose de bases conceptuelles générales permettant de mener une politique de sécurité cohérente (art. 7, al. 1, Org-DDPS[49]). Il garantit, en collaboration avec d'autres unités administratives de la Confédération, une politique de sécurité globale et clairvoyante sur le plan stratégique (art. 7, al. 2, Org-DDPS), y compris pour la politique de cybersécurité. Il élabore et assure le suivi des bases et des directives, garantit la coordination entre les services compétents au sein du DDPS et associe aux travaux d'autres services appartenant ou non à l'administration fédérale.

1. *Coordination* : le SEPOS coordonne de manière générale les activités de politique de sécurité du DDPS et, donc également ce qui concerne le niveau de la conception pour le domaine cyber. Cette activité comprend notamment le monitorage de la stratégie cyber du DDPS.

2. *Réseau et collaboration aux niveaux national et international* : le SEPOS garantit la cohérence de la gouvernance dans les relations du DDPS avec les partenaires nationaux et internationaux dans le cadre de la politique de sécurité établie. Il est l'interlocuteur des partenaires nationaux et internationaux du DDPS pour les questions de politique de sécurité. Il est responsable de la coordination entre les différents offices au sein du département et avec le DFAE pour ce qui concerne les relations internationales correspondantes. Il renforce les relations bi- et multilatérales avec les partenaires internationaux et établit le dialogue avec eux au niveau stratégique, par exemple dans le cadre du Cooperative Cyber Defence Centre of Exellence (CCD CoE) à Tallinn.

3. *Gestion CSS* : le SEPOS profite des relations du DDPS avec le Center for Security Studies (CSS) de l'EPFZ dans le domaine cyber ; il les gère et assure une représentation.

4. *Service spécialisé de la Confédération pour la sécurité de l'information* : ce service assure différentes tâches en lien avec la sécurité de l'information. Il conseille et soutient les autorités soumises à la loi du 18 décembre 2020 sur la sécurité de l'information (LSI)[50], leurs préposés à la sécurité de l'information et les cantons dans l'exécution de la LSI. Lorsque la sécurité de l'information de la Confédération est mise en danger, il donne des recommandations. Il peut aussi, sur mandat, procéder à un examen des risques en cas d'introduction d'une nouvelle technologie et assurer la gestion et la coordination de la sécurité de l'information dans des projets importants, qui incluent plusieurs autorités. Le service est l'interlocuteur des services nationaux, étrangers et internationaux et il rend compte chaque année au Conseil fédéral de la situation en matière de sécurité de l'information au sein de la Confédération[51]. Le service

[49] RS **172.214.1**
[50] RS **128**
[51] Art. 83 LSI

spécialisé de la Confédération pour la sécurité de l'information négocie les traités de protection des informations et veille à leur application, assumant ainsi le rôle d'autorité compétente en la matière (National Security Authority). En tant que point de contact national, cette autorité confirme la conformité du système (Security Accreditation Authority)[52].

3.4.3 Service de renseignement de la Confédération

Le SRC est un instrument de politique de sécurité de la Suisse. Ses tâches sont définies à l'art. 6 de la loi fédérale du 25 septembre 2015 sur le renseignement (LRens)[53]. La prévention et l'appréciation de la situation sont les tâches principales effectuées par le SRC à l'attention des décideurs politiques. Dans ce contexte, le SRC détecte et combat le terrorisme, l'extrémisme violent, l'espionnage, la propagation des armes de destruction massive et leurs vecteurs, les cyberattaques visant les infrastructures critiques ainsi que des événements relevant de la politique de sécurité qui se déroulent à l'étranger.

Les tâches du SRC dans le domaine de la cybersécurité sont les suivantes :

1. *Suivi de la situation en matière de cybermenace* : le SRC suit et analyse en permanence la situation sous l'angle de la cybermenace et, le cas échéant, les conséquences pour la Suisse. La recherche et le traitement des données visant à apprécier la menace au sens de l'art. 6, al. 2, LRens sont réglés aux chapitres 3 et 4 LRens[54]. Le SRC apprécie la menace dans le domaine cyber et, le cas échéant, informe au fur et à mesure les différents services fédéraux et les autorités d'exécution cantonales[55]. L'appréciation continue de la cybermenace conduit à l'élaboration de produits d'information destinés au grand public. Il s'agit en particulier du rapport de situation annuel du SRC : La Sécurité de la Suisse.

Selon la mesure 3 de la CSN, la responsabilité de développer le suivi de la situation échoit au SRC et à l'OFCS. La progression de la digitalisation des processus dans divers secteurs économiques augmente le besoin d'évaluer les menaces spécifiques qui pèsent sur ces secteurs. En réponse à ce besoin, il convient d'assurer un traitement adapté des informations pertinentes en fonction des différents groupes cibles[56]. L'OFCS octroie au SRC l'accès à des informations concernant l'identité ou le mode opératoire des auteurs de cyberattaques dans le but de déceler à temps et de prévenir les menaces pour la sûreté intérieure ou extérieure, d'apprécier la menace ou d'assurer un service d'alerte précoce en vue de protéger les infrastructures critiques au sens de l'art. 6, al. 1, let. a, ch. 2 et 5 LRens[57].

---

[52] Message du 22 février 2017 concernant la loi sur la sécurité de l'information, FF **2017** 2765, 2900.
[53] RS **121**
[54] Message du 19 février 2014 concernant la loi sur le renseignement, FF **2014** 2029, 2068.
[55] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 16.
[56] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 16.
[57] Art 76*a*, al. 2, LSIrev. Cf. Modification du 29 septembre 2023 de la loi sur la sécurité de l'information. Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques, FF **2023** 2296. Expiration du délai référendaire le 18 janvier 2024, sans que ce droit n'ait été invoqué.

2. *Traitement d'événement* : le SRC traite les cas qui relèvent de son domaine de compétence au sens de la LRens. Pour ce faire, il a accès à diverses sources d'information. Les mesures de recherche d'informations réglées par les chapitres 3 et 4 LRens s'appliquent également aux cyberincidents. Parmi les thèmes traités, le SRC s'occupe en particulier de l'espionnage utilisant des moyens cyber et de la menace contre les infrastructures critiques[58]. Le SRC a pour tâche de rechercher les informations nécessaires sur les menaces d'attaque ou les attaques qui se sont produites pour les services compétents et les soutenir ainsi dans leurs activités de défense[59].

3. *Produits d'analyse* : le SRC élabore des produits résultant de ses analyses à l'attention de l'administration fédérale et des décideurs politiques. Il communique ponctuellement par oral le résultat de ses recherches et de ses analyses aux services concernés.

4. *Attribution des cyberincidents importants du point de vue de la politique de sécurité* : l'attribution, qui consiste à identifier les auteurs d'une attaque, est un processus interdisciplinaire global, qui comprend l'analyse technique de l'incident, tient compte du contexte géopolitique et utilise toute la palette à disposition du renseignement pour la recherche d'informations. L'attribution est une tâche principale du SRC selon la CSN[60].

5. *Sensibilisation* : le SRC sensibilise les entreprises, les hautes écoles et les instituts de recherche de Suisse et du Lichtenstein au danger que représentent les menaces liées à l'espionnage et à la prolifération. Il étend cette démarche de sensibilisation aux menaces qui pourraient résulter des cyberattaques[61].

6. *Coopération* : le SRC peut collaborer avec d'autres services de la Confédération et des cantons, de même qu'avec des personnes privées, des entreprises et des organisations. La collaboration avec l'armée et avec l'étranger est aussi expressément prévue[62]. Une grande importance est accordée à la collaboration entre la Confédération et les cantons, raison pour laquelle la Confédération est tenue, en vertu de la LRens, d'informer les autorités cantonales compétentes des événements particuliers survenant dans le domaine d'activités du SRC et de l'état de la menace. Cet échange a lieu principalement via la CCPCS[63] et la CCDJP[64]. Le SRC peut mettre des informations à la disposition du Ministère public de la Confédération (MPC) à des fins de poursuite pénale lorsque, au vu de ses recherches, il soupçonne que des actes répréhensibles ont été commis[65]. L'OFCS apporte son soutien au SRC en lui fournissant des évaluations périodiques du nombre, du type et de l'ampleur des cyberattaques ainsi que, sur demande, des analyses techniques des cybermenaces[66].

[58] Art. 6, al. 1, let. a, ch. 4, et al. 5, LRens.
[59] Message LRens, FF **2014** 2029 (nbp. 54), 2067.
[60] Conseil fédéral suisse. « Cyberstratégie nationale (CSN) » (nbp. 8), p. 25.
[61] Art. 6, al. 6, LRens.
[62] Art. 9 à 12 LRens ; art. 1, al. 1, de l'ordonnance du 16 août 2017 sur le renseignement (ORens ; RS **121.1**).
[63] Conférence des commandantes et commandants des polices cantonales de Suisse
[64] Conférence des directrices et directeurs des départements cantonaux de justice et police
[65] Art. 60 LRens ; message LRens, FF **2014** 2029 (nbp. 54), 2088.
[66] Art 76*a*, al. 1, LSIrev (nbp. 57).

7. *Assistance administrative* : à l'instar de tout autre service officiel, le SRC a le droit et le devoir de fournir une assistance administrative dans les domaines où il est compétent et en mesure de le faire avec le personnel et les moyens techniques dont il dispose. Il peut fournir des moyens et méthodes de type opérationnel particuliers, par exemple des prestations de transmission, de transport et de conseil dont les autres services ne disposent pas[67].

3.4.4 Commandement Cyber

Les fonctions et compétences du commandement Cyber sont réglées par les art. 96 et 100, al. 1, let. c, LAAM, l'art. 11, let. d, de l'ordonnance du 7 mars 2003 sur l'organisation du Département fédéral de la défense, de la protection de la population et des sports (Org-DDPS) et l'ordonnance du 30 janvier 2019 sur la cyberdéfense militaire (en part. l'art. 4 ; OCMil)[68].

Les prestations du commandement Cyber se concentrent sur l'autoprotection cyber et sur les actions dans le cyberespace. Il est en outre le fournisseur unique de prestations informatiques critiques pour l'engagement de l'armée. Il fournit ces prestations en toutes situations avec du personnel de l'administration militaire et des formations de milice qui lui sont subordonnées. Les prestations du commandement Cyber relevant des opérations, des engagements et de l'appui sont coordonnées par le commandement des Opérations en tenant compte du contexte opératif et de l'effet global.

Les fonctions du commandement Cyber peuvent être réparties dans les domaines suivants :

1. *Technologies de l'information et de la communication* : le commandement Cyber planifie et assure le fonctionnement de l'informatique critique pour l'engagement de l'armée ainsi que pour le gouvernement et pour la gestion de crise nationale. De plus, il assure la disponibilité des infrastructures et des troupes d'information et de communication afin de garantir la capacité de commandement de l'armée[69].

2. *Coopération avec des tiers* : le commandement Cyber, en accord avec le secteur TNI[70] de la Chancellerie fédérale, fournit certaines prestations de son catalogue à l'administration fédérale. Il peut fournir des prestations dans le domaine des technologies de l'information et de la communication pour maintenir la capacité de conduite de tiers, dans la mesure où une base légale le prévoit[71].

3. *Cyberdéfense militaire* : le commandement Cyber est responsable de la défense contre les cyberattaques qui visent des systèmes et des réseaux militaires[72]. La cyberdéfense militaire comprend l'ensemble des actions menées dans le cyberespace dans le but de protéger et de défendre, aux niveaux de conduite militaro-stratégique et

[67] Art. 69 LRens ; message LRens, FF **2014** 2029 (nbp. 54), 2121.
[68] RS **510.921**
[69] Art. 96 LAAM ; art. 11, let. d, ch. 1 à 3, Org-DDPS.
[70] Secteur Transformation numérique et gouvernance de l'informatique
[71] Art. 11, let. d, ch. 4 et 5, Org-DDPS.
[72] Art. 100, al. 1, let. c, LAAM ; art. 11, let. d, ch. 6, Org-DDPS ; art. 4, al. 1, OCMil.

opératif, les prestations informatiques indispensables aux engagements de l'armée, et notamment[73] :

- Cyberdéfense : actions menées dans le cyberespace visant à identifier les attaques et la cyberexploration, et à protéger les ressources de l'armée.
- Cyberexploration : actions menées dans le cyberespace visant à y acquérir des informations.
- Cyberattaque : actions menées dans le cyberespace visant à perturber, à entraver ou à ralentir les ressources ou capacités adverses dans ou à travers le cyberespace.

4. *Exploration radio* : le commandement Cyber, ou plus exactement le service Actions dans le cyberespace et dans l'espace électromagnétique (ACEM), est responsable de l'exploration radio pour le SRC et le Service de renseignement de l'armée[74].

5. *Exploration du réseau câblé* : le commandement Cyber, ou plus exactement le service ACEM, effectue l'exploration du réseau câblé pour le SRC[75].

6. *Cryptologie* : le commandement Cyber assure le service de cryptographie de l'armée. Il effectue cette tâche dans sa fonction d'interlocuteur LSI du service spécialisé de la Confédération pour la sécurité de l'information en cas de questions techniques concernant des solutions cryptographiques[76].

Les tâches assumées par le commandement Cyber sont concrétisées à l'art. 4, al. 2, OCMil. Elles comprennent les actions menées dans le cyberespace, les mesures préventives visant à protéger les prestations informatiques indispensables aux engagements de l'armée, l'examen légal et pratique de nouvelles actions, le blocage de l'accès aux prestations informatiques indispensables aux engagements de l'armée, la garantie de disponibilité des informations techniques nécessaires, l'évaluation des systèmes compromis suite à une cyberattaque, l'entretien de contacts avec des services spécialisés, le soutien de l'engagement et de l'instruction dans le domaine de la cyberdéfense militaire et la documentation des mesures soumises à autorisation dans le cadre d'une action menée dans le cyberespace.

3.4.5 Office fédéral de l'armement (armasuisse) – Cyber-Defence Campus

En tant que centre technologique du DDPS, l'Office fédéral de l'armement assure l'acquisition de connaissances scientifiques et techniques à l'armée et au DDPS et couvre leurs besoins dans les domaines de la science, de la technologie et de l'innovation[77]. Il est responsable du domaine Science et technologies (armasuisse S+T). Pour assumer les compétences qui lui sont confiées et anticiper plus rapidement les développements dans le domaine cyber, armasuisse S+T a créé le Cyber-Defence Campus (CYD Campus). Ce campus met à la disposition du DDPS une plateforme d'anticipation et de savoir pour reconnaître et évaluer les tendances technologiques,

[73] Art. 1, al. 2, OCMil.
[74] Art. 1 et 3 de l'ordonnance du 17 octobre 2012 sur la guerre électronique et l'exploration radio (OGE ; RS **510.292**).
[75] Art. 24 ss ORens.
[76] Cf. art. 21 et 23 de l'ordonnance du 8 novembre 2023 sur la sécurité de l'information (OSI ; RS **128.1**).
[77] Art. 12, al. 1, let. b, Org-DDPS.

économiques et sociétales en matière cyber. Il sert d'interface entre le DDPS, l'industrie et les milieux scientifiques dans le domaine de la recherche, du développement et de l'instruction en matière de cyberdéfense. Le CYD Campus travaille étroitement avec des partenaires nationaux et internationaux à des fins d'échange de savoir et de ressources dans le domaine de la cybersécurité. Des hautes écoles et des entreprises industrielles font partie de ces partenaires.

Le CYD Campus se concentre sur trois tâches visant à renforcer la cyberdéfense suisse :

1. *Reconnaissance précoce des tendances dans le domaine cyber* : le CYD Campus effectue une veille globale des technologies et du marché. Pour ce faire, il développe et utilise une plateforme de veille technologique, publie des rapports et des analyses de tendance des technologies, présente des tableaux de bord dynamiques et contribue à établir des roadmaps et des radars sur la technologie. Le CYD Campus identifie les technologies et entreprises intéressantes (principalement des start-up) dans des environnements internationaux innovants comme la Trust Valley, la Silicon Valley, Israël ou le Royaume-Uni, et entretient un réseau de coopération.

2. *Recherche et innovation en matière de cybertechnologies* : le CYD Campus, en collaboration avec les milieux scientifiques et industriels, identifie les cyberrisques émergents et développe des solutions innovantes pour faire face efficacement aux menaces dans le cyberespace. Il assure et améliore la sécurité et la résilience des cybersystèmes existants.

3. *Instruction de cyberspécialistes* : au CYD Campus, environ 50 personnes – talents de niveau master, doctorat et post-doctorat, stagiaires de hautes écoles ou qui ont suivi le stage de formation cyber – sont formées chaque année pour relever les défis futurs ; ces formations sont proposées sous forme de stages, de travaux de master ou de fellowships. De plus, les spécialistes du CYD Campus établissent et accompagnent de nombreux projets estudiantins.

Le CYD Campus transfère par ailleurs de nouvelles cybertechnologies vers le DDPS et développe des démonstrateurs pour mieux les comprendre et les connaître. Il est aussi responsable des tests d'intrusion. Dans ce cadre, il examine la sécurité des systèmes informatiques et fournit des conseils en cas de questions complexes relevant de la sécurité ou de thèmes liés aux sciences des données lors d'acquisitions.

Le CYD Campus organise diverses manifestations dans le but d'élargir et d'encourager le savoir :

- le *Cyber Startup Challenge* (annuel), qui vise à repérer les start-up intéressantes pour le domaine cyber et réaliser avec elles des études faisabilité pour une utilisation au DDPS,
- des *hackathons* (plusieurs fois par an), qui visent à rassembler la communauté cyber suisse autour de diverses thématiques relevant de la cybersécurité et des sciences des données (p. ex. automobiles électriques, systèmes de contrôle industriels, communication par satellite, internet des objets),

- des *conférences, retraites et séminaires cyber* autour de diverses thématiques relevant de la cybersécurité et des sciences des données (p. ex. repas de midi transformé en séminaire), et
- un *entraînement cyber* dans le cadre du projet pilote du Cyber Training Center (CTC).

3.4.6 Office fédéral de la protection de la population

L'OFPP contribue à une protection globale de la population, de ses conditions d'existence et de ses biens culturels en cas d'événement causant des dommages majeurs, de catastrophe, de situation d'urgence ou de conflit armé. Lors d'événements d'ampleur nationale nécessitant la protection de la population, il coordonne le travail entre les cantons, les communes et des tiers et contribue à la maîtrise de l'événement [78].

Le traitement de l'insécurité au niveau cyber par l'OFPP est effectué au moyen des prestations de base de l'office, à savoir :

1. *Analyse au niveau national des risques de catastrophes et de situations d'urgence* : l'OFPP effectue régulièrement une analyse nationale des risques concernant les catastrophes et les situations d'urgence[79]. La dernière édition a permis de lister 44 dangers d'origine naturelle, technique ou sociétale. La cyberattaque faisait aussi partie des dangers étudiés. Un dossier a été établi pour chacun des 44 dangers[80]. Ces dossiers comprennent des scénarios structurés de manière systématique et envisagent les dommages possibles à l'aune de douze indicateurs. Le rapport d'analyse des risques et les dossiers des dangers servent de base à la planification et à la préparation aux événements. Des mesures préventives et mesures de précaution peuvent ainsi être prises afin de réduire les dommages potentiels, en tenant compte de la probabilité qu'un événement survienne.

2. *Stratégie nationale de protection des infrastructures critiques (PIC)* : la stratégie nationale PIC a pour but d'améliorer la sécurité en cas de défaillances et la sécurité de l'approvisionnement en biens et services essentiels (p. ex. électricité, télécommunications). Le Conseil fédéral a chargé les autorités de surveillance et de régulation compétentes de vérifier dans tous les secteurs critiques s'il existe des risques de perturbation ou de rupture d'approvisionnement graves et de prendre des mesures afin d'améliorer la résilience. Les cyberrisques (tels que des cyberattaques contre le réseau d'approvisionnement en électricité ou contre le réseau ferroviaire) sont également examinés, en tenant étroitement compte de la CSN. Si des directives supplémentaires (p. ex. concernant la cybersécurité) s'avéraient nécessaires pour des exploitants particuliers, elles seraient établies au moyen de modifications des bases légales sectorielles sous la responsabilité des offices spécialisés compétents. L'OFPP est responsable de la coordination pour la mise en œuvre de la stratégie PIC. La délégation du Conseil fédéral pour l'énergie, l'environnement et les infrastructures

[78] Art. 14 Org-DDPS.
[79] OFPP, Analyse nationale des risques de catastrophes ou de situations d'urgence <https://www.babs.admin.ch/fr/analyse-nationale-des-risques-de-catastrophes-ou-de-situations-durgence>.
[80] OFPP, Dossiers sur les dangers et scénarios <https://www.babs.admin.ch/fr/strategie-nationale-de-protection-des-infrastructures-critiques>.

accompagne ce processus[81]. L'inventaire des infrastructures critiques est un autre point fort de la stratégie nationale PIC dont s'occupe l'OFPP. Celui-ci est une importante base de planification et de décision dans la maîtrise de catastrophes, de situations d'urgence et de conflits armés (également en cas de cyberattaques massives). L'OFPP gère en outre une plateforme permettant d'améliorer la collaboration intersectorielle entre les autorités et les exploitants des infrastructures nationales d'importance critique.

3. *Systèmes de communication pour la conduite et l'intervention*[82]

- L'OFPP partage avec l'Office fédéral de la douane et de la sécurité des frontières (OFDF) la responsabilité du programme de maintien de la valeur de Polycom (WEP 2030)[83]. Polycom est le réseau radio de sécurité des autorités et organisations chargées du sauvetage et de la sécurité (AOSS) couvrant l'ensemble du territoire[84]. Son utilisation doit être assurée au moins jusqu'en 2030. Une grande partie de composants du système Polycom doivent être renouvelés en raison du changement technologique. Des mesures de maintien de la valeur s'imposent.
- L'OFPP coordonne le projet de conception et de réalisation d'un réseau de données sécurisé (RDS+). L'objectif de RDS+ est d'introduire un système sûr, hautement disponible et protégé contre les cyberattaques pour garantir l'alarme et l'information de la population en temps voulu et une communication de conduite et d'intervention efficace entre les AOSS. Le RDS+ doit en particulier assurer, en cas de catastrophe ou de situation d'urgence, l'échange de données à large bande entre les partenaires de la protection de la population. Il s'agit d'accroître la protection du réseau contre les cyberattaques de manière significative en l'isolant des autres réseaux, tout en permettant l'utilisation d'applications sécurisées en situation normale.

Le Conseil fédéral a décidé d'introduire un nouveau système mobile de communication sécurisée à large bande (CMS) pour répondre aux besoins futurs[85]. Les membres des forces de police, des services du feu et des services sanitaires ainsi que les exploitants d'infrastructures critiques et d'autres organisations dans le domaine de la protection de la population doivent être en mesure, pour remplir leur mission, d'échanger des images et des vidéos et d'accéder à des bases de données sécurisées. Ceci doit également être possible lorsque les réseaux mobiles existants sont surchargés ou endommagés, par exemple en cas de catastrophe naturelle, de cyberattaque, de panne d'électricité ou d'attaque terroriste. Le Conseil fédéral a chargé le DDPS d'élaborer d'ici l'été 2024 un projet comprenant une variante CMS combinée et qui sera soumis à consultation. CMS utilisera le réseau national de données sécurisé (RDS+) et remplacera progressivement le réseau radio de sécurité Polycom dès 2030. Ce système

[81] OFPP, Stratégie nationale de protection des infrastructures critiques <https://www.babs.admin.ch/fr/strategie-nationale-de-protection-des-infrastructures-critiques>.
[82] Chapitre 4 de l'ordonnance du 11 novembre 2020 sur la protection de la population (OProP ; RS **520.12**).
[83] OFPP, Maintien de la valeur de Polycom (WEP 2030) <https://www.babs.admin.ch/fr/maintien-de-la-valeur-de-polycom-wep-2030>.
[84] OFPP, Systèmes de communication pour la conduite et l'intervention <https://www.babs.admin.ch/fr/systemes-de-communication-pour-la-conduite-et-lintervention>.
[85] Art. 20 loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (LPPCi ; RS **520.1**) et art. 5 OProP.

permettra un gain de sécurité et des fonctionnalités importantes pour les organisations d'urgence et d'autres partenaires de la protection de la population : grâce à CMS, ceux-ci pourront non seulement mieux assumer leurs tâches en cas de catastrophe ou d'attaque terroriste, mais ils pourront aussi compter au quotidien sur un réseau de communication sécurisé à large bande[86].

L'OFPP assure en outre le fonctionnement du National Emergency Operations Center (NEOC, anciennement la CENAL), où se trouve aussi la Gestion fédérale des ressources (ResMaB pour *Ressourcenmanagement Bund*)[87]. ResMaB est à la fois une tâche de coordination et un instrument de la Confédération permettant de régler les besoins en ressources supplémentaires en cas de danger ou lors de dommages, en particulier lors d'événements complexes au niveau intercantonal, national et international. La coordination des ressources et l'attribution des prestations s'effectuent selon le principe de subsidiarité et en associant les acteurs impliqués dans la maîtrise de l'événement. Elles respectent des critères et des priorités déterminés par le comité de l'état-major partiel de la Gestion fédérale des ressources dans le cadre d'un processus consultatif. La coordination et l'allocation des ressources servent à utiliser ces moyens de façon ciblée pour la protection de la population et le maintien des conditions d'existence. ResMaB fonctionne en principe indépendamment de tout scénario. Il convient cependant de noter que le thème cyber n'y a pas fait jusqu'à maintenant l'objet d'une attention particulière.

Selon l'art. 3, al. 1 et 2 LPPCi[88], les organes de conduite, les organisations partenaires et des tiers collaborent et se préparent, dans le cadre de la protection de la population, à la maîtrise des événements. Les organisations partenaires de la protection de la population sont la police, les sapeurs-pompiers, les services de santé publique, les services techniques et la protection civile. Selon l'art. 3, al. 3, LPPCi, il est possible de faire appel à d'autres services ou organisations. L'OFCS peut ainsi, par exemple, être mis à contribution sur des questions cyber[89].

3.4.7 Office fédéral de la cybersécurité

L'OFCS est le centre de compétences de la Confédération en matière de gestion des cybermenaces et le premier interlocuteur des entreprises, des administrations, des établissements de formation et de la population dans ce domaine[90].

La description et les dispositions organisationnelles des tâches de l'OFCS se trouvent à l'art. 15*a* Org-DDPS. Avec la révision du chapitre 5 de la LSI, le Parlement a édicté une nouvelle base légale pour l'OFCS, qui précise également les tâches de celui-ci. Les dix tâches de l'OFCS, telles qu'elles sont données par l'Org-DDPS, vont être

[86] DDPS. Le Conseil fédéral prend une décision de principe concernant la communication mobile à large bande en situation de crise <https://www.vbs.admin.ch/fr/nsb?id=99545>.
[87] Art. 10 LPPCi et art. 6 OProP.
[88] Loi fédérale du 20 décembre 2019 sur la protection de la population et sur la protection civile (LPPCi ; RS **520.1**).
[89] Message du 21 novembre 2018 concernant la révision totale de la loi sur la protection de la population et sur la protection civile, FF **2019** 515, 533. Le message parle de MELANI, qui est devenu une partie du NCSC le 1er juillet 2020. Le NCSC est désormais l'Office fédéral de la cybersécurité (OFCS) depuis le 1er janvier 2024.
[90] Cf. art. 15*a*, al. 1, Org-DDPS.

examinées plus en détail ci-après. Cet exposé sera complété avec des informations tirées de la LSI révisée (LSIrev).

1. Coordination cyber : l'OFCS coordonne les travaux de la Confédération dans le domaine de la cybersécurité[91].

2. Analyses techniques : l'OFCS réalise des analyses techniques pour évaluer et contrer les cyberincidents et les cybermenaces, ainsi que pour identifier et éliminer les vulnérabilités dans le cadre de la protection de la Suisse contre les cybermenaces[92]. La recherche de sites Internet infectés ou de vulnérabilités fait aussi partie de ces tâches[93].

3. Réception des annonces de cyberincidents et de cybermenaces : l'OFCS reçoit les annonces de cyberincidents et de cybermenaces. Il gère à cet effet le guichet national en matière de cybermenaces[94]. Ce guichet de signalement a été développé à partir de MELANI et il est largement utilisé par les entreprises et la population[95]. Il reçoit aussi bien des annonces volontaires de cyberincidents que celles des cyberattaques, qui sont obligatoires[96].

4. Analyse des annonces de cyberincidents et cybermenaces : l'OFCS analyse les signalements au regard de leur importance pour la protection de la Suisse contre les cybermenaces[97]. L'OFCS peut, à la demande du service concerné, procéder à une évaluation de l'incident et faire des recommandations[98].

5. Publication d'informations sur les cyberincidents : l'OFCS publie des informations relatives aux cyberincidents dès lors que cela est utile à la protection contre les cybermenaces. Ces informations peuvent contenir des données de personnes physiques ou morales uniquement avec l'accord de celles-ci et dans la mesure où les caractères d'identification et les ressources d'adressage ont été utilisés de manière abusive, comme dans le cas de l'utilisation abusive d'un logo lors d'une attaque de type hameçonnage[99]. L'OFCS peut en outre publier des informations relatives à des vulnérabilités en indiquant le matériel informatique ou le logiciel concerné, à condition que le fabricant y consente ou qu'il n'ait pas éliminé la vulnérabilité dans le délai visé. Cette mesure peut s'avérer nécessaire pour éviter d'autres cyberattaques. L'OFCS est reconnu au niveau international en tant que service spécialisé en matière de vulnérabilités et il œuvre à la publication coordonnée des vulnérabilités détectées avec d'autres organismes étrangers et internationaux[100].

---

[91] Art. 15*a*, al. 2, let. a, Org-DDPS.
[92] Art. 15*a*, al. 2, let. b, Org-DDPS ; art. 73*a*, al 1, LSIrev (nbp. 57).
[93] Message du 2 décembre 2022 relatif à la modification de la loi sur la sécurité de l'information (Mise en place d'une obligation de signaler les cyberattaques contre les infrastructures critiques), FF **2023** 84, 26.
[94] Art. 15*a*, al. 2, let. C, Org-DDPS ; art. 73*a*, al. 2, let. d et art. 73*b*, al. 1 LSIrev (nbp. 57).
[95] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 25.
[96] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 26.
[97] Art. 15*a*, al. 2, let. C, Org-DDPS ; art. 73*a*, al. 2, let. d et art. 73*b*, al. 2, LSIrev (nbp. 57).
[98] Art. 73*b* al. 2, LSIrev (nbp. 57); message Obligation de signaler, FF **2023** 84 (nbp. 93), 26.
[99] Art. 73*c*, al. 1, LSIrev (nbp. 57) ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 27.
[100] Art. 73*c*, al. 2, LSIrev (nbp. 57) ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 27.

6. Sensibilisation et alerte des autorités, des organisations et des personnes : l'OFCS contribue à sensibiliser l'administration fédérale et le grand public aux cybermenaces en utilisant des moyens d'information ciblée. Il informe sur l'état de la situation et publie des instructions sur les mesures préventives ou réactives à prendre. L'OFCS alerte les autorités, les organisations et les personnes concernées en cas de cybermenace immédiate ou de cyberattaque en cours[101]. De plus, il publie régulièrement, sur la base de signalements reçus et d'analyses, des statistiques et rapports sur les cybermenaces afin de sensibiliser le public, de mettre en garde les autorités, organes et personnes touchés, et de fournir des recommandations.

7. Aide préventive aux exploitants d'infrastructures critiques dans la protection contre les cybermenaces : l'OFCS soutient préventivement les exploitants d'infrastructures critiques dans leur protection contre les cybermenaces. À cette fin, il met gratuitement à leur disposition différents outils. Les exploitants d'infrastructures critiques sont libres de profiter du soutien de l'OFCS ou pas. Les outils proposés peuvent être utilisés librement. Les outils principaux sont listés à titre d'exemple. Cette liste est non exhaustive[102].

- *Cyber Security Hub* : l'OFCS administre une plateforme de communication sur laquelle des organisations et des autorités établies en Suisse peuvent échanger avec lui ou entre elles des informations sur des cyberincidents ou des cybermenaces. Les responsables disposent ainsi à tout instant de l'état récent des connaissances. L'OFCS utilise aussi ce canal d'information sécurisé pour informer précocement les infrastructures critiques des modes opératoires qui n'ont pas encore été rendus publics ou qu'il ne peut pas publier pour des raisons de sécurité[103].

- L'OFCS met à la disposition des exploitants d'infrastructures critiques des informations techniques sur les cybermenaces actuelles (p. ex. vulnérabilités) et des recommandations sur les mesures préventives et réactives à mettre en place. Ces outils se limitent aux éléments pouvant s'avérer utiles aux infrastructures critiques de manière générale. L'OFCS ne fournit pas de conseils individualisés aux entreprises[104].

- Des instruments techniques et des instructions pour la détection précoce des cyberincidents sont un autre soutien proposé par l'OFCS. Ces instruments sont, par exemple, des règles de détection permettant d'identifier les flux de réseaux et les fichiers potentiellement nuisibles, des listes d'indicateurs techniques sur les attaques ou les tentatives d'attaques (*indicators of compromise*) ou des applications spécialisées servant à découvrir les modes opératoires et à se protéger contre ces attaques[105].

Certains de ces outils sont conçus de manière à être utiles à toutes les infrastructures critiques. Mais ils peuvent aussi être spécifiquement élaborés pour certains groupes

[101] Art. 15*a*, al. 2, let. e, Org-DDPS ; art. 73*a*, al. 2, let. b, LSIrev (nbp. 57).
[102] Art. 15a, al. 2, let. f, Org-DDPS ; art. 74 LSI ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 30.
[103] Art. 74, al. 2, let. a, LSIrev (nbp. 57) ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 30.
[104] Art. 74, al. 2, let. b, LSIrev (nbp. 57) ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 30.
[105] Art. 74, al. 2, let. c, LSIrev (nbp. 57) ; message Obligation de signaler, FF **2023** 84 (nbp. 93), 30s.

d'infrastructures ou pour certains domaines d'activité. Ils ne remplacent pas les dispositifs de protection individuels des infrastructures, mais peuvent y être intégrés[106].

8. Aide aux exploitants d'infrastructures critiques dans la gestion des cybermenaces : l'OFCS dispose d'une équipe d'intervention en cas d'urgence informatique, le Computer Emergency Response Team (CERT). Celui-ci tient lieu de service spécialisé national pour la gestion technique des cyberincidents ; il soutient les exploitants d'infrastructures critiques en cas d'incident.

Le soutien prend différentes formes, selon l'impact de l'incident sur le fonctionnement et l'organisme responsable de l'infrastructure critique. La distinction opérée ci-après est importante du point de vue de la subsidiarité.

- *Conseil technique* : dans tous les cas, l'OFCS peut venir en aide aux exploitants d'infrastructures critiques dans la gestion des cyberincidents et l'élimination des vulnérabilités en leur prodiguant des conseils techniques[107]. Il apporte son soutien sur demande et en étroite collaboration avec les organes concernés[108].

- *Soutien technique* : l'OFCS peut fournir un soutien technique aux exploitants d'infrastructures critiques lorsque des cyberincidents mettent en péril le fonctionnement de l'infrastructure concernée. S'il s'agit d'un exploitant privé, l'OFCS intervient subsidiairement aux services informatiques disponibles. Cela signifie qu'il ne doit pas y avoir de prestations commerciales équivalentes à ce moment-là sur le marché[109]. Que l'exploitant soit privé ou public, la décision d'intervenir est prise en fonction de l'organisme ou de l'autorité responsable et non pas du statut juridique de l'infrastructure critique[110]. S'il s'agit d'un exploitant public, le soutien est fourni sans que le principe de subsidiarité ne doive être examiné.

La contribution de l'OFCS à la gestion des incidents consiste en une analyse technique de l'attaque. Cette analyse vise à comprendre le plus rapidement possible quels sont les vecteurs d'attaque utilisés, à quelle tactique recourent les attaquants et quels sont leurs objectifs. Le résultat permet de déterminer et de mettre en œuvre des contre-mesures appropriées. Pour ce faire, l'OFCS collabore étroitement avec les autorités et les organisations concernées et leurs services de sécurité, s'il y en a. Il aide également à coordonner l'action des acteurs qui participent à la gestion technique. Au besoin, il peut aussi apporter un soutien sur place, auprès de l'autorité ou de l'organisation concernée. Les prestations de soutien de l'OFCS sont fournies à titre d'aide immédiate en cas d'urgence. Pour la restauration de données ou à la reconstruction de systèmes après l'incident, l'OFCS fournit seulement des conseils[111].

9. Soutien aux autorités : l'art. 76*a* LSIrev clarifie la répartition des rôles entre l'OFCS et le SRC. Il règle aussi quelles informations sont communiquées au SRC, aux autorités de poursuite pénale et aux services cantonaux responsables de la cybersécurité, et selon quelles modalités. L'OFCS apporte son soutien au SRC en lui fournissant des

[106] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.
[107] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.
[108] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.
[109] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.
[110] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.
[111] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 31.

évaluations du nombre, du type et de l'ampleur des cyberattaques ainsi que des analyses techniques des cybermenaces identifiées (image de la situation)[112]. Il donne également accès à des informations aux autorités de poursuite pénale et aux services cantonaux responsables de la cybersécurité. Ces informations peuvent, le cas échéant, se référer à des personnes[113].

10. Cyberstratégie nationale : l'OFCS élabore la cyberstratégie nationale (CSN) à l'intention du Conseil fédéral et coordonne sa mise en œuvre. En tant que bureau de la CSN, il contrôle sa gestion stratégique et prépare les séances du Groupe Cyber et du CP CSN. Fixée en accord avec les cantons, la CSN donne un cadre stratégique pour améliorer la prévention, la détection précoce, la réaction et la résilience afin de protéger la Suisse contre les cybermenaces[114].

3.5 Principales conclusions

La protection contre les cybermenaces relève de la responsabilité commune des milieux économiques, de la société et de l'État. En principe, chaque acteur est responsable de sa propre sécurité. Au sein du DDPS, les offices assument diverses tâches dans le domaine cyber.

Seuls deux types de prestations sont fournis à titre subsidiaire : le service d'appui de l'armée au sens de la LAAM et le soutien technique subsidiaire fourni par l'OFCS aux exploitants privés d'infrastructures critiques, au sens de la LSIrev. Lorsqu'il s'agit d'exploitants privés, l'OFCS intervient subsidiairement aux services informatiques disponibles, ce qui signifie qu'il ne doit pas y avoir de prestations commerciales équivalentes à ce moment-là sur le marché. Le soutien de l'OFCS aux exploitants publics n'est pas fourni à titre subsidiaire. Les autres tâches effectuées par le DDPS se répartissent en deux catégories : (1) des prestations fournies à des tiers, pour lesquelles la question du principe de subsidiarité a déjà été réglée par l'adoption de la loi correspondante et (2) des prestations fournies par les offices du DDPS à la Confédération elle-même et qui ne nécessitent donc pas d'examen du principe de subsidiarité.

4 Mesure

Les chapitres précédents ont expliqué le principe de subsidiarité et présenté les différentes tâches accomplies par les offices du DDPS en matière cyber. Le DDPS dispose de compétences cyber étendues aussi bien dans le domaine civil que militaire. Pour simplifier la collaboration entre ces deux domaines, la mesure suivante a été élaborée :

L'Office fédéral de la cybersécurité (OFCS) étudie, en collaboration avec le commandement des Opérations, le commandement Cyber, le Secrétariat général du DDPS, le Secrétariat d'État à la politique de sécurité et le Réseau national de sécurité, la création d'une base juridique permettant au commandement Cyber de fournir des

[112] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 50.
[113] Message Obligation de signaler, FF **2023** 84 (nbp. 93), 50.
[114] Art. 15*a*, al. 2, let. g, Org-DDPS.

prestations d'appui à l'OFCS selon un processus simplifié. L'OFCS proposera d'ici la fin 2026 plusieurs options au Conseil fédéral pour la suite de la procédure.

Cette mesure s'inscrit dans le contexte suivant. L'OFCS est l'interlocuteur central et le service d'assistance pour les exploitants d'infrastructures critiques en cas de cyberincidents. Il peut leur apporter un soutien. En cas de surcharge, l'OFCS a la possibilité de faire appel à d'autres offices fédéraux civils conformément à la LOGA ou à l'OLOGA. La situation est différente pour les prestations d'appui fournies par le commandement Cyber.

La structure de l'organisation du Groupement Défense est, sous bien des aspects, identique à celle de l'armée. Les bases légales sont différentes pour chacune des deux organisations. La loi sur l'armée s'applique pour l'armée et son commandement Cyber. En revanche, la partie administrative du commandement Cyber et son personnel sont soumis à la LOGA.

L'armée peut apporter un appui aux autorités civiles uniquement en vertu des dispositions de la loi sur l'armée. Il est donc nécessaire que les conditions d'un service d'appui au sens de l'art. 67 LAAM soient remplies. Par contre, l'administration militaire ne peut soutenir d'autres autorités civiles au sein de l'administration fédérale qu'en se fondant sur la LOGA et l'OLOGA.

Cet état de fait peut conduire aux difficultés suivantes : lorsque l'OFCS demande un soutien au sens de la LOGA et de l'OLOGA, seul le personnel de la Confédération peut intervenir. Pour que l'armée puisse soutenir l'OFCS, il est nécessaire de déposer une demande de service d'appui. Selon l'art. 70, al. 1, let. a, LAAM, il appartient au Conseil fédéral de décider d'un tel engagement.

Cette voie procédurale qui passe par le Conseil fédéral rend difficile une collaboration à la fois efficace et juridiquement fondée entre le commandement Cyber et l'Office fédéral de la cybersécurité, car dans le domaine cyber, il faut engager le personnel spécialisé de manière rapide et ciblée.

Afin de régler cette problématique et de permettre au commandement Cyber de fournir rapidement des prestations d'appui à l'OFCS, il s'agit d'examiner la possibilité de créer une base juridique permettant une procédure simplifiée en cas de cyberincident (p. ex. sur le modèle de l'appui en cas de catastrophe en Suisse).

Une telle base juridique permettrait à l'OFCS de demander plus facilement un appui cyber au commandement Cyber, et au commandement Cyber de proposer ses prestations à l'OFCS sans devoir passer par le Conseil fédéral. Avec une telle base juridique, il serait possible d'engager non seulement l'armée, mais également le Groupement Défense en vue d'une prestation d'appui.

Dans ce contexte, il y a lieu de tenir compte des particularités du domaine cyber. L'appui dans le domaine cyber doit notamment permettre à l'OFCS d'endiguer les dommages avant qu'ils ne surviennent ou de limiter leur potentiel. Un appui du commandement Cyber à l'OFCS permettrait à celui-ci de faire face à des situations de surcharge extrême et de pouvoir rapidement faire appel à du personnel *approprié* au

sens de l'art. 67, al. 1, let. d, LAAM, c'est-à-dire qualifié dans ce domaine hautement spécialisé.

En cas d'appui du commandement Cyber, l'OFCS conserverait la responsabilité de l'engagement (cf. art. 71 LAAM), comme pour un soutien au sens de la LOGA. Dans le cas d'un appui en cas de catastrophe en Suisse, l'autorité civile détermine aussi l'engagement des moyens ainsi que la mission en accord avec le commandement des Opérations. Elle assume la responsabilité globale de l'engagement (art. 8 OAMC). Il s'agira d'en tenir compte lors de l'examen de la base juridique pour un appui en cas de cyberincident, de façon à maintenir une séparation claire entre les intérêts civils et militaires. La simplification de la procédure de demande de service d'appui cyber ne doit en aucun cas mélanger les intérêts cyber civils et militaires.

Il convient en particulier d'assurer le maintien de la confidentialité des annonces ; il s'agit d'une condition essentielle pour que les entreprises continuent à faire parvenir des signalements à l'OFCS. Certaines prescriptions légales à l'intention du personnel de l'OFCS ont d'ailleurs été adaptées pour cette raison[115]. Afin de permettre une collaboration basée sur la confiance, l'OFCS et le commandement Cyber doivent clarifier la question de l'application des dispositions légales de l'OFCS aux spécialistes envoyés en appui par le commandement Cyber.

Il y a lieu de considérer les points suivants lors du traitement de la mesure :

- élaboration de scénarios qui présentent l'ampleur de la surcharge permettant de qualifier une situation comme nécessitant une prestation d'appui, et description de la prestation,
- lien avec les situations dans le domaine cyber, y c. délimitation du service actif,
- présentation du processus simplifié, y c. répartition des compétences,
- examen de l'utilité d'appliquer les neuf conditions du RNS relatives au service d'appui également pour les cas de cyberincident,
- vérification des possibilités de modification des bases légales afin de permettre un appui simple et rapide du commandement Cyber à l'OFCS, et
- élaboration, pour la suite de la procédure, de plusieurs options à l'intention du Conseil fédéral.

L'OFCS est responsable de la mise en œuvre de cette mesure. Il la traite en collaboration avec le commandement des Opérations, le commandement Cyber, le SG-DDPS, le SEPOS et le RNS. La mesure est mise en œuvre d'ici la fin 2026.

[115] L'obligation de dénoncer les infractions est suspendue (art. 73*d*, al. 3, LSI) et les informations portées à la connaissance du NCSC [OFCS] dans sa fonction de guichet de signalement sont soustraites au droit d'accès prévu par la LTrans (art. 4, al. 1*bis*, LSI). Message Obligation de signaler, FF **2023** 84 (nbp. 93), 26.

5 Remarques finales

Le postulat « DDPS. Subsidiarité et cybersécurité » a chargé le Conseil fédéral de produire un rapport dans lequel il expose la manière dont la notion de subsidiarité est réexaminée au sein du DDPS et dont elle est applicable, en particulier dans le cadre de la collaboration en matière de prestations de sécurité dans le cyberespace.

Le présent rapport a montré comment le principe de subsidiarité fonctionne et comment il est appliqué. Il a décrit comment la cybersécurité est comprise au sein de la Confédération et a détaillé les compétences des différents offices et groupes du DDPS en la matière. Cet état des lieux a montré que la collaboration entre les domaines civil et militaire peut être améliorée en ce qui concerne la subsidiarité, raison pour laquelle une mesure est proposée : il s'agit d'étudier la possibilité de créer une base juridique pour simplifier la procédure permettant au commandement Cyber de fournir des prestations d'appui en faveur de l'OFCS.